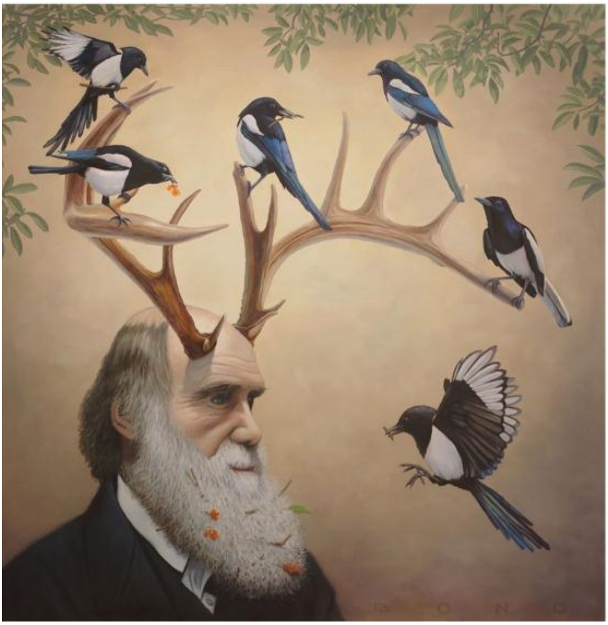
opción

Revista de Antropología, Ciencias de la Comunicación y de la Información, Filosofía,
Lingüística y Semiótica, Problemas del Desarrollo, la Ciencia y la Tecnología

Año 35, 2019, Especial N° 22

Revista de Ciencias Humanas y Sociales
ISSN 1012-1587/ ISSNe: 2477-9385
Depósito Legal pp 198402ZU45



Universidad del Zulia
Facultad Experimental de Ciencias
Departamento de Ciencias Humanas
Maracaibo - Venezuela

Opcion, Año 35, Nº Especial 22 (2019):*2899-2921*
ISSN 1012-1587/ISSNe: 2477-9385

A Review in Managing Cloud computing Security Issues and Future Research

Wisam Raad

Dijlah University College,Iraq; Department of computer science; Wisam.alazawi@duc.edu.iq

Abstract

Cloud computing is one of the most creative technical developments in the technology breakthrough era. It facilitates all aspects of life from business to social and family life. The rapidly growth of international businesses and the bomb of technological revolution in terms of adopting smart cities and governments, e-commerce and e-learning and etc., gave cloud computing a momentum because to can overcome the barriers of knowledge storage and transform in huge quantity. This made cloud computing topic one of the hottest in the literature. However, the popularity of cloud computing is not immune of risks, especially in security, which leaves a negative effect on the use of cloud computing. But also there is no way to avoid using cloud computing because it is the key driver for smoothening knowledge sharing and storage. Thus, academics and information technology developers are struggling hard to find solution for cloud security issues. In this paper, overview bout cloud computing issues will be discussed and commendations that need to be taken by future research to address those issues will be raised.

Keyword: Cloud, Computing, Security, Issues, Future, Research

Una revisión en la gestión de problemas de seguridad informática en la nube y la investigación futura

Resumen
La computación en la nube es uno de los desarrollos técnicos más creativos en la era del avance tecnológico. Facilita todos los aspectos de la vida, desde los negocios hasta la vida social y familiar. El rápido crecimiento de los negocios internacionales y la bomba de la revolución tecnológica en términos de adopción de ciudades inteligentes y gobiernos, comercio electrónico y aprendizaje electrónico, etc., dieron un impulso a la computación en la nube porque puede superar las barreras del almacenamiento de conocimiento y transformarse en grandes cantidad. Esto convirtió al tema de la computación en la nube en uno de los más candentes de la literatura. Sin embargo, la popularidad de la computación en la nube no es inmune a los riesgos, especialmente en seguridad, lo que deja un efecto negativo en el uso de la computación en la nube. Pero tampoco hay forma de evitar el uso de la computación en la nube porque es el controlador clave para facilitar el intercambio y el almacenamiento de conocimientos. Por lo tanto, los académicos y los desarrolladores de tecnología de la información tienen dificultades para encontrar una solución para los problemas de seguridad en la nube. En este documento, se discutirá una descripción general de los problemas de computación en la nube y se plantearán las recomendaciones que deben tomarse en futuras investigaciones para abordar esos problemas.

Palabra clave: Cloud, Computación, Seguridad, Problemas, Futuro, Investigación

Introduction

Cloud computing business models usually apply to digital tools such as networks, technologies and software that are delivered over the Web as cloud services (Enterprise Risk Management, 2009). Before customers continue utilizing the cloud storage, they need to check that the software suits their requirements and consider the problems involved with using this technology. Mobile cloud computing instead inherits traditional cloud computing's security risks in cases where the concept of mobile cloud implies linking mobile devices to a remote cloud (Fernando, Loke, & Rahayu, 2013). The software creator then develops, publishes and tracks the cloud network focused on applications and resources for the web consumers and cloud providers to use (Cayirci, 2013; NSTAC, 2012). Additionally, cloud computing service provides better compatibility, Scalability and on-demand network connectivity for other computing services such as servers, elements of the cloud network, operating systems, desktop programs, cloud virtualization resources (sharing and pooling resource), and cloud services (Jassas, Qasem, & Mahmoud, 2015). In common, Cloud computing is an important application of cloud processing, parallel computing and grid computing. The cloud computing is the result of applications of conceptual combination of Utilities cloud Computing, cloud Virtualization data, IaaS, SaaS, PaaS (Fu, 2016). Cloud computing refers to software applications, and infrastructure that the network provide that is used to these services in a cloud data center (Fu, 2016). Furthermore, Similar infrastructure vendors provide various complexity types of cloud resources. Thus, the cloud platforms are categorized into several categories, such as Software as a Service, Web as a Service or Application Infrastructure (Sakharkar, Dande, & Mate, 2017). All four modes of cloud computing will include one or more of four tiers of “on demand” computing. However, the accelerated advancement of applications by utilizing cloud infrastructure technologies contributes to the introduction of cloud resources through network pool and more.

Cloud service providers (CSPs) split the offerings into three categories: Software as a Service (SaaS), App as a Service (PaaS) and Network as a Service (IaaS);(Naji, Wu, & Gao, 2016). The data system will view software as a service without any program having to be enabled and operated on the system consumer’s device. Consumers of SaaS Services, who are usually cloud users of applications or software administrators and cloud developers, can access this type of software using the web of Internet or mobile applications Platform as a Service (PaaS) is a category of software that offers a framework to grow as a software for organizations that need an application creation case. Google App Engine, for example, is a common site as a service (Naji et al., 2016). In comparison, the service distribution models may be listed as SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service)(Weixiang and Lin 2016; Jakimoski 2016; Kaur and Zandu 2016). These delivery models are essential of the cloud and they show definite features like self-service, multitenancy, everywhere network, measured service and fast elasticity.

As shown in Figure 1. and The business models of providers, namely: Network as a Service (IaaS), Application as a Service (PaaS) , and Software as a Service (SaaS), may be given according to the abstraction layer of the scalability and functionality.(Mehmi, Sangal, Verma, & Parmar, 2016). Google App Server, Gmail , Google Documents, Microsoft Windows Azure and Amazon Elastic Compute Cloud (EC2) are the main instances of cloud computing today. (Kaur and Zandu 2016). According to (Li and Cui 2016), cloud computing resources through cloud computing platform is important for service (IaaS infrastructure services, PaaS and SaaS platform services applications and services) in the form of Cloud user demand for calls. A variety of commercial cloud services will play through building services for the development of a large portion of data services and provides a luxury extended elastic cloud resource pools. By using the cloud IaaS, PaaS or SaaS services, making full use of cloud-demand access, usage-based billing and elastic scalability and capability characteristics, can meet the large demand for data services, the build process for computing or storage resources, and greatly improving big data services development and deployment efficiency (Li and Cui 2016). The versatility of cloud-based computing, though, comes with the expense of customer data protection and privacy. Therefore, security issues about cloud users have become a major obstacle to the widespread growth of cloud computing (Dev, Sen, Basak, & Ali, 2012).

In the cloud storage world, service providers are concerned not only with the execution of customer services, but also with the expense of cloud service. (Gan and Zheng 2016). In turn, the customer can bring data and device storage into the cloud infrastructure in cloud computing service mode. However, the transparent function of cloud services that cause users to lose control of the data due to the lack of the integrity of the cloud service provider that can not be measured easily.

Cloud Service Models

Hence, the problem of security has become the primary concern for the users in cloud computing environment like data security and network security (Lu, 2016). The cloud service models involve Cloud Government Process as a Service (CGPaaS), Cloud Software as a Service (CSaaS), Cloud Platform as a Service (CPaaS), and Cloud Infrastructure as a Service (CIaaS) as can be seen in the Figure 2.2.

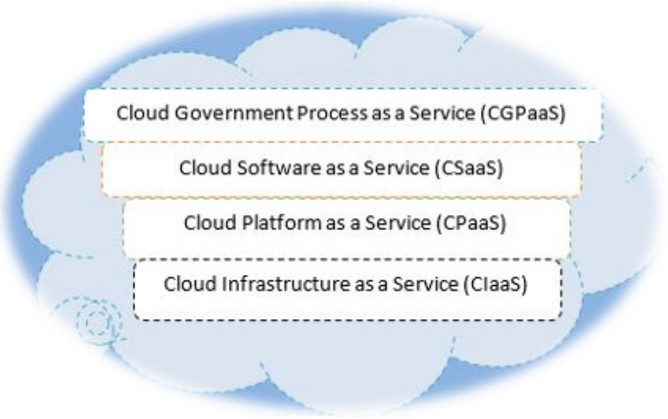

Cloud Government Process as a Service (CGPaaS)
Cloud Software as a Service (CSaaS)
Cloud Platform as a Service (CPaaS)
Cloud Infrastructure as a Service (CIaaS)

Figure 1 Cloud Service Models

Cloud Government Process as a Service (CGPaaS)

There have recently been significant attempts to improve the standard of E-Government services, especially cloud storage technologies. The efficient introduction of cloud infrastructure technologies presents the public sector with many benefits and the essence of which is cost savings. Most government agencies, especially in developed countries, are dedicated to embracing cloud technologies as a result of growing cloud adoption in e-government services (Aziz, Abawajy, & Chowdhury, 2013). Additionally, the providers of the cloud computing service always update their services and system which in case leave no negative effect on the services. Cloud-based e-government services will therefore experience a smooth move to modern technologies at no extra expense (Almunawar, 2015). Consequently, the opportunity to link easily to cloud services and implement identity management as a service is a strong force for most organizations (CA Technologies, 2014). Nevertheless, nowadays, the sudden traffic volume has come to forefront as a new challenge to the users of the e-government services. This problem often occurs when the government organizations and some internet companies are in the construction of data centers. Therefore, it must be in accordance with the peak value of planning capacity (Li, 2016). Governments are therefore involved in leveraging the platform to help combat the existing low penetration of internet connectivity and potential to boost economic development (Barclay and

Osei-Bryson 2010).

Despite, the importance of Cloud Government Process as a Service to government services efficiency, the security issues still encounter all government agencies, especially in developing countries. This problem makes the governments expose to risks associated with information, information systems, and technology (Paquette, Jaeger, & Wilson, 2010). Those issues may include data confidentiality and privacy, (Hashem et al., 2014), continuous service, as a loss of service (Bumpus, 2013), safety mechanisms (Khan, 2016). The majority of past studies with regard to cloud security in services were concern in discovering the cloud issues leaving a large body of the literature. Yet, the literature still lack to adequate studies in the cloud security management, especially in government services. In addition, many studies in the literature paid attention to explore and examine the effective factors towards cloud computing adoption. Study by, (Low, Chen, & Wu, 2011), Investigate the factors driving the acceptance of cloud services by high-tech firms. Centered on a questionnaire from 111 Taiwan-based high-tech companies, hypotheses were extracted and checked through logistical regression analysis, This study found that support for top management, firm size, competitive pressure and trading partner pressure characteristics have a significant effect on cloud computing adoption. However, those studies address this issue generally. In other words, past cloud computing studies focus on the overall factors that relate to service quality rather than security management specifications. Free few research examine the determinants of implementing cloud storage security focused on the company viewpoint of the customers. Research by (Alassafi, Alharthi, Walters, & Wills, 2017), i Examines the important security factors affecting Saudi government departments' adoption of cloud computing security. A theoretical model for three categories, Social Class of Cloud Protection Risks, Factors Group, and Perceived Cloud Safety was evaluated using the SPSS and Mean methods. The overall results shows that those three groups have positive effect on the cloud security adoption.

Indeed, past literature still lack to adequate research in cloud security management based on users' perspective. Even though, there are few studies attempted to explore the critical factors that are associated with cloud management security such as (Alassafi et al., 2017), this study narrowed the focus on three limited groups and used T test only. Therefore, it is recommended for future research to investigate computing security to include many factors that address management issues.

Cloud Software as a Service (CSaaS)

Cloud computing as a service (CSaaS) may include the maximum spectrum of enterprise apps accessible over the Internet (Khrisna and Harlili 2014) and provide some of applications that can be used by the web and is paid based on the usage (Sarddar, Sen, & Sanyal, 2016). Additionally, SaaS offers facilitates the users can access applications and databases. Users don't have to mount and operate the program on their local computers as it's really simple to manage in the SaaS. (Irfan, Usman, Zhuang, & Fong, 2015).

The Software-as-a-service provides hardware infrastructure and applications that can be accessed through a portal web where both the application and the data are available to service providers. The end-users may therefore access the service from anywhere (Enterprise Risk Management, 2009). In addition, the characteristics of software as a service are computerized billing, invoicing, cloud resources management, collaboration, security management, and service for desk management (Al-anzi, Yadav, & Soni, 2014). Software applications may provide features by bundled, open source and custom framework tools, like SaaS-based mobile solutions (Hanover, 2014). Cloud computing's SaaS layer often provides strictly controlled interfaces for users to access cloud storage resources, while the web provides specialized application service interfaces for departments of command and control.

This enables customers to track and regulate the activity of all ties within, establish organized and integrated command and management systems and conduct fast and efficient supervision and rescue (Lele and Lihua 2016). In the Software as a Service (SaaS) model, the user may rely on the service providers to handle the protection correctly. The supplier has to make certain the surety of the software in which multiple users cannot access to each other's data. Therefore, It is imperative that the consumer agrees that the appropriate protection procedures are taken and that the application is made accessible when necessary (Choudhary, 2007). Past studies attempted to categorize the issues in the software as service under different groups. For example, (Rashmi, Sahoo, & Mehfuz, 2013), provides a model that categorized Software as a Service (SaaS) into new and traditional which gathered number of issues. However, few studies linked the critical factors to mitigate the (SaaS) issues.

Hence, and focused on the aforementioned example, cloud service companies will consider a response to the information security problems current contact systems face. Simultaneously, they too should deal with other issues integrally hosted by the cloud computing paradigm. Future work is also called on to further address protection concerns in SaaS and determine their impact

Cloud Platform as a Service (CPaaS)

PaaS offers a forum for software creation and delivery projects by enabling whole mobile product lifecycle. The cloud service is usually responsible for the network control, the controlling of virtualization. Furthermore, cloud service provider will have runtime, middleware, operating system, network monitoring, servers , data storage and virtualization and other advantages for PaaS (Al-anzi et al. 2014). Through the Cloud Platform as a Service, developers will still have mobile apps, without caring about the poor infrastructure, and provide it to cloud customers. the servers and the Internet network (Irfan et al., 2015). Network as a Service models may also include an integrated infrastructure ecosystem for application developers who mainly build web-based mobile apps and infrastructure resources across the interfaces of the cloud providers. As seen in Figure 2, there are three methods of conveying competencies in cloud computing that are Software as a Service (SaaS), Application as a Service (PaaS), and Network as a Service (IaaS).

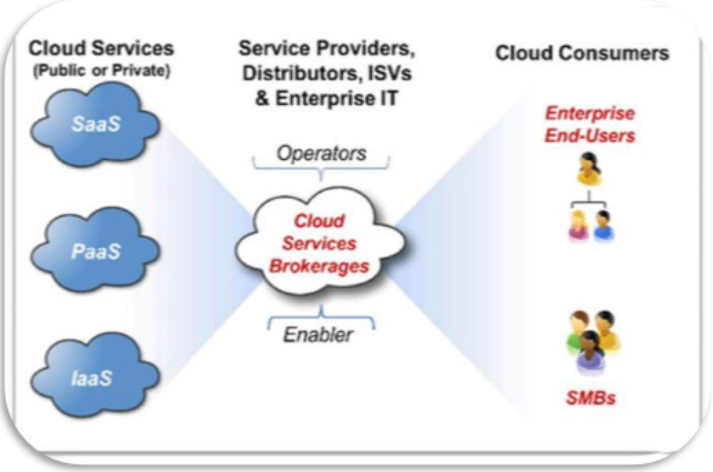


Figure 2. convey cloud computing competences

PaaS provider promotes application creation and can be accessed by using client. PaaS customers can be allocated in multiple dimensions, such as the number of users, the processing, storage and network resources consumed by the PaaS application, and the duration of platform use..”(Devi and Ganesan 2015). Cloud service provider sets requirements for cloud engineering toolkits and policies (Rajaei and Wappelhorst 2011). In fact, PaaS is on the third layer of the cloud infrastructure model and a SaaS divergence where the application of a company is delivered to the production community (Rajaei and Wappelhorst 2011). In cloud storage, specific application network or production setting, the framework layer is provided to customers as a software, i.e. PaaS: PaaS. As the upper layer of the network layer, the application layer is perceived to be the central layer of the whole cloud computing framework, providing resources such as delivery, dissemination, supervisory management, protection management, centralized competition regulation of the management system and the Internet of Things data tool (Lele and Lihua 2016).

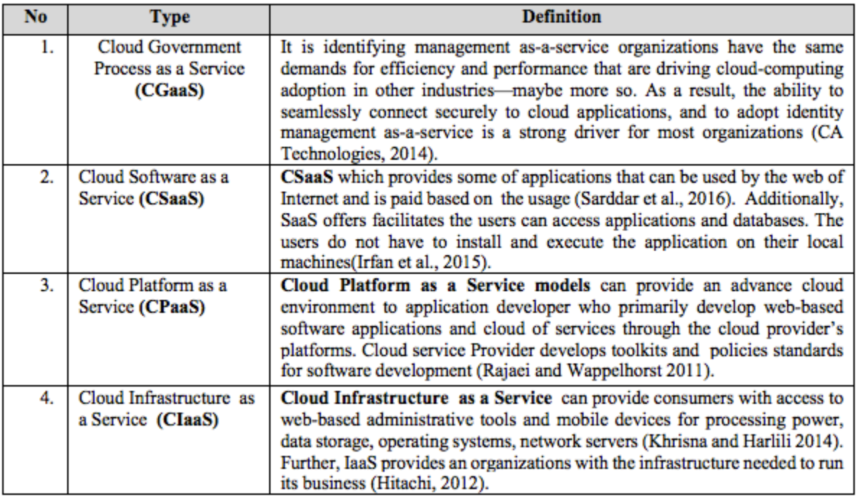
PaaS usually offers a parallel programming framework, checking like the Google Device Engine (Sarddar et al., 2016). Furthermore, ISP is one example of PaaS providers offering the network infrastructure, operating climate, and so on. PaaS providers can need to implement additional Public Cloud workloads (Weixiang and Lin 2016). Cloud providers often include a computing framework which usually includes the operating system, programming language execution setting, database and web server (Parode, Ghadage, & Ghorpade, 2014). A model was suggested (Almorsy, Grundy, & Ibrahim, 2011) That helps cloud service providers and consumers to achieve protection on their cloud platform. This is a little complicated due to the need of the consumer to specify in advance the type of protection controls required without adequate knowledge regarding the appropriate controls or active security criteria they may obtain from the suppliers. Risk assessment framework (Saripalli and Walters 2010) Proposed cloud protection initiatives, which classifies small, moderate which high-scale threats. Nevertheless, no note is made of the processes disposed to harm. Stages for a layout of the threat evaluation have been seen (Sengupta, Kaulgud, & Sharma, 2011) Through taking various acts to determine information protection and intentional commitment to confidentiality and governance concerns connected with software enforcement management. We have not yet established the key processes and controls that will resolve identification and access security issues (Devi and Ganesan 2015). Potential work is also called on to address threat compliance problems across a broad spectrum

Cloud Infrastructure as a Service (CIaaS)

The user does not handle the underlying cloud infrastructure but manages operating systems , data storage, programs for delivery apps and likely restricted manages (NSTAC, 2012). Furthermore, as a business model technology will provide users with links to web-based management resources and mobile devices for computing capacity, data collection, operating systems , network servers (Khrisna and Harlili 2014). Nevertheless, companies that use Infrastructure as a Service (IaaS) to include on demand raw cloud computing services, network bandwidth prices, and storage (Grindle, Kavathekar, & Wan, 2013). Furthermore, IaaS provides an organization with the necessary infrastructure to run its business (Hitachi, 2012). In reality, infrastructure as a utility is defined by (Al-anzi et al., 2014): Technology application computing, manual process management, complex balancing, network virtualization control, and the Internet cloud. However, as the backbone layer of cloud computing in the business system, cloud IaaS tier, infrastructure level will provide the upper layer with open cloud computing capabilities for customers who have functions and data storage as the regular cloud in services throughout the network (Lele and Lihua 2016). In addition, IaaS provides Cloud customers with resources for computing, infrastructure, servers and networking. Of instances the Amazon's elastic cloud. Furthermore, businesses can create their own private cloud based on their own apps, and workers may access the private cloud from various devices, such as desktops, tablet PCs, mobile phones, etc. Thus, the enterprises deploy their workloads to the public cloud based on needs (Weixiang and Lin 2016). IaaS software vendors deliver devices in the bulk of cloud infrastructure types-digital virtual machines, hybrid systems and other computing tools (Parode et al., 2014). Nonetheless, much of the assets of cloud computing are market structures such as IaaS (Infrastructure as a Service) (Yun and Li 2013). It's also the component that supplies the server's physical infrastructure so customers can load their own operating systems. The IaaS may be ideal for program needing tremendous resources (Phumcharoen, 2017). Table 1 therefore shows categories of cloud technology models as a service, cloud applications as a service , cloud application as a service, and cloud network as a service, and each cloud framework has its own cloud protection problem.

Such resources are accessible all around the planet on the Internet where the cloud serves as the central entry point for servicing all customers. Cloud infrastructure design also tackles large-scale data management problems such as the public cloud, proprietary cloud, group cloud and hybrid cloud (Sakharkar et al., 2017).

Table 1 Illustrates types of Cloud service models



No	Type	Definition
1.	Cloud Government Process as a Service **(CGaaS)**	It is identifying management as-a-service organizations have the same demands for efficiency and performance that are driving cloud-computing adoption in other industries—maybe more so. As a result, the ability to seamlessly connect securely to cloud applications, and to adopt identity management as-a-service is a strong driver for most organizations (CA Technologies, 2014).
2.	Cloud Software as a Service **(CSaaS)**	**CSaaS** which provides some of applications that can be used by the web of Internet and is paid based on the usage (Sarddar et al., 2016). Additionally, SaaS offers facilitates the users can access applications and databases. The users do not have to install and execute the application on their local machines(Irfan et al., 2015).
3.	Cloud Platform as a Service **(CPaaS)**	**Cloud Platform as a Service models** can provide an advance cloud environment to application developer who primarily develop web-based software applications and cloud of services through the cloud provider's platforms. Cloud service Provider develops toolkits and policies standards for software development (Rajaei and Wappelhorst 2011).
4.	Cloud Infrastructure as a Service **(CIaaS)**	**Cloud Infrastructure as a Service** can provide consumers with access to web-based administrative tools and mobile devices for processing power, data storage, operating systems, network servers (Khrisna and Harlili 2014). Further, IaaS provides an organizations with the infrastructure needed to run its business (Hitachi, 2012).

References

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

Alassafi, M. O., Alharthi, A., Walters, R. J., & Wills, G. B. (2017). A framework for critical security factors that influence the decision of cloud adoption by Saudi government agencies. Telematics and Informatics, 33,(3). https://doi.org/10.1016/j.tele.2017.04.010

Almorsy, M., Grundy, J., & Ibrahim, A. S. (2011). Collaboration-based cloud computing security management framework. Proceedings - 2011 IEEE 4th International Conference on Cloud Computing, CLOUD 2011, 364–371. https://doi.org/10.1109/CLOUD.2011.9

Almunawar, M. N. (2015). Benefits and Issues of Cloud Computing for E-Government. Review of Public Administration and Management, 3(1), 1–2.

Aziz, M. A., Abawajy, J., & Chowdhury, M. (2013). The Challenges of Cloud Technology Adoption in E-government. 2013 International Conference on Advanced Computer Science Applications and Technologies, 470–474. https://doi.org/10.1109/ACSAT.2013.98

Barclay, C., & Osei-Bryson, K.-M. (2010). Project performance development framework: An approach for developing performance criteria & measures for information systems (IS) projects. International Journal of Production Economics, 124(1), 272–292. https://doi.org/10.1016/j.ijpe.2009.11.025

Bumpus, W. (2013). NIST Cloud Computing Standards Roadmap. NIST Cloud Computing Standards, 1–3. https://doi.org/10.6028/NIST.SP.500-291r2

CA Technologies. (2014). Healthcare Security Solutions: Protecting your Organization, Patients, and Information.

Cayirci, E. (2013). Modeling and Simulation as A Cloud Service: A Survey. Proceedings of the 2013 Winter Simulation Conference, 389–400.

Choudhary, V. (2007). Software as a Service : Implications for Investment in Software Development The Paul Merage School of Business. Proceedings of the 40th Hawaii International Conference on System Sciences, 40(7), 1–10. https://doi.org/10.1109/HICSS.2007.493

Dev, H., Sen, T., Basak, M., & Ali, M. E. (2012). An approach to protect the privacy of cloud data from data mining based attacks. Proceedings - 2012 SC Companion: High Performance Computing, Networking Storage and Analysis, SCC 2012, 1106–1115. https://doi.org/10.1109/SC.Companion.2012.133

Devi, T., & Ganesan, R. (2015). Platform-as-a-Service (PaaS): Model and Security Issues. International Journal of Advances in Applied Sciences, 4(1), 13–23. https://doi.org/10.11591/telkomnika.v15i1.8073

Enterprise Risk Management. (2009). Managing Risk in Cloud Computing.

Fernando, N., Loke, S. W., & Rahayu, W. (2013). Mobile cloud computing: A survey. Future Generation Computer Systems, 29(1), 84–106. https://doi.org/10.1016/j.future.2012.05.023

Fu, Z. (2016). Research on the Prediction of the E-commerce Profit Based on the Improved Parallel PSO-LSSVM Algorithm in Cloud Computing Environment. International Journal of Grid and Distributed Computing, 9(6), 369–380.

Gan, Q., & Zheng, J. (2016). A New Algorithm to Improve Efficiency of Resource Scheduling in Clouding Computing Based on Extended Support Vector Machine. International Journal of Grid and Distributed Computing, 9(3), 125–134.

Grindle, M., Kavathekar, J., & Wan, D. (2013). A New era for the Healthcare Industry-Cloud Computing Changes the Game. In Accenture.

Hanover, J. (2014). Business Strategy: IDC MaturityScape — Cloud in Healthcare Provider.

Hashem, I. A. T., Yaqoob, I., Badrul Anuar, N., Mokhtar, S., Gani, A., & Ullah Khan, S. (2014). The rise of "Big Data" on cloud computing: Review and open research issues. Information Systems, 47, 98–115. https://doi.org/10.1016/j.is.2014.07.006

Hitachi. (2012). How to Improve Healthcare with Cloud Computing.

Irfan, M., Usman, M., Zhuang, Y., & Fong, S. (2015). A Critical Review of Security Threats in Cloud Computing. 2015 3rd International Symposium on Computational and Business Intelligence (ISCBI), 105–111. https://doi.org/10.1109/ISCBI.2015.26

Jakimoski, K. (2016). Security Techniques for Protecting Data in Cloud Computing. International Journal of Grid and Distributed Computing, 9(1), 49–56.

Jassas, M., Qasem, A., & Mahmoud, Q. (2015). A Smart System Connecting e-Health Sensors and the Cloud. Proceeding of the IEEE 28th Canadian Conference on Electrical and Computer Engineering Halifax, Canada, pp. 712–716. https://doi.org/10.1109/CCECE.2015.7129362

Kaur, K., & Zandu, V. (2016). Secure Data Classification Model in Cloud Computing Using Machine Learning Approach. International Journal of Grid and Distributed Computing, 9(8), 13–22.

Khan, M. A. (2016). A survey of security issues for cloud computing. Journal of Network and Computer Applications, Vol. 71, pp. 11–29. https://doi.org/10.1016/j.jnca.2016.05.010

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

Lele, Q., & Lihua, K. (2016). Technical Framework Design of Safety Production Information Management Platform for Chemical Industrial Parks Based on Cloud Computing and the Internet of Things. International Journal of Grid and Distributed Computing, 9(6), 299–314.

Li, J., & Cui, C. (2016). Mobile Cloud-based Big Data Library Management System. International Journal of Grid and Distributed Computing, 9(8), 335–344.

Li, Z. (2016). Design of Cloud Computing Platform for Education Laboratory. International Journal of Grid and Distributed Computing, 9(5), 217–228.

Low, C., Chen, Y., & Wu, M. (2011). Understanding the determinants of cloud computing adoption. Industrial Management & Data Systems, 111(7), 1006–1023. https://doi.org/10.1108/02635571111161262

Lu, K. (2016). Study on Data Privacy Monitoring of Cloud Computing and Access Control Strategy. International Journal of Grid and Distributed Computing, 9(7), 237–242.

Mehmi, S., Sangal, A., Verma, H., & Parmar, K. (2016). Economic Viability of Smart Grid Cloud in India. International Journal of Grid and Distributed Computing, 9(2), 61–72. https://doi.org/10.14257/ijgdc.2016.9.2.07

Naji, H., Wu, C., & Gao, S. (2016). A Semantic-Aware Approach for Automatic Cloud Services Composition. International Journal of Grid and Distributed Computing, 9(8), 181–196.

NSTAC. (2012). NSTAC Report to the President on Cloud Computing.

Paquette, S., Jaeger, P. T., & Wilson, S. C. (2010). Identifying the security risks associated with governmental use of cloud computing. Government Information Quarterly, 27(3), 245–253. https://doi.org/10.1016/j.giq.2010.01.002

Parode, V., Ghadage, S., & Ghorpade, N. (2014). Cloud Based Data Center in Implementing Wireless. International Journal of Advances In Computer Science and Cloud Computing, 2(2), 136–138.

Phumcharoen, J. (2017). Cloud Computing : The challenges of software business. International Journal of Applied Computer Technology and Information Systems, 6(2), 6–10.

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

Rashmi, Sahoo, G., & Mehfuz. (2013). Securing Software as a Service Model of Cloud Computing: Issues and Solutions. International Journal on Cloud Computing: Services and Architecture (IJCCSA), 3(4), 1–11. https://doi.org/10.5121/ijccsa.2013.3401

Sakharkar, V. S., Dande, M., & Mate, S. (2017). Cloud and Big Data : A Compelling Combination. IJESC, 7(3), 4867–4870.

Sarddar, D., Sen, P., & Sanyal, M. K. (2016). Central Controller Framework for Mobile Cloud Computing. International Journal of Grid and Distributed Computing, 9(4), 233–240.

Saripalli, P., & Walters, B. (2010). QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security. 2010 IEEE 3rd International Conference on Cloud Computing, 280–288. https://doi.org/10.1109/CLOUD.2010.22

Sengupta, S., Kaulgud, V., & Sharma, V. S. (2011). Cloud Computing Security--Trends and Research Directions. 2011 IEEE World Congress on Services, 524–531. https://doi.org/10.1109/SERVICES.2011.20

Weixiang, X., & Lin, J. (2016). Research on an Approach of Cloud Workloads Deployment to Public Cloud Based on Open Source Standard. International Journal of Grid and Distributed Computing, 9(3), 209–220.

Yun, F., & Li, H. (2013). Risk Prediction and Management for the Hybrid Cloud Computing Based on the Bank Model. 2013 Fourth International Conference on Intelligent Systems Design and Engineering Applications Risk, 4. https://doi.org/10.1109/ISDEA.2013.532

UNIVERSIDAD
DEL ZULIA

opción

Revista de Ciencias Humanas y Sociales

Año 35, Especial No. 22 (2019)

Esta revista fue editada en formato digital por el personal de la Oficina de Publicaciones Científicas de la Facultad Experimental de Ciencias, Universidad del Zulia.
Maracaibo - Venezuela

www.luz.edu.ve

www.serbi.luz.edu.ve

produccioncientifica.luz.edu.ve