Research on security architecture for cloud based Voice-Over Internet Protocol by securing infrastructures using hadoop clusters to Prevent Adaptive Anomaly Attacks in Cloud computing

S MP Qubeb, Ilango Paramasivam

ABSTRACT--- Cloud based Voice over Internet protocol (VoIP), is a new type of communication that uses Internet protocol to transfer the data packets which contains the audio data. For the past 20 years there has been an intensive research going on this field since this makes the calling system much cheaper than those taking place over PSTN (Public Switched Telephone Network). VoIP has been mainly taking place through cloud computing and this feature has its own issues but even has its own pros. This feature over cloud is facing many challenges in the terms of quality of services and security. This paper also describes the research or the development taking place in field of secured discussions. The network components and architecture have been discussed; the components described are call processors, gateways and many more. Different attacks possible on the VoIP have been discussed which include spoofing and SPIT. There are different VoIP solutions and they are based on either peer-to-peer (P2P) protocol or Session Initiation Protocol (SIP). In this paper, we have analysed about some of the essential security issues on cloud based VoIP for preventing the adaptive anomaly attacks and some other security issues of cloud computing by applying the algorithmic simulation in hadoop clusters.

keywords: Voice over Internet protocol (VoIP), Cloud computing, PSTN (Public Switched Telephone Network), Throughput, Security, adaptive anomaly attacks.

I INTRODUCTION

Since the invention of telephone in early 1900s, communication through telephone has not changed much but new technologies have emerged like digital circuits, DTMF. Changes over the years were behind the scenes and the basic functionality was same. But the service providers charge for each minor increment in service introduced. In late 1900s, many researchers, both in corporate and educational institutions, showed immense interest in carrying voice over IP networks, especially internet and the corporate intranets. This technology came to be known as VoIP or Voice-Over Internet Protocol.

A simple process is followed in which the audio or video is broke into small chunks. These broken chunks are transmitted over the IP network and are reassembled at the receiver's end. This is how two people communicate using audio and video. This idea is not new as there are many patents and research papers that date back to several decades. Several demonstrations also took place at various times over the years. Its principle is similar to that of voice recording using microphone. Instead of storing locally, it is sent over the IP network to other computers. The recorded sound is compressed into very small samples which are collected together into larger chunks. These are then placed into data packets for transmission over the IP network. This whole process is referred to as packetization. Before the emergence of VoIP, Internet was limited mainly to academics use. Moreover, VoIP is not limited to only voice communication. It also means video and data conferencing. Real-time Text communication (RTT) and video telephony are the future scope of VoIP. But, large efforts like proper marketing are required to reflect these facts. Because of the VoIP, we can use our desktop as well as wireless phones for communication. Video calling is also possible because of VoIP. Not only this, VoIP has applications like electronic white boarding, text chat and application sharing. However, this does not imply that VoIP is limited to desktop or laptop computers. It can be implemented to a lot of hardware devices.

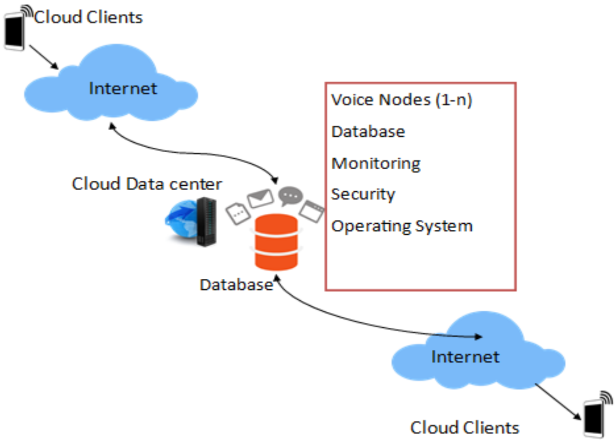

Fig.1 Cloud based VoIP Architecture

Revised Manuscript Received on August 30, 2019.

* Correspondence Author

S MP Qubeb*, School of CSE, Research Scholar@ Bharatiyar University, Tamil nadu, India. (Email: qubebjntu@gmail.com)

Dr.Ilango Paramasivam, Professor, Dept. Of CSE, PSG Institute of Technology and Applied Research, Coimbatore-641062.India. (Email: dr.p.ilango@gmail.com)

Retrieval Number: F9378088619/19©BEIESP
DOI: 10.35940/ijeat.F9378.088619
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

VoIP is also gaining a momentum within the market because it has been viewed as a free calling system. It is being made up to a level where it can match PSTN and can replace the legacy carried by the PSTN. A very few people are actually acknowledged with this fact that the daily international calling can only take place through VoIP due to the availability large bandwidths .

Well this system has its own pros and cons, so as the part of pros we can say that calling anywhere is going to become cheap and easily available, the connectivity is going to increase and the better connectivity will actually be taking place. Now coming to the cons part which are many and the field of interest for the cons are QoS(Quality of Service) and security issues. Well QoS basically means the Quality of the sound which the receiver, receives at the other end is been going through many problem and the problems are Delay, Jitter, Packet loss, echo and Throughput in cloud services [12].

These problems have been taking place because of the congestion taking place over the network and there were many condition put over on VoIP to check it's QoS and it was seen that the bandwidth was affecting the sound heard on the receiver side . There have been many new schemes which have been inserted or made to compare the level of sound heard, which includes objective and subjective methods. The next major challenges faced by the VoIP are the security issues. Security acts as a very important for VoIP because any important information to be transferred can be hacked into by the attackers and this will result in major losses. One of the major techniques of hacking the network is SPIT and spoofing. The attacks on the VoIP are easy since it is in the form of Data Packets being transferred from on node to another instead of Voice signals which are generally analogue signals. There are many network components which are exposed and need to be scanned at every point of time to prevent them from being attacked in the cloud servers [13].

The quality of the voice degradation is directly proportional to level of security being created, like the encryption and decryption algorithm which will result in packet delay. So this are basically the cons of the VoIP but there are certainly many researches taking place over this field to make it transparent for use. VoIP has many applications which are Skype, Viber, Reliance Jio and many more and the greatest thing about this software are that they are able to provide the best communication at almost free rates. In this paper, VoIP is reviewed starting with its characteristics. Different advantages of VoIP are discussed and related difference has been noted down between VoIP and PSTN. VoIP being an emerging technology faces some issues, threats and security problems which are discussed here with their possible solutions. Different algorithms and methods for solving the major security problem are discussed in the following paragraphs. Different applications of VoIP have been studied and compared. A study is done on the most popular application of VoIP i.e. Skype through various geographically separated cross region routers [14].

This Literature survey will take you from the history of VoIP to its present evaluation and application.

II. LITERATURE SURVEY

This [1] paper discusses about how the VoIP is implemented using various VoIP protocols and VoIP data processing and its configuration. It describes currently used 3 protocols for VoIP: SIP (Session Initiation Protocol), MGCP (Media Gateway Controller Protocol) and H.323 protocols. H.323 consists of family of protocols used for call setups, registration and other functions and are transported over TCP/UDP protocols. SIP was defined for creating and terminating sessions between two or more clients. It is simpler and hence more popular than H.323 protocols. MGCP helps in communication between separate decomposed VoIP gateway components. It manages calls and conferences and doesn't define a mechanism for call agents. It mentions about the components of VoIP: CODEC (Coder-Decoder), playout buffer and packetizer and how the analog voice signals are converted into digital signals to be compressed and encoded into formats using voice codec. To the encoded voice, protocol headers like UDP (User Datagram Protocol), RTP (Real-Time Transport Protocol) and IP (Internet Protocol) are attached from different layers among which UDP is preferred one. Quality of VoIP is determined by delay, jitter, packet loss, throughput and echo. How VoIP calls are available in traditional phones is also discussed. These are done using dedicated routers, adapters, softphones, and dedicated VoIP phones. VoIP calls are prone to attacks like SIP and RTP. Risk analysis will identify the vulnerabilities. This [2] paper discusses about the research and practices of VoIP by consumers and enterprises. . It tells how the VoIP is better than the legacy networks and that the developments in VoIP technology are plentiful. It describes currently used 3 protocols for VoIP: SIP (Session Initiation Protocol), MGCP (Media Gateway Controller Protocol) and H.323 protocols. Comparison of the quality of service is done among the various protocols. Information about original 802.11 MAC protocol is given and its role in the implementation of the VoIP technology. Components of different protocols for VoIP are explained with their pros and cons. QoS (Quality of Service) is measured as Jitter, Delay, Packet Loss, Echo and Throughput. Measures to attain secure VoIP connections are talked about to avoid the security issue. Some of these measures are strong network architecture, avoiding use of soft-phones, maintaining proper security environment and keeping good backup power. VoIP signalling and media transmission protocols (IAX,SIP, H.323 and RTP) explains specific security mechanisms. VoIP is open to many threats like social threats that are directly against humans, eaves dropping, modification threats and interception in which unauthorized signalling takes place Denial of service threats, service abuse threats, physical access threats and interruption of service threats. This [3] paper discusses about the various advantages and disadvantages of VoIP, its background, problems, capacity over WLAN and security. Advantages are low expenditure, flexibility etc and disadvantages like dependency on bandwidth of internet, no guarantee of quality of service etc.

It also discusses the various standards for the communication field and the background and characteristics of WLAN. Characteristics like edibility, scalability, simplicity, mobility and cost effectiveness are talked about. It is similar to LAN but in this, transmission is via RF or IR and not cables or wires. Two WLAN configurations: Infrastructure-less mode and Infrastructure mode are used to attain high speed video, voice and audio services. IEEE 802.11 MAC is the protocol given by IEEE to provide good service for WLAN. It also discusses the capacity and security of VoIP.

This [4] paper discusses about the detailed definition of VoIP and its comparison with the circuit-switched services. It tells how the VoIP is better than the legacy networks and that the developments in VoIP technology are plentiful. Comparison of the quality of service is done among the various protocols. Information about original 802.11 MAC protocol is given and its role in the implementation of the VoIP technology. VoWLAN systems are introduced in the paper and their significant role in providing good QOS for the VoIP. But the basic issues like delay, packet-loss, jitter, throughput and echo also exist in these systems. Calculation of capacity of VoIP over WLAN is explained. The two method are objective and subjective. Objective further has two subdivisions: Intrusive and Non-Intrusive. Subjective methods has subparts: PSQM (Perceptual Speech Quality Measure), PESQ (Perceptual Evaluation of Speech Quality), PAMS (Perceptual Analysis Measurement System) and E-Model.

This [5] paper mainly reviews about the security and the threats on the VoIP network. It discusses the various advantages and disadvantages of VoIP. VoIP is cost-effective, has very good quality of service and bandwidth as compared to PSTN. Components of different protocols for VoIP are explained with their pros and cons. VoIP has many software and hardware requirements like full-duplex sound card, headset with mic and a broadband connection. VoIP is vulnerable to many security attacks due to lower cost organisation to achieve better quality of service. Measures to attain secure VoIP connections are talked about to avoid the security issue. Some of these measures are strong network architecture, avoiding use of soft-phones, maintaining proper security environment and keeping good backup power. Mahbub Hassan and Alfandika Nayandoro in their paper ‘Internet Telephony: services, technical challenges and products’ had talked about the new technology of internet based voice calling and its challenges. VoIP had come to rise in many sectors. Enterprises can use this technology for their regular intra office calling and can save huge costs. Unlike PSTN (Public Switched Telephone Network), IP telephony uses the imaginary second line i.e. one for accessing internet and the other for voice calls. The main advantage that Mahbub and Alfandika define here is the low cost than PSTN because of the packet switching technique where all calls share the same network resources. Major problems faced by VoIP are the packet loss. Results from this paper say that upgrading the IP network can decrease the packet loss and using techniques like silence substitution, packet substitution and packet interpolation damaged packet can be retrieved. This paper concludes that VoIP is new immerging low cost technology but it still has some issues to be considered and removed. Here they were not able to give clear solution for the problem of packet delay in VoIP.

This [6] paper mainly defines the Voice-Over Internet Protocol and talks about the history of the same. It also talks VoIP attacks, risks and how to protect against them. Service and availability limitations are discussed. The VoIP gained popularity in the mid-90s but was not sufficiently mature. The marketing structure and tech reality was nowhere close. Protocols for the implementation are SIP, H.323 and MGCP (Media Gateway Controller Protocol).

The data is converted from analog to digital signals, encoded into voice codecs standardised by ITU-T (International Telecommunication Union-Telecommunication) and a header is attached. QoS (Quality of Service) satisfies customer’s needs. Higher the satisfaction, higher is the qos. It is measured as Jitter, Delay, Packet Loss, echo and throughput. VoIP is configured using the dedicated routers, adapters (USB), Software-controlled phones (softphones) and dedicated VoIP phones. VoIP is vulnerable to many attacks like malformed message, SIP flooding and spoofing attack which is further of two types: IP and URI. We can protect against these risks using Voice VLAN which enables to allow simultaneous access but it increases the complexity for the security and confidentiality. The availability of VoIP is hindered due to power outages and bandwidth.

This [7] paper presents the deep analysis of Voice-Over Internet Protocol security concerns. It has a brief introduction of the basics of VoIP. Main feature of VoIP technology is that it is deployed using centralized client-server architecture It tells that the main vulnerable components are the operating system of VoIP applications, VoIP protocols, the network devices (switch, router), management interfaces and the VoIP application. These vulnerabilities can be exploited for different attacks. The different types of attacks are: confidentiality, social context, integrity and attacks against availability. These attacks aim to interrupt services using call flooding, denial of service, spoofed messages, malformed messages and call hijacking. An attack against social context aims on how to change the social context among communication parties so that an attacker can misrepresent as a trusted one and pass wrong data to the target user. To stop these attacks, and hence help the deployment of VoIP systems, VoIP signalling and media transmission protocols (IAX,SIP, H.323 and RTP) explains specific security mechanisms as part of the protocols, or recommend mixed solution with other security protocols (SRTP, IPS etc).

This [8] paper describes VoIP (Voice-Over Internet Protocol) and its security concerns. Business concerns of its implementation, its components and relevant issues related to security. The components of VoIP are network components, end-user equipment, call processors, protocols and gateways. Network includes switches, routers and firewalls. The new VoIP system is installed over the existing IP network.

End-user is used to access VoIP to communicate with other end and the connection is either physically-cabled or wireless. Call processors are software whose function includes phone number to IP translation, call setup and its monitoring, signal coordination, user authorization and bandwidth control. Protocols are of various types but the two which are most common are SIP and H.323. H.323 is set of protocols whereas SIP, Session Initiation Protocol is a signalling protocol. Gateways handle the call origination, detection and conversion from analog to digital. Its three functional types are SG (Signalling Gateways), MG (Media Gateways) and Media Controllers. Denial of Service is a major concern as it prevents delivery of services. It is the result of VoIP components being unavailable or unavailable bandwidth. Other concerns are web servers, databases, other VoIP service providers, electrical power and physical security.

This [9] paper presents a survey of VoIP security and research. It tells us that VoIP has higher flexibility, reduced costs and richer feature sets as compared to PSTN (Public Switched Telephony Network). It discusses the findings with respect to actual vulnerabilities, brief overview of SIP and threat model given VoIP Security Alliance. SIP is protocol of application-layer standardized by IETF. It supports multiple network components like PSTN bridges and operate over TCP, UDP and SCTP. VoIP is open to many threats like social threats that are directly against humans, eaves dropping, modification threats and interception in which unauthorized signalling takes place Denial of service threats, service abuse threats, physical access threats and interruption of service threats.

This [10] paper discusses about the background of VoIP, its potential benefits, legal and ethical issues, security concerns and social problems that VoIP can introduce. VoIP was formed as an alternative form of communication in which average phone network was not involved. It is fast, more reliable and usable around the world. The great feature of VoIP is that it is free as copared to the home telephone which has a monthly bill. It helps to connect to various people around the world. Applications that support VoIP demand users to have an account that brings up security and privacy questions. Call interception can lead to vulnerabilities of information out in the world. Security concerns can be linked to legal and ethical issues.

III. ANALYSIS AND MODELLING

With respect to the prevention of adaptive anomaly attacks problem, the Levy flight function has been modified. One of the Levy flight mechanisms has non-deterministic adjustment and mean which is known as Mantegna's algorithm. As a contrast to Brownian random walks technique, Levy flights have efficient exhaustive search space. The adjustment of levy distribution is represented as follows.

$\sigma^2(t) \sim t^{2-\rho}$ where $1 \leq \rho \leq 2$

According to the equation stated above, adjustment σ^2 of Levy flights distribution prologs to greater extent as related to linear relationship of Brownian arbitrary walks which expressed as $\sigma^2 \rightarrow t$. Through this we can able to detect and analyse to prevent the attacks by the following calculations.

IV. ALGORITHM FOR SECURING CLOUD SERVERS USING CLUSTERS

Servers (Infrastructures) security using clusters

```
Start the process by initializing the Hash table in VM
InfraSec (IS) = SAFE servers in GET request;
$C^U$= Cloud User,
IS=hoard the users MAC address in server;
Ensure each time $C^U$ in servers hash, If (IS==Hash($C^U$(MAC)))
{
Else If($C^U$<3)
{
ADDRESS=Get Users address (MAC);
MAC-1 = HASH { IS(f(MAC))}
Cloud Server =MAC-1;
If (IS=$C^U$)
{
User Request accepted by the Server
Auto sending the response
}
Else
{
Add the users MAC-1ADDR to the Probe list,
Print : "Deny permission to enter the network"
}}
}
Else
{
MAC address accepted
Auto sending the response
}
End
```

The above algorithm is basically suits for detecting and preventing the adaptive anomaly attacks in the cloud server. Also, its focuses on the MAC address based security, hence the DoS(Denial of Service) attacks and R2L (Remote to Local) attacks can be prevented easily.

Steps:

Step 1: Start the Process by deploying the Hash table in cloud servers VM

Step 2: Initialize the Server Infrastructure for transmitting the request named GET

Step 3: Cloud User (C^U) Initialization with key Hash into server; IS= Store and Retrieving the users MAC from cloud server

Step 4: In each login, the address will be validated with MAC

Step 5: only 3 requests from C^U will be accepted, else the request will be made as a log in Hash of the server

Step 6: Then, Print: "Deny permission to enter the network", as the C^U been detected as malicious attacker

Step 7: Else "MAC address accepted and Auto sending the response".

Step 8: Repeat the process.

V. RESULTS AND DISCUSSION

The adaptive anomaly attack detection time with 10 features and 41 features using classifiers is given in Fig.3 and Fig.4. The individual attack detection time with support vector classifier has been measured with selected 10 features and 41 features are shown in fig.3. Time consumed for attack testing with 41 features is drastically high when compared to attack detection time of 10 selected features. The attack detection time using normal classifier with 10 selected features and 41 features is given in Fig.4. It conveys that the attack testing time with selected features is less than the 41 features.

On the other hand, it also conveys that support vector classifier is better than the normal classifier to provide an accurate detection rate. The parameters taken are DoS (Denial of Service) attacks, Probe attack, Remote to Local (R2L) and User to Root (U2R) Attacks.

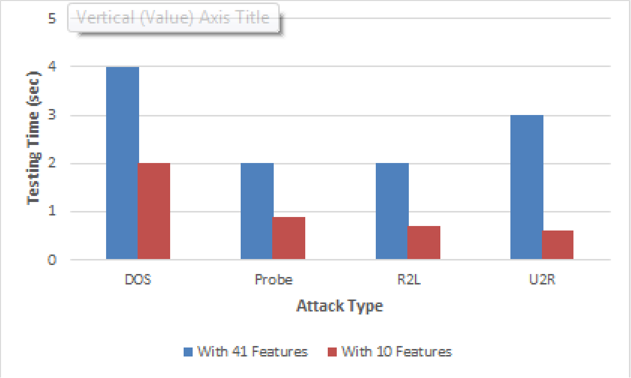

Fig. 3 Representation of testing time (sec) for attacks using support vector classifier for 10 features and 41 features

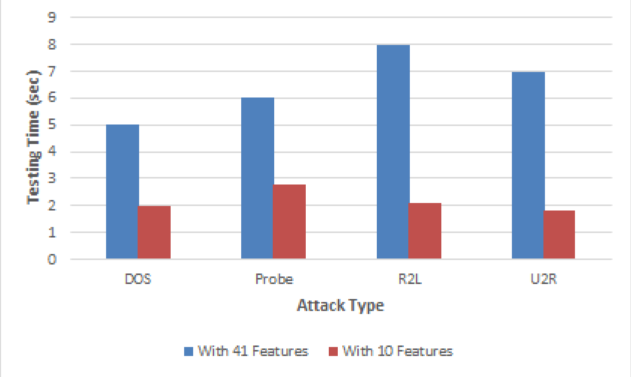

Fig. 4 Representation of testing time (sec) for attacks using normal classifier for 10 features and 41 features

The performance of the proposed work is based on two facts. Firstly, each individual in servers processes its own boundary neighbours which make the enriched interaction with their neighbourhood, which provides the intensification performance of cloud based server. Secondly, the Levy flight mechanism among the individuals can process the population diversity to an extent, which favours the exploration performance.

V. CONCLUSION

VoIP (Voice over Internet Protocol) is one of the important technologies that have been emerged in recent years. The change from circuit based switching to packet based switching has benefited big and small enterprises and different users. Compared to the old technology of PSTN, it is a lot cheaper and efficient option for voice and even video calling. This paper contains detailed study about the VoIP and reviews all the advantages, problems faced by this emerging technology and its applications over various sectors. VoIP reduces the cost factor for the user but there's a question about its security. Some other problems faced by VoIP are about the packet loss and packet delay which has been reviewed and solutions were provided. An analysis was performed on skype, a major application of VoIP. A lot more case studies have to be done on different application of VoIP and an effective way to secure VoIP from the threats should be made. For future work, the quality of service of VoIP should be considered to prevent the various types of attacks into the cloud server.

REFERENCES

1. Voice over Internet Protocol, Rahul Singh1, Ritu Chauhan, Dept. of Computer Science and Engineering International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471.Vol. 3 Issue 1, January-2014, pp: (15-23), Impact Factor: 1.147
2. A.D. Keromytis, "Voice over IP: Risks, Threats and Vulnerabilities," Proc. Cyber Infrastructure Protection (CIP) Conf., 2009; www. cs.columbia.edu/~angelos/Papers/ 2009/cip.pdf.
3. VoIP over WLAN Networks, Pankaj Kumar, Arun Verma, Shaili Singhal, International Journal of Scientific & Engineering Research, Volume 6, Issue 5, May-2015, ISSN 2229-5518
4. VoIP over Wireless LAN, Mudusu.Srinu , Mr. Shailesh, Department of Electrical Engineering, ISAR International Journal of Electrical and Electronic Ethics - Volume 1 Issue 1, Jan – Feb 2016
5. Security and Risk Analysis of VoIP Networks, S.Feroz and P.S.Dowland, Network Research Group, University of Plymouth, United Kingdom
6. Security on Voice over Internet Protocol from Spoofing Attacks, Sanjay Kumar Sonkar, Rahul Singh, Ritu Chauhan, Ajay Pal Singh, International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 3, May 2012
7. VoIP Technology: Security Issues Analysis, Amor Lazzez,Taif University, Kingdom of Saudi Arabia, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2, Issue 4, July – August 2013 ISSN 2278-6856
8. Voice-Over Internet Protocol (VoIP) and Security, Greg S. Tucker, October 26, 2004, GIAC Security Essentials Certification (GSEC), Practical Assignment, Version 1.4c, Option 1
9. A Survey of Voice over IP Security Research, Angelos D. Keromytis, Symantec Research Labs Europe, France, A. Prakash and I. Sen Gupta (Eds.): ICISS 2009, LNCS 5905, pp. 1–17, 2009._c Springer-Verlag Berlin Heidelberg 2009
10. Voice Over Internet Protocol, Bridgie R. Weber,George Mason University, IT 103
11. A Survey on Voice over IP over Wireless LANs: World Academy of Science, Engineering and Technology 71 2010
12. Sekaran, Kaushik, Mohammed S. Khan, Rizwan Patan, Amir H. Gandomi, Venkata Krishna Parimala, and Suresh Kallam. "Improving the Response Time of M-Learning and Cloud Computing Environments Using a Dominant Firefly Approach.", Volume: 7, Page(s): 30203 - 30212, DOI: 10.1109/ACCESS.2019.2896253, IEEE Access (2019).
13. Sekaran, Kaushik, and P. Venkata Krishna. "Big Cloud: a hybrid cloud model for secure data storage through cloud space." International Journal of Advanced Intelligence Paradigms 8, no. 2 (2016): 229-241.
14. Sekaran, Kaushik, and P. Venkata Krishna. "Cross region load balancing of tasks using region-based rerouting of loads in cloud computing environment." International Journal of Advanced Intelligence Paradigms 9, no. 5-6 (2017): 589-603.