iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** V **Month of publication:** May 2018

DOI: http://doi.org/10.22214/ijraset.2018.5203

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

Meta-Analysis of the Security Vulnerabilities in the Cloud Computing Services and Potential Solutions

Ahmad Alshammari[1], Prof. Mohamed A. Zohdy[2], Dr. Debatosh Debnath[3], Dr. Richard Olawoyin [4] Dr.Andrew Rusek[5]
[1]*PhD. Student, School of Engineering and Computer Science, Oakland University, Rochester, United States*
[2]*Professor, School of Engineering and Computer Science, Oakland University, Rochester, United States*
[3]*Associate Professor, School of Engineering and Computer Science, Oakland University, Rochester, United States*
[4]*Assistant Professor, School of Health Sciences, Oakland University, Rochester, United States*
[5]*Professor, School of Engineering and Computer Science, Oakland University, Rochester, United States*

I. INTRODUCTION

Cloud computing refers to the internet based next generation computing systems which are highly scalable distributed, and offers services to the academic, industrial and scientific communities. The study performed by (1, 2) demonstrated that cloud computing is one of the top ten technologies in the 21 Century with great prospect of being employed by various organizations and companies across the globe. It is conveniently accessible and ubiquitous on-demand services which allow the users access to the shared pool of computing resources such as data storage, services, applications, and servers with minimal management effort or interaction of providers of cloud services [3]. NISH defined the cloud computing as "a model for shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort and service provider interaction" [4]. The cloud computing service model depends on internet for provision of data storage and applications which are stored on the servers; and the customers access these services using the web browsers [5, 6]. Hence, the cloud computing efficiently and effectively makes use of many computing technologies including Web 2.0, service-oriented architecture, virtualization, and many other technologies depending on the internet for their executions [7]. Cloud computing is the representation of maturity of the foregoing technologies which provide services to the customers in the market [8, 9]. The cloud computing as an internet-based service model has two key characteristics; elasticity and multi-tenancy. The elasticity enables the services of the cloud computing as scalable, and provision of the services based on the demands and preferences of the customers, whilst the multi-tenancy is related to the provisioning of the services to multiple customers while maintaining the same level of quality and services [10, 11]. Both features intend to improve the agility, collaboration, rapid adaptation to the demand triggered fluctuations utilization of resources and availability of services without spatio-temporal restrictions in the cost-effective manner [12]. Due to ability of the cloud computing systems to provide with wide range of services ranging from computationally intensive services to the light-weight applications, they have assumed tremendous attraction for the different levels of business operations depending on IT resources [4, 12]. The adoption of cloud computing enables the organizations to reduce the upfront IT investment for purchasing IT infrastructures, software development and licensing various applications. Besides, governments showed an expression of interest in adopting the cloud computing applications in order for reducing the operational costs of the public projects, and enhancing the reachability, availability, and capabilities of their services delivered to the public domain [13, 14]. Although there is the plethora of benefits of the services and applications delivered to the customers through the cloud computing model, but there are significant issues and challenges in the way of successful adoption; and the most important one is the security issue which is reported to hamper the adoption of cloud computing in different organizations [5, 14]. As the cloud computing model is still in its infancy, due to which it involves uncertainty at different levels such as applications, data storage, data access points, network, hosting. The Service level agreements (SLA) does not include specific guarantees about the security and privacy of the customer's data hosted on the servers of the cloud providers [15, 16]. The data from the multiple tenants exist on the same server without solid security controls over the data from each individual user. In addition, the instance of hosting valuable data from the customers on the publicly accessible servers enhances the probabilities of attack from malicious agents [17].

Considering the stance of the cloud provider on the security issue, they are reluctant to the guarantee securities due to increased expenditure required to purchase security licenses and solutions, burden on the resources and complicated nature of security issue in terms of achieving permanent success in the context of delivery of cloud computing services (discussed in the later sections of the paper). However, putting the security issue on the backburner is the not the solution, as it does cast negative impact on improvement of productivity, performance and revenues of the cloud providers. Therefore, it is paramount to identify the key security issues

periodically due to dynamic nature of the cloud computing services, analyse the root causes and put forth the potential solutions to resolve such issues. This will be useful and resourceful to the cloud providers and security solution vendors in terms of having improved insight into the security challenges and subsequently in tackling the security challenge in more effective and efficient manner. Furthermore, out attempt in reviewing the security issues is also important for researchers to identify the gaps and emerging dimensions of the security issue in order to plan the future research projects for combating with this issue effectively.

II. PREVIOUS WORK ON THE SECURITY ISSUES

The issue of security has been dissected by previous researchers from different perspectives in the cloud computing services. The security issues to cloud computing Cloud computing are discussed by [4], the authors analysed various case studies of developers, cloud providers and customers in order to highlight the security issues. Another research showed some security related barriers in adoption of cloud computing such as instances of compromise on customers' data, vulnerabilities, risks and impact on the business. Similar results were produced by many other studies [6, 7]. The security issue related to SLA were discussed by Balachnadra et al [56] with the objective of highlight security risks to the data stored in the servers, data recovery and data segregation. Kreimer et al [57] dissected the security issues such as risks to privacy of valuable or highly sensitive data, payment and integrity of data; and they described various standards for management of security issues: open virtualization format, ISO/IEC 27001 and ITIL. Some studies have described the security issues encountered by only the technical side of cloud computing such as attacks due to flooding issue, XLM based attacks [Kreimer et al., 2010]. Some research works highlighted security issues related to the cloud platform based services [18, 19]. Hashizume et al [21] discussed main vulnerabilities of the cloud computing services and grouped the threats. Subashini et al [10] analysed vulnerabilities to the SaaS model, and focussed only on the service delivery related security issues.

In our research paper, we focussed on cloud computing services presented as part of different layers in the cloud computing architecture, and root causes of security issues associated with each layer and characteristics of the cloud computing as discussed by the previous literature. The presentation of security issues in cloud computing in an organic whole will help the researchers to better understand the security risks and provide solutions based on empirical research.

III.SECURITY IN THE THREE-LAYERED CLOUD COMPUTING MODEL

The cloud computing offers the services to customers in three domains which constitute each layer, thereby giving rise to three service models under umbrella of the cloud computing. The first layer provides the services in the domain of software and related applications, and is called software as a service (SaaS) layer. In this layer, different software and applications are operated on the cloud provider's infrastructure, and the customers are allowed to access these software using thin interface called web-browsing. The example of SaaS is a web-based email (14).

In the second layer, the services are provided using the platform, and are referred to "platform as a service (PaaS)" (35). The customers are allowed to use the platform authorised by the cloud provider to develop their own applications and software without reliance on installation of platforms on their machines. For example, the consumers develop the higher-level services from the software development frameworks and operating system support offered by the cloud provider (36). The third layer is called infrastructure as a service (IaaS) which has the capability to provide for customers with different computing resources, data processing, networks and storage, and allows the deployment of arbitrary software including applications and operating support systems (37).

Considering the security implications to the SaaS, the provision of the security rests with the cloud provider due to increasing degree of abstraction and minimal control of customer over the functionality and extensibility. In contrast to SaaS, PaaS offers greater degree of control and extensibility to customer over the services, which is mainly because of the relatively less level of abstraction involved in designing these services. IaaS even provides with more control to customers over managing security in comparison to PaaS and SaaS [Mather et al., 2009].

Understanding the interdependencies of IaaS, PaaS and SaaS is vital for analysing the security problems encountered by the cloud computing services [Cloud Security Alliance, 2011]. The relationship between these layers can be seen in the figure 1, and it can be seen that IaaS comes forms the foundation on which both PaaS and SaaS are supported, which indicates that any violation of security to the SaaS will influence the security parameters of the PaaS and SaaS and vice versa. This also demonstrated that if attacker launches malicious attack on the security of any layer, it most likely affects the security of other layers as well due to their interdependent relationship. On one hand, each layer of the cloud computing carries some flaws which are prone to security

attacks; on the other hand, there are some security challenges which may affect all of these cloud computing layers due their relationships with each other [Chang and Ramachandran, 2016].

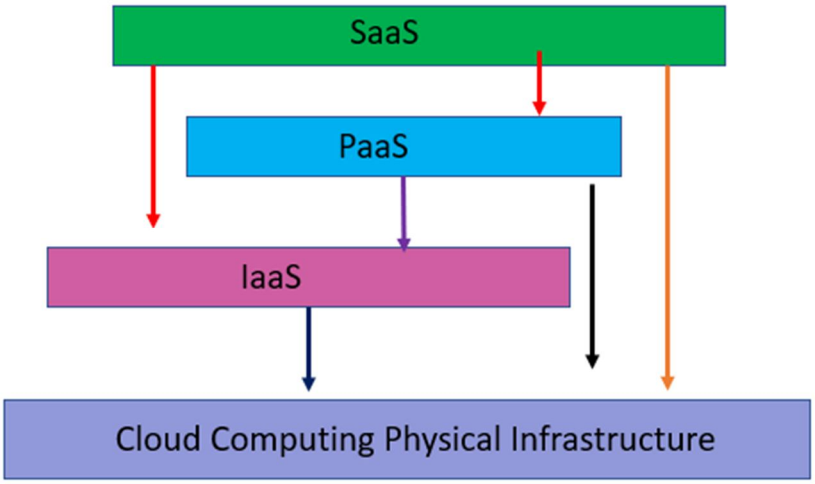


Figure 1: The relationship between three layers in cloud computing infrastructure

Furthermore, the security risks come from controlling the individual layers by different providers, which may complicate the security threats. For instance, SaaS provider relies on the PaaS provider for the provisions of development environment [20, 21, 22], similarly, the PaaS provider depends on the IaaS provider for provision of infrastructure. Importantly, each provider is responsible for the control of security threats to the services provided by his services. Against this backdrop, it become even more difficult and confusing to locate the responsibility of a cloud provider in the event of an attack [23, 24, 25]. Taken together, the security challenges encountered by the cloud computing layers/models are complex in nature, and demands the diagnosis of root causes of each problem whenever and wherever it is faced.

IV. SECURITY ISSUES TO SOFTWARE-AS-A-SERVICE (SAAS)

Under SaaS model, the cloud provider provides various applications and services ranging from businesses applications (e.g., ERP, CRM, SCM) down to conferencing software and email [26, 27, 28, 29, 30]. The customers adopting SaaS services may face security issues at four levels: applications, multi-tenancy, data security and accessibility.

Applications are developed by the SaaS providers, and provided to the customers though internet medium using the web-browsing option. The web-based applications carry risks and vulnerabilities to the security attack from the malicious agents targeting the web-browsers in order for stealing the sensitive data and compromising the functionalities of the user's computers [31, 32, 41]. The security challenges to the SaaS applications are the same as that of web-based applications. However, the security solutions developed for normal web-based applications could not prove effective against security attacks targeted at SaaS ones; therefore, new approaches and solutions are required to tailored in order to thwart attacks on SaaS sponsored applications. Open Web Application Security Projects concluded the similar findings, and identified ten most critical security threats to the SaaS [33, 42].

Multi-tenancy exposes the SaaS to some security vulnerabilities such as data leakage. In multi-tenancy, the SaaS provider provides the services to the multiple users in the single instance, and the data is more likely to be stored in the same database [33, 34, 43]. Saving data in the same database from multiple users enhances of the risk of data leakage between the users [44]; therefore, the previous it is quite incumbent upon the governmental agencies and cloud providers to devise the policies concerning the storage of data from each user separately [24, 25, 35].

Data security is the prime concern of users, which is reported to be a major obstacle in the ay of adoption of SaaS by the organizations, and this concern is exacerbated by the fact that users of SaaS reply on the SaaS providers to manage the security risks with less control at their disposal [12, 21, 36]. In SaaS model, the organizational data is processed and stored by the users, which are stored on the provider's datacentres. Hence, the providers are responsible for ensuring the security and privacy of the attack or diver any security threats to their datacentres. In addition, the cloud providers also provide the data backup services in the case of any disastrous situation, however it inherits security risks in its own right. There is also tradition that cloud providers

subcontract with the third part to hire the data backup services, and often there is no compliance frameworks or regulations exist between the providers and subcontractors [27, 30]. In the provision of SaaS applications, the providers bear the responsibility of stipulating the policies regarding data segregation, privacy and security which must not only be followed by providers and they also be implemented at the level of third parties subcontracted by them [32, 37].

V. SECURITY ISSUES TO PLATFORM-AS-A-SERVICE (PAAS) MODEL

Two forms of security issue are faced PaaS. The first one is related to the PaaS platform, and second one is associated with the applications hosted on PaaS. As these applications are derived from either the PaaS providers or the web-based components offered by third parties. The security of PaaS is the whole responsibility of the PaaS provider, however, the security of their part web-based applications is not promised or guaranteed by the providers, which means that they are vulnerable to web-based security attacks.

The service oriented architecture used by the PaaS model is also vulnerable to security threats such as Man-in-the-hole attack, replay attack, DOS attacks, XLM attacks, input validation associated attacks, and dictionary attacks [9, 16]. The researchers have pointed to the development of WS-security standards and authorization and annual authentication in order for controlling the security threats posed to the PaaS [8, 11, 20]. In addition, there is acute need of policies which should distribute the responsibility of managing PaaS security threats among the cloud providers, users and the third parties.

In addition, the APIs are delivered by PaaS providers to organizations in order to fulfil their business, security and management functions, however these APIs may offer some security risks to the user's data as they are provided with security standards and controls. The APIs should be provided with strict controls and standards to ensure security such as OAuth [46].

Additionally, the applications hosted on PaaS are changed frequently because developers face the dilemma of securing the applications. The changes in applications affects the security of PaaS and system development life cycle [21]. The developers must realize the fact that each change in the applications can increase the security risks to them, therefore, changes should be planned in such a way that they should not affect the integrity of application [47, 42]. The developers should be educated about the secure application development techniques in order to minimize the vulnerabilities of PaaS application to security threats [29. 48]. Storage of data in different locations under different legal arrangements may also pose serious security and privacy risks, and this demands the education of developers about legal regimes and their impact on the security of PaaS [8, 12].

VI. SECURITY ISSUES TO THE INFRASTRUCTURE-AS-A-SERVICE (IAAS)

IaaS model of cloud computing offers a wide range of service in the form of virtualized systems such as networks, servers and storage which are accessed via internet [17]. The users are allowed to run any arbitrary software of their interest while keeping the full control on the allocated resources [49]. In contrast to other two models (PaaS and SaaS), the users have better control over the security of applications as long as long there is no security holes in the 'virtual machine monitoring' [47]. Nonetheless, the underlying processes, computing, storage infrastructure is not under the control of users, as they are under direct control of cloud provider. The security issues in IaaS may result from mobility, communication, modification and monitoring processes which must be regulated to minimize the security threats [51].

Virtualization enables the users to create, copy, migrate and share the contents with other users, and this creates new opportunities for malicious attackers to manipulate with shared or migrated information [31, 43, 44]. Thus security of virtual machine is as important as that of physical machine, and flaw in either of them compromises the security of the IaaS applications [19]. Virtual machines are infected by malwares and viruses in the same fashion as does the physical machines. However, securing virtual environments is far more complex and challenging due to interconnection complexity and uncontrollable entry points compared to physical machines. In addition, the virtual machines have both physical and virtual boundaries which further render the existing solutions futile to secure the virtualized environments [24].

Hypervisor i.e. virtual machine monitor is the low-level software which is introduced to monitor the functionalities of the virtual machine. The migration module transferring the hypervisor to virtual machine can be comprised by the malicious agent which can transfer the virtual machine to a malicious server [54, 55]. In addition, the virtual machine is migrated between physical servers in order for performing different optimization functions such as maintenance, load balancing and fault-tolerance. Though this feature is really useful, but it creates opportunities for attackers to steal the virtual environment during migration process, thereby raising security issues to the virtual machines [52, 53, 47].

Furthermore, there is a common rule that when more than one virtual machines are located on the same server, they can share all resources between each other including memory, CPU and I/O. This renders the virtual machine prone to the malicious attach. For

instance, a malicious virtual machine may communicate with other authentic virtual machines by bypassing the rules defined by security module of virtual machine monitor, thereby stealing the valuable information about the virtual machines [21].

In contrast to the physical machines, virtual machines have the ability to store templates with the information regarding their original users, which can be seen by a new user working on the virtual machine, whereby compromising the data security of individual users. Compared to the physical machines, the virtual machines can be exposed to injection of images carrying malicious codes in the files or templates of the virtual machine or even the stored images can be stolen from the virtual environment. Therefore, it is paramount on the cloud providers to guarantee the security of virtual images repository in order for minimizing the security threats [46, 49].

The rolling back to the previous state is another important feature of the virtual environment in the event of errors, nevertheless, this very feature exposes it to the vulnerabilities and security threats. Rolling backs require the user to take 'snapshot' of the virtual machine, which may propagate the configuration errors and expose the virtual machine to security risks from the malicious agents [12, 44].

The network infrastructure sharing among different users renders the virtual network vulnerable to attacks, as the sharing of resources provider's opportunities to attackers to perform the cross-tenants attack [20]. Many studies have pointed to the potential of interconnectivity enhanced by the virtual networks to increase the probability of attacks on the virtual environment [51, 52]. Some studies suggested to configure virtual networks using routed and bridged approaches for minimizing the security threats, however, it was found that these approaches more likely increase the chances of sniffing and spoofing related attacks on the virtual networks [45, 52].

VII. CONCLUSION

Though cloud computing services and applications hold great promise to fulfil the customer's requirements, and represents the matured form of IT technologies, but the adoption of these services among the organizations and individual users is still slow which is mainly because of the security issues encountered by the cloud computing services. Our paper discussed the vulnerabilities of the cloud computing model (s) to the security attacks, and potential solutions presented in the literature. We discovered in the literature that most of security threats results from the technology associated issues such as virtualization and service oriented architecture. Interdependency of three layers/models (PaaS, IaaS, SaaS) also make the cloud computing services vulnerable to the security risks. Multi-tenancy is really important dimension of the cloud computing services, and is a source of security threats, which require the vertical solution from the SaaS layer to the infrastructure layer. Such solutions may involve the development of physical-like boundaries separating datasets of users from each other. The solutions already existing for the physical environment are non-applicable to the virtual environment. The traditional security solutions for data protection, hosting, and web-applications are discussed, but they are immature to be applied for minimization of security risks to the cloud computing applications. As discussed in paper, the virtual networks, data storage and virtualization are exposed to security threats in cloud computing. The level of security threats different between three layers of cloud computing: IaaS, PaaS, SaaS.

Based on the security issues discussed in this paper, we proposed the following solutions to thwart the security risks.

A. The security solutions should focus on the abstraction issue, during which all security risks should be modelled at the development stage and holistic approach should be adopted to reduce the impact all possible risks to security of cloud computing.

B. Security solutions should be made inherent to the cloud computing architecture where flexibility and elasticity should be hallmark to the cloud computing applications.

C. While maintaining the multitenancy arrangement for maximization of resources, vertical solution for separation of users' data from each other should be integrated into the cloud computing datacenters.

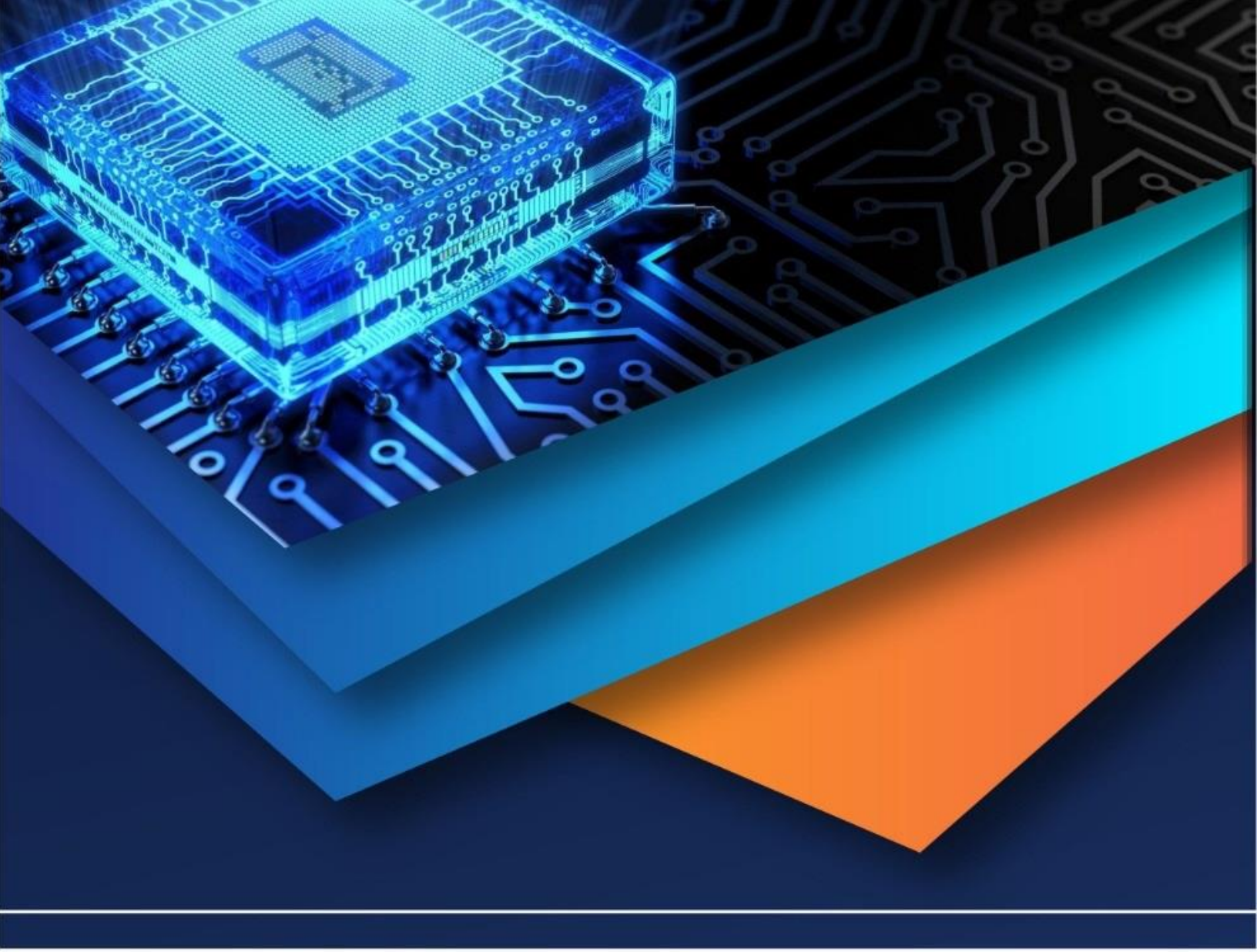
D. The developers should be educated about the impact of changes on security, flexibility and periodicity should be enhanced in the process of development of applications.

E. The developers should consider the use of secure techniques and approaches which can improve the flexibility and efficiency of applications.

REFERENCES

[1] Padhy, R. P., Patra, M. R., & Satapathy, S. C. (2011). Cloud computing: security issues and research challenges. International Journal of Computer Science and Information Technology & Security (IJCSITS), 1(2), 136-146.
[2] Rimal, B. P., Choi, E., & Lumb, I. (2009). A Taxonomy and Survey of Cloud Computing Systems. NCM, 9, 44-51.
[3] AlJahdali, H., Albatli, A., Garraghan, P., Townend, P., Lau, L., & Xu, J. (2014, April). Multi-tenancy in cloud computing. In Service Oriented System Engineering (SOSE), 2014 IEEE 8th International Symposium on (pp. 344-351). IEEE.
[4] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.
[5] Zhao, G., Liu, J., Tang, Y., Sun, W., Zhang, F., Ye, X. P., & Tang, N. (2009, November). Cloud Computing: A Statistics Aspect of Users. In CloudCom (pp. 347-358).
[6] Zhang, S., Zhang, S., Chen, X., & Huo, X. (2010, January). Cloud computing research and development trend. In Future Networks, 2010. ICFN'10. Second International Conference on (pp. 93-97). Ieee.
[7] Marinos, A., & Briscoe, G. (2009, December). Community cloud computing. In CloudCom (Vol. 5931, pp. 472-484).
[8] Dillon, T., Wu, C., & Chang, E. (2010, April). Cloud computing: issues and challenges. In Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on(pp. 27-33). Ieee.
[9] Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. IEEE Security & Privacy, 8(6), 24-31.
[10] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.
[11] Mell, P., & Grance, T. (2009). Effectively and securely using the cloud computing paradigm. NIST, Information Technology Laboratory, 2(8), 304-311.
[12] So, K. (2011). Cloud computing security issues and challenges. International Journal of Computer Networks, 3(5), 247-55.
[13] Agrawal, D., Das, S., & El Abbadi, A. (2011, March). Big data and cloud computing: current state and future opportunities. In Proceedings of the 14th International Conference on Extending Database Technology (pp. 530-533). ACM.
[14] Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. Journal of internet services and applications, 1(1), 7-18.
[15] Buyya, R., Yeo, C. S., & Venugopal, S. (2008, September). Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities. In High Performance Computing and Communications, 2008. HPCC'08. 10th IEEE International Conference on (pp. 5-13). Ieee.
[16] Patel, P., Ranabahu, A. H., & Sheth, A. P. (2009). Service level agreement in cloud computing.
[17] Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107.
[18] Calero, J. M. A., Edwards, N., Kirschnick, J., Wilcock, L., & Wray, M. (2010). Toward a multi-tenancy authorization system for cloud services. IEEE Security & Privacy, 8(6), 48-55.
[19] Chen, D., & Zhao, H. (2012, March). Data security and privacy protection issues in cloud computing. In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on (Vol. 1, pp. 647-651). IEEE.
[20] Motahari-Nezhad, H. R., Stephenson, B., & Singhal, S. (2009). Outsourcing business to cloud computing services: Opportunities and challenges. IEEE Internet Computing, 10(4), 1-17.
[21] Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(1), 5.
[22] Ren, K., Wang, C., & Wang, Q. (2012). Security challenges for the public cloud. IEEE Internet Computing, 16(1), 69-73.
[23] Pearson, S., & Benameur, A. (2010, November). Privacy, security and trust issues arising from cloud computing. In Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on (pp. 693-702). IEEE.
[24] Behl, A., & Behl, K. (2012, October). An analysis of cloud computing security issues. In Information and Communication Technologies (WICT), 2012 World Congress on (pp. 109-114). IEEE.
[25] Jasti, Amarnath, Payal Shah, Rajeev Nagaraj, and Ravi Pendse. "Security in multi-tenancy cloud." In Security Technology (ICCST), 2010 IEEE International Carnahan Conference on, pp. 35-41. IEEE, 2010.
[26] Behl, A. (2011, December). Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. In Information and communication technologies (WICT), 2011 world congress on (pp. 217-222). IEEE.
[27] Tianfield, H. (2012, October). Security issues in cloud computing. In Systems, Man, and Cybernetics (SMC), 2012 IEEE International Conference on (pp. 1082-1089). IEEE.
[28] Rhoton, J., & Haukioja, R. (2011). Cloud computing architected: solution design handbook. Recursive Press.
[29] Yang, L., Cao, J., Yuan, Y., Li, T., Han, A., & Chan, A. (2013). A framework for partitioning and execution of data stream applications in mobile cloud computing. ACM SIGMETRICS Performance Evaluation Review, 40(4), 23-32.
[30] Xiao, Z., & Xiao, Y. (2013). Security and privacy in cloud computing. IEEE Communications Surveys & Tutorials, 15(2), 843-859.
[31] Leymann, F., & Fritsch, D. (2009). Cloud computing: The next revolution in IT. Proceedings of the 52th Photogrammetric Week, 3-12.
[32] Gonzalez, N., Miers, C., Redigolo, F., Simplicio, M., Carvalho, T., Näslund, M., & Pourzandi, M. (2012). A quantitative analysis of current security concerns and solutions for cloud computing. Journal of Cloud Computing: Advances, Systems and Applications, 1(1), 11.
[33] Sengupta, S., Kaulgud, V., & Sharma, V. S. (2011, July). Cloud computing security--trends and research directions. In Services (SERVICES), 2011 IEEE World Congress on (pp. 524-531). IEEE.
[34] Celesti, A., Tusa, F., Villari, M., & Puliafito, A. (2010, July). Three-phase cross-cloud federation model: The cloud sso authentication. In Advances in Future Internet (AFIN), 2010 second international conference on (pp. 94-101). IEEE.
[35] Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). NIST cloud computing reference architecture. NIST special publication, 500(2011), 292.
[36] Chang, V., Kuo, Y. H., & Ramachandran, M. (2016). Cloud computing adoption framework: A security framework for business clouds. Future Generation Computer Systems, 57, 24-41.
[37] Mather, T., Kumaraswamy, S., & Latif, S. (2009). Cloud security and privacy: an enterprise perspective on risks and compliance. " O'Reilly Media, Inc.".

[38] Cloud Security Alliance (2011) Security guidance for critical areas of focus in Cloud Computing V3.0.. Available: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
[39] Chang, V., & Ramachandran, M. (2016). Towards achieving data security with the cloud computing adoption framework. IEEE Transactions on Services Computing, 9(1), 138-151.
[40] Juels, A., Molnar, D., & Wagner, D. (2005, September). Security and Privacy Issues in E-passports. In Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on(pp. 74-88). IEEE. Ju, J., Wang, Y., Fu, J., Wu, J., & Lin, Z. (2010, June). Research on key technology in SaaS. In Intelligent Computing and Cognitive Informatics (ICICCI), 2010 International Conference on (pp. 384-387). IEEE.
[41] Krutz, R. L., & Vines, R. D. (2010). Cloud security: A comprehensive guide to secure cloud computing. Wiley Publishing.
[42] Grossman, R., & Gu, Y. (2008, August). Data mining using high performance data clouds: experimental studies using sector and sphere. In Proceedings of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining (pp. 920-927). ACM.
[43] Hogan, M., Liu, F., Sokol, A., & Tong, J. (2011). Nist cloud computing standards roadmap. NIST Special Publication, 35.
[44] Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data security and privacy in cloud computing. International Journal of Distributed Sensor Networks, 10(7), 190903.
[45] Hamdaqa, M., Livogiannis, T., & Tahvildari, L. (2011). A Reference Model for Developing Cloud Applications. In CLOSER (pp. 98-103).
[46] Yang, J., & Chen, Z. (2010, December). Cloud computing research and security issues. In Computational intelligence and software engineering (CiSE), 2010 international conference on (pp. 1-3). IEEE.
[47] Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009, September). On technical security issues in cloud computing. In Cloud Computing, 2009. CLOUD'09. IEEE International Conference on (pp. 109-116). IEEE.
[48] Dahbur, K., Mohammad, B., & Tarakji, A. B. (2011, April). A survey of risks, threats and vulnerabilities in cloud computing. In Proceedings of the 2011 International conference on intelligent semantic Web-services and applications (p. 12). ACM.
[49] Dawoud, W., Takouna, I., & Meinel, C. (2010, March). Infrastructure as a service security: Challenges and solutions. In Informatics and Systems (INFOS), 2010 the 7th International Conference on (pp. 1-8). IEEE.
[50] Owens, K. (2009). Securing virtual compute infrastructure in the cloud. Whitepaper. SavvisCorp.[Online]. Available: http://www. savvis. com/en-us/info%5Fcenter/documents/hos-whitepaper-securingvirutalcomputeinfrastructureinthecloud. pdf.
[51] Jasti, A., Shah, P., Nagaraj, R., & Pendse, R. (2010, October). Security in multi-tenancy cloud. In Security Technology (ICCST), 2010 IEEE International Carnahan Conference on(pp. 35-41). IEEE.
[52] Garfinkel, T., & Rosenblum, M. (2005, May). When Virtual Is Harder than Real: Security Challenges in Virtual Machine Based Computing Environments. In HotOS.
[53] Venkatesha, S., Sadhu, S., Kintali, S., & Barbara, S. (2009). Survey of virtual machine migration techniques. Memory.
[54] Sharath, V., Sadhu, S., & Kintali, S. (2009). Survey of virtual machine migration techniques. Memory.
[55] Kandukuri, B. R., & Rakshit, A. (2009, September). Cloud security issues. In Services Computing, 2009. SCC'09. IEEE International Conference on (pp. 517-520). IEEE.
[56] Kresimir Popovic , Zeljko Hocenski, "Cloud computing security issues and challenges," in The Third International Conference on Advances in Humanoriented and Personalized Mechanisms, Technologies, and Services, 2010, pp. 344-349



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY