AN ANALYTICAL REVIEW OF CHALLENGES IN CLOUD COMPUTING

Tummapudi Sunil
Research Scholar
Department of Computer Science and Engineering
OPJS University, Churu Rajasthan.

Dr. Vijay Pal Singh
Research Guide
Department of Computer Science and Engineering
OPJS University, Churu Rajasthan.

Abstract

In the business world, cloud computing is the most promising implementation of utility computing at present due to its main advantages over traditional utility computing, including elasticity, which enables clients to dynamically scale up or down resources during execution time. However, despite being in its nascent phase, cloud computing continues to face challenges related to a lack of standardization. The primary obstacles to the adoption of cloud computing are security concerns. Therefore, apprehensive sectors, including government organizations (ministries), exhibit a reluctance to embrace cloud computing on account of the potential loss of sensitive data while it is hosted in the cloud; the lack of transparency regarding the security mechanisms employed by Cloud Service Providers (CSPs) to safeguard their data and applications; and the uncertainty surrounding data location. These factors collectively impede the adoption of the agile computing paradigm. The purpose of this study is to examine and categorize the challenges associated with the deployment of cloud computing, an area of significant interest that requires further investigation.

Keywords: *Cloud Computing, Cloud Computing Issues*

Introduction

The networking concept of cloud computing may launch massive applications. It's "hardware and systems software in the data centers that provide those services, as well as applications delivered as services over the Internet." [1]. Its simplicity and cloud of services approach have made cloud computing popular across companies and industries. Users may utilize the cloud of services to secure cloud computing systems and increase everyday users. Cloud computing is prevalent in industry and academics. Business processes are dispersed and designed with loose coupling, and the cloud of services will link different services using diverse techniques and patterns. Companies may use cloud computing and shared data storage. It beats creating website content. Cloud computing offers organizations secure, cost-effective cloud infrastructure and flexible data storage [2]. Cloud computing may provide internet-based dynamically scaled virtualized cloud resources. Cloud computing has transformed cloud service delivery and consumption. The license is Creative Commons Attribution 3.0. This paper must include the title, journal reference, DOI, and author(s) credit when republished. 1 development speeds up application development and saves IT resources [3].

Cloud computing presents security management concerns notwithstanding its benefits [4–5]. The challenges include customer skepticism of data security and privacy, business laziness, governance loss, and supplier compliance uncertainty. Security has become increasingly difficult when data security [6], users' privacy [7], network security, platform, and infrastructure problems join the cloud paradigm. Recent research across disciplines emphasizes the necessity for cloud computing security management in all application domains to avoid such risks. The latest cloud security management reduces concerns. It releases servers, storage, networks, cloud apps, and cloud services and enables flexible data access on cloud storage, virtualization, and virtual data centers. Their cloud security conceptual model addresses data protection, legal and standard requirements, policy, and government organization compliance and regulations. We studied many security challenges since they vary. The classification of cloud computing sub-problems will assist future academics identify solutions. This study surveyed 23 Iraqi government agency IT department managers to classify security problems. They identified mobility and cloud government apps, cloud security services and applications, cloud security data, cloud network security, and cloud security platform and infrastructure.

Literature Review

Cloud Computing Issues

Cloud computing technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, concurrency control, and memory management have several security vulnerabilities [8]. Cloud computing is utility computing. Most people and businesses shift their work to the cloud, where workloads become increasingly diverse when cloud providers grow or refresh clusters with new computers. Government agencies operate apps and data transmission in their private cloud before moving it to the public cloud. Cloud computing technology has various security vulnerabilities that jeopardize data integrity and confidence. This emphasizes the need for cloud computing security standards and rules to safeguard users. Despite efforts to design effective cloud computing, virtualization, multi-tenancy, data encryption technology, trusted cloud, and cloud data sensitive confidentiality issues continue to cause business and management problems for cloud service security [9]. Government and non-government organizations struggle to identify cloud security risks and establish and prepare plans to assist them embrace cloud computing technology initiatives for enterprises. As shown in Figure, cloud computing environments face several key cloud security challenges, including mobility and application security [10], cloud security services and applications [11], cloud network security [12], and cloud security platform and infrastructure [13].

Mobility and Cloud Government Application security issues

Mobile computing is expanding, but its security, disconnections, and mobility make it challenging to use [14].Customers routinely exchange cloud data. Encrypting data in transit and cloud storage protects privacy. Third-party CSPs and their clients are legally distinct. Customer organizations may be accountable for CSP failure. A cloud client firm that fails to comply is less likely to incur CSP legal penalties [15]. Organisations must handle cloud provider flexibility, sensitive data protection, legal and standards challenges, software development life cycle management, portability and interoperability, and cloud platform dependability and latency. Legal definition and organizational charter assist determine the vision, missions, tasks, and capabilities of major cloud computing actors. The policy is a basic challenge. Open Security Architecture (OSA) frameworks may be used in security architecture software. Schematics show data traffic flow management for safe cloud computing and cloud security requirements at each level. Cloud mobile applications may request external cloud services via interfaces [18]. Mobile Web services must have frequent network failure, poor processing, and little bandwidth [37]. Mobility and cloud government application security issues are covered here.

Table 1 Issues for Mobility and Cloud Government Application Security Based on Studies

Mobility and Cloud Government Application security issues	Related works
Lack of Standards, Legally, and Policy	[16]–[19].
Loss of Security Governance	[20]–[22].
Malicious Insider Threats in the Cloud Computing	[23], [24][25]
Cloud Computing Regulatory Requirements and Cloud Compliance Challenges	[22], [26]–[29].
Cloud Computing Portability and Interoperability	[30][31]
Biometric Security System for Cloud Computing Environment	[32][33][34][35]

Cloud Security Services and Application Issues

Security concerns at the service and application levels affect cloud computing system performance, quality, and SLAs [41]. How can mobile cloud computing systems ensure data availability? What fault-tolerance (FT) methods provide smooth operation and service? [42]. Thus, cloud services may scale to meet user requirements. Cloud capabilities may be instantly and elastically extended to meet unexpected demand and decreased to free up idle resources. However, the cloud service provider must regularly monitor the cloud to ensure it is secure from hackers and other attackers who want to steal personal information or damage user privacy. According to the study below, Table 0 lists cloud security service and application issues.

Table 2. Issues for Cloud Security Services and Application Based on Studies

Cloud Security Services and Application Issues	Related works
Cloud Service Level Agreement (SLAs) and Quality of Service	[36]–[45]. [22], [43], [46]–[54].
Trusted for Cloud Services	[2], [16], [24], [43], [48], [52], [54].
Access Control in Cloud Computing Environment	[23], [25], [27], [28], [55].
Security of Cloud Interfaces and API	[38], [48], [58]–[62].
Availability of Cloud Data	

Cloud Security Data

Cloud computing data is owned by numerous parties who must be trusted.

Thus, unauthorized users should not access such data [52], [54], [59]. Original data must be password-protected by data management systems with security guard services in trusted and cloud computing environments. Cloud data management password-protects all cloud data entry, storage, and backup [63]. In addition, cloud data storage stores integrity data in logical pools. Cloud customers may save their data on a distant server to avoid costly local storage and brand costs and access it anytime, anyplace [64].

Table 3: Issues for Cloud Security Data Based on Studies

Cloud Security Data Security	Related works
Cloud Data Privacy Security	[16], [17], [22], [25], [27], [31], [58], [65].
Data Protection in Cloud Computing	[2], [54], [55], [47].
Environments	
Cloud Data Confidentiality Issues	[48], [49], [52], [54].
Cloud Data Limitations and Segregation	[31], [62], [60]–[61].
Cloud Data Integrity	[16], [24], [27], [52], [54], [59].
Cloud Data Eavesdropping Attack and Leakage	[23], [33], [39], [55], [57].

Cloud Network Security Issues

Network security concerns include cloud network security. Cloud computing enables constant, effortless, and instantaneous network access to a repository of configurable networks that can be rapidly provisioned and provided at no cost, with minimal service provider communication or management effort [67]. As a result of the relatively recent computing paradigm that Cloud Computing represents, there is considerable ambiguity regarding the means by which network security can be achieved and the progression of application security to Cloud Computing [62]. One of the challenges associated with cloud networks is the increased response time of nodes during data communication via cooperative caching [8].

Table 4: Issues for Cloud Network Security Based on Studies

Cloud Network Security issues	Related works
Detection and Recovery	[2], [15], [31], [52], [55], [59].
Flow Control for Secure Cloud Computing	[2], [27], [43], [58].
Cloud Account or Cloud Service Hijacking	[19], [40], [63], [64] .
Cloud Network Traffic Analysis and control	[21], [25], [45], [65].
Bandwidth Cost in the Cloud	[26], [50], [51], [58]].
Distributed Denial of Service (DDoS) Attacks for the Cloud	[2], [15], [47], [66].

Cloud Security Platform and Infrastructure Issues

The cloud infrastructure is safeguarded by encryption and a reliable cloud. There is also no standard service contract that covers all cloud services and organization needs. A real-time warning system may be developed and deployed on cloud infrastructure using cloud computing [44]. Instead, cloud computing gives Cloud Management Agents an elastic architecture to acquire streaming resources as needed.

Multi-cloud providers support several platforms and provide expanding capability packages. Infrastructure security underpins cloud computing security, offering protection via the cloud's top security layer. Infrastructure security includes software and hardware security, intrusion defense, redundant data backups, intrusion detection, and network security prevention. This study focuses on cloud infrastructure security, which worries end-users. Thus, a centralized cloud insecurity security solution and its scenarios and methodology are proposed.

Table 5: Issues for Cloud Security Platform and Infrastructure Based on Studies

Cloud Security Platform and Infrastructure Issues	References
Cloud Platform Reliability and Latency The multi-tenancy in the Cloud Scalability and Capability in the Cloud	31], [65], [71]– [68]. [15], [24], [27],

Cloud Security Issue Factors

Cloud computing networks, databases, operating systems, virtualization, resource scheduling, transaction management, concurrency control, and memory management may provide security risks [8]. Cloud computing is utility. Business customers rent cloud computing. Resources should be managed well to suit client QoS and cloud datacenter resource utilization. Workloads diversify as more individuals and organizations migrate to the cloud. Cloud companies routinely add machines to clusters, diversifying cloud computing capabilities [69]. However, government organizations run programs and data transfer in their own clouds before moving them to the public cloud. Cloud computing presents several security issues, but standards and guidelines should be developed as soon as possible [43].

Every organization wants cloud computing for profitability, interoperability, capacity, and scalability. Network connectivity defined cloud computing and highlighted public, private, hybrid, and community cloud service models. Virtualization, multi-tenancy, data encryption, trustworthy cloud, and cloud data sensitive secrecy provide new business and management threats to cloud service security [9]. Cloud computing transforms IT service delivery. Lower costs, scalability, flexibility, cloud storage data access, capacity utilization, efficiency, performance, and mobility enhance business and IT [40]. The organization may assess cloud security issues and develop a plan to use cloud computing [60]. Cloud computing issues may hurt businesses, therefore risk management is necessary to balance operational and financial expenses and protect data, networks, platform information systems, and technologies [70]. Users and companies worry about mobile cloud computing's potential, security, privacy, practicality, and accessibility [53, 57]. Thus, cloud computing success depends on security issues. Identifying, categorizing, and mitigating cloud computing security risks may improve system success. Businesses and users concern about cloud security, data privacy, feasibility, and accessibility [56]. The cloud has security vulnerabilities such [28]: Major data storage, detection, recovery, and backup sites. Incorrect key storage may encrypt data. Only authorized users with keys should have flexible access to critical data storage. Policies should control keys [45].

Conclusion

All companies are using cloud computing to improve data storage, transformation, interchange, and profitability. It enhances interoperability, capability, and scalability. Cloud computing was defined by this network connectivity, including public, private, hybrid, and community models. The IT service delivery paradigm is changing with cloud computing. Business and IT departments benefit from cost savings, scalability, cloud storage flexibility, optimum capacity usage, improved performance, mobility, and efficiency. Despite its advantages, cloud computing has security management issues such consumers' lack of faith in data privacy and security, organizational inertia, governance erosion, and provider compliance. The cloud model has introduced platform and infrastructure challenges, user privacy and network security, and model data security, complicating security. This study highlighted cloud computing security issues. Cloud computing deployment raises five main difficulties, according to the report. These issues include cloud service and application security, data protection, network security, and security platforms and architecture. These challenges provide a chance to study security issues by establishing an empirical model or technological method.

References

1. *M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "A View of Cloud Computing," Commun. ACM, vol. 53, no. 4, pp. 50– 58, 2010.*

2. *K. Jakimoski, "Security Techniques for Protecting Data in Cloud Computing," Int. J. Grid Distrib. Comput., vol. 9, no. 1, pp. 49–56, 2016.*

3. *Z. Hong-lie, L. Xin, L. I. U. Yan-ju, and L. Cheng, "Research on Cloud Resource Section Method for the Multi-layer Ontology," Int. J. Grid Distrib. Comput., vol. 9, no. 1, pp. 193– 200, 2016.*

4. *A. N. Khan, M. L. Mat Kiah, S. U. Khan, and S. A. Madani, "Towards secure mobile cloud computing: A survey," Futur. Gener. Comput. Syst., vol. 29, no. 5, pp. 1278–1299, 2013.*

5. *A. M.-H. Kuo, "Opportunities and Challenges of Cloud Computing to Improve Health Care Services," J. Med. Internet Res., vol. 13, no. 3, p. e67, 2011.*

6. *L. M. Kaufman, "Data security in the world of cloud computing," IEEE Secur. Priv., vol. 7, no. 4, pp. 61–64, 2009.*

7. *M. B. Mollah, M. A. K. Azad, and A. Vasilakos, "Security and privacy challenges in mobile cloud computing: Survey and way ahead," Journal of Network and Computer Applications, vol. 84. pp. 38–54, 2017.*

8. *D. Sarddar, P. Sen, and M. K. Sanyal, "Central Controller Framework for Mobile Cloud Computing," Int. J. Grid Distrib. Comput., vol. 9, no. 4, pp. 233–240, 2016.*

9. *Z. Gao, Y. Li, H. Tang, and Z. Zhu, "Management Process Based Cloud Service," in International Conference on Cyberspace Technology (CCT 2013), 2013, pp. 278–281.*

10. *A. Botta, W. de Donato, V. Persico, and A. Pescapé., "Integration of cloud computing and internet of things: a survey.," Futur. Gener. Comput. Syst., vol. 56, p. 684–700, 2016.*

11. *D. A. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M. Freire, and P. R. M. Inácio, "Security issues in cloud environments: a survey," Int. J. Inf. Secur., vol. 13, no. 2, pp. 113–170, 2014.*

12. *V. Inukollu, S. Arsi, and S. Ravuri, "Security Issues Associated With Big Data in Cloud Computing," Int. J. Netw. Secur. Its Appl., vol. 6, no. 3, pp. 45–56, 2014.*

13. *H. Rasheed, "Data and infrastructure security auditing in cloud computing environments," Int. J. Inf. Manage., vol. 34, no. 3, pp. 364–368, 2014.*

14. *N. Fernando, S. W. Loke, and W. Rahayu, "Mobile cloud computing: A survey," Futur. Gener. Comput. Syst., vol. 29, no. 1, pp. 84–106, 2013.*

15. *A. LLP, W. Chan, E. Leung, and H. Pili, "Enterprise Risk Management for Cloud Computing," 2012.*

16. A. Tuli, N. Hasteer, M. Sharma, and A. Bansal, "Exploring Challenges in Mobile Cloud Computing: An Overview," Confluence 2013: The Next Generation Information Technology Summit (4th International Conference). p. 6, 2013.

17. NSTAC, "NSTAC Report to the President on Cloud Computing," 2012.

18. F. Al-anzi, S. Yadav, and J. Soni, "Cloud Computing: Security Model Comprising Governance, Risk Management and Compliance," in 2014 International Conference on Data Mining and Intelligent Computing (ICDMIC), 2014, pp. 1–6.

19. R. Matt, "Cybersecurity and Cloud Computing in the Health Care and Energy Sectors: Perception and Reality of Risk Management," 2013.

20. E. Takamura, C. Gomez-rosa, K. Mangum, and F. Wasiak, "MAVEN Information Security Governance , Risk Management , and Compliance (GRC): Lessons Learned," in 2014 IEEE Aerospace Conference, 2014, pp. 1–12.

21. J. Adjei, "Explaining The Role of Trust in Cloud Service Acquisition," in 2014 2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, 2014, pp. 283–288.

22. S.-T. Lai and F.-Y. Leu, "A Security Threats Measurement Model for Reducing Cloud Computing Security Risk," in 2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2015, pp. 414–419.

23. P. Anand, J. Ryoo, H. Kim, and E. Kim, "Threat Assessment in the Cloud Environment – A Quantitative Approach for Security Pattern Selection," in IMCOM '16, 2016, p. 8.

24. E. Cayirci, "Modeling and Simulation as A Cloud Service: A Survey," in Proceedings of the 2013 Winter Simulation Conference, 2013, pp. 389–400.

25. A. Michalas, N. Paladi, and C. Gehrmann, "Security Aspects of e-Health Systems Migration to the Cloud," in 2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom) Security, 2014, pp. 212–218.

26. P. Hazarika, V. Baliga, and S. Tolety, "The Mobile-Cloud Computing (MCC) Roadblocks," in 2014 Eleventh International Conference on Wireless and Optical Communications Networks (WOCN), 2014, pp. 1–5.

27. M. Bamiah, S. Brohi, and S. Chuprat, "Cloud Implementation Security Challenges," in Proceedings of 20l21ntemational of Cloud Computing, Technologies, Applications & Management, 2012, pp. 174–178.

28. F. Al-Musawi, A. H. Al-Badi, and S. Ali, "A Road Map to Risk Management Framework for Successful Implementation of Cloud Computing in Oman," in 2015 International Conference on Intelligent Networking and Collaborative Systems, 2015, pp. 417–422.

29. J. K. Ganlea, K. Afriyie, and A. Y. Segbefia, "Microcredit: Empowerment and Disempowerment of Rural Women in Ghana," World Dev., p. Pages 335–345, 2015.

30. E. Aruna, A. Shri, and A. Lakkshmanan, "Security Concerns and Risk at Different Levels in Cloud Computing," in 2013 International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), 2013, pp. 743–746.

31. Shanthini and S. Swamynathan, "Genetic-based biometric security system for wireless sensor-based health care systems," in Proceedings of the 2012 International Conference on Recent Advances in Computing and Software Systems, RACSS 2012, 2012, pp. 180–184.

32. G. Ahammed, R. Banu, and N. Fathima, "An Approach to Secure Communication in IoT (Internet of Things)," in CONFERENCE ON INTERNET OF THINGS, 2016, no. February, p. 315.

33. Klein, "Cloudy Confidentiality : Clinical and Legal Implications of Cloud Computing in Health Care," Anal. Comment., vol. 39, no. 4, pp. 571–578, 2011.

34. A. Wadhawan and A. Bhatia, "Neural Network Based Intelligent Retrieval System for Verifying Dynamic Signatures," Int. J. Adv. Sci. Technol., vol. 83, no. 2015, pp. 27–40, 2015.

35. M. Alhomidi and M. Reed, "Security Risk Analysis as a Service," in 2013 8th International Conference for Internet Technology and Secured Transactions, ICITST 2013, 2013, pp. 156– 161.

36. A. Khan, M. Fayaz, A. S. Shah, and F. Wahid, "Critical Analysis of Cloud Computing Software Development Process Models," Int. J. Softw. Eng. Its Appl., vol. 10, no. 11, pp. 451– 466, 2016.

37. Arianyan, M. Ahmadi, and D. Maleki, "A Novel Taxonomy and Comparison Method for

Ranking Cloud Computing Software Products," Int. J. Grid Distrib. Comput., vol. 9, no. 3, pp. 173–190, 2016.

38. M. Carroll, A. Merwe, and P. Kotzé, "Secure Cloud Computing: Benefits, Risks and Controls," in Information Security for South Africa -2011, 2011, pp. 1–9.

39. J. S. Sengar and R. Sharma, "Review : Ad-Hoc Cloud Architecture & Modern Cryptography," Int. J. Grid Distrib. Comput., vol. 9, no. 6, pp. 45–50, 2016.

40. H. Rajaei and J. Wappelhorst, "Clouds & Grids: A Network and Simulation Perspective," in Conference: 2011 Spring Simulation Multi-conference, SpringSim '11, Boston, MA, USA, 2011, pp. 143–150.

41. C. O. Rolim, F. L. Koch, C. B. Westphall, J. Werner, A. Fracalossi, and G. S. Salvador, "A Cloud Computing Solution for Patient ' s Data Collection in Health Care Institutions," no. ii, pp. 95–99, 2010.

42. J. S. Sengar, "SURVEY : Reputation and Trust Management in VANETs," Int. J. Grid Distrib. Comput., vol. 8, no. 4, pp. 301–306, 2015.

43. S. Bouchenak, G. Gheorghe, G. Chockler, H. Chockler, and A. Shraer, "Verifying Cloud Services: Present and Future," ACM SIGOPS Oper. Syst. Rev., vol. 27, no. 2, pp. 6–19, 2013.

44. N. Sasikaladevi, "Trust Based Cloud Service Composition Framework," Int. J. Grid Distrib. Comput., vol. 9, no. 1, pp. 99–104, 2016.

45. V. Saranya, S. Ramya, R. Kumar, and T. Nalini, "Efficient and Parallel Data Processing and Resource Allocation in the Cloud by u sing Nephele ' s Data Processing Framework," Int. J. Grid Distrib. Comput., vol. 9, no. 3, pp. 33–40, 2016.

46. M. Irfan, M. Usman, Y. Zhuang, and S. Fong, "A Critical Review of Security Threats in Cloud Computing," in 2015 3rd International Symposium on Computational and Business Intelligence (ISCBI), 2015, pp. 105–111.

47. P. Senthil, N. Boopal, and R. Vanathi, "Improving the Security of Cloud Computing using Trusted Computing Technology," Int. J. Mod. Eng. Res., vol. 2, no. 1, pp. 320–325, 2012.

48. S. Al-anzi, A. A. Salman, and N. K. Jacob, "New Proposed Robust, Scalable and Secure Network Cloud Computing Storage Architecture," no. May, pp. 347–353, 2014.

49. V. Akshaya and T. Purusothaman, "Business Intelligence as a Service in Analysis of Academic Courses," Int. J. Appl. Eng. Res., vol. 11, no. 4, pp. 2458–2467, 2016.

50. S. Kai, T. Shigemoto, T. Kito, S. Takemoto, and T. Kaji, "Development of Qualification of Security Status Suitable for Cloud Computing System," in Proceedings of the 4th international workshop on Security measurements and metrics - MetriSec '12, 2012, p. 17.

51. M. M. A. Ghosh, R. R. Atallah, and S. S. A. Naser, "Secure Mobile Cloud Computing for Sensitive Data: Teacher Services for Palestinian Higher Education Institutions," Int. J. Grid Distrib. Comput., vol. 9, no. 2, pp. 17–22, 2016.

52. K.-F. Ho, H. Hirai, Y.-H. Kuo, H. Meng, and K. Tsoi, "Indoor Air Monitoring Platform and Personal Health Reporting System: Big Data Analytics for Public Health Research," in 2015 IEEE International Congress on Big Data, 2015, no. 2, pp. 309–312.

53. A. Priya, T. Meena, and M. Devi, "Efficient Approach for Data Retrievability on Cloud Storage Systems," IJSRSET, vol. 2, no. 2, pp. 408–412, 2016.

54. Suo, Z. Liu, J. Wan, and K. Zhou, "Security and Privacy in Mobile Cloud Computing," in 2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC), 2013, pp. 655–659.

55. R. Kumar and S. Rajalakshmi, "Mobile Cloud Computing: Standard Approach to Protecting and Securing of Mobile Cloud Ecosystems," in Proceedings - 2013 International Conference on Computer Sciences and Applications, CSA 2013, 2013, pp. 663–669.

56. P. Srivastava, "Multiple Key Based Architecture to Secure Cloud Database," vol. 4, no. September, pp. 1–7, 2015.

57. N. Ahmed and A. Abraham, "Modeling Security Risk Factors in a Cloud Computing Environment," J. Inf. Assur. Secur., vol. 8, no. 2013, pp. 279–289, 2013.

58. S. Mazur, E. Blasch, Y. Chen, and V. Skormin, "Mitigating Cloud Computing security risks using a self-monitoring defensive scheme," Aerosp. Electron. Conf. (NAECON), Proc. 2011 IEEE Natl., pp. 39–45, 2011.

59. P. Rohmeyer and T. Ben-zvi, "Managing Cloud Computing Risks in Financial Services Institutions," in 2015 Proceedings of PICMET '15: Management of the Technology Age, 2015, pp. 519–526.

60. K. Hashizume, D. Rosado, E. Fernández-

Medina, and E. Fernandez, "An analysis of security issues for cloud computing," J. Internet Serv. Appl., vol. 4, no. 5, pp. 1–13, 2013.

61. D. G. Rosado, R. Gómez, D. Mellado, and E. Fernández-Medina, "Security Analysis in the Migration to Kashyap Rajesh and Sarika Sharma, "Security Challenges and Issues in Cloud Computing – The Way Ahead," Int. J. Innov. Res. Adv. Eng., vol. 2, no. 9, pp. 32–35, 2015.

62. B. S. Al-Attab and H. S. Fadewar, "Security Issues and Challenges in Cloud Computing," Int. J. Emerg. Sci. Eng., vol. 2, no. 7, pp. 22–26, 2014.

63. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A Survey of Mobile Cloud Computing : Architecture , Applications , and Approaches," Wirel. Commun. Mob. Comput. -, no. Cc, pp. 1–38, 2013.

64. M. Vermaat, S. Sebok, S. Freund, J. Campbell, and M. Frydenberg, Discovering Computers 2016: Tools, Apps, Devices, and the Impact of Technology. 2016.

65. M. I. M. Hanifah, R. C. Omar, N. H. N. Khalid, A. Ismail, I. S. Mustapha, I. N. Z. Baharuddin,

66. R. Roslan, and W. M. Z. Zalam, "Integrated Geo Hazard Management System in Cloud Computing Technology," IOP Conf. Ser. Mater. Sci. Eng., vol. 160, p. 12081, 2016.

67. A. Soofi and M. I. Khan, "Encryption Techniques for Cloud Data Confidentiality," Int. J. Grid Distrib. Comput., vol. 7, no. 4, pp. 11–20, 2014.

68. D. Tse, "Challenges on Privacy and Reliability in Cloud Computing Security," in International Conference on Information Science, Electronics and Electrical Engineering (ISEEE), 2014, 2014, pp. 1181–1187.

69. L. Xu and J. Li, "Building Efficient Resource Management Systems in the Cloud : Opportunities and Challenges," Int. J. Grid Distrib. Comput., vol. 9, no. 3, pp. 157–172, 2016.

70. B. Al-shargabi and O. Sabri, "A study of Adopting Cloud Computing from Enterprise Perspective using Delone and Mclean IS Success Model," Int. J. Comput. Sci. Inf. Secur., vol. 14 S1, no. February, p. 5500, 2016.

71. A. Khrisna and Harlili, "Risk Management Framework with COBIT 5 and Risk Management Framework for Cloud Computing Integration," in 2014 International Conference of Advanced Informatics: Concept, Theory and Application (ICAICTA) Risk, 2014, pp. 103–108.