Issues and Challenges in Securing the Cloud Environment: A Literature Review

Surbhi Gaur*
Savleen Kaur**

Abstract

The emerging awareness and implementations of cloud services and its underlying technologies instigate the urge for security requirements being up to date, despite of the fact that this technology and its application are not latest. It is still challenging to assess what types of requirements have been researched most, and which are still under-researched even though cloud computing security requirements have been inscribed in publications earlier as well. A systematic literature review has been carried out by this paper by describing cloud computing security requirements from publications between January 2012 and December 2013. Requirements will be categorized in a framework and their frequency of research will be assessed by this. Changes will be identified in the assessment of requirements and proposed solutions. It has been observed that the most researched sub-factors of security requirements are: Access Control, Data Integrity and Privacy & Confidentiality. Most under-researched areas are Recovery and Prosecution, with Non-repudiation and Physical Protection closely followed. Instead of the new solutions several enhancements and nested methodologies in current approaches were identified.

Keywords: Access control, Cloud Computing, Data integrity, Recovery, Repudiation, Security Requirements, Security factors, Software as a Service

Introduction

An emerging term or paradigm that involves the use of configurable computing resources (hardware, software, and network) with its intention to offer an aid to a consumer [57] is Cloud computing (CC). Its fundamental business model include at least two actors [52], by enabling ubiquitous, convenient, on-demand network access [57] A cloud provides a cloud service user (CSU) the privilege of access to an application (software), platform or infrastructure "as a service". This term in turn signifies that a CSU is making use of a service offered by a cloud service provider (CSP).Although the software and its supporting systems are running and data is stored on providers computing machines [57], depending on the service type, web Browser, mobile app or desktop application are usually responsible for delivering or transferring this said service on the client side. By definition of the NIST (National Institute of Standards and Technology), the Cloud Computing model holds three service models. They are remarked to as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [57]. Network as a Service (NaaS) is also recognized as forthcoming service type in the vehicle and telecommunication field [53] by recent publications. The CSUs are assured either more or less control over the connected computing resources by counting on the type of cloud and its deployment model (private, community, public, hybrid [57]). Thus the degree of control is directly related to security matters, and security has been rated as the huge challenge for all kinds of cloud services as administered by a survey of IDC [34]. Due to this detailed insight into this field is needed. Public clouds or (public) SaaS security is the main focus of this paper, since they assimilate and cover a great

Surbhi Gaur*
IINTM, GGSIPU
Savleen Kaur**
IINTM, GGSIPU

Table 1: Results of literature search[43]

	security AND SaaS	security AND SaaS
Scopus	12 - of 121 (10%)	20 - of 399 (5%)
Web of Science	13 - of 126 (10%)	15 - of 489 (3%)
Google Scholar	2 of 81.100	2 of 54.800

amount of essential security aspects of the other service levels and deployment models due to hierarchical relations and their implications [25, 57].

The reacquired requirements, along with their frequency of research and addressed solutions of literature review, will be evaluated in a framework by Firesmith [14].

The problem statement and research questions are framed in the next sub-sections. The research method is portrayed in section –Method of Research, the section- Related work, describes the research work which was done for the paper and the next section analyze the papers according to the proposed framework. The Discussion section deals with the analysis on the findings, and validity threats and conclusions are presented in last section.

Problem Statement

The emerging awareness and implementations of cloud services and its underlying technologies instigate the urge for security requirements being up to date, despite of the fact that this technology and its application are not latest. It is still challenging to assess what types of requirements have been researched most, and which are still under-researched.

To provide an exhaustive and structured overview of the types of security requirements investigated in the area of cloud computing and the proposed solutions to deal with these requirements is the objective of this paper. This paper hereby informs fellow researchers on what is known in published empirical studies regarding security requirements in cloud computing and pinpoints to those types of security requirements that have received much research effort and those that have been under-researched. For quickly finding and addressing the gaps in cloud security issues, it further inscribes and helps consultants and developers by providing the detailed overview.

Research Questions

The following research questions (RQs) are used for this paper.

RQ1: What are the cloud security requirements that have been addressed in recent publications (2012-2013)?

RQ2: What are the solutions offered to them?

RQ3: Which cloud security requirements have been under-researched?

Method of Research

For research questions [26], the literature sources have been found on Google Scholar, Web of Science and Scopus.

It was found in the initial literature review, that to allow addressing and categorization of security requirements, different frameworks have been published [12, 17, 51]. In this study, Firesmith[14] framework is chosen. This framework was chosen as other authors used it[5] and a comparison findings had to be done with their study. Hence, a common platform was needed. This framework is made of 9 sub-factors which define the hierarchy of the decomposition of security [14]. This literature review will then identify the most researched and the most under-researched areas.

Related Work

In an earlier work**,** Mariana Carroll et. al. [13] already approached a systematic review. In that paper, overview was given on the cloud computing benefits and security risks as a general guideline to assist management in the implementation of cloud

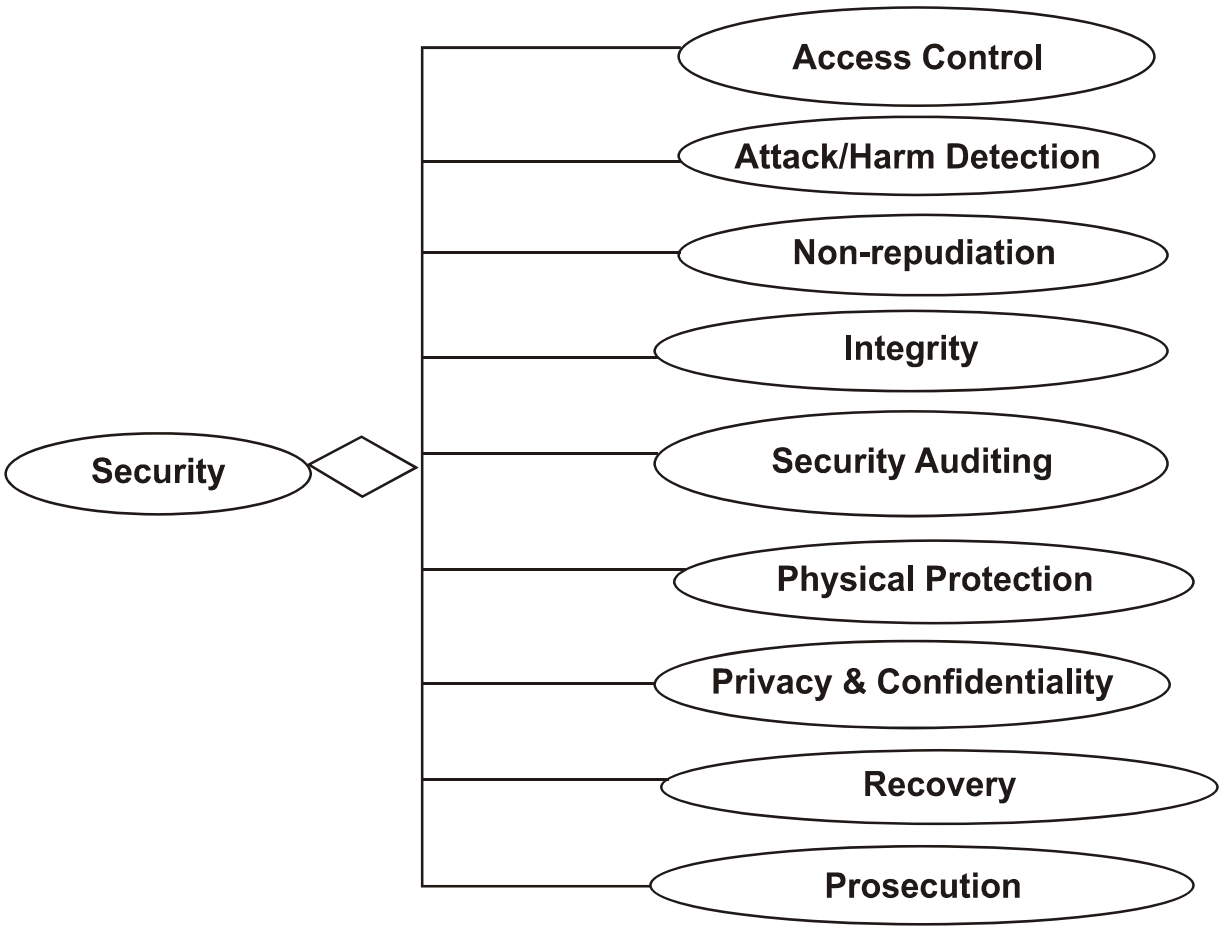

Fig. 1: Taxation of security requrement[14]

computing processes, procedures and controls. To ensure completeness, availability of applications, integrity and data in the cloud, consideration should be given. To reduce the security risks in cloud computing, some controls were introduced. The controls included data security, administration and control, logical access, network security, physical security, compliance and virtualization.

Additional work exists, as several researchers have studied the field of cloud computing and its issues and challenges earlier, but an assessment seems to be missing [2, 61, 66].

Classification of Literature by Security Sub-factor

The Firesmith[14] framework is used to enforce the identification of areas which are much researched in comparison to other subjects on a per sub-factor basis. This will be the basis for providing the answer for RQ3 and to determine suggestions for future work and research.

As indicated in figure 1, the framework consists of 9 sub-factors. All the 9 sub-factors will be explained with the findings from the corresponding sources of literature that belong to each factor.

In the following sub-sections, the sub-factors are discussed and their future solutions.

Access Control

Access Control is defined as the "degree to which the system limits access to its resources only to its authorized externals" [43]. Authorized externals can be defined as human users, services or programs fragments, any kind of systems or devices. It is a

combination of Identification, Authentication and Authorization. All the three when combined together controls and supervises the permissions granted to those users who can prove their true identity and then be allowed for further privileges over the resources. When the permission is granted over a range of resources, access control has to hold on to this state, till the temporary access is not terminated successfully.

The LAP (Lightweight Authentication Protocol) [49] is defined to enhance security in authentication. The basic standards to define one solution for Grid and Cloud computing was proposed in [56] by the name of interoperable security protocol. Research in [37] uses the SAPS (Single Attribute Protection Scheme) whereas the MADAC model [19] makes use of multi attributes and dynamic access control.

Similarly research in [21, 32, 15, 31, 59, 4, 15, 66, and 2] also makes use of access control.

Attack/Harm Detection

This sub-factor determines "the degree to which attempted or successful attacks (or their resulting harm) is detected, recorded and notified" [68]. Solutions which can be offered for this are: (1) passive prevention and detection and (2) counteractive solutions. SOTA model [9] and its neural network, the Cloud Protector, contain various Cloud Trace back methods to face such threats and attacks. Similarly the work in [3, 55, 7, and 33] also conducts the attack/harm detection.

Non-Repudiation

Non-repudiation is defined as "the degree to which a party to an interaction (e.g., message, transaction, transmission of data) is prevented from successfully repudiating (i.e., denying) any aspect of the interaction" [43].

An issue of guaranteeing privacy and integrity is denying a user from private data which is currently transmitted or accessed, the solutions are provided hereby in [35, 15].

Similarly authors of [38, 45] also deal with this sub-factor.

Integrity

Integrity can be defined as "To protect the components of the system from intentional and unauthorized harm or corruption" [43].Integrity requirements can be separated from hardware integrity, data integrity, software integrity and personnel integrity. The papers which focused on data integrity are [20, 56, 68].

SLA (Service Level Agreements) is the most common technique which covers requirements in this category. SLA is contract between CSP and CSU [68]. It also defines certain standards and the architecture of the cloud. ACID properties must be followed to perform access or transactions on the database [54]. Other security techniques are treated by the frameworks like dispersed data storage and cryptographic [50]. Research in [41] defines the principle agent model to develop the strategies to ensure data integrity.

In cloud computing, there is a highly important concept of Cloud Computing. It means realization of a virtual environment rather than a physical machine provided. The advantages of virtualization are scalability, security and cost-benefits. It manages to reduce damage of malicious applications, isolates faults, viruses or intrusions from other VM's [29]. Other important feature in clouds is Multi-tenancy. CSP's are provided for more effective and efficient resource utilization, by partitioning and sharing mainly services [54]. Similarly papers [32, 22, 45, 9, 8, 15 and 42] focuses on this sub-factor.

Security Auditing

This sub-factor take care of the security requirements, in which security personnel are allowed to audit the status, use the status and the check as to how much the security mechanisms are susceptible, by scrutinizing the security related events.

In [6], it is mentioned that the security auditing is a part of an approach known as dynamic verification approach. It differs from the static approaches as it

Table 2: Papers focusing on multiple security requirements[14]

Ref.	Requirements	Solution
[40]	data violation, network (access threats), integrity & redundancy, isolation, logging, channel protection	best practices, conceptual framework
[29]	security models, security strategies, risk analysis	analysis of security models, issuing of security strategies
[59]	general security, privacy & trust, cryptography	MULTI (for each subject)
[5]	Security concerns, protection, multi tenants, iris, HAIL, global challenge	Range of protection mechanisms + auditing framework
[44]	general cloud security; confidentiality, integrity	5 deployment models
[16]	access & identity, trust, privacy, auditing	Security Management as a Service (SMaS) model
[23]	security issues, technical security measures, multiple requirements	5 countermeasure models (current security technologies)
[62]	attack threats, cloud reference model, CRM,	Security Model SM_CRM
[27]	Trusted Platform, User Enabled Collaboration, Security Groups, Data Security, CSU&CSV attestation	4 FPGA based solutions
[54]	survey, security of service delivery models, data risk, current solutions	state of the art security solutions / best practices
[24]	taxonomy for cloud security issues, taxonomy, responsibilities	cloud security architecture model

is achieved traditionally, with the help of examining the execution of the systems and checking and substantiating its accordance against a rule set.The solution set provided by [6] deals with:

(i) Architecture which is 3-layered.

(ii) Monitoring rules have to be expressed in a new language.

(iii) To improve the monitoring engines, there is need for new approach known as a finite state machine approach.

Similarly papers [26, 1, 47] deal with the security auditing concept.

Physical Protection

It shows the degree to which the system protects itself and its components against physical attacks [68]. Physical Attacks mentions the natural causes, for ex. Earthquakes and demolition of infrastructure by natural disasters, and theft of physical machines or hardware by a malicious invader.

Focus on physical protection is not there in any of the paper.

Privacy and Confidentiality

Privacy and confidentiality refers to the degree to which unauthorized parties are prevented from obtaining sensitive information [68]. Privacy is generally found to be directly related to access control requirements. For a high degree of privacy and confidentiality, strict access control mechanisms are enforced. [59, 54]

Privacy consists of two requirements: (i) during access, storage and transmission of data from CSU

through the internet, confidentiality is ensured. (ii) To ensure the protection of CSU's private data from CSP.

The paper in [35] describes the SaaS application framework using Information Gateway, to confirm confidentiality. To ensure a safe data routing, a dynamic control mechanism is used over a executing location. Different techniques for data encryption and data mash up for auditing, is used in the model.

Similarly the papers in [58, 37, 48, 15, 31, 36, and 67] also deal with this sub-factor.

Recovery

Recovery refers to the degree to which unintentional manipulated, corrupted or 'lost' data may be partially or possibly fully recovered [68]. Recovery may be instant or approachable as an optional functionality for either CSU's or CSP's [14].

It must be noted that none of the papers deals with this sub-factor as a main topic. Recovery may be taken care with hardware or software technique. Contracts are defined in the SLA for data recovery by the cloud providers [50, 68].

Similarly paper [26] also deals with it.

Prosecution

There can be reasons of Prosecution:

1. The ability and legislative permission of law enforcement to investigate, seize and prosecute systems subject to breaking the law
2. The ability to prosecute suspicious or malicious actions and users within the cloud domain. To some extent this can be connected to security auditing.[68]

In [1, 26] the solutions are provided through a different means.

Multiple sub-factors

Papers explaining multiple security requirements are termed as 'MULTI'. In Table 2, the requirement column specifies general requirements being issued by the paper's authors for solutions.

Discussion

The in-depth study of the literature and its categorization among various sub-factors has been noticed of consuming more time than previously assumed and planed. Not only each paper had its own language and style of narration but also study of the proposed interconnections, terms and proposal of solutions had to be done in greater detail for gaining conclusive insights into terminology, overlaps and approaches.A personal inference of the author on the other hand was made that a qualitative and careful classification would be instead the cause of a conclusive textual review of the remaining paper.

Sub-factor specific sections indicate that it was sometimes difficult to discriminate and categorize a paper on the basis of major topics it handles. As acknowledged by the detailed classification table in the Appendix, there are two or maybe three options to do so for some papers. Not for all papers the distinctive major topic (following the inclusion criteria) could be identified and the paper categorized accordingly. Hence the following approach was introduced: for each paper posing problems in identifying the boundaries and major topic, two or three topics were identified, with one relating to the classified sub-factor and the rest being referred to as "connection". E.g. [11] was identified to be tackling both access control requirements and confidentiality. The paper was thus classified for the first, while a connection-count was noted due to privacy & confidentiality requirements.

This approach aims to slightly balance the strict separation between the security sub-factors. To the current reader it might already be surprising that privacy & confidentiality (along with requirements focusing on 'trust') only amount to 4 out of 50 papers. Taking the connection-factor into account, we found that 10 more papers have an immediate linkage regarding this as equal level of relevancy in their topic's scope.

Table 3: Distribution of papers on security sub-factors[14]

Security sub-factor	Amount	Connections	% of total
Multi	11		22
Access Control	14	5	28
Attack/Harm Detection	5	1	10
Non- Repudiation	1	3	2
Integrity	10	6	20
Security Auditing	5	5	10
Physical Protection	0	3	0
Privacy & Confidentiality	4	10	8
Recovery	0	0	0
Prosecution	0	0	0
Total	50	33	100
Exclusions	7		

Table 3 shows the overall distribution of the selected publications classified to the corresponding security sub-factor. Connections refer to the counts of whether this sub-factor was tackled as another (2nd major) topic in already otherwise classified items because of blurred boundaries. Narrow classification details can be reviewed in the Appendix.

The most investigated security requirements as suggested by Table 3 is Access Control, being the topic of research in about 28% of the contained publications Integrity which is the topic of 20% of the papers in our review is the second most studied requirement. It is also observed that 22% of all papers investigated multiple security requirements. This is not surprising, as dependencies exist among the types of security requirements as described earlier (e.g. [7, 48, 38, 31]).

In General, for example, to separate the following correlations (triples) was difficult during the classification phase:

- (Access control), data integrity, privacy
- "Data security": mostly mentioned to as this term, it includes a combination of (data) integrity and access control, even non-repudiation
- Security auditing, data integrity, privacy
- Attack/harm detection, (physical protection), security auditing

In the treated literature, the security sub-factors non-repudiation, physical protection, recovery and prosecution have not been researched and only minor references and statements about these could be made. Solutions for recovery and non-repudiation might not be researched in connection with cloud computing or the SaaS terminology as a background is One of the reason for it, but instead general forms of security requirements. Because of our criteria of inclusion/exclusion, our scope to search for publications in the sectors of computer science, engineering and business was narrowed down by us. We accept that the hardware recovery might be a topic of research posted in field with mathematical engineering background.

Limitation of the literature search by subject area might lead to an inadequacy of investigation in the prosecution sub-factor. Also there seem to be no realistic techniques or possibilities to prevent prosecution from governmental bodies as indicated, although data encryption to provide confidentiality is of major importance.

Furthermore many papers deal with multiple requirements, even when they were devoted to a specific sub-factor. The boundaries of these research efforts sometimes seem blurry due to the overlaps with other sub-factors as mentioned earlier.

It might not be surprising that physical protection for example seems to be an under-researched area in security requirement. Data integrity and recovery are directly related to this sub-factor. In case of physical theft e.g. by using information dispersal techniques, recovering and restoring data could be easily done as described by virtualization, data dispersion and multi-tenancy.

Conclusions & Future Work

This paper deals with the in-depth overview of the research done to answer the three research questions asked. The main points of the research are mentioned below:

RQ1: What all cloud security requirements have been addressed in recent publications (2011-2013)?

After the review it was found out that the below given factors have been heavily used: Attack/Harm Detection, Non-Repudiation, Security Auditing, Privacy & Confidentiality, Access Control and Integrity. Out of all these factors the most researched factors are the last three requirements.

RQ2: What are the solutions offered to them*?*

The solutions to these requirements range from the use of Private Key Infrastructure, authentication and authorization protocols , VM isolation and fork mechanism towards transmission and calculation of encrypted data, auditing schemes and countermeasure protection mechanisms. These solution techniques are not limited to only one factor but with the combination of many other factors.

RQ3: Which cloud security requirements have been under-researched?

The most under researched factors in security requirements are Recovery and Prosecution, Non-Repudiation and Physical Protection.

References

1. A. A. Deshmukh, A. Mihovska, and R. Prasad, “A cloud computing security schemes: - TGOS and TMS”, Trivandrum, 2012.
2. A. Behl, and K. Behl, “Security paradigms for cloud computing”, Phuket, 2012.
3. A. Chonka, and J. Abawajy, “Detecting and mitigating HX-DoS attacks against cloud web services”, Melbourne, 2012.
4. A. Chonka, Y. Xiang, W. L. Zhou, and A. Bonti, “Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks”, Journal of Network and Computer Applications, 34, 4 (Jul 2011), 1097-1107.
5. A. Juels, and A. Oprea, “New approaches to security and availability for cloud data”, Communications of the ACM, 56, 2 2013, 64-73.
6. A. Munoz, J. Gonzalez and A. Mana, “A Performance-Oriented Monitoring System for Security Properties in Cloud Computing Applications”,[*Computer Journal*, 55, 8 (Aug 2012)], 979-994.
7. A. T. Monfared, and M. G. Jaatun, “Monitoring intrusions and security breaches in highly distributed cloud environments”, Athens, 2011.
8. B. Loganayagi, and S. Sujatha, “Enhanced cloud security by combining virtualization and policy monitoring techniques”, Coimbatore, 2012.
9. B. Loganayagi, and S. Sujatha, “Improving Cloud Security through Virtualization”, Tirunelveli, 2011.

10. B. Kitchenham, "Procedures for performing systematic reviews", [*Keele, UK, Keele University*, 332004], 2004.

11. B. P. Gopularam, and N. Nalini, "Mechanism for secure content publishing for reporting platform hosted on public could infrastructure", Bangalore, 2013.

12. C. B.Haley, R.Laney, J. D. Moffett, and B. Nuseibeh, "Security requirements engineering: A framework for representation and analysis", *IEEE Transactions on Software Engineering*, 34, 2008, 133-153.

13. C. Mariana, A. Merwe, P. Kotze, "Secure Cloud Computing :Benefits, Risks and Controls"

14. D. Firesmith, "Specifying reusable security requirements", *Journal of Object Technology*, 3, 1 2004, 61-75.

15. D. H.Tran, H. L. Nguyen, W. Zha, and W. K. Ng, "Towards security in sharing data on cloud-based social networks", Singapore, 2011.

16. D. Krishnan, and M. Chatterjee, "Cloud security management suite - Security as a service", Trivandrum, 2012.

17. D. Mellado, C. Blanco, L. E. Sánchez, and E. Fernández-Medina, "A systematic review of security requirements engineering", [*Computer Standards and Interfaces*, 32, 4 2010], 153-165. -

18. D. Zissis, and D. Lekkas, "Addressing cloud computing security issues", [*Future Generation Computer Systems-the International Journal of Grid Computing and Escience*], 28, 3 (Mar 2012), 583-592.

19. D.Yan, F. Yang and Y. Tet, "Servies security architecture and access control model for cloud computing", [*China Communications*], 8, 6 2011, 44-50.

20. G. Chen, J. Miao, F. Xie, and H. Mao, "A framework for storage security in cloud computing", Guangzhou, 2013.

21. G. H. Cho, and S. A. Lee, "A secure service framework for handling security critical data on the public cloud", Guangzhou, 2012.

22. H. Elham, A. Lebbat, and H. Medromi, "Enhance security of cloud computing through fork virtual machine.", Agadir, 2012.

23. H. Lee, J. Kim, Y. Lee, and D. Won, "Security Issues and Threats According to the Attribute of Cloud Computing", Jeju Island, 2012.

24. H. Tianfield, "Security issues in cloud computing", Seoul, 2012.

25. I. Iankoulova, and M. Daneva, "Cloud computing security requirements: A systematic review. Valencia", 2012.

26. I.Gul, A. Ur Rehman, and M. H. Islam, "Cloud computing security auditing", Gyeongju, 2011.

27. J. A. M. Mondol, and Ieee ,"Cloud Security Solutions using FPGA", 2011.

28. J. Gibson, D. Eveleigh, R. Rondeau, and Q. Tan, "Benefits and Challenges of Three Cloud Computing Service Models", 2012.

29. J. H.Che, Y. M. Duan, T. Zhang, and J. Fan, "Study on the security models and strategies of cloud computing", Tirunelveli, 2011.

30. J. S.Wang, C. H.Liu, G. T. R. Lin, and Ieee, " How to Manage Information Security in Cloud Computing", Anchorage, 2011.

31. J. Zhu, and Q. Wen, "SaaS access control research based on UCON", Guangzhou, 2012.

32. J.Ilanchezhian, V.Varadharassu, A. Ranjeeth, and K. Arun, "To improve the current security model and efficiency in cloud computing using access control matrix", Tamilnadu, 2012.

33. J.Yang, C.Wang, C. Liu, and L. Yu, "Cloud computing for network security intrusion detection system", [*Journal of Networks*, 8, 1 2013], 140-147.

34. K. Popoviæ, and Z. Hocenski, "Cloud computing security issues and challenges", Opatija, 2010.

35. K. Nishikawa, K. Oki, and A. Matsuo, "SaaS application framework using information gateway enabling cloud service with data confidentiality", Hong Kong, 2012.

36. L. Li, Q. Z. Li, Y. L. Shi, and K. Zhang, "A New Privacy-Preserving Scheme DOSPA for SaaS", Taiyuan, 2011.

37. L. Li, Q. Z. Li, Y. L. Shi, and K. Zhang," SAPS: A Single Attribute Protection Scheme for SaaS", [*Information-an International Interdisciplinary Journal*], 15, 1 (Jan 2012), 275-282.

38. L. Tingting, and Z. Yong, "A Decentralized Information Flow model for SaaS application security", Hong Kong, 2013.

39. M. Auxilia, and K. Raja, "A semantic-based access control for ensuring data security in cloud computing", Tiruvannamalai, 2012.

40. M. D Aime, A. Lioy, P. C. Pomi, and M. Vallini, "Security Plans for SaaS", Torino, 2011.

41. M. Xiao, and L. Chen, "Integrity auditing strategy design for data storage security in cloud computing", [*Journal of Computational Information Systems*], 8, 23 2012), 9779-9789.

42. N. K.Sehgal, S. Sohoni, Y.Xiong, D.Fritz, W. Mulia, and J. M. Acken, "A Cross Section of the Issues and Research Activities Related to Both Information Security and Cloud Computing",[Iete Technical Review, 28, 4 (Jul-Aug 2011)], 279-291.

43. P. Hover, "Cloud Computing Security Requirements and Solutions : a systematic Literature review"

44. P. J. Kaur, and S. Kaushal, "Security Concerns in Cloud Computing", Chandigarh, 2011.

45. P. S. Kumar, and R. Subramanian, "Homomorpic Distributed Verification Protocol for Ensuring Data Storage Security in Cloud Computing", [*Information-an International Interdisciplinary Journal*],14, 10 (Oct 2011), 3465-3476**.**

46. R. M. Savola, and J. Ahola, "Towards remote security monitoring in cloud services utilizing security metrics", Tbilisi, 2012.

47. R. Marty, "Cloud application logging for forensics", TaiChung, 2011.

48. R. Rajagopal, and M. Chitra, "Trust based interoperability security protocol for grid and Cloud computing", Coimbatore, 2012.

49. S. C.Wang, W. P .Liao, K. Q.Yan, S. S. Wang, and S. H. Tsai, "Security of cloud computing lightweight authentication protocol", Kaohsiung, 2013.

50. S. K. Sood, "A combined approach to ensure data security in cloud computing", [*Journal of Network and Computer Applications*], 35, 6 (Nov 2012), 1831-1838. -

51. S. L. Pfleeger, "A framework for security requirements", [*Computers and Security*, 10, 6 1991], 515-523.

52. S. Leimeister, M. Böhm, C. Riedl, and H. Krcmar, "The business perspective of cloud computing: Actors, roles, and value networks", Pretoria, 2010.

53. S.Rangarajan, M.Verma, A. Kannan, A. Sharma, and I. Schoen, "V2C: a secure vehicle to cloud framework for virtualized and on-demand service provisioning", [In *Proceedings of the Proceedings of the International Conference on Advances in Computing, Communications and Informatics* (Chennai, India, 2012)],ACM.

54. Subashini, S. and Kavitha, V. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34, 1 2011), 1-11.

55. T.Karnwal, S. Thandapanii, and A. Gnanasekaran," A filter tree approach to protect cloud computing against XML DDoS and HTTP DDoS attack", Chemnai, 2013.

56. T. Rohini, "Comparative Approach to Cloud Security Models", Mumbai, 2011.

57. Technology, N. I. o. S. a," The NIST Definition of Cloud Computing", U.S. Department of Commerce, Gaithersburg, 2011. -

58. V. P. Lijo, and S. Kalady, "Cloud Computing Privacy Issues and User-Centric Solution", Bangalore, 2011.

59. W. A. Jansen," Cloud Hooks: Security and Privacy Issues in Cloud Computing", Koloa, Kauai, 2011.

60. W. F Ouedraogo, F. Biennier, and P. Ghodous, "Adaptive security policy model to deploy business process in cloud infrastructure", Porto, 2012.

61. W. Jia, and S. Sun, "Research on the security issues of cloud computing", Wuhan, 2013.

62. X. L. Li, J. H. Chen, M. Luo, and Ieee ,"A Simple Security Model based on Cloud Reference Model", 2011.

63. X.Cao, L. Xu, Y. Zhang, and W. Wu, "Identity-based proxy signature for cloud service in SaaS", Bucharest, 2012.

64. Y. C. Wang, and S. Chen, "Analysis of Informatization Construction for SMEs with SaaS model", Shenzhen, 2011.

65. Y. J.Guo, C. G.Zhang, and L. Q.Tian, "Digital media distributing protocol based on cloud computing and proof of security", *XitongFangzhenXuebao / Journal of System Simulation*, 24, 2012, 2431-2433+2438.

66. Y. Zhang, and Y. Zhang," Cloud computing and cloud security challenges", Hokkaido, 2012.

67. Y.Chou, O. Levina, and J. Oetting, "Enforcing confidentiality in a SaaS cloud environment", Belgrade, 2011.

68. Z. Xiao, D. Hong-tao, C. Jian-quan, L. Yi, and Z. Lei-jie, "Ensure Data Security in Cloud Storage", Guanxi, 2011.