iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** XII **Month of publication:** December 2018

DOI:

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 XII, Dec 2018- Available at www.ijraset.com

Highlighting the Vital Cypher by Means of Forming Insight about Cloud Computing through Virtualization

Vikash. S[1], Praveen. T[2], Anita. P[3], Suganya. V[4], Reshmi. S[5]
[1, 2, 3, 4]*Student, Department of Computer Science and Applications, Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India.*
[5]*Faculty, Department of Computer Science and Applications, Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India.*

***Abstract:** Cloud computing is the next generation for augmentation of technology which going to rule entire world in engaged factor. It is one of the best growing technologies among all other sectors where user can able to access the data from anywhere and at any time easily. Virtualization is another tie-up in cloud computing resources to develop the virtual perception or version of a resource which is sub-divided as independent environment. Being a developing factor, apart from its successor it also faces many challenging situations to make the usage wider. This paper deals with ideology of virtualization concept in computing.*
***Keywords:** cloud computing, virtualization, hypervisor, IAAS, PAAS, and SAAS.*

I. INTRODUCTION

Cloud computing is the progressed version of parallel computing, distributed computing, grid computing and virtualization technology which describe the outline of a new era. Cloud computing services are first presented by Amazon, Google, and Microsoft and now many other new business firms were evolved. It is emerging rapidly and no doubt it is the next cohort technology where humans will be using it anywhere and at any time. Cloud computing is the basic change occurring in the arena of IT. Virtualization is the keystone of cloud computing. Virtualization in cloud computing brings about great challenges in the field of data privacy protection. By using the virtualization, we get more flexible and capable allocation of resources. Today the IT world is look forward for the services provided by the cloud computing. It is a common term for anything that includes conveying facilitated services over the internet. Marc Benioff, the founder of sales force highlighted that “The cloud services companies of all sizes...The cloud is for everyone. The cloud is a democracy.” Cloud computing term became “popular some time in OCT 2007 when IBM and Google announced collaboration in that domain. This was followed by IBM’s announcement of the “Blue cloud” effort. Since then, one and all are talking about “cloud computing”. Of course, there is also the certain Wikipedia entry.

This journal highlights the perception of “virtualization in cloud computing”- some of the issues it tries to address, associated research topics, and a “cloud” implementation available today.

II. CLOUD COMPUTING

Cloud computing is an online data storage unit which can be manipulated, accessed, retrieved and configured. It is a computing environment in which large amount of data is stored in a large pool either public pool or private pool from which the user can access the file or data. Cloud computing is a direct approach to cost beneficial services around the world using the IT principle of reusability.

A. Layout

Cloud computing architecture is configured into three layers they were

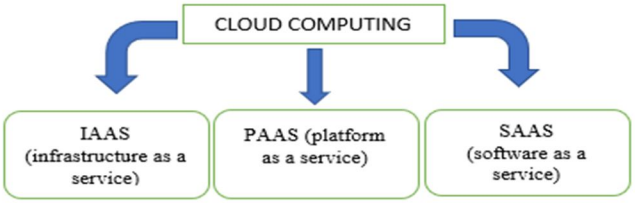


Figure1. Cloud computing layers

Our browser and application run on the top these layers hosted in a cloud environment.

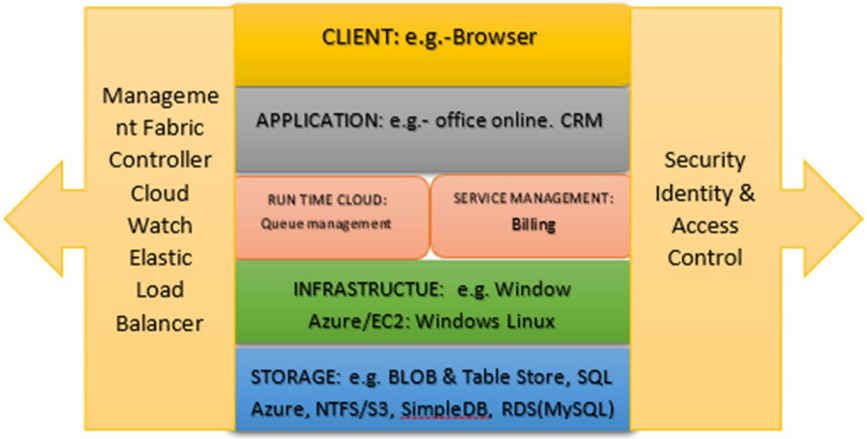


Figure2. Client level computing

Cloud computing comprises both the front end and back end.

1) The mobile phones are the PCs which are visible to the end user are called front end.

2) The software and the data storage units which are hidden by the end user are called back end.

Cloud architecture comprises of various technologies, layers, components, deployment models and other essentials.

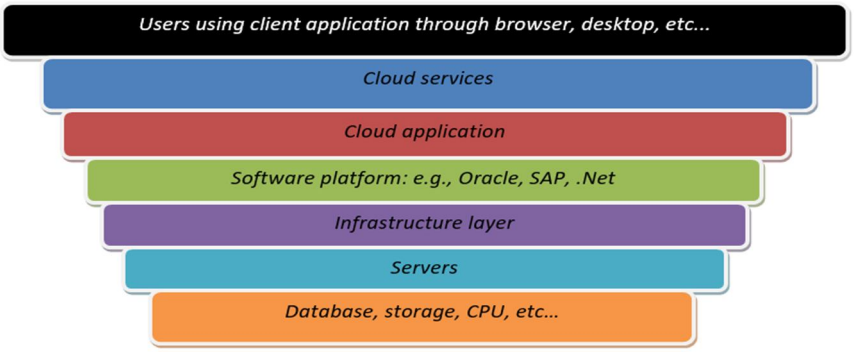


Figure3. Elements in cloud architecture

III. VIRTUALIZATION

Virtualization was invented around 1960's by the IBM. It is an innovative technology inkling which has ability to run in multiple operating systems and share the under lying hardware resources. In other words, virtualization is the process by which one computer have ability to host several other computers virtually. The virtual machine and server is facilitated by software known as "hypervisor". It acts as a link between the hardware and resources such as CPU usage regarding memory allotment. Virtualization is available for a wide range of technologies and is also an open source.

A. Strategy of Virtualization

Types of virtualization architecture include:

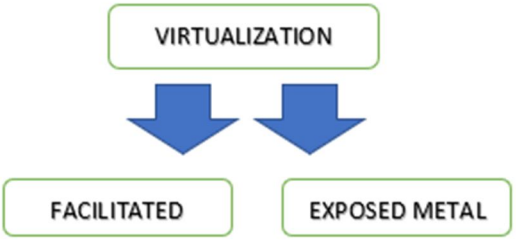


Figure4. Virtualization categories

Operating system (OS) acts as an interface between the hardware and the software. So, in the facilitated architecture, OS must be installed in the hardware and formerly software called hypervisor (i.e. virtual machine screen) ought to be introduced on the hardware. This helps to install different operation framework in the equipment. Now virtual machine seems to run like a normal physical machine by running all the applications. Here hypervisor can directly can able to communicate with the equipment for working with the operation framework because of its uncovered metal design. Instead in the exposed metal, the working framework communicates only with hypervisor. But both the virtualization architecture, use data center as the medium of storing information. Thus, facilitated virtualization architecture technique is considered as most useful improvement of the program level, running legacy operation and it support different operating systems.

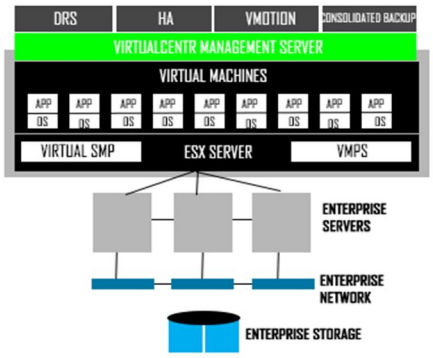


Figure5. Virtualization management server

B. Various Techniques Involved In Virtualization

1) *Full Virtualization Technique:* Full virtualization is designed to hide the physical work of the machine and other logical phase from the user and allows and the process in the virtual framework. The application doesn't know that the process is undertaken in the virtual environment, so they do the process like the process of the physical machine. This helps to run the program as usual and it provides complete isolation of various applications to high security. Examples are Microsoft Virtual Server (virtual PC) and VMware ESX server Software
2) *Para-Virtualization Technique:* Para-virtualization is the process of working with the virtual machine where the hidden hardware is similar and not identical to the physical hardware. Here change in operating system is required to run application in the virtual environment. Hypervisor software helps to provide alternate version of the physical machine. It helps to gives user defined execution of the output unlike the full virtualization. Para-virtualization is mainly utilized by Xen, Denali, VMware ESX Server and Linux.
3) *Application Virtualization Technique:* In application virtualization, a server application can run by client locally by utilizing the available local resources. Such virtualization resources are kept running in small virtual environment containing essentials to execute the essentials. In Application virtualization all the clients have default attached to the application environment virtually.
4) *Resource Virtualization Technique:* Resource virtualization directs to storage volumes, name spaces and the network resources. There are different ways in dealing with resource virtualization they are: combining enormous individual's segments into bigger resource pool. Cluster computers are other means of hardware to frame the super computers with large amount of resources.
5) *Storage Virtualization Technique:* Storage virtualization is a form of resource virtualization in which storage is made by collecting all the physical storage resources that are scattered over the system and then it helps to structures the logical storage. Logical storage aggregates the scattered physical resources into single storage device to the users.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue XII, Dec 2018- Available at www.ijraset.com

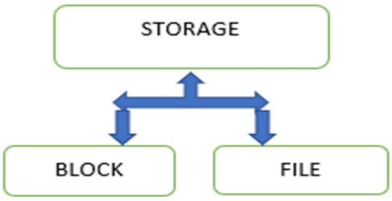


Figure6. Storage space

6) *Desktop Virtualization Technique:* Desktop virtualization comprises of all the essentials of an operating systems and their applications and client information from hidden end user.

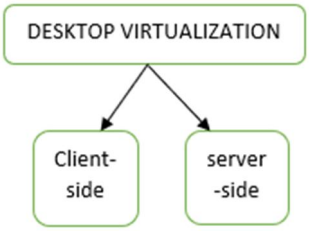


Figure7. Desktop virtualization faces

In server-side applications are executed remotely from the central server through Remote Display Protocol.

7) *Network Virtualization Technique:* Network virtualization was accomplices by three technologies:

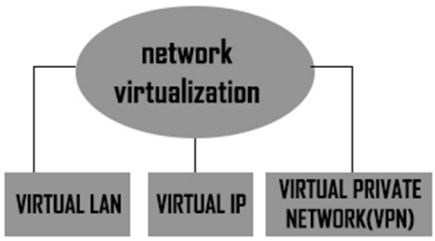


Figure8. Network technologies

Network virtualization is contained an arrangement of advances of the system and isolates it into small executable parts. In network virtualization large number of system can be connected into a single network or it can be sub divided into smaller units.

IV. VIRTUALIZATION FEATURES IN CLOUD COMPUTING

Virtualization in cloud computing is the process making both the hardware, software, OS, storage space or some other network devices into virtual objects. IT enterprises are responsible for these virtual objects. They daily manage the changes occurring in the virtual objects than in the physical environment and rectify the problem encountered by the users. Virtual clouds are scalable (easy to change) and agile (move quickly and easily). Cloud computing can be used without virtualization concept, but it is inefficient and difficult to use. As cloud computing theme is “pay-as-use” and “infinite” virtualization concept is implemented into cloud computing.

A. Benefits of virtualization in cloud computing:

Cloud computing is dependent on virtualization for easier management of resources. Main advantages are that it can able to manage all the resources in a single hosting environment. Virtualization leads to increase in the security level in cloud computing. It helps in resource sharing and reduces managing cost in recent trends. Virtual resources face server crisis on managing and data monitoring. it plays a major role in providing an availability for the challenging issues provided by cloud. Virtual portioning capabilities are assisted by the software called hypervisor which directly runs on the hardware.

B. Security Outbreaks Violated In Virtualization In Cloud Computing

Cloud computing is main part of a business firm. Many hackers were developed to destroy the good progress of a well-developed corporate sector. Security attack is used to violate the normal cloud functioning. There were many attacks employed by the hackers to disturb the cloud data from the user.

1) *Denial of Service Attack (DOS):* In DOS attack the valid user is not able to get the data stored in the cloud. The hacker requests more and more invalid information from the cloud with invalid address while the cloud server is busy in processing the invalid information from the hacker. The valid user request is paused while the server is busy with the invalid request from the hacker. It is the DOS attack. This attack is also known as driven by downloading or data spoofing attack.
2) *Malware Injection Attack:* In malware injection attack the hacker creates a malware or threat which looks as such as an existing cloud information. While the user tries to get the proper information from the cloud, unknowingly the malware code created by the attacker gets downloaded. It is the malware injection attack.
3) *Wrapping Attack:* In wrapping attack, the hacker inserts the malware or malicious element in SOAP (Simple Object Access Protocol) message structure in Transport Layer Service (TLS). After inserting the malware, the message is copied to the original cloud server interrupting the cloud service. This is called wrapping attack.
4) *Flooding Attack:* In flooding attack without problems, it is using to create fake data and whenever the server is stuffed, and it allocates the job to the nearest server and specific server to become offloading. While handling the requests, server first validates the authority of the requested requests. The authenticity must be validated by the invalid requests and the flooding of the system caused by the memory allocation and checks by the CPU utilization.
5) *Data Stealing Attack:* Data stealing attack is used to verify the user account in traditional approach. The information for user account and password are steeled by the data stealing attack. In this attack, the challenger of activity has been departed by the user about the confidential information.
6) *Side Channel Attack:* In side channel attack, by inserting malicious adjacent a target cloud server system to compromise the cloud system. This attacker targeting the system implementation of cryptographic algorithms and it has an effective security. To evaluating these systems, it is significant for secure system design to side channel attacks for flexibility. Side Channel attack makes use of two steps to attack: VM CO-Residence and VM Extraction. VM CO-Residence is a placement item attacker can often place as a target occasion on the same physical machine and VM Extraction is to find out in sequence about co-resident instances.
7) *Authentication Attack:* Authentication is a virtual service and frequently targeted and hosted in a pathetic issue. The authentication processes are protected by the mechanisms and the methods and are mostly targeted by the attackers. The architecture of cloud computing consists of IaaS, SaaS and Paas. In IaaS to find out the sequence protection and data encryption confidentially by the transmitted data. The data communication is the most suitable and possible solution for the cloud computing. The management of data belonged to the service provider's necessity be authorized by the enterprises as a replacement for the service providers.

C. Remedial Keys

1) *Dos Attack:* DOS attack can be prevented with the help of the prior automated switches which analysis the packet rate flow. This attack mainly states the traffic happened due to both authorized and unauthorized users at the same time. At the mean state firewalls can be introduced to deny the access protocol if a simple attack coming from the unusual IP addresses. By using switches, we can able to limit the rate limit of the packet inspection and filtering them. Similarly, routers can also be used for limiting the packet rate. Due to DOS attack there is flood of data provided in routers. There are two concepts included for solving DOS attack, they are:

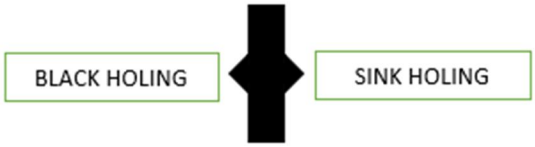


Figure9. Remedial measures for DOS attack

a) *Black Holing:* to make the process more efficient and to avoid network infrastructure attack all the packets in the traffic are sent here.

b) Sink Holing: it helps to rote only valid IP addresses, but it can able to manage the serious server-side attacks.

2) *Malware Injection Attack:* To prevent malware injection, attack the user is allowed create an account in cloud and the server creates a virtual machine (VM) image in cloud storage system. File allocation table helps to determine the current code executed by the user and simultaneously file integrity is also maintained. So that the user accesses the same cloud data server check for the previously stored virtual image for the confirmation and provides the original data.

3) *Wrapping Attack:* For presentation of wrapping attack increase in the security of the message is necessary to prevent from malware. An additional bit called STAMP bit is included in the signature value and included in SOAP header to prevent the attacker by changing the signature value by using the method called XML signature wrapping.

4) *Flooding Attack:* For flooding attack message passing technique is used which helps to easy communication between the servers. When the server is overloaded it employees a new server which contains the destination request of the overloaded server and PID is used to find the valid requests from the customers and it is encrypted with the help of hash value implementation.

5) *Data Stealing Attack:* Data stealing attack can be prevented by providing a unique id to the customers at the time of logging in to use the system. When the session gets expired, PID generators help to commit the task which is stored inside the hypervisor.

6) *Side Channel Attack:* In side channel attack, it can able to access the secret information/data from the hardware very easily. So that security level should be gained up in cloud computing to prevent the side channel attack. This can be enhanced with the help of introducing virtual firewall appliance and random encryption-decryption combination to tighten the security level in front-end and back-end of the could computing architecture. This combination process is followed in banking sectors to avoid side channel attacks.

7) *Authentication Attacks:* The common factors among the people are creating simple username and pass code of knowledge-based authentication. Instead if the pass code is created based upon exception of some financial institutes, so that the authentication of data can be processed on behalf of the enterprise but that belongs to user side server providers. Thus, this helps to make it little complicated for the phishing attacks.

V. CONCLUSION

We have completed the new wave in the computer field “virtualization in cloud computer”. This will turn the leaf of our lives in the trivial future. In the cloud computing helps to identify the problems and its resources are ubiquitous, scalable, highly virtualized. In virtualization technology the virtual servers could lead to complete revolution in the computing industry. We discuss the security challenges and benefits and futures of cloud computing. This concept provides a brand-new occasion for the evolution of mobile application and to retain a very thin layer for user application. The solution to this will become apparent.

REFERENCES

[1] Reshmi. S, and M. Anand Kumar, “A REVIEW ON OBFUSCATION AND HEURISTICS ALGORITHM IN NETWORK VIRTUALIZATION”, International Journal of Advanced Research in Computer Science, IJARCS & ISSN No. 0976-5697, Volume 8 (8), Sep-Oct 2017, Pg. : 264-268, DOI: http://dx.doi.org/10.26483/ijarcs.v8i8.4651.

[2] Reshmi. S, Kritika. B and Deepa. B, “SHIELDING NETWORK VIRTUALIZATION USING CBC-MAC FOR IMMINENT INTERCONNECTED NETWORKS”, International Journal of Computer Science and Mobile Applications, IJCSMA & ISSN: 2321-8363, Impact Factor: 4.123, Volume 5 (10), Oct 2017, pg.: 123-130.

[3] Reshmi. S, and M. Anand Kumar, “IMPLEMENTATION ON IDENTIFYING PACKET MISBEHAVIOR IN NETWORK VIRTUALIZATION”, ARPN Journal of Engineering and Applied Sciences & ISSN 1819-6608, VOL. 13, NO. 4, 20th February 2018, Pg: 1284-1296. [4]. M. Anand Kumar, Dr. S. Karthikeyan (2011), “Security Model for TCP/IP Protocol Suite”, Journal of Advances in Information Technology, 2[2], 87-91.

[4] M. Anand Kumar and Dr. S. Karthikeyan (2012),” Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms” International Journal of Computer Network and Information Security”, 4[2]: 22-28

[5] M. Anand Kumar and Dr. S. Karthikeyan 2012),” A New 512 Bit Cipher - SF Block Cipher” International. Journal of Computer Network and Information Security”, 4[11]:55-61.

[6] Dr. M. Anand Kumar. And Dr. S. Karthikeyan (2013),” An Enhanced Security for TCP/IP Protocol Suite” International Journal of Computer Science and Mobile Computing, 2[11]:331-338.

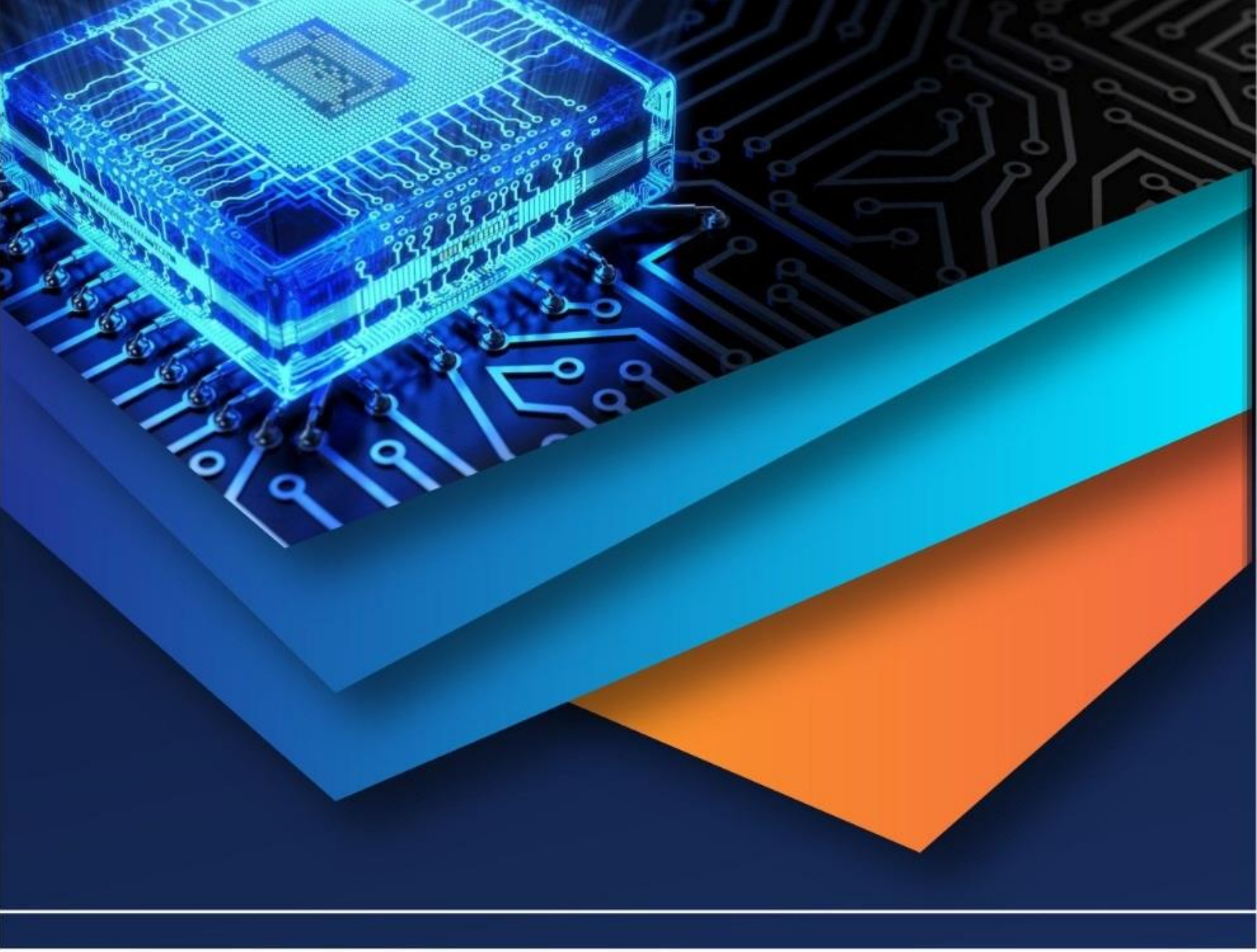
[7] Manar Jammala, Taranpreet Singh, Abdallah Shami, RasoolAsal, Yiming Li, “Software-Defined Networking: State of the Art and Research Challenges”, Elsevier’s Journal of Computer Networks, October 2014, 72(1), Doi no: 10.1016/j.comnet.2014.07.004.

[8] Munoz-Arcentales Jose, Zambrano-Vite Sara, Marin-Garcia Ignacio, “Virtual Desktop Deployment in Middle Education and Community Centers Using Low-Cost Hardware”, International Journal of Information and Education Technology, 2013 December, 3(6), Doi no: 10.7763/IJIET. 2013. V3.355.

[9] Mohamed Ali Kaafar, Laurent Mathy, Thierry Turletti, Walid Dabbous, “Real attacks on virtual networks: Vivaldi out of tune”, In Proceedings of the SIGCOMM workshop on Large Scale Attack Defense LSAD, 2006 September, 1(1), Doi no: 10.1145/1162666.1162672.

[10] A. J. Younge, R. Henschel, J. T. Brown, G. von Laszewski, “Analysis of Virtualization Technologies for High Performance Computing Environments”, Cloud Computing (CLOUD), 2011 IEEE International Conference, 2011 July, 1(1), Doi no: 10.1109/CLOUD.2011.29.

[11] Ali Dorri and Hamed Nikde, "A new approach for detecting and eliminating cooperative black hole nodes in MANET", Information and Knowledge Technology (IKT), 7th Conference onIEEE, 2015.
[12] Pooja and Chauhan. R. K, "An assessment-based approach to detect black hole attack in MANET", Computing, Communication & Automation (ICCCA), 2015 International Conference on. IEEE, 2015.
[13] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, Yoshiaki Nemoto, "Detecting Black hole Attack on AODV based Mobile Ad hoc networks by Dynamic Learning Method", International Journal of Network Security, 2007 Nov,5(3), Doi no: 10.1.1.183.2047.
[14] Anand A. Aware and Kiran Bhandari, "Prevention of Black hole Attack on AODV in MANET using hash function", Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), 3rd International Conference on IEEE, 2014.
[15] Kriti Patidar and Vandana Dubey, "Modification in routing mechanism of AODV for defending blackhole and wormhole attacks", IT in Business, Industry and Government (CSIBIG), 2014 Conference on IEEE, 2014.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY