A critical Analysis on Cloud Computing Issues

Ravi Shanker Singh[1]

Dr.Sayed Hauider Abbas [2]

Phd Researchscholar, Department Of Computer Science ,Sunrise University, Alwar(Raj.)India[1]

Assistant Professor, Department Of Computer Science ,Sunrise University, Alwar(Raj.)India[2]

Abstract

Cloud computing is the most promising current implementation of utility computing in the business world, because it provides some key features over classic utility computing, such as elasticity to allow clients dynamically scale-up and scale-down the resources in execution time. Nevertheless, cloud computing is still in its premature stage and experiences lack of standardization. The security issues are the main challenges to cloud computing adoption. Thus, critical industries such as government organizations (ministries) are reluctant to trust cloud computing due to the fear of losing their sensitive data, as it resides on the cloud with no knowledge of data location and lack of transparency of Cloud Service Providers (CSPs) mechanisms used to secure their data and applications which have created a barrier against adopting this agile computing paradigm. This study aims to review and classify the issues that surround the implementation of cloud computing which a hot area that needs to be addressed by future research.

Keywords: *Cloud, Computing, Security, Issues*

1. Introduction

Cloud computing becomes a promising networking for infrastructure pattern which can deploy large-scale application in a cost-effective method. It is defined as "applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services [1]. Recently, cloud computing has been widely adopted by the industry and organizations due to its usability and simple cloud of services-oriented models. The number of cloud users can access the cloud of services to keep on the increasing daily and safe systems in the cloud computing environments. Cloud computing technology plays an important role in academic and industry organizations. The business processes are composed and implemented in the distributed loosely coupled environments and the composite of services which includes more services and thus the cloud of services will be connected by varies patterns and approaches. Cloud computing is providing organizations to use shared data storage and cloud resources. It is better than to develop with the own platforms. Further, cloud computing provides companies to have a data flexible, secure system, and cost-effective cloud infrastructure [2]. Additionally, the cloud computing can provide on demand dynamically scalable virtualized cloud resources via the web of internet. indeed, the cloud computing has not only changed the way of providing cloud services but influenced the way of application development, which helps companies to save IT resources during the lifecycle and shorten application development time [3].

Despite, the advantages of the cloud computing, it still surrounded by several issues that are associated with security management [4] includes lack of trust in data security and privacy by users, organizational inertia, loss of governance, and uncertain provider's compliance [5]. The security issue became extra complex under the cloud model as new scopes have arrived into the problem scope associated to the model data security [6], users' privacy [7], network security, platform and infrastructure issues. Recently, studies from various disciplines emphasized to the importance of cloud computing security management in all areas of application to mitigate those issues. The new version of cloud security management consists of the processes and methods that are useful to reduce cloud security issues. It also includes characteristics like on-demand service provision, virtualization and virtual data centers, and

high flexibility access to data on cloud storage and release of service provision like storage, network, cloud applications, servers and its cloud services. Indeed, they present the conceptual model for cloud security that involved components such as data privacy, legally and standard, policy, compliance and regulatory issues of government organizations. Due to the fact that there are many types of security issues, this study reviewed many types of security issues. This study also classified the sub-issues of cloud computing under structured groups which helps future research to explore the related solution. To classify the security issues in the government, this study interviewed the managers of information technology department in 23 of Iraqi government departments and they classified the security issues under five main groups which are: - mobility and cloud government application security issues, cloud security services and application issues, cloud security data, cloud network security issues and issues for cloud security platform and infrastructure.

2. Literature Review

2.1. Cloud Computing Issues

There are many cloud security issues appear in different type of technologies which include networks, databases, operating systems, virtualization, resource scheduling, transaction management, concurrency control and memory management are used in cloud computing [8]. The cloud computing is designed as computing utility. The majority of individuals and enterprises use to migrate their work into the cloud, workloads which became more heterogeneous because the cloud computing resources are much more heterogeneous as cloud providers constantly scale or update the clusters with new generations of machines. For example, the government organizations run applications and data transfer in their own the private cloud and then transform it to the public cloud. Nevertheless, there are many security issues exist in the cloud computing technology that threaten the data credibility and confidently. This emphasis to the important to design a cloud computing security with relevant standards and policies to protect the users. Despite, there are major efforts made to design effective cloud computing, the cloud service security is still facing new business and management problems arising from virtualization, multi-tenancy in the cloud, and data encryption technology, trusted cloud and cloud data sensitive confidentiality issues [9]. The government and non-government organizations are struggling to identify the features of cloud security issues and then build and prepare plan that can help them to make appropriate decision toward a successfully adoption of cloud computing technology projects for organizations. There are several key cloud security challenges within the cloud computing environment as shown in Figure, which include mobility and application security issues [10], cloud security services and applications issues, cloud security data issues [11], cloud network security issues [12] and cloud security platform and infrastructure issues [13].

2.1.1. Mobility and Cloud Government Application security issues

Despite the growth usage of mobile computing, exploiting its full potential advantages is difficult due to its inherent problems such as secure resource, frequent disconnections, and mobility [14]. Data in the cloud is typically in a shared environment alongside with data from other customers. Encryption is critical to protect data sensitive confidentiality and privacy of the data while in transiting and in cloud storage. Legally, third-party cloud service providers (CSPs) and their customer organizations are distinct enterprises. It the CSP fails in its responsibilities, it could have legal liability implications for the CSP's customer organizations. In contrast, if a cloud customer organization fails in its responsibilities, it is less likely to be exposure to legal implications of the CSP [15]. There are some responsibilities for the organizations such as flexibility access issue of cloud providers, protect sensitive data in the cloud computing, understand legally and standards issues, software development life cycle management, portability and interoperability, and cloud platform reliability and latency. The policy is a foundational issue that is related to legal definition and organizational charter to facilitate and guide the establishment of the vision, missions, responsibilities, and authorities of major actors in cloud computing organization. Open Security Architecture (OSA) provides frameworks that are easily integrated into software applications for the security architecture community. Its patterns are based on schematics that show the data traffic flow control for secure cloud computing and particular implementation with policies implemented at each step for the cloud security issues. The cloud mobile applications can connect and request services hosted on a remote cloud computing by interfaces [18]. However, mobile Web services need to consider additional constraints other than standard Web services: frequent loss of connectivity, low

computational resources, and low bandwidth [37]. In this section, the mobility and cloud government application security issues are discussed.

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]. [30][31]
Cloud Computing Portability and Interoperability	
Biometric Security System for Cloud Computing Environment	[32][33][34][35]

2.1.2. Cloud Security Services and Application Issues

Service and application-level issues relate to the security factors concerned with performance measurements of the cloud computing system, and the quality of service and cloud service level agreement [41]. For example, in what ways do mobile cloud computing systems ensure data of availability; what are the fault- tolerance (FT) mechanisms employed to ensure smooth execution and uninterrupted service [42]. Therefore, cloud of services able to extend dynamically to meet user on demand and requirements. Additionally, capabilities of the cloud can be rapidly and elastically increased to meet immediate demand and scaled down to release unused resources. However, monitoring should be done by the cloud service provider frequently to ensure that the cloud is secure and not infected by the malicious code that have been uploaded to the cloud by the hackers or attackers with the purpose of stealing sensitive data or even damaging the information of users. Further, Table 0, illustrates the issues for cloud security services and application based on studies bellow.

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	

2.1.3. Cloud Security Data

Generally, the data in cloud computing belongs to different owners in the cloud computing resources which must be trusted. Therefore, unauthorized users should be forbidden from that data or information [52], [54], [59]. In trusted and cloud data sensitive confidentiality refers to original data that must keep in a password protected by data management systems with security guard services in the cloud computing environments. All cloud data are entered, stored and backed-up in a password protected by the management of data in the cloud computing [63]. Besides, the cloud data storage is a model of data storage in which the integrity data is stored in logical pools. It allows cloud users to store their data in a remote server to get rid of expensive local storage and managing brand cost and then flexibility access data of interest anytime and anywhere [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 Environments	[2], [54], [55], [47].
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].

2.1.4. Cloud Network Security Issues

Cloud network security is one of the network security issues. Cloud Computing permits ever-present, convenient, on-demand network access to a shared pool of configurable networks that can be quickly provisioned and free with negligible management effort or service provider communication [67]. Due to the fact that the Cloud Computing embodies a comparatively new computing model, there is an important deal of vagueness about how security at network can be attained and how applications security is progressed to Cloud Computing [62]. The cloud network issues are the higher response time of nodes while performing data communication through co-operative 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].

2.1.5. Cloud Security Platform and Infrastructure Issues

Security of the cloud infrastructure relies on trusted cloud and cryptography. In addition, no standard service contract exists that covers the ranges of cloud services available and the needs of different organizations. Beside that the cloud computing technology allow to design and implemented a real time alert system on top of the cloud infrastructure [44]. However, cloud computing offers an elastic infrastructure that Cloud Management Agents can use to obtain streaming resources that match the demand. Also, multi cloud providers support different platforms and offer constantly changing packages of capabilities. Further, infrastructure security is the basis of cloud computing security, mainly in the cloud for the upper layer of security services to provide security, infrastructure security by hardware and software security, can be a variety of intrusion defence, redundant backup of data, intrusion detection and prevention in network security. Cloud infrastructure security issues the risk associated end-user's concern and is also the focus this work's research direction. Therefore, the centralized security solution for insecurity cloud is proposed and the scenarios of this system and methods after that constructed.

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

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

3. Cloud Security Issue Factors

Many cloud security issues can obtain from different technologies that including networks, databases, operating systems, virtualization, resource scheduling, transaction management, concurrency control and memory management are used in cloud computing [8]. Additionally, cloud computing is designed as computing as a utility. Customers rent computing resources in the cloud to complete their work. Then to ensure the quality of service (QoS) requirements defined by customers and guarantee the resource utilization in the cloud datacentres, effective resource management systems should be considered. Therefore, more individuals and enterprises migrating their work into the cloud, workloads in the cloud become more heterogeneous. Meanwhile, cloud computing resources are much more heterogeneous as cloud providers constantly scale or update the clusters with new generations of machines [69]. However, in reality government organizations run applications and data transfer in their own the private cloud and then transmute it to the public cloud. While there are many security issues exist in the cloud computing technology, cloud security should design relevant standards and policies as soon as possible [43].

Cloud computing is a new emerging technology, which every organization these days wants to adapt for its business for more profitability, interoperability, capability, and scalability. This network communication defined cloud computing, highlighted all the cloud service models likes public, private, hybrid and community cloud computing. In addition to information security risks under traditional IT architecture, cloud service security is still facing new business and management risk arising from virtualization, multi-tenancy in the cloud, and data encryption technology, trusted cloud and cloud data sensitive confidentiality issues [9]. However, cloud computing is changing the current IT delivery model for services. Benefits for business and IT include reduced costs, scalability, flexibility access to data on cloud storage, capacity utilization, higher efficiencies, performance, and mobility [40]. The enterprise will be able to identify the features of cloud security issues and then build and prepare plan that can help them to make appropriate decision toward a successfully adoption of cloud computing technology projects for organizations [60]. Generally, cloud computing's issues can bring negative effects on any companies or organizations, therefore an effective risk management is needed to balance the operational and financial cost as well as proactive actions to secure data, network, platform information systems and technologies [70]. According to [53], understanding the true potential of mobile cloud computing and identifying issues with mobile cloud security, privacy, feasibility and accessibility remain a major concern for both the customers and the enterprises [57]. Therefore, the presence of cloud security issues and challenges have critical influence on the success of cloud computing systems. Thus, it is critical to identify and classify control various issues during cloud computing environments by using controlling mitigation techniques those security issues, the success rate of cloud computing systems could be increased. Cloud security, cloud data privacy, feasibility and accessibility remain a major concern for both the users and the enterprises [56]. There are several key cloud security challenges within the cloud environment such as [28]: Key stores that must be protected in data storage, detection and recovery and in backup. Improper key storage may lead to encryption data. Flexibility accesses to key data storage have to be limited to the authorized personnel who require the individual keys. These keys ought to be under policies governing them [45].

4. Conclusion

Cloud computing is a new emerging technology, which every organization these days adapt it to facilitate the flexibility of their businesses in terms data storage, exchange, transform which enable them to upgrade their

profitability, interoperability, capability, and scalability. This network communication defined cloud computing, highlighted all the cloud service models likes' public, private, hybrid and community cloud computing. The cloud computing is changing the current IT delivery model for services. Benefits for business and IT include reduced costs, scalability, and flexibility access to data on cloud storage, capacity utilization, higher efficiencies, performance, and mobility. Despite, the advantages of the cloud computing, it still surrounded by several issues that are associated with security management, includes lack of trust in data security and privacy by users, organizational inertia, loss of governance, and uncertain provider's compliance. The security issue became extra complex under the cloud model as new scopes have arrived into the problem scope associated to the model data security, users' privacy network security, and platform and infrastructure issues. This study was designed to highlight the cloud computing security issues. The finding of this study emphasises that there are five main issues associated with cloud computing implementation which are Mobility and Cloud Government Application security issues, Cloud Security Services and Application, Cloud Security data, cloud network security issues and cloud security platform and infrastructure issues. These issues form an open room for future research to fill up security issues gap through providing either technical approach or empirical model to mitigate these issues.

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] C. 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] B. 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] C. 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] E. 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] F. 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] H. 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

[62] 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.

[63] 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.

[64] H. 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.

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

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