iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** V **Month of publication:** May 2014

DOI:

www.ijraset.com

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

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

An analysis of current security issues and solutions for cloud computing

Vibha Sahu[1], Brajesh Dubey [2],Dr S.M.Ghosh [3]

[1]*Dr.C.V.RAMAN UNIVERSITY, BILASPUR, INDIA*

PHD SCHOLAR

[2]*DR.C.V.RAMAN UNIVERSITY, BILASPUR, INDIA*

MPHIL SCHOLAR

[3]*RCET, BHILAI(C.G.)INDIA*

ASSO.PROF.

Abstract: ***The progress of cloud computing services is accelerating the rate in which the organizations outsource their computational services or sell their idle computational resources. Even though migrating to the cloud remains attractive trend from a financial perspective, there are several other features that must be considered by companies before they decide to do so. One of the most important part refers to security: while some cloud computing security issues are inherited from the solutions adopted to create such services, many new security questions that are particular to these solutions also arise, including those related to how the services are organized and which kind of service or data can be placed in the cloud. Aiming to give a better understanding of this complex scenario, Here we identify and classify the main security concerns and solutions in cloud computing, and giving an overview of the current status of security in this emerging technology.***

Keywords: ***cloud computing, problems, issues, security.***

1. INTRODUCTION

Security is a key requirement for cloud computing combine as a robust and feasible versatile solution [1]. This view is shared by many distinct groups, academia researchers[2,3], business decision makers [4] and government organizations [5,6]. Many similarities in these viewpoints indicate a grave concern on crucial security and legal obstacles for cloud computing, including service availability, data confidentiality, provider lock-in and status fate sharing [7]. These concerns have their origin not only on existing problems, directly inherited from the adopted technologies, but also related to new issues derived from the work of essential cloud computing features like scalability, resource sharing and virtualization like data leakage and hypervisor weakness. The different between these classes is more easily specialized by analyzing the definition of the essential cloud computing characteristics proposed by the NIST (National Institute of Standards and Technology), which gives the SPI model for services (SaaS, PaaS, and IaaS) and deployment (private, public, community, and hybrid).

Due to the ever growing interest in cloud computing, there is effort to evaluate the current trends in security. An trustworthy reference in this area is the risk assessment developed by ENISA (European Network and Information Security Agency) [5]. It Not only does list risks and vulnerabilities, but it also offers a survey of related works and research suggestions. A equally work is the security guidance provided by the Cloud Security Alliance

(CSA)[6], which defines security domains congregating specific functional aspects from governance and conformity to virtualization and identity management. The main aim of this article is to identify, categorize, organize and quantify the main security concerns and solutions associated to cloud computing. Aiming to organize this information into a useful tool for comparing, relating and classifying already identified concerns and solutions as well as future ones. We discuss not only deeper analysis of the main security frameworks currently available, but also we discuss further the security features related to virtualization in cloud computing, a fundamental yet still underserved field of research.

2. CLOUD COMPUTING SECURITY PROBLEMS

References such as CSA's security guidance and top threats analysis, ENISA's security assessment and the cloud computing definitions from NIST emphasize various security issues related to cloud computing that require further studies for being properly handled and for enhancing technology approval and adoption. Emphasis is given to the difference between services in the form of software (SaaS), platform (PaaS) and infrastructure (IaaS), which are commonly used as the fundamental basis for cloud service categorization. Here we identify the main problems in the area and group them into a model. Every category includes several potential security problems, resulting in a classification with sections.

1. Network security: -

Problems associated with network communications and configurations regarding cloud computing infrastructures. The ideal network security solution is to have cloud services as an extension of customers' existing internal networks [13], adopting the same protection measures and security precautions that are locally implemented and allowing them to extend local strategies to any remote resource or process [14].

(a) Transfer security: Distributed architectures, huge resource sharing and virtual machine (VM) instances synchronization imply more data in transit in the cloud, thus requiring VPN mechanisms for protecting the system against sniffing, spoofing, man-in-the-middle and side-channel attacks.

(b) Firewalling: Firewalls defend the provider's internal cloud infrastructure against insiders and outsiders [15]. They also enable VM isolation, filtering for addresses and ports, prevention of Denial-of-Service(DoS) and detection of external security assessment procedures. Efforts for developing reliable firewall and similar security measures particular for cloud environments [16,17] reveal the advise for adapting existing solutions for this new computing standard.

(c) Security configuration: Configuration of

Protocols, systems and technologies to provide the needed levels of security and privacy without compromising performance or efficiency.

2. Interfaces: -

Focus all issues related to user, administrative and programming interfaces for using and controlling clouds.

(a) API: Programming interfaces (important to IaaS and PaaS) for accessing virtualized

Resources and systems must be protected to stop malicious use [19-23].

(b) Administrative interface: Enables remote

Control of resources in an IaaS (VM management), development for PaaS (coding, deploying, testing) and application tools for SaaS (user access control, configurations).

(c) User interface: End-user interface for

Exploring provided resources and tools (service itself), meaning the need of adopting

Measures for securing the environment [24-27].

(d) Authentication: Mechanism required to enable access to the cloud [28]. Most services rely on regular accounts [20] consequently being susceptible to a plethora of attacks [31-35] whose consequences are boosted by multi-tenancy and resource sharing.

3. Data security:

Protection of data in terms of confidentiality, availability and integrity (which can be applied not only to cloud environments, but any solution requiring basic security levels).

(a) Cryptography: Most employed practice to secure sensitive data [37], required by industry, state and federal regulations [38].

(b) Redundancy: Essential to avoid data loss. Most business models rely on information technology for its core functionalities and processes [39,40] and, thus critical data integrity and availability must be ensured.

(c) Disposal: Elementary data disposal techniques are insufficient and commonly referred as deletion [41]. In the cloud, the complete destruction of data, including log references and hidden backup registries, is an important requirement [42].

4. Virtualization:

Isolation between VMs, hypervisor vulnerabilities and other problems associated to the use of virtualization technologies [43].

(a) Isolation: Although logically isolated, all VMs share the same hardware and consequently the same resources, allowing malicious entities to exploit data leaks and cross-VM attacks [44]. The concept of isolation can also be applied to more fine-grained assets, such as computational resources, storage and memory.

(b) Hypervisor vulnerabilities: The hypervisor is the main software component of virtualization. Even though there are known security vulnerabilities for hypervisors, solutions are still scarce and often proprietary, demanding further studies to harden these security aspects.

(c) Data leakage: Exploit hypervisor vulnerabilities and lack of isolation controls in order to leak data from virtualized infrastructures, obtaining sensitive customer data and affecting confidentiality and integrity.

(d) VM identification: Lack of controls for identifying virtual machines that are being used for executing specific process or for storing files.

(e) Cross-VM attacks: Includes attempts to estimate provider traffic rates in order to steal cryptographic keys and increase chances of VM placement attacks.

5. Governance:

Issues related to (losing) administrative and security controls in cloud computing solutions.

(a) Data control: Moving data to the cloud means losing control over redundancy, location, file systems and other relevant configurations.

(b) Security control: Loss of governance over security mechanisms and policies, as terms of use prohibit customer-side vulnerability assessment and penetration tests while insufficient Service Level Agreements (SLA) lead to security gaps.

(c) Lock-in: User potential dependency on a particular service provider due to lack of well-established standards (protocols and data formats), consequently becoming particularly vulnerable to migrations and service termination.

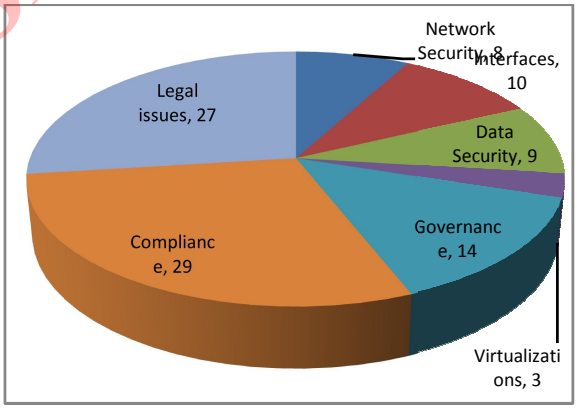


Figure 1 Security problems with grouped categories

6. Compliance:

Includes requirements related to service availability and audit capabilities.

(a) Service Level Agreements (SLA): Mechanisms to ensure the required service availability and the basic security procedures to be adopted [49].

(b) Loss of service: Service outages are not exclusive to cloud environments but are more serious in this context due to the interconnections between services (e.g., a SaaS using virtualized infrastructures provided by an IaaS), as shown in many examples. This leads to the need of strong disaster recovery policies and provider recommendations to implement customer-side redundancy if applicable.

(c) Audit: Allows security and availability assessments to be performed by customers, providers and third-party participants. Transparent and efficient methodologies are necessary for continuously analyzing service conditions and are usually required by contracts or legal regulations. There are solutions being developed to address this problem by offering a transparent API for automated auditing and other useful functionalities.

(d) Service conformity: Related to how contractual obligations and overall service requirements are respected and offered based on the SLAs predefined and basic service and customer needs.

7. Legal issues:

Aspects related to judicial requirements and law, such as multiple data locations and privilege management.

(a) Data location: Customer data held in multiple jurisdictions depending on geographic location are affected, directly or indirectly, by law-enforcement measures.

(b) E-discovery: as a result of law-enforcement measures, hardware might be confiscated for investigations related to a particular customer, affecting all customers whose data were stored in the same hardware. Data disclosure is critical in this case.

(c) Provider privilege: Malicious activities of provider insiders are potential threats to confidentiality, availability and integrity of customers' data and processes' information.

(d) Legislation: Juridical concerns related to new concepts introduced by cloud computing [61].

3. CLOUD COMPUTING SECURITY SOLUTIONS

When analyzing credentials for solutions, we used the same approach mentioned in the beginning of the section. The results are showed in Figure2, which shows the percentage of solutions in each category defined in section "Cloud computing security problems", these concerns are highly relevant but a large number solutions are already available for tackling them. The situation is completely different when we analyze technical aspects such as virtualization, isolation and data leakage.

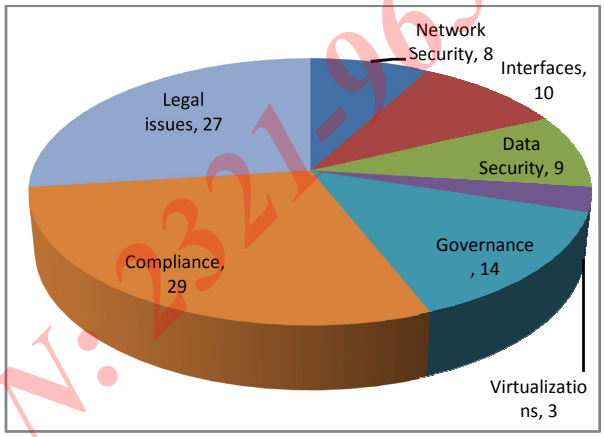


Figure 2 Security solutions with grouped categories

Indeed, virtualization amounts for 12% of problem references and only 3% for solutions. For this specific issue, special care has been taken when assessing the most popular virtual machine solution providers (e.g., XEN, VMWARE, and KVM) aiming to verify their concerns and available solutions. A conclusion from this situation is that such concerns are also significant but yet little is available in terms of solutions. This indicates the need of evaluating potential areas still to be developed in order to provide better security conditions when migrating data and processes in the cloud.

COMPARISON

The differences between problem and solution citations presented in the previous sections can be observed in Figure 3. Axis values correspond to the number of citations found among the references studied. Blue areas represent concern

Citations and lighter red indicates solutions, while darker red shows where those areas overlap. In other words, light red areas

are problems with more citations for solutions than problems, they might be meaningful problems, but there are many solutions already addressing

Them, while blue areas represent potential subjects that have received little attention so far, indicating the need for further studies.

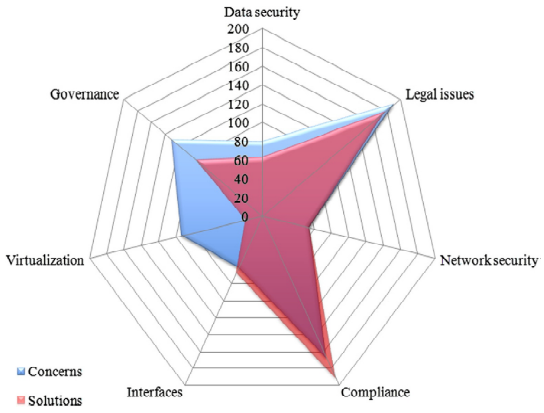


Figure 3 Comparison between citations

The results for grouped categories are showed in Figure3. It shows that virtualization problems represent an area that requires studies for addressing issues such as isolation, data leakage and cross-VM attacks; on the other hand, areas such as compliance and network security cover concerns for which there are already a significant number of solutions or those are not considered highly relevant. Finally, considering virtualization as key element for future studies, five virtualization-related problems: isolation of computational resources, such as memory and storage capabilities, hypervisor vulnerabilities, data leakage, cross-VM attacks and VM identification. The contrast related to isolation and cross-VM attacks is more evident than for the other issues. However, the number of solution citations for all issues is notably low if compared to any other security concern, reaffirming the need for further researches in those areas.

4. CONCLUSION

Considering the points raised in the previous section, a straightforward conclusion is that cloud security includes many old and well-known issues – such as network and other infrastructural vulnerabilities, user access, authentication and privacy – and also new concerns derived from new technologies adopted to offer the sufficient resources (mainly virtualized ones), services and auxiliary tools. These problems are summarized by isolation and hypervisor vulnerabilities (the main technical concerns according to the studies and graphics presented), data location and e-discovery (legal aspects), and loss of governance over data, security and even decision making (in which the cloud must be strategically and financially considered as a decisive factor). Another point observed is that, even though adopting a cloud service or provider may be easy, migrating to another is not. After moving local data and processes to the cloud, the lack of standards for protocols and formats directly affects attempts to migrate to a different provider even if this is motivated by legitimate reasons such as non-fulfillment of SLAs, outages or provider bankruptcy. Consequently, the first choice must be carefully made, as SLAs are not perfect and services outages happen at the same pace that resource sharing, multi-tenancy and scalability are not fail proof. After a decision is made, future migrations between services can be extremely difficult in terms of time and costs; this task will require a broad work for bringing all data and resources to a local infrastructure before redeploying them into the cloud. Finally, the analysis of current trends for cloud computing reveals that there is a considerable number of well studied security concerns, for which plenty solutions and best practices have been developed, such as those related to legal and administrative concerns. On the other hand, many issues still require further research effort, especially those related to secure virtualization.

5. FUTURE SCOPE

Security is a crucial aspect for providing a reliable environment and then enables the use of applications in the cloud and for moving data and business processes to virtualized infrastructures. Many of the security issues identified are observed in other computing environments: authentication, network security and legal requirements. However, the impact of such issues is intensified in cloud computing due to characteristics such as multi-tenancy and resource sharing, since actions from a single customer can affect all other users that inevitably share the same

resources and interfaces. On the other hand, efficient and secure virtualization

represents a new challenge in such a context with high distribution of complex services and web based applications, thus requiring more sophisticated approaches. At the same time, our quantitative analysis indicates that virtualization remains an underserved area regarding the number of solutions provided to identified

Concerns. It is strategic to develop new mechanisms that provide the required security level by isolating virtual machines and the associated resources while following best practices in terms of legal regulations and compliance to SLAs. Among other requirements, such solutions should employ virtual machine identification, provide an adequate separation of dedicated resources combined with a constant observation of shared ones, and examine any attempt of exploiting cross-VM and data leakage. A secure cloud computing environment depends on several security solutions working harmoniously together. However, in our studies we did not identify any security solutions provider owning the facilities necessary to get high levels of security conformity for clouds. Thus, cloud providers need to orchestrate / harmonize security solutions from different places in order to achieve the desired security level. We learned that Amazon changed the XEN source code in order to include security features, but unfortunately the modified code is not publicly available and there appears to be no article detailing the changes introduced. Given these limitations, a deeper study on current security solutions to manage cloud computing virtual machines inside the cloud providers should be a focus of future work in the area. Working on a testbed based on OpenStack for researches related to identity and credentials management in the cloud environment. This work should address basic needs for better security mechanisms in virtualized and distributed architectures, guiding other future researches in the security area.

6. REFERENCES:

1. IDC (2009) Cloud Computing 2010 –Update.

slideshare.net/JorFigOr/cloud-computing-2010-an-idc-update

2. Armbrust M, Fox A, Griffith R, Joseph AD, Katz RH, Konwinski A, Lee G, Patterson DA, Rabkin A, Stoica I, Zaharia M (2009) Above the Clouds: A Berkeley View of Cloud Computing. Technical Report UCB/EECS-2009-28, niversity of California at Berkeley, eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html

3. Rimal BP, Choi E, Lumb I (2009) A Taxonomy and, Survey of Cloud Computing Systems. In: Fifth International Joint Conference on INC, IMS and IDC, NCM ’09, CPS. pp44–51

4. Shankland S (2009) HP’s Hurd dings cloud computing, IBM. CNET News

5. Catteddu D, Hogben G (2009) Benefits, risks and recommendations for information security. European Network and Information Security Agency,enisa.europa.eu/act/rm/files/deliverables/cloudcomputing-risk-assessment

6. CSA (2009) Security Guidance for Critical Areas of Focus in Cloud Computing.

7. Mather T, Kumaraswamy S (2009) Cloud Security and privacy: An Enterprise Perspective on Risks and Compliance.1st edition. O’Reilly Media

8. Chen Y, Paxson V, Katz RH (2010) What’s New About Cloud Computing Security? Technical Report UCB/EECS-2010-5,University of California at Berkeley,eecs.berkeley.edu /Pubs/TechRpts/2010/EECS-2010-5.html

9. Mell P, Grance T (2009) The NIST Definition of Cloud Computing. Technical Report 15, National Institute of Standards and Technology,

www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf

10. Ibrahim AS, Hamlyn-Harris J, Grundy J (2010) Emerging Security Challenges of Cloud Virtual Infrastructure. In: Proceedings of APSEC 2010 Cloud Workshop, APSEC ’10

11. Gonzalez N, Miers C, Red´ıgolo F, Carvalho T, Simpl´ıcio M, Naslund M, Pourzandi M (2011) A quantitative analysis of

current security concerns and solutions for cloud computing. In: Proceedings of 3rd IEEE CloudCom. Athens/Greece: IEEE Computer Society

12. Hubbard D, Jr LJH, Sutton M (2010) Top Threats to Cloud Computing. Tech. rep., Cloud Security Alliance. cloudsecurityalliance.org/ research/projects/top-threats-to-cloud-computing

13. Tompkins D (2009) Security for Cloud-based Enterprise Applications.

http://blog.dt.org/index.php/2009/02/security-for-cloud basedenterprise- applications/

14. Jensen M, Schwenk J, Gruschka N, Iacono LL (2009) On Technical Security Issues in Cloud Computing. In: IEEE Internation Conference on Cloud Computing. pp 109–116

15. TrendMicro (2010) Cloud Computing Security - Making Virtual Machines Cloud-Ready. Trend Micro White Paper

16. Genovese S (2009) Akamai Introduces Cloud-Based Firewall. cloudcomputing.sys-on.com/node /1219023

17. Hulme GV (2011) CloudPassage aims to ease cloud server security management. http://www.csoonline.com/article/658121/cloudpassageaims-to-ease-cloud-server-security-mgmt

18. Oleshchuk VA, Køien GM (2011) Security and Privacy in the Cloud – A Long-Term View. In: 2nd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology (Wireless VITAE), http://dx.doi.org /10.1109/WIRELESSVITAE.2011.5940876

19. Google (2011) Google App Engine. code.google. com/appengine

20. Google (2011) Google Query Language (GQL). code.google.com/intl/en/appengine/docs/python/overview.html

21. StackOverflow (2011) stackoverflow.com/questi ons/1823536/does-using-non-sql-databasesobviate-the-need-for-guarding-against-sql-injection22. Rose J (2011) Cloudy with a chance of zero day. www.owasp.org/images/1/12/Cloudy with a chance of 0 day Jon Rose-Tom Leavey.pdf

23. Balkan A (2011) Why Google App Engine is broken and what Google must do to fix it. aralbalkan.com/1504

24. Salesforce (2011) Salesforce Security Statement. salesforce.com/company/privacy/security.jsp

25. Espiner T (2007) Salesforce tight-lipped after phishing attack. zdnet.co.uk/news/security-threats/2007/11/07/salesforce-tight-lipped-after-phishing-attack-39290616/

26. Yee A (2007) Implications of Salesforce Phishing Incident. ebizq.net/blogs/securityinsider /2007/11/-implications of salesforce phi.php

27. Salesforce (2011) Security Implementation Guide.login.salesforce.com/help/doc/en/salesforce security impl guide.pdf

28. Li H, Dai Y, Tian L, Yang H (2009) Identity-Based Authentication for CloudComputing. In: Proceedings of the 1st International Conference on CloudComputing, CloudCom ’09

29. Amazon (2011) Elastic Compute Cloud (EC2). aws.amazon.com/ec2/

30. Kaufman C, Venkatapathy R (2010) Windows Azure Security Overview.

31. McMillan R (2010) Google Attack Part of Widespread Spying Effort.PCWorld

32. Mills E (2010) Behind the China attacks on Google. CNET News

33. Arrington M (2010) Google Defends Against Large Scale Chinese Cyber Attack

34. Bosch J (2009) Google Accounts Attacked by Phishing Scam. BrickHouse Security Blog

35. Telegraph T (2009) Facebook Users Targeted By Phishing Attack. The Telegraph

36. Pearson S (2009) Taking account of privacy when designing cloud computing services. In: Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, CLOUD ’09

37. Musthaler L (2009) Cost-effective data encryption in the cloud. Network World

38. Yan L, Rong C, Zhao G (2009) Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based

Cryptography. In: Proceedings of the 1st International Conference on Cloud Computing, CloudCom ’09

39. Tech C (2010) Examining Redundancy in the Data Center Powered by the Cloud and Disaster Recovery. Consonus Tech

40. Lyle M (2011) Redundancy in Data Storage. Define the Cloud

41. Dorion P (2010) Data destruction services: When data deletion is not enough. SearchDataBackup.com

42. Mogull R (2009) Cloud Data Security: Archive and Delete (Rough Cut).

securosis.com/blog/cloud-data-security-archive-and-delete-rough-cut/

43. Messmer E (2011) Gartner: New security demands arising for virtualization, cloud computing. http://www.networkworld.com/news/

2011/062311-security-summit.html

44. Ristenpart T, Tromer E, Shacham H, Savage S (2009) Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds.

In: Proceedings of the 16th ACM conference on Computer and communications security, CCS ’09. New York, NY, USA, ACM, pp 199–212,

doi.acm.org/10.1145/1653662.1653687

45. Chow R, Golle P, Jakobsson M, Shi E, Staddon J, Masuoka R, Molina J (2009) Controlling data in the cloud: outsourcing computation without outsourcing control. In: Proceedings of the 2009 ACM workshop on,

Cloud computing security, CCSW ’09. New York, NY, USA, ACM, pp 85–90,

http://doi.acm.org/10.1145/1655008.1655020

46. Sadeghi AR, Schneider T, Winandy M (2010) Token-Based Cloud Computing - Secure Outsourcing of Data and Arbitrary Computations

with Lower Latency. In: Proceedings of the 3rd international conference on Trust and trustworthy computing, TRUST ’10

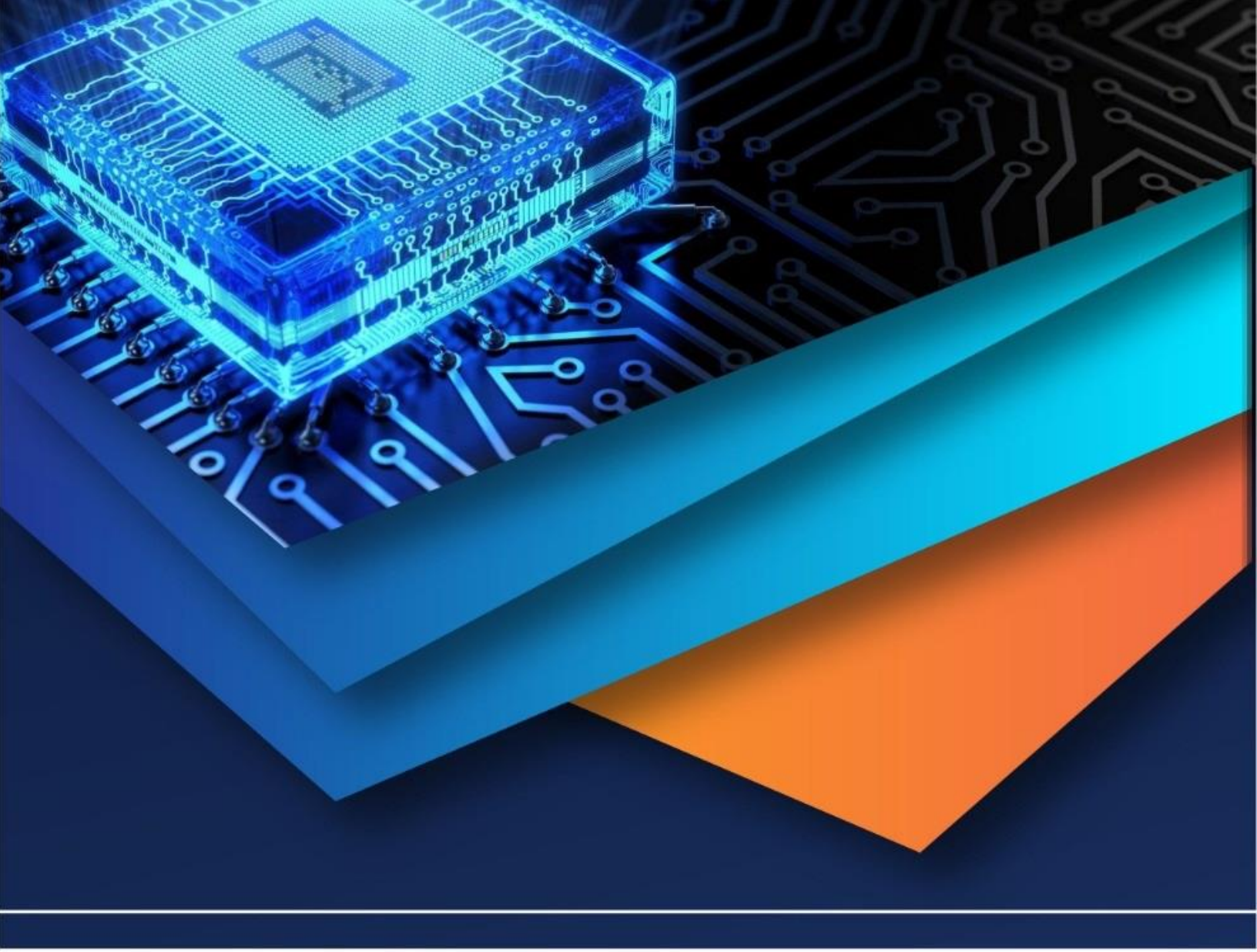
47. Brandic I, Dustdar S, Anstett T, Schumm D, Leymann F (2010) Compliant

Cloud Computing (C3): Architecture and Language Support for User-driven Compliance Management in Clouds. In: 2010 IEEE 3rd International Conference on Cloud Computing. pp 244–251, http://dx.

doi.org/10.1109/CLOUD.2010.42

48. Brodkin J (2008) Gartner: Seven cloud computing security risks. http://

www.infoworld.com/d/security-central/gartner-seven-cloudcomputing-security-risks-853.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY