iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** VIII **Month of publication:** August 2016

DOI:

www.ijraset.com

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

Volume 4 Issue VIII, August 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A review on Cloud Computing Security issues and Threat

Dheeraj Pal[1], Divya Gautam[2]
Computer Science & Engineering, Amity University, Madhya Pradesh

Abstract: ***Cloud computing is a combination of traditional technology of computing and various other technologies such as parallel computing, distributed computing etc. The major goal is to achieve a complete system having capabilities of computing by providing low cost computing environment. Different organizations get virtual space to deploy applications or run operations over it. Various services of cloud are given by some third party who possesses the arrangement. As this environment is totally based on third party so its difficult to maintain data security, confidentiality, availability of resources, so if in any case some live attack occurs like DDoS attack, then it is very difficult to cope up. In this research we are going to discuss various types of vulnerabilities and threats to cloud computing environment, also the methods to mitigate those security issues.***
Keywords: Cloud Computing, Security issues, Threats of Cloud computing, Attacks cloud computing.

I. INTRODUCTION

Privacy is gaining in importance across the globe, often involving laws and regulations, relating to the acquisition, storage and use of personally identifiable information (PII). Typically, privacy implies limitations on the use and accessibility of PII, with associated requirements to tag the data appropriately, store it securely and to permit access only by appropriately authorized users. This requires appropriate controls to be in place, particularly when the data is stored within a cloud provider's infrastructure. The ISO 27018 standard (in preparation) addresses the controls required for PII. In many countries, numerous laws, regulations and other mandates require public and private organizations to protect the privacy of personal data and the security of information and computer systems. When data is transferred to a cloud computing environment, the responsibility for protecting and securing the data typically remains with the consumer (the *data controller* in EU terminology15), even if in some circumstances, this responsibility may be shared with others. When an organization relies on a third party to host or process its data, the data controller remains liable for any loss, damage, or misuse of the data. It is prudent, and may be legally required, that the data controller and the cloud provider enter into a written (legal) agreement that clearly defines the roles, expectations of the parties, and allocates between them the many responsibilities that are attached to the data at stake.

It is critical that privacy issues are adequately addressed in the cloud contract and service level agreement (SLA). If not, the cloud consumer should consider alternate means of achieving their goals including seeking a different provider, or not putting sensitive data into the cloud computing environment. For example, if the consumer wishes to place HIPAA-covered information into a cloud computing environment, the consumer must find a cloud service provider that will sign a HIPAA business associate agreement or else not put that data into the cloud computing environment. Enterprises are responsible for defining policies to address privacy concerns and raise awareness of data protection within their organization. They are also responsible for ensuring that their cloud providers adhere to the defined privacy policies. Consumers have an ongoing obligation to monitor their provider's compliance with its policies. This includes an audit program covering all aspects of the privacy policies including methods of ensuring that corrective actions will take place

II. RELATED WORK

Many researchers have conducted work related to the security and privacy problem in cloud computing [6, 22, 39-43, 55, 59-64]. We summarize this work here: In [6] Popovic et al. presented some standards that can be used to address security issues in cloud computing such as: Information Technology Infrastructure Library (ITIL), International Organization for Standardization (ISO 27001/27002) and Open Virtualization Format (OVF). In [22] Ramgovind et al. presented guidelines for managing cloud security which include: cloud governance, cloud transparency and cloud computing security impacts. In [39] the authors proposed an Effective Privacy Protection Scheme (EPPS) to provide the appropriate privacy protection for cloud services. EPPS satisfies users' privacy requirements and maintains system performance simultaneously. First, they analyzed the privacy level users require and quantified the security degree and performance of encryption algorithms. Then, an appropriate security composition is derived by

the results of analysis and quantified data. Their simulation results showed that the EPPS not only fulfils users' privacy requirements but also maintains the cloud system performance in different cloud environments. The execution results show that EPPS outperforms other security schemes by 35% to 50%. In [40] in order to satisfy the assurances of cloud data integrity and availability and enforce the quality of cloud storage services for users, the authors proposed a highly efficient and flexible distributed storage verification scheme with two salient features. By utilizing a homomorphic token with distributed erasurecoded data, their scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server(s). Unlike most prior work, the new scheme further supports secure and efficient dynamic operations on outsourced data, including: block modification, deletion and appending. Extensive security and performance analysis showed that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attacks, and even server collusion attacks. The work in [41] studied the problem of ensuring the integrity of data storage in Cloud Computing. In particular, the authors considered the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The introduction of TPA eliminated the involvement of the client through the auditing of whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for cloud computing. They stated that a significant step toward practicality is the support for data dynamics via the most general forms of data operation, such as block modification, insertion, and deletion, since services in cloud computing are not limited to archive or backup data only. While prior work on ensuring remote data integrity often lacks support for either public auditability or dynamic data operations, this work achieves both. The authors showed how to construct an elegant verification scheme for the seamless integration of these two salient features in their protocol design. In particular, to achieve efficient data dynamics, they improved the existing proof of storage models by manipulating the classic Merkle Hash Tree construction for block tag authentication. To support efficient handling of multiple auditing tasks, they explored the technique of bilinear aggregate signature to extend their main result into a multiuser setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis showed that the proposed schemes are highly efficient and provably secure.

Most of the work mentioned above seem to focus on certain aspects of the security and privacy problem in cloud computing. In this work we provide a framework for security and privacy that serves as a comprehensive guidance for achieving higher security level in the clouds. The framework gives guidelines on most of the aspects of secure clouds including: security and privacy requirements, attacks and threats that clouds are vulnerable to and risks and concerns about cloud security. Moreover, we propose a generic security model for cloud computing that helps satisfy its security requirements and protect the clouds against various malicious behaviors.

III. FRAMEWORKS FOR SECURE CLOUD

It consists of three essential security components; each of them includes important challenges related to cloud security and privacy. These components are: Security and privacy requirements: identifies security and privacy requirements for the cloud such as authentication, authorization, integrity, etc. Attacks and threats: warns from different types of attacks and threats to which clouds are vulnerable. Concerns and risks: pay attention to risks and concerns about cloud computing.

IV. SECURITY AND PRIVACY

Security concerns confidentiality, availability and integrity of data or information. It also includes Authentication, Authorization and Access control (AAA). On the other hand, privacy concerns the adherence to various legal and non legal norms. It includes: consent, purpose restriction and legitimacy which all ensure that a cloud deployment meets the requirements imposed by law. It may also include transparency, governance and compliance. The International Standards Organization (ISO), in ISO 7498-2 [21, 23], suggested a number of information security requirements.

There are a number of security risks associated with cloud computing that must be adequately addressed.

A. Loss of governance

For public cloud deployments, consumers necessarily cede control to the cloud provider over a number of issues that may affect security. At the same time, cloud service level agreements (SLA) may not offer a commitment to provide such capabilities on the part of the cloud provider, thus leaving gaps in security defenses.

B. Responsibility ambiguity

Given that use of cloud computing services spans across the consumer and the provider organizations, responsibility for aspects of security can be spread across both organizations, with the potential for vital parts of the defenses to be left unguarded if there is a

Volume 4 Issue VIII, August 2016
ISSN: 2321-9653

failure to allocate responsibility clearly. The split of responsibilities between consumer and provider organizations is likely to vary depending on the model being used for cloud computing (e.g. Iaas versus SaaS).

C. Isolation failure

Multi-tenancy and shared resources are defining characteristics of public cloud computing. This risk category covers the failure of mechanisms separating the usage of storage, memory, routing and even reputation between different tenants (e.g., so-called guest-hopping attacks).

D. Vendor lock-in

Dependency on proprietary services of a particular cloud provider could lead to the consumer being tied to that provider. Services that do not support portability of applications and data to other providers increase the risk of data and service unavailability.

E. Compliance and legal risks

Investment in achieving certification (e.g., industry standard or regulatory requirements) may be put at risk by migration to use cloud computing if the cloud provider cannot provide evidence of their own compliance with the relevant requirements or if the cloud provider does not permit audit by the cloud consumer. It is the responsibility of the cloud consumer to check that the cloud provider has appropriate certifications in place, but it is also necessary for the cloud consumer to be clear about the division of security responsibilities between the consumer and the provider and to ensure that the consumer's responsibilities are handled appropriately when using cloud computing services.

F. Key Steps to ensure that data involved in cloud computing activities is properly secured

Controls	Descriptions
Create a data asset catalog	A key aspect of data security is the creation of a data asset catalog, identifying all data assets, classifying those data assets in terms of criticality to the business (which can involve financial and legal considerations, including compliance requirements), specifying ownership and responsibility for the data and describing the location(s) and acceptable use of the assets. Relationships between data assets also need to be cataloged. An associated aspect is the description of responsible parties and roles, which in the case of cloud computing must span the cloud service consumer organization and the cloud service provider organization.

Apply confidentiality, integrity and availability	• The key security principles of confidentiality, integrity and availability are applied to the handling of the data, through the application of a set of policies and procedures, which should reflect the classification of the data. • Sensitive data should be encrypted, both when it is stored on some medium and also when the data is in transit across a network - for example, between storage and processing, or between the provider's system and a consumer user's system. o An extra consideration when using cloud computing concerns the handling of encryption keys - where are the keys stored and how are they made available to application code that needs to decrypt the data for processing? It is not advisable to store the keys alongside the encrypted data, for example. • Integrity of data can be validated using techniques such as message digests or secure hash algorithms, allied to data duplication, redundancy and backups. • Availability can be addressed through backups and/or redundant storage and resilient systems, and techniques related to the handling of denial-of-service attacks. There is also a need for a failover strategy, either by using a service provider who offers this as part of their service offering, or if the provider does not offer resiliency as a feature of their services the consumer may consider self provision of failover by having equivalent services on standby with another provider.

V. VARIOUS TYPES OF ATTACKS AND THREATS

Attacks and Threats Before defining types of attacks in clouds, we must identify the attackers themselves and their impact on the security of cloud systems. Cloud attackers may be categorized as follows:

A. Random

The most common type of attackers uses simple techniques to randomly scan the internet in order to find vulnerable computers. They deploy well known tools that should be easily detected.

B. Weak

Weak attacks are semi-skilled attackers who target specific cloud providers by customizing publicly available tools for specific targets.

C. Strong

These are organized, skilled and well financed groups of attackers who target particular applications and users of the cloud. Generally, they form criminal groups specialized in large scale attacks.

D. Substantial

These are motivated, highly skilled attackers who can't be easily detected either by the organizations they attack or by the law enforcement and investigative organizations specializing in e-Crime or cyber security. Attacks on cloud computing can be classified according to cloud service models and they are described below [24, 25,101]: In SaaS the most common attacks are.

E. Wrapping attacks

These attacks occur between the web browser and the server by altering the Simple Object Access Protocol (SOAP) messages for two persons, the user and the attacker. When using XML signatures for authentication or integrity, the most well known attack is XML Signature Element Wrapping.

F. Browser-based attacks

A browser attack alters the signature and encryption of SOAP messages. The security of Web browsers is defended against some types of attack such as phishing attack, SSL certificate spoofing, and attacks on browser caches. In PaaS there are some types of attack such as:

1) *Cloud injection attacks:* It attempt to create malicious service implementation modules or virtual machine instances for the opponent to be executed against intention. Examples for these modules are SQL injection, OS command injection and cross site scripting [64]. The threat occurs when considering the new instance to be a valid instance. To avoid this attack, a hashing algorithm should be used.
2) *Metadata spoofing attacks:* include reengineering Web Services' metadata descriptions. To defend against this threat, verification techniques should be used.

In IaaS, the most important attack is the flooding attack that is represented as:

a) *Denial of service attacks:* occur when an attacker sends a lot of malicious requests to the server and consumes its available resources, CPU and memory. When the server reaches its maximum capacity, it offloads the received requests to another server. In cloud computing, due to the large number of cloud users (multitenancy) who share the cloud infrastructure the problem of Distributed DoS (DDoS) attacks becomes of much greater impact than that in single tenant architecture. The problem is further magnified when the cloud has no sufficient resources to provide customers with services [65]. The cloud system works against the attacker by providing more computational power.
b) *Buffer overflow attacks:* when buffer overflow occurs, the attacker is able to overwrite data specialist in program execution to execute his malicious program. Privilege escalation: utilizes a vulnerability that comes from any programming errors and aims to access the protected resources without permission.

VI. SUMMARY FOR CLOUD COMPUTING AND THEIR COUNTERMEASURES

Attacks and threats	Mitigation
Wrapping attacks	Increase security during message passing from the web server to the web browser by using the SOAP message
Cloud injection attacks	Use hash algorithms
Metadata spoofing attacks	Use verification techniques
Denial of Service (DoS)	Provide more computational power and resources
Abuse and Nefarious Use of Cloud Computing	Improve credit card fraud detection-Apply strict registration and validation rules-Perform extensive examination of network traffic
Insecure Interfaces	Analyse the security model of the API- Employ strong authentication, access control and encryption techniques- Understand the dependency chain of the API
Malicious Insiders	Require transparency in all information security issues- Define security breach notification processes- Enforce strict hiring requirements and HR assessment
Shared technology	Conduct vulnerability scanning

VII. CONCLUSION

In this paper, we reviewed the literature for security challenges in cloud computing and proposed a framework that identifies security and privacy requirements, attacks, threats, concerns and risks associated to the deployment of the clouds. We believe that more effort should be exerted by both cloud vendors and organizations to provide a highly protected, safe and sound cloud computing environment. On the other hand, we suggest that future research should be directed towards the management of risks

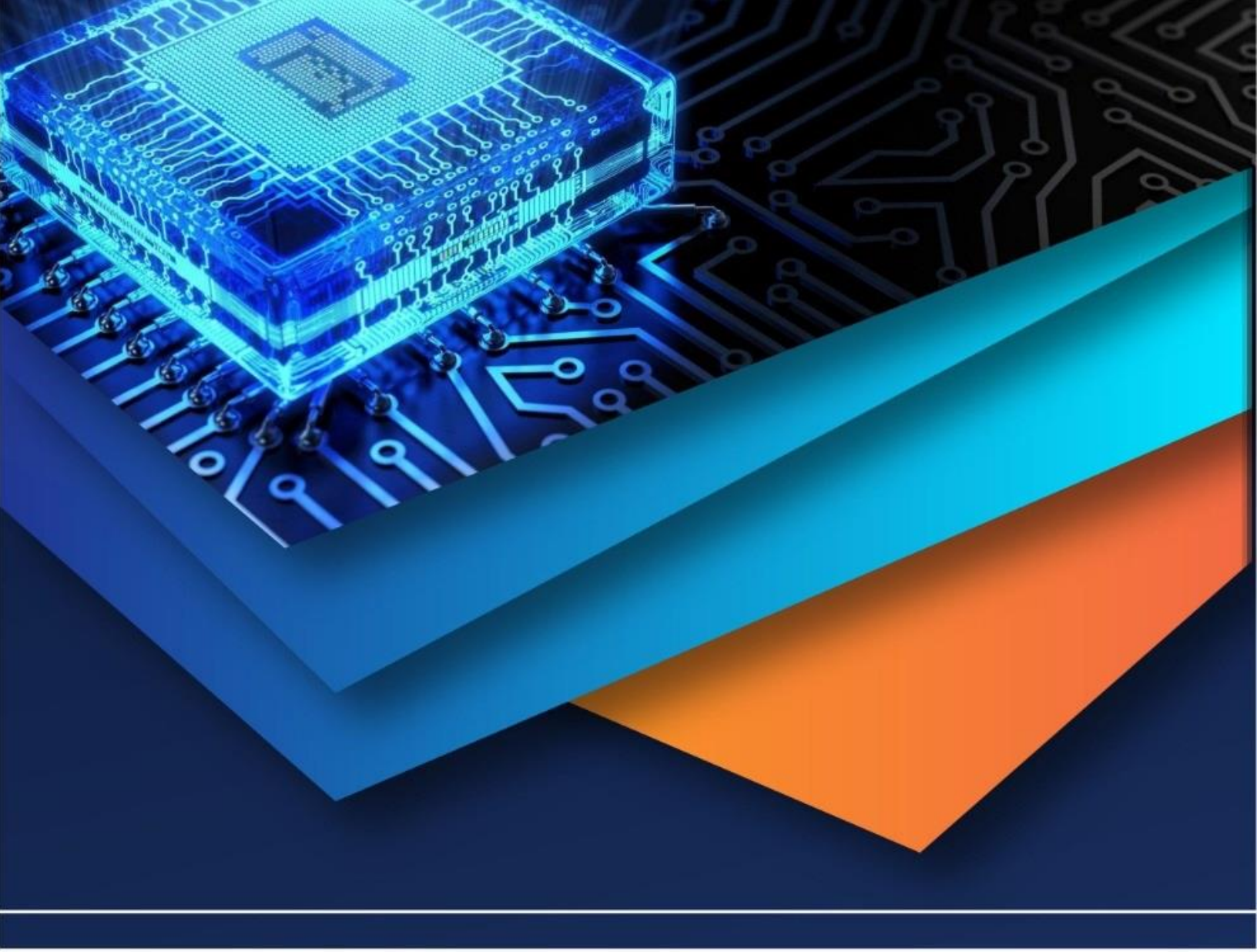
associated with cloud computing. Developing risk assessment helps organizations make an informed decision as to whether cloud computing is currently suitable to meet their business goals with an acceptable level of risks. However, managing risks in cloud computing is a challenging process that entails identifying and assessing risks, and taking steps to reduce it to an acceptable level. We plan to pursue research in finding methods for qualitative and quantitative risk analysis in cloud computing. These methods should enable organizations to balance the identified security risks against the expected benefits from cloud utilization.

REFERENCES

[1] GTSI Group, "Cloud Computing - Building a Framework for Successful Transition," White Paper, GTSI Corporation, 2009.
[2] L. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A Break in the Clouds: Towards a Cloud Definition," ACM SIGCOMM Computer Communication Review, Volume 39 Issue 1, pages 50- 55, January 2009.
[3] M. Boroujerdi and S. Nazem, "Cloud Computing: Changing Cogitation about Computing," World Academy of Science, Engineering and Technology, 2009.
[4] Michael Miller, "Cloud Computing Pros and Cons for End Users", icrosoftpartnercommunity.co.uk, 2009.
[5] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing," UC Berkeley Reliable Adaptive Distributed Systems Laboratory, 2009.
[6] Kresimir Popvoic and Zeljko Hocenski, "Cloud Computing Security Issues and Challenges" MIPRO, Opatijia, Croatia, May 24-28, 2010.
[7] Radu Prodan and Simon Ostermann, "A Survey and Taxonomy of Infrastructure as a Service and Web Hosting Cloud Providers", 10th IEEE/ACM International Conference on Grid Computing, 2009
[8] http://en.wikipedia.org/wiki/Cloud_computing
[9] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing" Communication of the ACM, Vol. 53, No. 4, April 2010.
[10] K. Chard, S. Caton, O. Rana and K. Bubendorfer, "Social Cloud: Cloud Computing in Social Networks" 3rd IEEE International Conference on Cloud Computing, Miami, FL, USA, July 5-10,2010.
[11] L. Tang, J. Dong, Y. Zhao and L. Zhang "Enterprise Cloud Service Architecture" 3rd IEEE International Conference on Cloud Computing,Miami, FL, USA, July 5-10,2010.
[12] W. Jansen and T.Grance "Guidelines on Security and Privacy in Public Cloud Computing", NIST Draft Special Publication 800-144, 2011. http://csrc.nist.gov/publications/drafts/800-144/Draft-SP- 800-144_cloud-computing.pdf
[13] N. Robinson, L. Valeri, J. Cave, T. Starkey, H. Graux, S. Creese and P. Hopkins, "The Cloud: Understanding the Security, Privacy and Trust Challenges", RAND Corporation, 2010. http://cordis.europa.eu/fp7/ict/security/docs/the-cloudunderstanding-security-privacy-trust-challenges- 2010_en.pdf
[14] NIST, http://www.nist.gov/itl/cloud/index.cfm
[15] CloudComputingvs.Virtualizationhttp://www.learncomputer.com/cloud-computing-virtualization/
[16] Wikipedia , http://en.wikipedia.org/wiki/Virtualization
[17] Y. Luo,"Network I/O Virtualization for Cloud Computing",IEEE Computer Society,Oct. 2010.
[18] W. Tsai, X. Sun, J. Balasooriya, "Service-Oriented Cloud Computing Architecture" 7th IEEE International Conference on Information Technology, 2010.
[19] T. Dillon, C. Wu and E. Chang, "Cloud Computing: Issues and Challenges", 24th IEEE International Conference on Advanced Information Networking and Appications, 2010.
[20] Introduction to Cloud Computing, White Paper,Dialogic Corporation, 2010.
[21] ISO, http://www.iso.org/iso/home.htm
[22] Ramgovind S, Eloff MM and Smith E. "The Management of Security in Cloud Computing" Information Security for South Africa (ISSA), Sandton, Johannesburg, 2-4 Aug, 2010.
[23] ISO. ISO 7498-21989. "Information Processing Systems- Open Systems Interconnection. ISO 7498-
[24] N. Gruschka and M. Jensen, "Attack Surface: A Taxonomy for Attacks on Cloud Services", 3rd IEEE International Conference on Cloud Computing, Miami, FL, USA, July 5-10,2010.
[25] K. Zunnurhain and S. Vrbsky, "Security Attacks and Solutions in Clouds", 2nd IEEE International Conference on Cloud Computing Technology and Science, Indianapolis, USA, Nov. 30- Dec. 3,2010.
[26] http://www.cloudsecurityalliance.org/
[27] SecureCloud 2010, http://www.cloudsecurityalliance.org/sc2010.html
[28] Cloud Security Alliance "Top Threats toCloud Computing V1.0", March 2010.
[29] J. Bordkin, "Gartner:Seven Cloud-Computing Security Risks", 2008.
[30] M. Yildiz, J. Abawajy, T. Ercan and A. Bernoth," A Layered Security Approaches for Cloud Computing Infrastrucure", 10th International Symposium on Pervasive Systems, Algorithms, and Networks,2009.
[31] CSA, "Security Guidance for Critical Areas of Focus on Cloud Computing V2.1", 2009.
[32] A.Albeshri and W.Caelli, "Mutual Protection in a Cloud Computing Environment", IEEE 12th International Conference on High Performance Computing and Communications (HPCC), Melbourne, 1-3 September 2010.
[33] Q. Tong and Z. Shen," The security of Cloud Computing System Enabled by Trusted Computing Technology", 2nd International Conference on Signal Processing Systems (ICSPS),2010.
[34] J. Yang and W. Huang, "New network security based on Cloud Computing", Education Technology and Computer Science (ETCS), 2010.
[35] V. Sarathy, P. Narayan, and R. Mikkilineni, "Next generation Cloud Computing Architecture" 2nd International IEEE Workshop On collaboration & Cloud Computing, 2010.
[36] P. Mell and T. Grance, "The NIST Definition of Cloud Computing" Recommendation of NIST, Special Publication 800-145, 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[37] http://www.idc.com.
[38] "Cloud Computing Security Considerations", Cyber Security Operation Cenetre, Technical report, 2011.
[39] I. Chuang, S. Li, K. Huang, and Y. Kuo, "An effective privacy protection scheme for cloud computing", In Proceeding of the 13th International Conference on Advanced Communication Technology (ICACT), 2011
[40] C. Wang, Q. Wang, K. Ren, and W .Lou, "Towards Secure and Dependable Storage Services in Cloud Computing", IEEE Transactions on Services Computing, Issue:99 , 2011.
[41] Q. Wang, C. Wang, K. Ren W. Lou, and J. Li, " Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing" IEEE Transactions on Parallel and Distributed Systems, Volume : 22 , Issue:5, 2011.
[42] C. Băsescu, A. Carpen-Amarie, C.Leordeanu, A. Costan, and G. Antoniu, "Managing Data Access on Clouds: A Generic Framework for Enforcing Security Policies", In proceeding of IEEE International conference on Advanced Information Networking and Applications (AINA), 2011
[43] R. Sravan Kumar and A. Saxena, "Data integrity proofs in cloud storage", Third International Conference on Communication Systems and Networks (COMSNETS), 2011.
[44] Federal Information Processing Standards Publication 197,"Specification for the Advanced Encryption Standards (AES)", 2001.
[45] S. Fluhrer, I. Mantin, and A. Shamir, "Weakness in the Key schedualing algorithm of RC4", 8th Annual International Workshop on Selected Areas in Cryptography, Springer-Verlag London, UK, 2001.
[46] http://en.wikipedia.org/wiki/Cryptographic_hash_function
[47] https://cloudsecurityalliance.org/research/initiatives/securityguidance/
[48] http://www.opengroup.org/jericho/
[49] http://www.sharedassessments.org/value/
[50] http://www.enisa.europa.eu/
[51] http://csrc.nist.gov/archive/aes/rijndael/wsdindex.html
[52] Shucheng Yu, Cong Wang,KuiRen and Wenjing Lou, " Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", 2010
[53] M. Johnsson and A. Azam, "Mobile One Time Passwords and RC4 Encryption for Cloud computing", Technical report, IDE1108, March 2011.
[54] http://en.wikipedia.org/wiki/Two-factor_authentication
[55] Z. Wang, "Security and Privacy Issues Within Cloud Computing" IEEE Int. conference on computational and Finformation sciences, Chengdu, China, Oct. 2011.
[56] James B.D. Joshi, Elisa Bertino, Usman Latif, Arif Ghafoor, "A Generalized Temporal Role-Based Access Control Model",IEEE Computer Society, 2005.
[57] Moonam Ko, Gail-joon Ahn, Mohamed Shehab, "Privacy enhanced User-Centric Identity Management", IEEE International Conference on Communications, 2009
[58] Cong Wang, Qian Wang, Kui Ren, Wenjing Luo, "Privacy preserving public audting for data storage security in Cloud Computing", IEEE Communication Society, 2010
[59] C. Deletre, K. Boudaoud and M. Riveill, "Cloud computing security and data concealment" IEEE symposium on computers and communications (ISCC), Greece, June 28-July 1, 2011
[60] E. Mathisen, "Security Challenges and Solutions in Cloud Computing" 5th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST2011), Daejeon, Korea, 31 May -3 June 2011.
[61] Almorsy, M. Grundy, J. Ibrahim, A.S., "Collaboration- Based Cloud Computing Security Management Framework" IEEE Int. confernce on cloud computing (CLOUD), 4-9 July 2011.
[62] A. Tripathi and A. Mishra, "Cloud computing security considerations" IEEE Int. conference on signalprocessing, communication and computing (ICSPCC), 14-16 Sept., Xi'an, Shaanxi, China, 2011
[63] Shubhashis Sengupta, Vikrant Kaulgud and Vibhu Saujanya Sharma, "Cloud Computing Security – Trends and Research Directions" IEEE World Congress on Services, 4-9 July 2011
[64] Vadym Mukhin, Artem Volokyta, "Security Risk Analysis for Cloud Computing Systems" The 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Prague, Czech Republic, 15-17 September 2011
[65] Sabahi, F., "Cloud computing security threats and responses", IEEE 3rd International Conference on Communication Software and Networks (ICCSN), , 27-29 May 2011
[66] Gul, I. , ur Rehman, A. and Islam, M.H. , "Cloud computing security auditing", The 2nd International Conference on Next Generation Information Technology (ICNIT), 21-23 June 2011
[67] Ko, R.K.L., Kirchberg, M. and Bu Sung Lee, "From system-centric to data-centric logging - Accountability, trust & security in cloud computing", Defense Science Research Conference and Expo (DSR), 3-5 Aug. 2011
[68] Cheung, D.W., "Security on cloud computing, query computation and data mining on encrypted database" IEEE Technology Time Machine Symposium on Technologies Beyond 2020 (TTM), 1-3 June 2011
[69] Srivastava, P. , Singh, S. , Pinto, A.A. , Verma, S. ,Chaurasiya, V.K. and Gupta, R., "An architecture based on proactive model for security in cloud computing" International Conference on Recent Trends in Information Technology (ICRTIT), 3-5 June 2011
[70] Jun-jie Wang and Sen Mu, "Security issues and countermeasures in cloud computing" IEEE International Conference on Grey Systems and Intelligent Services (GSIS), 15-18 Sept. 2011
[71] Zech, P., "Risk-Based Security Testing in Cloud Computing Environments", IEEE Fourth International Conference on Software Testing, Verification and Validation (ICST), 21-25 March 2011
[72] Jansen, W.A., "Cloud Hooks: Security and Privacy Issues in Cloud Computing", 44th Hawaii International Conference on System Sciences (HICSS), 4-7 Jan 2011
[73] Haoyong Lv and Yin Hu, "Analysis and Research about Cloud Computing Security Protect Policy" International Conference on Intelligence Science and Information Engineering (ISIE), 20-21 Aug. 2011

[74] Tanimoto, S. , Hiramoto, M., Iwashita, M., Sato, H. and Kanai, A., "Risk Management on the Security Problem in Cloud Computing" First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering (CNSI), 2011
[75] Xuan Zhang, Nattapong Wuwong, Hao Li, and Xuejie Zhang, "Information Security Risk Management Framework for the Cloud Computing Environments", 10th IEEE Int. Conf. on Computer and Information Technology (CTI 2010).
[76] Wang, Jen-Sheng, Liu, Che-Hung and Lin, Grace TR, "How to manage information security in cloud computing", IEEE International Conf. on Systems, Man, and Cybernetics (SMC), 9-12 Oct. 2011
[77] Bao Rong Chang, Hsiu Fen Tsai, Zih-Yao Lin and Chi- Ming Chen, "Access Security on Cloud Computing Implemented in Hadoop System", Fifth International Conference on Genetic and Evolutionary Computing (ICGEC), Aug. 29-Sept. 1 2011
[78] Xiaodong Sun, Guiran Chang and Fengyun Li, "A Trust Management Model to Enhance Security of Cloud Computing Environments" Second International Conference on Networking and Distributed Computing (ICNDC), 21-24 Sept. 2011
[79] Mahmood, Zaigham "Data Location and Security Issues in Cloud Computing" International Conference on Emerging Intelligent Data and Web Technologies (EIDWT), 7-9 Sept. 2011
[80] Minrui Jia "Cloud Security of Cloud Computing Application" International Conference on Control, Automation and Systems Engineering (CASE), 30-31 July 2011
[81] Xue Jing and Zhang Jian-jung, "A Brief Survey on the Security Model of Cloud Computing", 9th Int. Symposium on Distributed Computing and Applications to Business, Engineering and Science, 2010.
[82] Hay, B., Nance, K. and Bishop, M., "Storm Clouds Rising: Security Challenges for IaaS Cloud Computing" 44th Hawaii International Conference on System Sciences (HICSS), 4-7 Jan. 2011
[83] Mana, A., Munoz, A. and Gonzalez, J., "Dynamic security monitoring for Virtualized Environments in Cloud computing", 1st International Workshop on Securing Services on the Cloud (IWSSC), 6-8 Sept. 2011
[84] Huang, Chun-Ting, Qin, Zhongyuan and Kuo, C.-C. Jay, "Multimedia storage security in cloud computing: An overview", IEEE 13th International Workshop on Multimedia Signal Processing (MMSP), 17-19 Oct. 2011
[85] Grobauer, B., Walloschek, T. and Stocker, E., "Understanding Cloud Computing Vulnerabilities" IEEE Security & Privacy March-April 2011
[86] Hemant, P., Chawande, N.P., Sonule, A. and Wani, H., "Development of servers in cloud computing to solve issues related to security and backup" IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS), 15-17 Sept. 2011



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY