IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

HIGH PERFORMANCE AND SECURITY TECHNIQUES FOR PROTECTING DATA IN CLOUD COMPUTING

N. Pradheep[1*], M. Venkatachalam[2], M. Saroja[2], V. Sivasooriya[3]

[1]*Department of Electronic & Communication, Salem Sowdeswari College, Salem-10.*

[2] *Associate Professor, Department of Electronics, Erode Arts and Science College, Erode-9.*

[3] *Research Scholar, Department of Electronics, Erode Arts and Science College, Erode-9.*

Abstract:

From the past few years, there has been a fast growth in Cloud Computing. With the increasing number of companies resorting to use resources in the Cloud, there is a requirement for protecting the data of some users using centralized resources. Some major tasks that are being faced by Cloud Computing are to secure, protect and process the data which is the property of the user. The foremost aim of this study is to understand the security threats and identify the suitable security techniques used to mitigate them in Cloud Computing. The main objectives of this study are: To recognize the security issues and the techniques used in the present world of Cloud Computing. To recognize the security challenges, those are expected in the future of Cloud Computing. To suggest counter process for the future challenges to be faced in Cloud Computing. In this study, we have used two study methods. As a outcome we have recognized the total of 43 security challenges and 43 security techniques. The majority measured attribute is confidentiality (31%) followed by integrity (24%) and availability (19%). The impact of identified mitigation techniques is mainly on security (30%), followed by performance (22%) and efficiency (17%). Also we have recognized 17 future challenges and 8 mitigation training. The identification of security experiments and mitigation methods in large number of services of Cloud Computing is a very challenging task. In the method of identification from study methods (SLR and Survey), we had identified a satisfactory number of challenges and mitigation methods which are being used at current and also in upcoming Cloud Computing.

Keywords: Challenges, Big Data, Cloud Computing, Privacy, Security, Techniques.

Introduction:

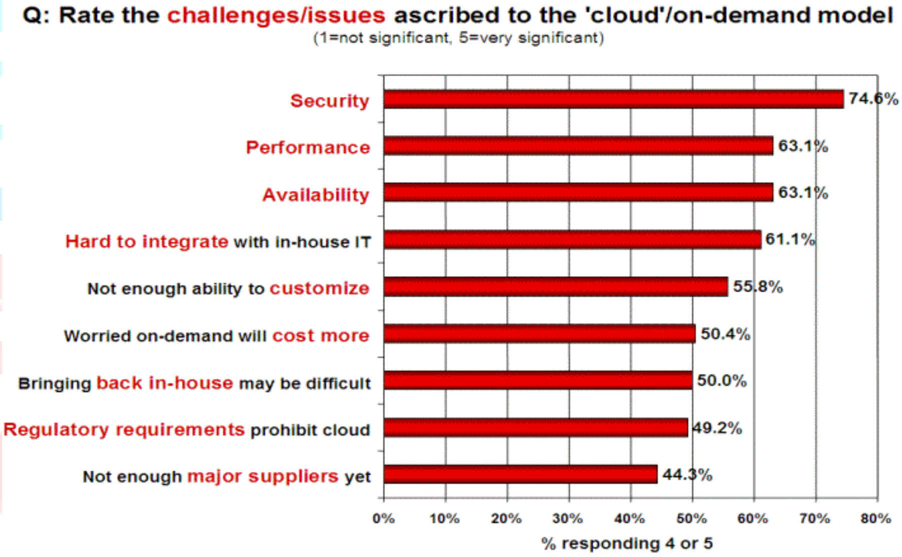
Cloud is a computing model that mentions to both the applications derived as facilities over the Internet, the hardware and system software in the data centers that provide those facilities. Cloud Computing is treated as the high potential example used for deployment of applications on Internet [2]. This idea also explains the applications that are broaden to be accessible through the Internet. Cloud applications use big data centers and effective servers that host web applications and services.

Cloud Computing is rapidly being acknowledged as a universal access application on the Internet. A lot of care has been given to the Cloud Computing concept in deriving standard definitions. However, the descriptions of Cloud Computing remain controversial. But here we have careful the standard definition which was given by the National Institute of Standards and Technology (NIST): “Cloud Computing is model for allowing ubiquitous, convenient, on exact network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be quickly provisioned and released with minimal management determination or service supplier interaction”, [1].

According to NIST, the cloud model is collected of three service models:

- Software as a Service (SaaS): The ability provided to the consumer is to use the provider's applications running on a cloud organization. The applications are accessible from a number of client devices through both a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud organization including network, servers, operating systems, storage, or even separate application capabilities, with the possible exception of limited user-specific application formation settings [3].
- Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or learned applications formed using programming languages, libraries, services, and tools supported by the provider. The customer does not succeed or control the underlying cloud group including network, servers, operating systems, or storage, but has control over the organized applications and possibly configuration settings for the application-hosting environment [4].
- Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can contain operating systems and applications. The consumer does not deal with or control the underlying cloud infrastructure but has control over operating systems, storage, and organized applications; and possibly limited control of select networking components (e.g., host firewalls) [4].

Importance of Security in Cloud Computing:



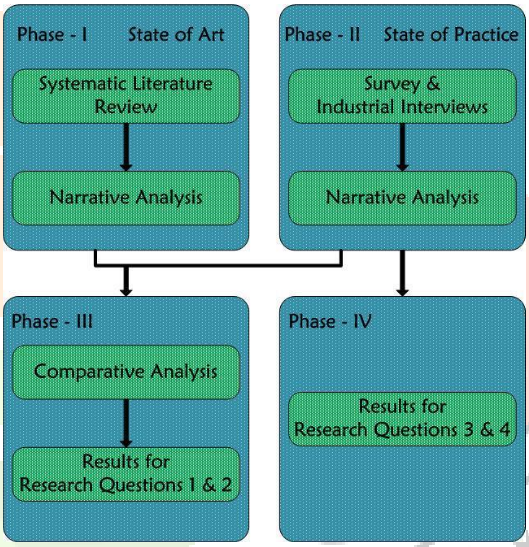
Source: IDC Enterprise Panel, August 2008 n=244

The above arithmetical resulted graph signifies the grades of the survey which was conducted by the IDC (International Data Corporation) in August, 2013 amongst senior business executives and IT professionals regarding the challenges/issues which mainly disturb the performance of Cloud Computing. And the survey results show security at the top of the list which states its importance related to other parameters of Cloud Computing [5]. During a keynote speech to the Brookings Institution policy forum, "Cloud Computing for Business and Society", Microsoft General Counsel Brad Smith also highlighted data from a survey commissioned by Microsoft for calculating attitudes on Cloud Computing among business leaders and the general population in January 2010 [39, 40]. The survey found that while 58% of the general population and 86% of the senior business leaders are very much eager about the potential of Cloud Computing and more than 90% of these same people are very much worried about the security, access and privacy of their own data in the Cloud. The survey results show that the security is the main challenge amongst all the parameters that disturb the performance and growth of Cloud Computing [6].

Important Security Issues in the Cloud

Even though, the virtualization and Cloud Computing carries wide range of dynamic resources, the security fear is generally perceived as the huge issue in the Cloud which makes the users to fight themselves in adopting the technology of Cloud Computing. Some of the security issues in the Cloud are conversed below: Integrity: Integrity makes sure that data held in a system is a proper demonstration of the data intended and that it has not been modified by an authorized person. When any application is running on a server, backup monotonous is configured so that it is safe in the event of a data-loss incident. Usually, the data will backup to any portable media on aneven basis which will then be stored in an off-site location [9]. Availability: [37] Availability ensures that data processing resources are not made absent by malicious action. It is the simple hint that when a user tries to access something, it is available to be accessed. This is vital for mission critical systems [38]. Availability for these systems is important that companies have Business Continuity Plans (BCP‟s) in direct for their systems to have unemployment [7]. Confidentiality: Confidentiality ensures that data is not disclosed to illegal persons. Confidentiality loss occurs when data can be viewed or read by any individuals who are illegal to access it. Loss of confidentiality can occur physically or electronically. Physical confidential loss takes place through social engineering. Electronic confidentiality loss takes place when the clients and servers aren’t encrypting their communications [8].

Study Methodology:


Phase - I State of Art
Systematic Literature Review
Narrative Analysis
Phase - II State of Practice
Survey & Industrial Interviews
Narrative Analysis
Phase - III
Comparative Analysis
Results for Research Questions 1 & 2
Phase - IV
Results for Research Questions 3 & 4

Study Design

In this study work, we studied the previous work in order to acknowledge the current knowledge to answer the study questions. Most of the previous study works were done with outdated literature review which has low scientific value due to non- rigorous and partial approach. Where the systematic literature review has is of highly defined characteristics with more clear scientific standpoint [10]. So we have assumed the systematic literature review (SLR) as a primary study method, survey and interviews are measured as secondary study method. The outlook of the studyapproaches which are used to answer the study questions is shown in figure [36].

Systematic Literature Review:

A methodical literature review is a means of classifying, calculating and interpreting all available study related to a particular study question, topic or phenomenon of interest [11]. Systematic reviews aims to current a fair evaluation of a study topic by using a trustworthy, rigorous and auditable methodology. A systematic literature review synthesizes existing work in a way that is fair and seen to be fair. Systematic review must be assumed in accordance with a predefined search strategy [35]. The search strategy must allow the completeness of the study to be assessed. In particular, studier’s performing a systematic review must make every struggle to identify and report study that does not support their preferred study hypothesis as well as identifying and reporting study that supports it [12]. Systematic reviews are mainly undertaken to summarize the existing evidence, identifying the gaps in current study and providing a framework for new study activities [13]. The main features that differentiate a systematic literature review from a traditional literature review are:

- Systematic Literature Review addresses the specified study questions by defining a review protocol.
- Systematic review defines search strategy that objects to detect as much of the related literature as possible.
- Systematic reviews need inclusion and exclusion criteria to assess each potential primary study.

We adopted the guidelines and systematic process by kitchen ham [14] in this study work. Systematic review is conducted mainly in three phases:

- Planning the review: Associated with identification of need for a review and emerging the review protocol.
- Conducting the review: Associated with selection of primary studies, quality assessment, data extraction and data synthesis [33].
- Reporting the review: Related with reporting the results and documenting the process.

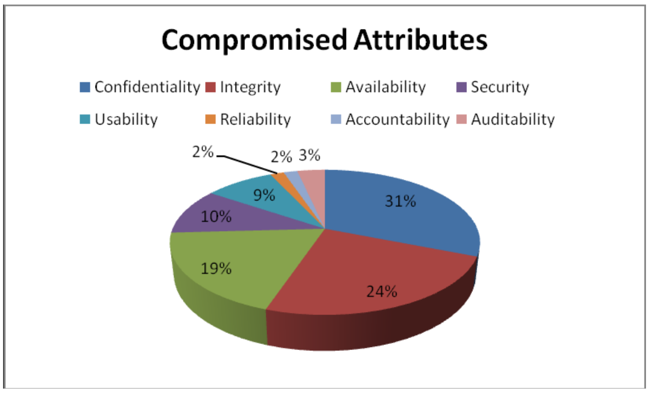
Survey:

Survey is also one of the potential study methods. Survey signifies one of the most common types of measureable scientific study. In survey study, the studier selects respondents from population and maintains a standardized survey. The survey can be a written document that is completed by the person being surveyed.

Results and Analysis:

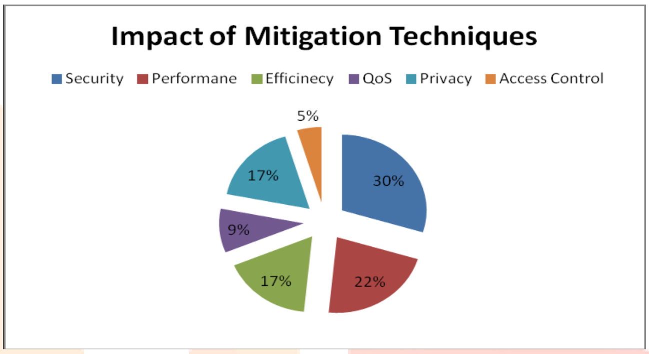
The paper review consist the results from SLR and Survey. In this we have stated the recognized security challenges and mitigation techniques from SLR also given information about survey participants and clarified the analysed results from the survey [15].

From the investigation, we have identified 43 security challenges during the SLR. The detailed description of these challenges is obtainable in Appendix A [31, 32]. The record of recognized challenges are WS- security, Phishing attack, Wrapping attack, Injection attack, IP spoofing, Tampering, Repudiation, Information Disclosure, Denial of service, Elevation of privilege, Physical security, WLAN‟s security, Direct attacking technique, Replay attack, Man-in-the middle attack, Reflection attack, Interleaving, Timeliness attack, Self-adaptive storage resource management, Client monitoring, Lack of trust, Weak SLAs, Perceived lack of reliability[16], Auditing, Back door, TCP hijacking, Social engineering, Dumpster diving, Password guessing, Trojan horses, Completeness, Roll back attack, Fairness, Data leakage, Computer network attack, Denial of service, Data security, Network security, data locality, Data segregation, Backup, Data integrity, Data manipulation. In the part of the study, we find some of the Cloud Computing characteristics which are threats to Cloud Computing [30]. As a part of the result the compromised attributes in Cloud Computing is described in appendix A, they are Confidentiality, Integrity, Availability, Security, Accountability, Usability, Reliability and Auditability. The files of the most make threats attributes are in fig. the fig. displays that Confidentiality 31% and Integrity 24% recorded most threaten, while comparing with usability, reliability, accountability and audit ability which recorded less than the 10%[17].



From the investigation, we have recognized 34 security techniques during the SLR. The detailed description of these techniques is presented in Appendix B[18]. The summary include character based authentication, RSA algorithm, Dynamic Intrusion decision system, Multi tenancy based access control model, TLS Handshake, Public key homomorphic, Third party auditor, probabilistic sampling technique, Diffle – Hellman key exchange, Private face recognition, MACs, Data coloring and water marking [29], A novel Cloud dependability model, KP-ABE, RBAC, ARVTM, Security assertion markup language, TPM, Proof of irretrievability, Fair MPNR protocol, Sobolorder, Redundant array of self-governing Net storages, Handoop distributed file system, self-cleansing intrusion tolerance, searchable symmetric encryption, Provable data possession, Privacy manager, Time bound ticket based mutual authenticationscheme, Security Access Control Service[19], The Service Level Agreement, Intrusion recognition system. The beyond cited mitigation techniques have strong impact on the Performance, Security, Efficiency, QoS, Privacy and Access control of Cloud Computing. The clear mitigation techniques somehow boost the overall services in Cloud Computing environment. The result is shown in figure [20].

Cloud Computing is a new model. Cloud Computing became popular since decade. To find out the security specialist in Cloud Computing is complex. In total, we got 16 number of partially and concluded responses from the real time survey. However, many do have related experience in Cloud Computing and IT security [21]. The adopted specialists have experience from 1 to 31 years. The Name, country, professional role and experience in related field is presented in the table below:



Name	Country	Professional Role	Experience in IT Sector (Years)	Experience in Cloud Computing (Years)	Experience in Security domain (Years)
Martin Bergling	Sweden	Information security consultant, IBM	23	1	23
Dan Ahlstrom	Sweden	Former CISO, development	17	2	17
Jan Hendler	Sweden	IT-Security Manger, Swedish Custom	20	4	20
BengtAckzell	Sweden	Security Expert	31	0	20 +
Daniel Gustafsson	Sweden	Technical advisor Blackberry, Logica	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A	N/A
Arun Taman	USA	Software Engineer, Oracle	14	4	4
N/A	N/A	N/A	18	0	11
Prajwal Kumar	India	Data base Developer	20	8	10
Johan Trodsson	Sweden	Studyer& Lead Architecture	8	4	0
Pethururaj	India	Enterprise Architect, Sify Software Ltd.	5	3	1
N/A	N/A	N/A	N/A	N/A	N/A
Omar Abduljabbar	India	Infrastructure Architect, MTN.	15	3	10
Sherif	Egypt	Manager Mobinil	10	0	10
Bengtakeclaesson	Sweden	Operational manager	10	3	6
N/A	N/A	N/A	N/A	N/A	N/A

In the portion of the Survey, we have recognized totally 18 Security challenges which are possible to be challenged in the future of Cloud Computing [22]. We summarized these upcoming security challenges based on the opinions from experts. The results are included:

- Eaves dropping
- Hypervisor viruses
- Authorized Interception point
- Virtual machine security
- Reliable transaction
- Risk of multiple Cloud tenants
- Smart phone data slinging
- Abuse and nefarious use of Cloud Computing
- Insecure application programming interfaces
- Malicious insiders
- Shared technology vulnerabilities
- Service and traffic hijacking
- Privacy – Personal information about many people will be handled by IT companies all over the world. No one will know who is retrieving user data.
- Espionage – National secret information might be handled by IT companies in other countries, but do we really know who is working at these enterprises?
- Business intelligence – Business confidential will be handled by IT companies all over the world. No one knows who is accessing user company's data.
- Data ownership – When data is transferred to the Cloud it is significant for many organizations to be assured of the continued control of the data, i.e. their ownership should never be challenged [23].
- Availability – The availability must be at least as high as for traditional solutions. Probably higher, since downtime probably will affect many users simultaneously and thus be covered by media. Compare the difference between small accidents (e.g. car) and large accidents (e.g. airplane). Even though many small accidents may be worse than one large, the media coverage (and other things) make the larger ones seem so much worse [24].
- Transparency – Using Cloud services has to be as simple as traditional solutions.

The compromised attributes are confidentiality, security, availability and integrity.

Validity Threats:

In our revision, we have data from Systematic Literature Review (SLR), survey and consultations. Comparison of results from SLR, interviews and survey is hard. We have measured this threat due to inconsistency in data [25]. To overcome this we have used Narrative Examination for Systematic Literature Review and interview data for proper organization of the data. After receiving the survey data we have thoroughly associated the Narrative Analysis results with the survey results, by this we were able to remove redundancy and inconsistencies in our data [26].

There are numerous problems with conducting survey. One of the major challenges is the redundancy in data interpretation by the practitioners [27]. The redundancy happens when understanding the question and the answers might be interpreted in another sense which might not be related for our work. Based on the understanding of the question her/his answers might differ. To rise above this threat we made sure that the questionnaire is obviously understandable,

- We have used terminologies related to Cloud computing which are mostly used in the industrial context.
- We have conducted a pilot test with Cloud Computing professionals.

Based on the feedback of Cloud Computing professionals, survey questionnaire was reformulated. Hence, the chance of internal validity has been reduced [28].

Conclusion:

The classification of security testing's and mitigation techniques in Cloud Computing is challenged by allowing for the large number of services. Most of the responses from survey, noted that Cloud Computing will place dominant and expandable data transactions. Because it offers many flexible services, provides easy, individualized and instant access control to the services and information where they are for the users. In the growth of identification from the study methods SLR and Survey, we have recognized acceptably number of challenges and mitigation techniques in current and future Cloud Computing.

In the upcoming, the people will access and share their software applications through online and access information by using the remote server networks instead of depending on primary tools and information hosted in their personal computers because of flexibility in Cloud Computing. The security issues in Cloud Computing are always one of the main studytopics for studiers and designers to investigate the appropriate solutions every time. From the perspective of this paper, we suggest that to find abest and suitable security solutions for the specific services in the Cloud. There is a scope to propose the guidelines to overcome the upcomingexperiments like physical security, espionage, transparency, data ownership, hypervisor viruses and malicious insiders in Cloud security. To concentrate on more specific areas like regulatory and compliance issues, jurisdiction laws, etc.

References:

1. Ahmed S, Raja M. (2010) 'Tackling Cloud security issues and forensics model', *High Capacity Optical Networks and Enabling technologies (HONET)* , 19-21 Dec, pp. 190-195.
2. Ahuja R. (June 2011) 'SLA Based Scheduler for Cloud storage and Computational Services', International Conference on Computatonal Science and Applications (ICCSA), 258-262.
3. D. Zissis and D. Lekkas" Addressing Cloud Computing Security Issues", Future Generation Computing Systems, pp: 583-592, 2012
4. Albeshri A, Caelli W. (Sept 2010) 'Mutual Protection in a Cloud Computing Environment', 12th IEEE International Conference on High performance Computing and Communications (HPCC), 641-646.
5. Almulla S, Chon YeobYeun. (March 2010) 'Cloud Computing Security management ', 2nd International Conference On Engineering Systems Management and Its Applications , 1-7.
6. Rashmi, Sahoo, G. and Mehfuz, S. "Securing Software as a Service Model of Cloud Computing: Issues and Solutions". International Journal on Cloud Computing: Services and Architecture, 3(4), 1-11. Doi: 10.5121/ijccsa.2013.3401,2013
7. B. lagesse. (Mar.2011) 'Challenges in Securing the Interface between the cloud and Pervasive Systems', 2011 IEEE International Conference on Pervasive Computing and Communications Workshops, 106-110.
8. Brenner Michel, Wiebelitz Jan. (may 31, 2011) 'Secret program execution in the Cloud applying homomorphic encryption', Digital Ecosystems and Technologies Conference (DEST), 5th IEEE International Conference 2011, 114-119.
9. C. C Ragin. (1997) 'Turning the tables: How case - oriented study challenges variable oriented study', *Comparative social study*, vol. 16, pp. 27-42.
10. Casola, V., Cuomo, A., Rak, M. and Villano, U." The CloudGrid approach: Security analysis and performance evaluation". Future Generation Computer Systems, 29, 387–401. doi:10.1016/j.future.2011.08.008,2013.
11. Ibrahim AbakerTargio, IbrarYaqoob, Nor BandrulAnuar, SalimahMokhtar, Abdullah Gani, SameeUllah Khan, "The Rise of "Big Data on Cloud computing": Review and open studyissues"Information Systems, 47-2015.
12. C. C Ragin. (2000) *Fuzzy set science*, Chicago: The university of Chicago.
13. Chang Lung Tsai, Uei –Chin Lin. (Aug 2010) 'Information Security issue of enterprises adopting the application of Cloud Computing', 6th International Conference on Networked Computing and Advanced Information Management (NCM), 645-649.
14. N. Pradheep, M. Venkatachalam, M. Saroja and S. Prakasam (2016), "Image Data Security Concerns in Cloud Computing: A Review", Elixir International Journal of Computer Engineering, 99(2016), pp-43093-43095.
15. Chenguang Wang, Huaizhi Yan. (Dec 2010) 'Study of Cloud Computing security based on Private Face Recognition', International Conf. on Computational Intelligence and Software Engineering , 1-5.
16. Cong Wang, Kuiren. (2010) 'Toward publicly auditable secure cloud data storage services', *Network ,IEEE*, vol. 24, no. 4, July, pp. 19-24.

17. Cong Wang, Qian Wang. (March 2010) 'Privacy Preserving Public Auditing for Data storage security in Cloud Computing', INFOCOM 2010, IEEE, 1-9.
18. Cong Wang, Qian Wang. (2009) 'Ensuring data storage security in Cloud Computing', International Workshop on Quality of Service, 1-9.
19. C. Wohlin. (2000) *Experimentation in Software engineering: an introduction*, 6th edition, International series in software engineering, Springer.
20. Dawei Sun, Guiran Chang. (Sept.2010) 'A Dependability Model to Enhance Security of Cloud Environment Using System-Level Virtualization Techniques', Pervasive Computing Signal Processing and Applications, 305-310.
21. N. Pradheep, Venkatachalam M, Saroja M, Prakasam S (2016), ‘Privacy and security issues in cloud computing using DaaS models”, Indian Journal of Science, 2016, 23(87), pp-863-866.
22. Dawod W, Takouna I. (March 2010) 'Infrastucture as a service security: challenges and solutions', 7th International Conference on Informatics and Systems (INFOS), 1-8.
23. The rise of “big data on cloud computing”: Review and open study issues Ibrahim AbakerTargioHashem, IbrarYaqoob ,NorBadrulAnuar , SalimahMokhtar , AbdullahGani , SameeUllahKhan , Information Systems , 2015.
24. Doelitzscher F, Reich C. (July 2010) 'Designing Cloud services adhering to Government privacy Laws ', IEEE 10th International Conf. on Computer and Information Technology, 930-935.
25. D.K. Mishra. (Sept.2010) 'Tutorial: Secure Multiparty Computation for Cloud Computing Paradigm by Durgesh Kumar Mishra', Second International Conference on Computational Intelligence, Modelling and Simulation, xxiv-xxv.
26. Ford R.B. (2011) 'Information Security in the Cloud', *Network Security*, vol. 2011, no. 4, April, pp. 15-17.
27. Gul I, Rehman A. (June 2011) 'Cloud Computing Security Auditing', 2nd International Conference on next Generation Information Technology (ICNIT), 143-148.
28. Hao Z, Zhong S. (June,2011) 'A Time-Bound Ticket-Base Mutual Authentication Scheme for Cloud Computing', *International Journal of Computers, Communications and Control*, vol. 6, no. 2, June, pp. 227-235.
29. N. Pradheep, M. Venkatachalam, M. Saroja and S. Prakasam (2017), “A Cloud Computing Solution for Securely Storing and Accessing Patients Medical Data”, Journal of Advance Study in Dynamical & Control Systems, 12-Special Issue, August 2017, ISSN:1943-023X, pp-614-622.
30. Huimei Wang, Ming Xian. (May 2011) 'Cloud Evaluation method of Network Attack resitance Ability', Network Computing and Information Security (NCIS), 239-243.
31. Jaatun M.G, Nyre A. A. (March 2011) 'An approach to confidentiality control in the Cloud', Vehicular Technology, Information Theory and Arreospace and Electronic systems Technology, 2nd International Conference on Wireless Communication,1-5.
32. Jensen M, Schwenk J. (Sept.2009) 'On Technical Security Issues in Cloud Computing', IEEE International Conference on Cloud Computing, 109-116.
33. JiaWeiwei Zhu, Haojin Cao. (10-15 April, 2011) 'A Secure data service mechanism in mobile Cloud Computing', Computer Communications Wrokshops (INFOCOMWKSHPS), IEEE Conference 2011, 1060 - 1065.
34. Jin Li, Gansen Zhao. (2010) 'Fine-Grained Data Access Control Systems with User Accountability in Cloud Computing', 2nd International Conference on Cloud Computing Technology and Science, 89-96.
35. Jun Feng, Yu Chen. (Jan 2010) 'Bridging the Missing link of Cloud data storage security in AWS ', 7th IEEE conf. on Consumer Communications and Networking Conference (CCNC), 1-2.
36. Jun Feng, Yu Chen. (Jan 2011) 'Enhancing Cloud storage security against rool- back attacks with a new fais multi party non-repudation protocol', Consumer Communications and Networking Conference (CCNC), IEEE conference 2011, 521-522.
37. Jun Feng, Yu Chen. (Sept 2010) 'Analysis of Integrity Vulnerabillities and a Non repudation Protocol for Cloud Data Storage Platforms', 39th International Conf. on Parallel Processing Workshops (ICPPW), 251-258.
38. Jun-Ho Lee, Min-Woo Park. (feb. 2011) 'Multi level Intrusion Detection System and Log management in Cloud Computing', Advanced Communication Technology (ICACT), 13th International Conference 2011, 552-555.
39. Kai Hwang, Deyi Li. (2010) 'Trusted Cloud Computing with Secure Resources and Data coloring', *Internet Computing*, vol. 15, no. 05, October, pp. 14-22.
40. Kai Zhang, Ying Song. (july,2010) 'Trusted Connection System based on Virtual Machine Architecture', 3rd IEEE International Conference on Computer Science and Information Technology, 192-196.