iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** IV **Month of publication:** April 2018

DOI: http://doi.org/10.22214/ijraset.2018.4378

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 IV, April 2018- Available at www.ijraset.com

An Optimized Approach to Handle DDOS Attack on Cloud Network

Rajni Garg
Computer Science, Guru Nanak College, Moga

Abstract: ***The cloud computing is happening technology which is most commonly used now days. As more and more users are accessing the cloud the cloud security is under danger. In order to resolve the problem the security mechanism within the cloud has to be implemented. Cloud is prone to number of attacks. Most common attack over the cloud is DDOS. It is distributed Daniel of service. The main operation of the DDOS is to block the resources which are present over the cloud. The cloud computing will depend over the sensors. The sensors have very limited memory. In order to resolve the problem proposed work is suggested. In existing system measures are not taken in order to prevent the attack or to resolve the problem permanently. In the proposed system using cloud sim tool, White List will be maintained that indicate the services which are required within system. The services which are not in the white list will be blocked.***
Keyword: DDOS, cloud computing, cloud SIM, Mobile Cloud Computing

I. INTRODUCTION

A Distributed denial of service (DDOS) attack is a DOS attack utilizing multiple distributed attack sources. Typically, the attackers use a large number of controlled bots distributed in different locations to launch a large number of DOS attacks against a single target or multiple targets. With the rapid development of bot nets in recent years, the attack traffic scale caused by DDOS attacks has been increasing, with the targets including not only business servers, but also internet infrastructures such as firewalls, routers and DNS system as well as network bandwidth, the attack influence sphere has also become broader. The remainder of this paper is organized as follows. We are also describes variety of available DDOS algorithms.

Cloud computing provides a wide range of computing resources from servers and storage to enterprise applications. Cloud computing is a hosting environment that is immediate, flexible, scalable, secure and available. The computing resources from cloud can be easily and quickly accessed and released after use with very less management effort. The concept of Cloud Computing can be used in mobile applications running on SMDs to boost up their performance. With the integration and support of Cloud Computing into the complex mobile applications, the term Mobile Cloud Computing (MCC) arises.

A. Cloud and Services Provided

The cloud computing is one of the most commonly used technology. The cloud is used in order take a backup of the data which is used in case of mobiles and other devices. As cloud is exposed to more and more users, the security is becoming a issue. There exist data centers in case of the cloud. The data center is the one which is going to provide the resources to the user. the work load is distributed in case of cloud. This is known as Load Balancing. In case of Load Balancing the load will be equally distributed among the large number of data centers. No data center will going to get partial load. If data center goes down it is possible to ensure that work is not going to be stopped. The work will be continuously down through the other centers. In cloud computing load balancing will ensure that one resource is not overwhelmed or underutilized. The architecture of cloud will involve the following layers

B. Cloud Service Model

Cloud computing is a delivery of computing where massively scalable IT-related capabilities are provided —as a service across the internet to numerous external clients. This term effectively reflects the different facets of the Cloud Computing paradigm which can be found at different infrastructure levels.

Cloud Computing is broadly classified into three services: —"IaaS", "PaaS" and "SaaS". Cloud Computing have some different utility services.

The various service models are as follows:

1) *IaaS (Infrastructure as a service) model:* IaaS is the delivery of technology infrastructure as an on demand scalable service. The main concept behind this model is virtualization where user have virtual desktop and consumes the resources like network, storage, virtualized servers, routers and so on, supplied by cloud service provider. . Usage fees are calculated per CPU hour,

data GB stored per hour, network bandwidth consumed, network infrastructure used per hour, value added services used, e.g., monitoring, auto-scaling etc. Examples: Storage services provided by AmazonS3, Amazon EBS. Computation services: AmazonEC2, Layered tech and so on.

2) *PaaS (Platform as a service) model:* It refers to the environment that provides the runtime environment, software deployment framework and component on pay to enable the direct deployment of application level assets or web applications. PaaS is a platform where software can be developed, tested and deployed. It means the entire life cycle of software can be operated on a PaaS. This service model is dedicated to application developers, testers, deployers and administrators. Examples: Google App Engine (GAE), Microsoft Azure, IBM Smart Cloud, Amazon EC2, salesforce.com and jelastic.com and so on.
3) *SaaS (Software as a service):* SaaS is a model of software deployment where an application is hosted as a service provided to customers across the Internet. Through this service delivery model end users consume the software application services directly over network according to on-demand basis. For example, Gmail is a SaaS where Google is the provider and we are consumers.

C. Cloud Security

In spite of its popularity, however, cloud computing has raised a range of significant security and privacy concerns which hinder its adoption in sensitive environments. The transition to cloud computing model exacerbate security and privacy challenges, mainly due to its dynamic nature and the fact that in this model hardware and software components of a single service span multiple trust domains. In the cloud, data and services are not restricted within a single organization's perimeter. This dynamism of data introduces more risk and complicates the problem of access control.

Therefore, compared with the traditional models, in cloud computing model ensuring confidentiality and integrity of the end-users' data is far more challenging. Moreover, cloud services are usually multi-tenancy services, meaning that a single infrastructure, platform, or software provides its services to multiple mutually untrusted parties simultaneously. Therefore, confidentiality of these parties' data need to protected against each other. However, in some cases these parties may want to collaborate and share some data with each other in a controlled manner and thus there should be a mechanism that allows them to collaborate. Layered architecture of cloud computing requires different levels of security considerations. In this work we are mainly concerned with the problem of identity management and access control in application and service level. We introduce a set of multi-party protocols specifically designed for cross-domain integrated cloud services. The main objective of these protocols is to provide more visibility and control to the end-user and close the gap between capabilities of existing solutions and new requirements of cloud based requirements.

Even though, the virtualization and Cloud Computing delivers wide range of dynamic resources, the security concern is generally perceived as the huge issue in the Cloud which makes the users to resist themselves in adopting the technology of Cloud Computing. Some of the security issues in the Cloud are discussed below:

1) *Integrity:* Integrity makes sure that data held in a system is a proper representation of the data intended and that it has not been modified by an authorized person. When any application is running on a server, backup routine is configured so that it is safe in the event of a data-loss incident. Normally, the data will backup to any portable media on a regular basis which will then be stored in an off-site location.
2) *Availability:* Availability ensures that data processing resources are not made unavailable by malicious action. It is the simple idea that when a user tries to access something, it is available to be accessed. This is vital for mission critical systems. Availability for these systems is critical that companies have business continuity plans (BCP"s) in order for their systems to have redundancy.
3) *Confidentiality:* Confidentiality ensures that data is not disclosed to unauthorized persons. Confidentiality loss occurs when data can be viewed or read by any individuals who are unauthorized to access it. Loss of confidentiality can occur physically or electronically. Physical confidential loss takes place through social engineering. Electronic confidentiality loss takes place when the clients and servers aren't encrypting their communication.

D. DDos Localization

Distributed denial of services attack usually occurs in wireless networks. It is an attack where multiple systems comprise together and target a single system causing a denial of service. A denial of service (DOS) is an attack with a purpose of preventing legitimate users from using a specified network resource such as website, web service or computer system. A DDOS attack is distributed a large scale attempt by malicious users to flood the victim network with an enormous numbers of packets. DDOS is composed as shown in Fig. First attacker build a network of vulnerable nodes which are used to initiate the attack. The vulnerable nodes called handler and agents. These handler and agents are then installed with tools called attack tools, which allow the handler and agents to

carry out attacks under the control of the attacker. The attacker motivates the handler to start the attack, the handler then motivate the agents. The agents flood the victim.

As the Internet becomes an integral part in many people's lives, the need to keep servers protected, online, and available has become increasingly important. In recent years, denial-of-service (DoS) attacks and distributed DoS (DDoS) attacks have become more sophisticated and effective at obstructing this availability. In 2000, several online companies such as eBay, Amazon.com, CNN.com, and Yahoo were all affected by a large scale DDoS attack. During this attack, their websites were rendered virtually unreachable to many Internet users, resulting in severe financial losses, in addition to the many unsatisfied customers. In 2002, several root Domain Name System (DNS) servers were brought down by yet another DDoS attack .

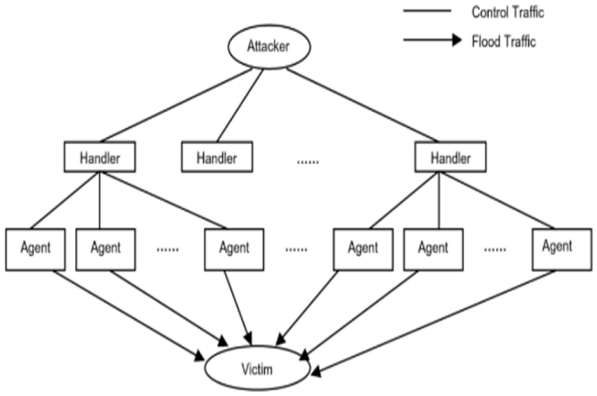


Fig Representing DDOS attack

II. LITERATURE REVIEW

The proposed system is using Cloud Computing, Security mechanisms, DDos localization techniques to detect malicious users. All of these are described in this section.

(Alani 2014)Cloud computing referred to the delivery of on-demand computing resources everything from applications to data centers—over the Internet on a pay-for-use basis. By using this service you can use any resource without being present there. In healthcare it plays a vital role because we can easily access the cloud resources by using internet. People have no time to visit the healthcare places.

(Assunção et al. 2014) Cloud is used to manage large amount of data. Health care system requires lots of space to maintain the data of patient and cloud is the one of the best way. As cloud have lot of storage space and it is easy to access data from there by using single click. With this facility there is no need to be present there. Any mobile user can access the data of cloud.

(Mohammed et al. 2014) By building an Android platform based mobile application for the healthcare domain, which uses the idea of Internet of Things (IoT) and cloud computing we can provide a facility to the peoples. The whole data can be uploaded to the user's private centralized cloud or a specific medical cloud, which keeps a record of all the monitored data and can be retrieved for analysis by the medical personnel. Though the idea of building a medical application using IoT is good and cloud help the user to diagnose his disease.

(Guilloteau et al. 2012) Privacy is increasingly important in the online world. It is widely accepted that cloud computing has the potential to make the information of user private. The secure processing of personal data in the cloud is a huge challenge. Adoption of privacy-enhancing technologies to support such activities in the cloud will help in handling personal data at the international level.

(Zissis and Lekkas 2012) From the security perspective, a number of unchartered risks and challenges have been introduced from this relocation to the clouds, deteriorating much of the effectiveness of traditional protection mechanisms. As a result to evaluate cloud security by identifying unique security requirements and to present a viable solution that eliminates these potential threats is required. We can use specific security characteristics within a cloud environment. The proposed solution calls upon cryptography, specifically Public Key Infrastructure operating in concert with SSO and LDAP, to ensure the authentication, integrity and confidentiality of involved data and communications.(Wang et al. 2009) Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. In contrast to traditional solutions, IT services are under proper physical, logical and personnel controls; Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which

have not been well inferred. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service. Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. Extensive security and performance analysis shows that the proposed system is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

(Wang et al. 2012) Cloud computing economically enables the exemplar of data service outsourcing. However, to protect data privacy, sensitive cloud data have to be encrypted before outsourced to the commercial public cloud, which makes effective data exertion service a very challenging task. Although traditional searchable encryption techniques allow users to securely search over encrypted data through keywords, they support only Boolean search and are not yet sufficient to meet the effective data utilization need that is immanently demanded by large number of users and huge amount of data files in cloud.

(Ning, Liu, and Yang 2015) The Internet of Things (IoT) is becoming an attractive system paradigm to realize interconnections through the physical, cyber, and social spaces. During the interactions among the ubiquitous things, security issues become noteworthy, and it is significant to establish enhanced solutions for security protection. In this work, we focus on an existing U2IoT architecture (i.e., unit IoT and ubiquitous IoT), to design an aggregated-proof based hierarchical authentication scheme (APHA) for the layered networks. Concretely, 1) the aggregated-proofs are established for multiple targets to achieve backward and forward anonymous data transmission; 2) the directed path descriptors, homomorphism functions, and Chebyshev chaotic maps are jointly applied for mutual authentication; 3) different access authorities are assigned to achieve hierarchical access control. Meanwhile, the BAN logic formal analysis is performed to prove that the proposed APHA has no obvious security defects, and it is potentially available for the U2IoT architecture and other IoT applications.

(Lonea, Popescu, and Tianfield 2013) This paper is focused on detecting and analyzing the Distributed Denial of Service (DDoS) attacks in cloud computing environments. This type of attacks is often the source of cloud services disruptions. Our solution is to combine the evidences obtained from Intrusion Detection Systems (IDSs) deployed in the virtual machines (VMs) of the cloud systems with a data fusion methodology in the front-end. Specifically, when the attacks appear, the VM-based IDS will yield alerts, which will be stored into the Mysql database placed within the Cloud Fusion Unit (CFU) of the front-end server. We propose a quantitative solution for analyzing alerts generated by the IDSs, using the Dempster-Shafer theory (DST) operations in 3-valued logic and the fault-tree analysis (FTA) for the mentioned flooding attacks. At the last step, our solution uses the Dempsters combination rule to fuse evidence from multiple independent sources. Keywords: cloud computing, cloud security, Distributed Denial of Service (DDoS) attacks, Intrusion Detection Systems, data fusion, Dempster-Shafer theory.

(Yu et al. 2014) Cloud is becoming a dominant computing platform. Naturally, a question that arises is whether we can beat notorious DDoS attacks in a cloud environment. Researchers have demonstrated that the essential issue of DDoS attack and defense is resource competition between defenders and attackers. A cloud usually possesses profound resources and has full control and dynamic allocation capability of its resources. Therefore, cloud offers us the potential to overcome DDoS attacks. However, individual cloud hosted servers are still vulnerable to DDoS attacks if they still run in the traditional way. In this paper, we propose a dynamic resource allocation strategy to counter DDoS attacks against individual cloud customers. When a DDoS attack occurs, we employ the idle resources of the cloud to clone sufficient intrusion prevention servers for the victim in order to quickly filter out attack packets and guarantee the quality of the service for benign users simultaneously. We establish a mathematical model to approximate the needs of our resource investment based on queueing theory. Through careful system analysis and real-world data set experiments, we conclude that we can defeat DDoS attacks in a cloud environment.

A. Problem Definition

During the last few years, there has been a sharp increase in the number of network-based computer attacks. This has lead many researchers to study this field in great depth in order to develop novel methods that are capable of eliminating this threat from today's computer networks. This chapter presents a summary of some of the most recent work on the mitigation techniques of common DoS and DDoS attacks. The work that is summarized in this chapter deals primarily with attacks on the transport layer, attacks on the network layer, and a thorough introduction to the concept of the mitigation technique known as client puzzles. It is very difficult to secure data from intruders. Now in our proposed system we detect the malicious nodes as well as correct them.

It is very difficult to detect the intruder in cloud computing to find the malicious user. The malicious user can detect the data from the cloud environment. So in our proposed system we will detect the intruders in cloud network as well as stop them to steal the data.

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

B. Proposed System

DDOS algorithm is a distance based algorithm. DDOS localization algorithm is created for detecting and removing wormhole attack. In our algorithm we have included distance based algorithm also. In cloud system malicious nodes steal the data without authorization of user. The malicious node then act in place of the other node. The malicious activity performed by the node will make the actual node to be accounted for and punished. In order to resolve the problem random key will be utilized. The DVHOP with random key hence is proposed.

1) Algorithm

In the proposed algorithm we will consider the following steps

a) Generate random Ids for the nodes.
b) Assign the Ids to the nodes.
c) Detect the malicious Entry
d) If Malicious(Node) then
e) Block the node
Else
f) Move onto next step in sequence
End of if
g) Calculate localization Error
h) Stop

The above algorithm will be used to determine whether the attack has occurred on the node or node. If attack does occur on the system than node which is malicious is blocked. Otherwise node is allowed to perform the suggested operation. In the end localization error will be calculated. From the experiment it is proved that localization error in case of proposed system is less as compared to the previous algorithm.

C. Ddos And Localization Algorithm

The DDOS algorithm is a range free algorithm. In this algorithm distance between nodes is not important. As long as it is possible to transfer the data, then data can be transferred. The DDOS algorithm is divided into following steps

Unknown node and compute nodes each beacon minimum hops.

1) Beacon nodes broadcast their locations to the neighbours of information packets, including the jump number field is initialized to 0. Receiving node records to each beacon nodes having the minimum number of hops, ignoring a beacon node from the same large number of hops a packet. Then hop count plus one, and forwarded to the neighbours. Through this method, all nodes in the network to be able to record each beacon node under the minimum number of hops.
2) Compute unknown node and beacon node's actual hop distance. Each beacon nodes according to the first stage record other beacon nodes position information and the distance hops, using the equation (1) estimate the average hop actual distance. 2) Calculate and obtain the unknown node average hop distance. Beacon nodes by saving the coordinates of the other beacon nodes and the minimum number of hops using the equation (1) in the network calculate the average hop distance:

$$c_i = \sum_{i \neq j} \frac{\sqrt{(x_i - x_j)^2 - (y_i - y_j)^2}}{\sum_{i \neq j} hop_{ij}}$$

D. Equation 1 Calculate The Average Hop Distance

Here x and Y are the co-ordinates of the beacon nodes.

3) Using trilateration measurement or maximum likelihood estimation method to calculate its own position. Unknown node uses the second phase to each record jump distance beacon nodes using trilateration measurement or maximum likelihood estimation method to calculate their coordinates. There exist more accurate equation which can be used in order to enhance the performance of the DVHOP algorithm.

$D=D/2+d_{ab}/2hop_{ab}$

E. Equation 2 To Enhance The Performance Of The Ddos Algorithm

Here D is the original average hop distance d_{ab} is the distance between the nodes between a and b. hop_{ab} is the hops between the anchor nodes.

The localization is the mechanism of determining the path that exists between source and the destination. The DDOS algorithm is prone to attacks. One of the common attacks is DDOS which means distributed denial of service attack. This attack will going to consume the resources associated with the node and cause the traffic to be jammed. In order to solve the problem random key is proposed. With the help of random key every node within the localization process is assigned a random id which will be difficult to guess by the intruder or malicious node. Hence the security will be enhanced. Also the localization error is reduced .

The proposed algorithm is as follows

DDOS WITH RANDOM KEY

a) Generate random Ids for the nodes.
b) Assign the Ids to the nodes.
c) Detect the malicious Entry
d) If Malicious(Node) then
e) Block the node
Else
f) Move onto next step in sequence
End of if
g) Calculate localization Error
h) Stop

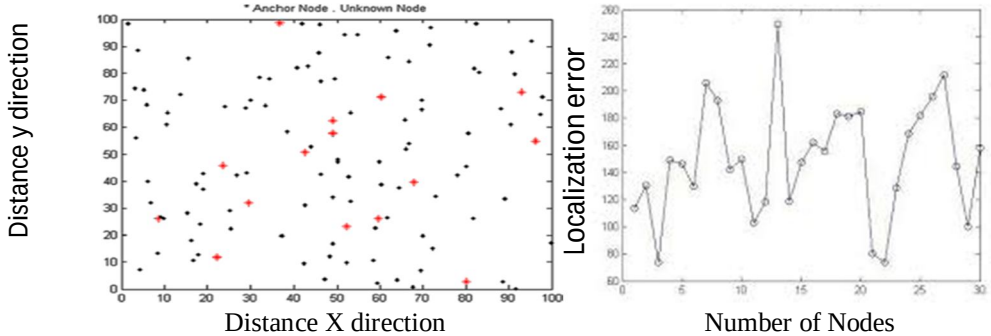
III. RESULTS AND DISCUSSION

The above algorithm will be used to determine whether the attack has occurred on the node or node. If attack does occur on the system than node which is malicious is blocked. Otherwise node is allowed to perform the suggested operation. In the end localization error will be calculated. From the experiment it is proved that localization error in case of proposed system is less as compared to the previous algorithm.

Distance	Number of nodes	Range	Localization Error
200	300	50	34.689
150	250	40	32.0987
180	270	45	33.564
190	300	30	30.879
250	310	35	34.1232

Table 1 : localization without the node capture attack

In the table above we take 200m distance between anchor and unknown nodes .The legion of nodes taken is 300 and the sensing capacity of sensing node is in range 0-50. It shows the localization errors between the nodes without node capture attack is 33.07078.The result in terms of the plot will be as described below:



A. Figure Representing Localization Without The Node Capture Attack

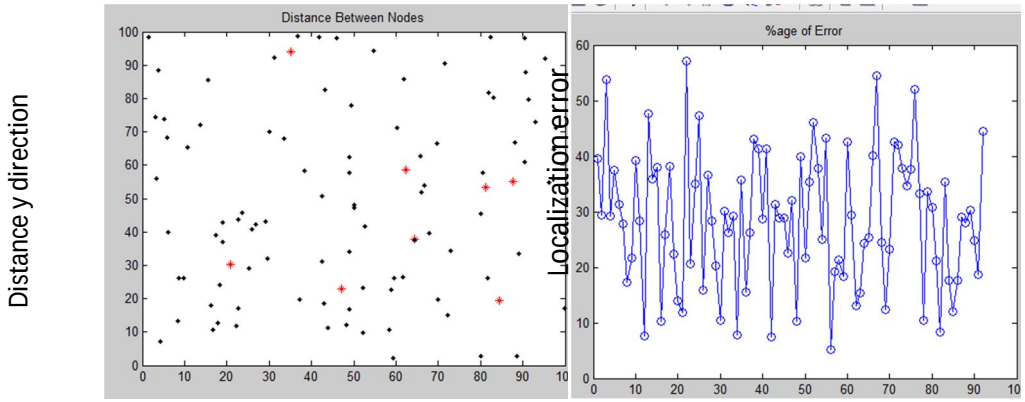
The diagram describes the plotting of nodes along x and y axis by considering the distance associated with every node. The second figure elaborate the localization error when node capture attack is not present.

Distance	Number of nodes	Range	Localization Error
200	300	50	54.685
150	250	40	50.2987
180	270	45	52.4563
190	300	30	49.7658
250	310	35	51.9876

Table 2 : localization without the node capture attack

In the table above we take 200m distance between anchor and unknown nodes .The legion of nodes taken is 300 and the sensing capacity of sensing node is in range 35-50. It shows the localization errors between the nodes in case of existing system is 51.83868.The result in terms of the plot will be as follows:

The DDOS algorithm with node capture attack is shown through the following simulation.



B. Figure Representing Node Capture Attack With Localization Error

This figure describes the node plotting along x and y axis and second figure describe the localization error in case of Node Capture attack. The percentage of error is high in this case.

IV. CONCLUSION AND FUTURE WORK

In the proposed system we covered an overview of the DDOS problem, available DDOS attack , defence challenges and principles, and a classification of available DDOS prevention algorithms. This provides better understanding of the problem and enables a security administrator to effectively equip his arsenal with proper prevention algorithms for fighting against threat. The current prevention algorithms reviewed in this paper are clearly far from adequate to protect internet from DDOS attack. The main problem is that there are still many insecure algorithms over the internet that can be compromised to launch large scale coordinated DDOS attack. The localization error will be minimized in this case. The graphs will be generated and performance is shown accordingly.

The proposed system will overcome this problem using DDOS technique. The random key technique will allocate the random id to the nodes which will be difficult to adapt and hence cannot be overtaken by the malicious entry. The implementation will be complex and time consuming. In the future less complex strategy should be formed so that DDOS problems can be resolved consuming less time in nature.

REFERENCES

[1] Alani, Mohammed M. 2014. "Securing the Cloud: Threats, Attacks and Mitigation Techniques." Journal of Advanced Computer Science & Technology 3(2):202. Retrieved (http://www.sciencepubco.com/index.php/JACST/article/view/3588).

[2] Assunção, Marcos D., Rodrigo N. Calheiros, Silvia Bianchi, Marco A. S. Netto, and Rajkumar Buyya. 2014. "Big Data Computing and Clouds: Trends and Future Directions." Journal of Parallel and Distributed Computing 79:3–15. Retrieved (http://www.sciencedirect.com/science/article/pii/S0743731514001452).

[3] Catarinucci, Luca et al. 2015. "An IoT-Aware Architecture for Smart Healthcare Systems." IEEE Internet of Things Journal 2(6):515–26. Retrieved February 23, 2016 (http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7070665).

[4] Chen, Xu. 2015. "Decentralized Computation Offloading Game for Mobile Cloud Computing." IEEE Transactions on Parallel and Distributed Systems 26(4):974–83. Retrieved May 3, 2016 (http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6787113).

[5] Chung, Pau-Choo Julia. 2014. "Impacts of IoT and Wearable Devices on Healthcare." Pp. 2–2 in Proceedings of the 12th International Conference on Advances in Mobile Computing and Multimedia - MoMM '14. New York, New York, USA: ACM Press. Retrieved February 28, 2016 (http://dl.acm.org/citation.cfm?id=2684103.2684181).

[6] Darsena, Donatella, Giacinto Gelli, Antonio Manzalini, Fulvio Melito, and Francesco Verde. n.d. "Live Migration of Virtual Machines among Edge Networks viaWAN Links." 1–10. Retrieved May 27, 2016 (http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=6633553).

[7] Guilloteau, Stéphane, France Télécom Orange, France, and Venkatesen Mauree. 2012. "Privacy in Cloud Computing." Media Informatics (March):26. Retrieved (http://www.itu.int/en/ITU-T/techwatch/Pages/cloud-computing-privacy.aspx\nhttp://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000160001PDFE.pdf).

[8] Hashizume, Keiko, David G. Rosado, Eduardo Fernández-Medina, and Eduardo B. Fernandez. 2013. "An Analysis of Security Issues for Cloud Computing." Journal of Internet Services and Applications 4(1):5. Retrieved (http://www.jisajournal.com/content/4/1/5).

[9] Kao, Yi-Hsuan and Bhaskar Krishnamachari. 2014. "Optimizing Mobile Computational Offloading with Delay Constraints." Pp. 2289–94 in 2014 IEEE Global Communications Conference. IEEE. Retrieved May 15, 2016 (http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=7037149).

[10] Karypis, George and Vipin Kumar. 1998. "Multilevelk-Way Partitioning Scheme for Irregular Graphs." Journal of Parallel and Distributed Computing 48(1):96–129. Retrieved May 3, 2016 (http://www.sciencedirect.com/science/article/pii/S0743731597914040).

[11] Katsipoulakis, Nick R., Konstantinos Tsakalozos, and Alex Delis. 2013. "Adaptive Live VM Migration in Share-Nothing IaaS-Clouds with LiveFS." Pp. 293–98 in 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, vol. 2. IEEE. Retrieved May 27, 2016 (http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=6735439).

[12] Liu, Jiaqiang, Yong Li, and Depeng Jin. 2014. "SDN-Based Live VM Migration across Datacenters." Pp. 583–84 in Proceedings of the 2014 ACM conference on SIGCOMM - SIGCOMM '14, vol. 44. New York, New York, USA: ACM Press. Retrieved May 27, 2016 (http://dl.acm.org/citation.cfm?id=2619239.2631431).

[13] Lonea, A. M., D. E. Popescu, and H. Tianfield. 2013. "Detecting DDoS Attacks in Cloud Computing Environment Dempster-Shafer Theory (DST)." International Journal of Computers Communications & Control 8(1):70–78.

[14] McFerren, Graeme, Terence van Zyl, Marna van der Merwe, and Martella du Preez. 2008. "User Requirements for Sensor Web Based Scientific Workflows in the Cholera Research Domain." Pp. V – 136 – V – 139 in IGARSS 2008 - 2008 IEEE International Geoscience and Remote Sensing Symposium, vol. 5. IEEE. Retrieved May 7, 2016 (http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4780046).

[15] Mohammed, Junaid et al. 2014. "Internet of Things: Remote Patient Monitoring Using Web Services and Cloud Computing." Pp. 256–63 in 2014 IEEE International Conference on Internet of Things(iThings), and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom). IEEE. Retrieved January 26, 2016 (http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7059670).

[16] Ning, Huansheng, Hong Liu, and Laurence T. Yang. 2015. "Aggregated-Proof Based Hierarchical Authentication Scheme for the Internet of Things." IEEE Transactions on Parallel and Distributed Systems 26(3):657–67. Retrieved May 3, 2016 (http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6767153).

[17] Okuhara, Masayuki, Tetsuo Shiozaki, and Takuya Suzuki. 2010. "Security Architectures for Cloud Computing." Fujitsu Scientific and Technical Journal 46(4):397–402.

[18] Pathre, Ayonija, Chetan Agrawal, and Anurag Jain. 2013. "Identification of Malicious Vehicle in Vanet Environment From Ddos Attack." Journal of Global Research in Computer Science 4(6):1–5.

[19] Riazul Islam, S. M., Md Humaun Kabir, and Mahmud Hossain. 2015. "The Internet of Things for Health Care: A Comprehensive Survey." IEEE Access 3:678–708. Retrieved October 24, 2015 (http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7113786).

[20] Rohokale, Vandana Milind, Neeli Rashmi Prasad, and Ramjee Prasad. 2011. "A Cooperative Internet of Things (IoT) for Rural Healthcare Monitoring and Control." Pp. 1–6 in 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE). IEEE. Retrieved February 28, 2016 (http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=5940920).

[21] Ruj, Sushmita, Milos Stojmenovic, and Amiya Nayak. 2014. "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds." IEEE Transactions on Parallel and Distributed Systems 25(2):384–94. Retrieved May 3, 2016 (http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6463404).

[22] Strunk, A. and W. Dargie. 2013. "Does Live Migration of Virtual Machines Cost Energy?" Pp. 514–21 in 2013 IEEE 27th International Conference on Advanced Information Networking and Applications (AINA). IEEE. Retrieved May 27, 2016 (http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=6531798).

[23] Waidyasooriya, Hasitha Muthumala and Masanori Hariyama. 2016. "Hardware-Acceleration of Short-Read Alignment Based on the Burrows-Wheeler Transform." IEEE Transactions on Parallel and Distributed Systems 27(5):1358–72. Retrieved May 3, 2016 (http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7122348).

[24] Wang, C., Q. Wang, K. Ren, and W. J. Lou. 2009. "Ensuring Data Storage Security in Cloud Computing." Iwqos: 2009 Ieee 17th International Workshop on Quality of Service 37–45\n302. Retrieved (<Go to ISI>://000274551300005).

[25] Wang, Cong, Ning Cao, Kui Ren, and Wenjing Lou. 2012. "Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data." IEEE

Transactions on Parallel and Distributed Systems 23(8):1467–79.

[26] Wang, Hongbing, Zuling Kang, and Lei Wang. 2016. "Performance-Aware Cloud Resource Allocation via Fitness-Enabled Auction." IEEE Transactions on Parallel and Distributed Systems 27(4):1160–73. Retrieved May 3, 2016 (http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7094282).

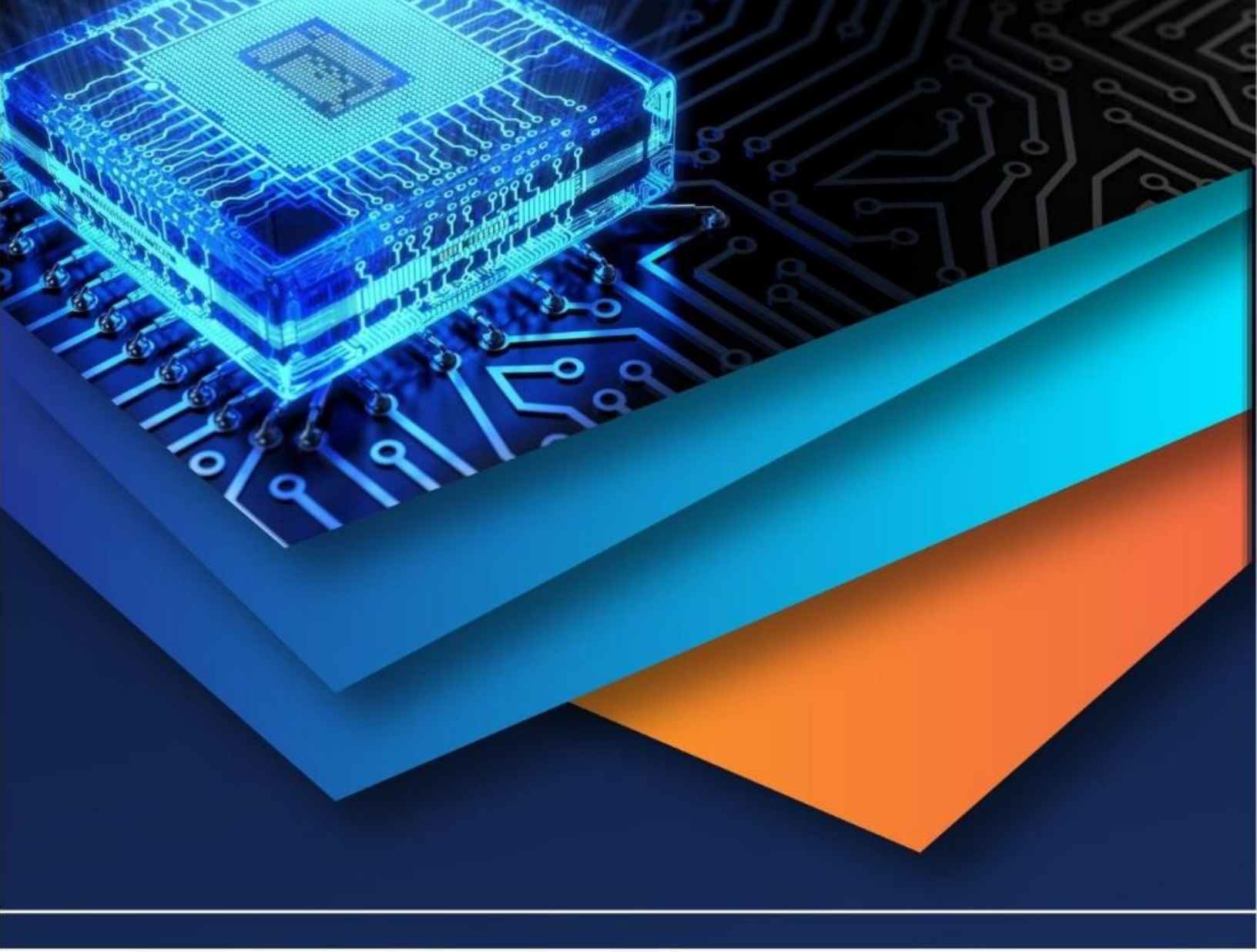
[27] Yu, Shui, Yonghong Tian, Song Guo, and Dapeng Oliver Wu. 2014. "Can We Beat DDoS Attacks in Clouds?" IEEE Transactions on Parallel and Distributed Systems 25(9):2245–54. Retrieved April 20, 2016 (http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6567859).

[28] Zhang, Sheng, Zhuzhong Qian, Zhaoyi Luo, Jie Wu, and Sanglu Lu. 2016. "Burstiness-Aware Resource Reservation for Server Consolidation in Computing Clouds." IEEE Transactions on Parallel and Distributed Systems 27(4):964–77. Retrieved May 3, 2016 (http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7091926).

[29] Zhang, Weida, King Tin Lam, and Cho Li Wang. 2014. "Adaptive Live VM Migration over a WAN: Modeling and Implementation." Pp. 368–75 in 2014 IEEE 7th International Conference on Cloud Computing. IEEE. Retrieved May 27, 2016 (http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=6973763).

[30] Zhu, Zhaomeng, Gongxuan Zhang, Miqing Li, and Xiaohui Liu. 2016. "Evolutionary Multi-Objective Workflow Scheduling in Cloud." IEEE Transactions on Parallel and Distributed Systems 27(5):1344–57. Retrieved May 3, 2016 (http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7127017).

[31] Zissis, Dimitrios and Dimitrios Lekkas. 2012. "Addressing Cloud Computing Security Issues." Future Generation Computer Systems 28(3):583–92. Retrieved (http://dx.doi.org/10.1016/j.future.2010.12.006).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY