Elastic Virtualized Network Security Based on Multi-Tenant using Progressive Route Scheduling in a Cloud Data Center

Udhayakumar U., Murugaboopathi G.

Abstract: ***Information security in the cloud has become a serious problem on the Internet. There are safety standards created by the resource in traditional computing. The public cloud providers, secure transfer, and the use of public resources due to the availability of the Internet is the cloud facing distributed data centers. Providing the required level of security, approaching adopting various security components such as security watchdog, IDS / IPS system, security framework, access control framework, security management and so on. In this proposed system to improve the data transmission security to introduce proposed algorithm Elastic virtualized network security (eVNS) for extended security service which utilizes the progressive route scheduling (PRS) and promotes the security consumption for Inbound rule based on the virtualized security load balancer. We have presented a virtual cloud for a network that is secure and robust security group protocols by any compromised or faulty node in the network. In contrast to the traditional snapshot aggregation approach in data centers, the eVNS-PRS proposed algorithm resembles the unicasting it's sensed information to create a new target security group based on the routing table. This makes the system more fault-tolerant and increases the availability of information in the network. Simulations performed with the proposed algorithm have demonstrated its effectiveness.***

Keywords: cloud computing routing, data center, network security, security groups, target group, virtual load balancer

I. INTRODUCTION

In a cloud-based architecture, many tenant vehicles share the benefits of size, economics, customers, businesses, and consumers with shared infrastructure and databases, while utilizing cost and performance benefits. Housing hardware may be shared where virtual machines or servers are running, or they share a database table, where A is the data in line B of the client and the other maybe with the client. Many customers of cloud services have two types of tenants. In both cases, safeguard measures are "necessary" to ensure that tenants do not pose a risk of data loss to one another, in terms of abuse and privacy violations. Multi-tenant protection is proprietary (ie, IaaS and SaaS) and must be provided by all layers of the cloud service provider. Cloud service providers want their customers to have the latest, and the best available options. Tenants should listen to them and identify common responsibilities for the safety and security of their tenant's path. Lack of security expertise is not a barrier to adopting cloud services, but the key is to create secure automation professionals when it comes to the cloud, but they wanted to make sure they were a beginner.

Network operators who want to provide security services to a large number of customers with existing technologies face some limitations in basic management and cost. The software-defined network paradigm of network-functionalized virtualization and the software-defined network paradigm seeks to gain greater flexibility, configurability and agility to overcome these limitations. Unfortunately, the problem with using security services and deciding how to configure them is that there is no simple solution to the multicultural problem. In this article, network operators will use the various actors involved in the constraints represented by the security application of the model to determine the needs of customers to meet while minimizing the cost for optimal allocation needed can provide. This model can be used to pursue the size and set of the initial system architecture, or to dynamically adapt it to support a user's security policy. Our pre-validation has shown that our delivery model has generated high cost and performance advantages over traditional methods.

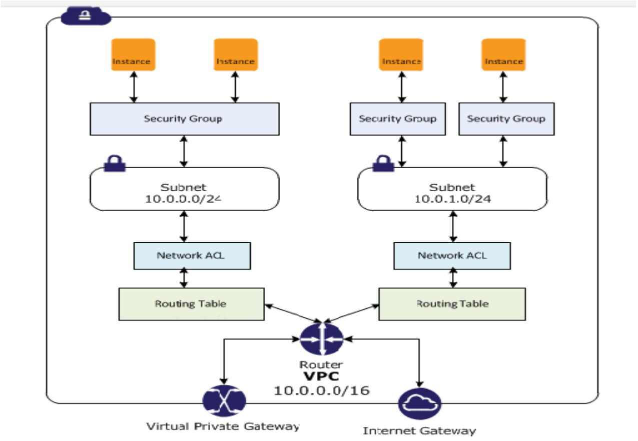

Figure 1: Elastic virtual network security

Security issues are the origin of social technology. The Cloud Security Alliance provides a security guarantee designed to promote best practices within the cloud computing framework. These issues are at least as easy as cloud-related or computer or network intrusions or moveable attacks.

Revised Manuscript Received on February 05, 2020.

* Correspondence Author
Udhayakumar U.*, PhD Scholar, Department of Computer Science, Bharathiar University, Coimbatore, India.
Email: udhayakumar.msc@gmail.com
Murugaboopathi G., Associate Professor, Department of Computer Science and Engineering, Kalasalingam Academy of Research and Education, Tamilnadu, India. Email: gmurugaboopathi@gmail.com

Cloud providers claim that security measures and processes are more mature than the average enterprise test that solves most of these problems.

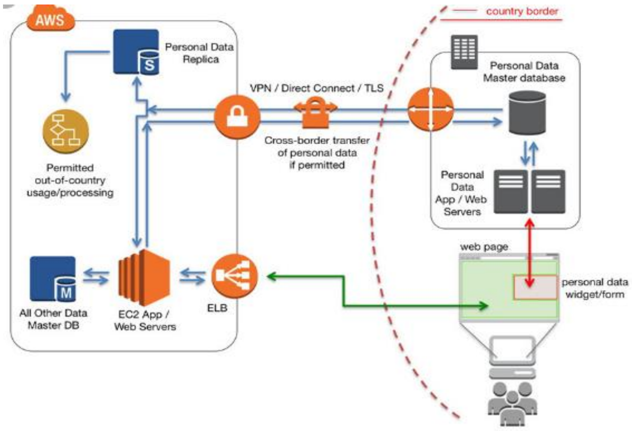
AWS
Personal Data Replica
S
Permitted out-of-country usage/processing
VPN / Direct Connect / TLS
Cross-border transfer of personal data if permitted
country border
Personal Data Master database
Personal Data App / Web Servers
web page
personal data widget/form
M
All Other Data Master DB
EC2 App / Web Servers
ELB

Figure 2: Cloud security on direct connect progressive routing

In this legal third-party data and applications is complex and poorly understood. There is also a potential lack of control, transparency and latency data. Part of the reason is the publicity of cloud computing, which can be achieved independently, but keep to the monitoring requirements of actual transparency in the cloud. Data is stored on cloud computing, remote sites to improve resource utilization. Then it needs our fixed data and available only to authorized users. It is necessary to ensure that external outsourcing and third-party publications publish the required data.

In our view, we recommend that you use computing as a measure for companies deploying to trusted cloud computing and crypto applications. These measures need to reduce how much cloud fears of computing today, and we must believe and provide evidence of the participation of the Cloud Intelligence Business Intelligence Advantage. A secure cloud computing environment relies on identifying security solutions. Current security in-depth research methods for addressing different cloud security issues need to focus on.

II. RELATED WORK

Details of investigating security issues arising due to the nature of cloud computing. A survey presented in the literature to address security issues also raised recent solutions. A brief view of the cloud also highlights the security vulnerabilities of mobile computing. Finally, it was given an open discussion agenda and directions for future research.

The use of virtualized resources, which allows multi-tenants to correspond to the same physical resources, presents a number of security issues. Assigning a complete separation of many tenants and resources is a complex task that requires a higher level of security. In the following discussion, cloud security is the challenge faced by our proposed calculations. There is a lot of work looking at the security challenges of the cloud from a service object model perspective. This article elaborated on three areas: problem (a) construction, (ii) communication issues, and (c) abstract issues based on contract and legal issues. Some clouds use computing technology without prejudice to a particular service model. Instead, virtualization can affect both, for example, more than one model to be affected. Therefore, we look at the challenge independent of the level of the abstraction service mode.

The assignment problem is a combination with a non-convex shape, it is a versatile problem is an NP-difficult packing variant. For these reasons, we use special heuristics on addresses, so-called multi-objective genetic algorithms (MOGAs), to inspire the natural process of problem evolution, MOGAs are often effectively complex of the problem [9].

Many regional VMs are placed in cloud computing environments using similar resource management. Therefore, it can be considered in conjunction with fuzzy decision levels to maximize energy efficiency. Simulation results show what is needed to meet the demands of users who satisfy the layered VM configuration [10].

AWS EC2 IaaS, such as critical cloud services, will help many companies to establish data centers to provide high-performance computing resources and reduce the cost of computer hardware maintenance can do. Internet data center services, including distributed denial of service (DDOS) attacks, can suffer from a number of security risks [11].

However, in a widely accepted environment, it has been hampered by major security issues. Firewalls and traditional security techniques are not enough for rule-based user data protection cloudy scenes [12].

The early adoption of data center operators, has recently become the application of public telecommunications networks, and is accessing, pioneering the use of projects in metro networks, central office architecture data centers (lines), etc. [13].

Providers can quickly assign and service consumers to meet the response and execution times that need to be assigned to each consumer, and demand the right data center for a distributed data center. Adaptive resource allocation model, consumer allocation, appropriate data center [14].

In this architecture, the major security enhancement comes from the fact that in a general sense a local area network. In this architecture, such as ISP transport services between local area network function endpoints and strictly centralized applications [15].

Datacenter needs in the traditional model, as well as reduce data redundancy and waste, to reduce local data upload and distribution between each level router, but also to improve efficiency [16].

Indeed, one of the key concerns of cloud computing is security. Virtualization is an important feature of cloud computing. It focuses on the security of virtual networks in virtualized environments. First, we analyzed the security issues on Xen-based platforms, as well as the security issues that existed in the virtual machines discussing the list of virtual networks [17]. In fact, Target reviewed the general architecture of the mobile cloud computing system, as well as the introduction of generic mobile cloud services by app developers and marketers.

It highlights some of the major challenges and costs, but is there a possibility for less investment in application design,

the role of mobile architecture in cloud computing, as well as the design industry applications, the shift to cloud computing systems [18].

Organizational information security systems need to integrate information security infrastructure. Enterprise Private Cloud is global management of network security systems and engineering issues, and private clouds can cripple the entire network [19].

To take advantage of these benefits, in a previous article we presented a platform called Telecommunications Network Services (TAAS). This sharing of cloud resources affects the entire mobile network, especially the software-defined network (SDN) network function virtualized (NFV) security [20].

Via the public cloud, public transport access to road conditions and accessible car or public transport information, public cloud and current driving records and private cloud combined user information related to users, hybrid with private cloud You can access the cloud. Whether cloud computing at VANET requires a network and information security. At this time, many types of secure VANETs have focused solely on information, communication and neglect of information storage [21].

A broad source of city administration is a conservative platform, some of which is important information on national security and benefits. As a result, information resource protection systems develop legitimate users of information security and operations [22].

The key drivers of cloud computing adoption are efficiency and cost-effectiveness, as it promises better scalability of the original enterprise system. With all the benefits of cloud technology available, there are still some security issues that can be fully addressed by outside organizations as information and computer components [23].

First, an automated method for modeling network threats and obtaining information to automatically generate an attack graph. By generating, using symbolic model checking algorithms, and visualizing attack graphs. Next, the two security metrics are calculated by combining the features of the diagram clouds and the attack Markov chain [24].

The cloud is generally divided into small entities called nodes. These will be each management system (s) seen together. Also, due to the lack of knowledge in emerging fields, there are standards / models that have not attracted worldwide attention from the above, especially to meet issues for the customer perspective [25].

III. ELASTIC VIRTUALIZED NETWORK SECURITY BASED ON PROGRESSIVE ROUTE SCHEDULING

The network security system such as a firewall, DPI, IDSs, etc., offers its own specialized network services that were introduced to the cloud computing strategic network. The security paradigm comes as the industry-standard servers and high-performance network security off-the-shelf devices move a function from a special-focus planning request to a network that separates the network functionality of the underlying scenario. Therefore, the network service implements a new secure eVNS- our data center, which is executed by network nodes or end users can be located there by physical or virtual machines, broken down into multiple sources.

In this study, the optimization of the eVNS-PRS method for resource utilization. In this proposed to implement an effective chain security requirement based on individual resource usage and business solution.

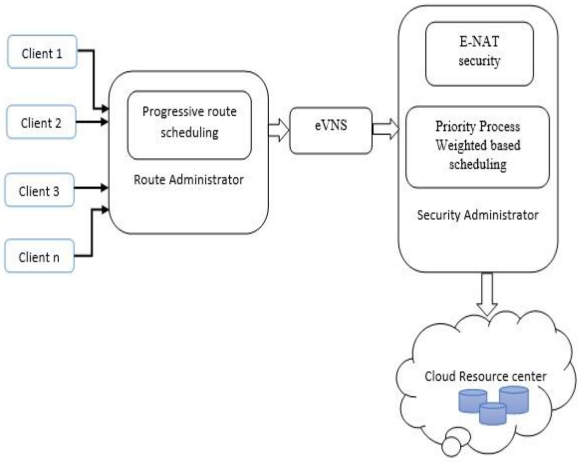

Figure 3: Proposed eVNS-PRS block diagram

Follow figure 3 shows the number of users access the cloud resource securely help of two administrators there are security administrators and route administrators. The datacenter creates a private subnet and a public subnet. The only difference is that there is no Internet gateway to a dedicated subnet. For example, let someone who doesn't want to access the user database server and place it on a dedicated subnet. The web server requires an Internet connection.

a. Progressive route scheduling on the subnet

It can even make a connection back to own local system. Routing and subnets determine whether routing tables and applications can access the cloud resource. We recommend that layer client architecture and separate private subnets from the database tier. Subnets and Network Address Translation (NAT), which may use access to cloud resources, but are more susceptible to external attacks. This is similar to a network team and a demilitarized zone (DMZ), where the firewall location does. Use different routing tables to create private and public subnets that help secure our API to its hosts in our database but do not communicate with any inappropriate actors.

The dimension ordered Progressive routing algorithm is generally used to allocate the subnet and route for the cloud machine. In the Progressive - routing algorithm, R-plane usually called a horizontal direction and Nt-plane usually called a Vertical Plane. In reality, the Progressive routing algorithm R-plane is considered as the sender of VPNs, Nt-plane becomes a Subnets. Therefore, the operation of the Progressive routing algorithm is derived above.

Algorithm steps

Route support (Es) is measured as follows:

$$Es = \frac{\sum_{i=1}^{size(R)} R(i).subnet}{distance(R)} \times \frac{\sum_{i=1}^{size(R)} R(i).NT}{distance(R)} \quad \text{--(1)}$$

The transmission support (Ts) is measured as follows:

$$Ts = \frac{\sum_{i=1}^{size(R)} R(i).NT \Big/ \sum_{i=1}^{size(R)} R(i).NRT}{distance(R)} \times \frac{\sum_{i=1}^{size(R)} R(i).subnet}{distance(R)} \quad \text{--(2)}$$

Where, RT – number of retransmissions.
Similarly, Subnet support (Ls) is measured as follows:

$$Ls = \frac{\sum_{i=1}^{size(R)} R(i).route > ETh}{distance(R)}$$, Eth – Availability subnets. -- (3)

```
Route R = $\int_{i=1}^{size(LR)} Max(LR(i).DTS)$   --(4)
For each subnet s
    If s$\in R$ then
        s.mode = wake
    Else
        s.mode = sleep
    End
Forward packet through the route identified.
Stop
```

Algorithm Steps

```
Begin
  Inbound Rule Ir= add (Incoming data policy $\sqrt{routeid \in userid}$)
  Outbound Rule Or= add (outgoing data Policy$\sqrt{routeid \in userid}$))
  Route table Rt= $\prod_{Or}^{Ir} Rid(i) + ClientIP$   ---(5)
      For each Rid
      For each client i=1: n
          Means (Ci) = C1+C2+C3+…..+Ck
          For each route j=1: k
              Rid = variant route value (Cj)
              If(Cj)≠(Cj+1)
              Add(Rid) else reroute Ci
              End if
          End for
      End for
Traffic Analysis Ta= Cip Ω Rid
Traffic feature Tf
= $\approx \frac{\sum_{Rid}^{size(Cid)} + e^{-i\omega t}\{Route\ Process\ Time\}}{number\ of\ route(Rn) + Total\ Processing\ time})$   ---(6)
    Ta= $\sum_{n=0;} Cip \oslash Tf$   ---(7)
  End for
End
```

The placement issues are selected for allocation module requirements, tenant security services that meet the requirements. The placement and constraint module must ensure that the requirements are met. Security features, transportation constraints and resource requirements to be considered in the selection process.

b. Priority Process Weighted based scheduling

After all incoming requests, whether Saas, PaaS or IaaS, is activated and it will start looking for all possible and available resources in the database. In the search process, there are two options, a resource, not so if it is available in CC (Cloud Center). Even if the resources have been discovered by the Scheduler, it is possible that the VM involved is too small or overloaded, and different actions are expected to be resolved in both cases.

$$CloudCenterStatus = {}_{1}^{0}CC \text{ ------ (1)}$$

Where, CC as cloud center and 0 is cloud statues is load low and 1 is load high

Algorithm steps

Input: Receive request from client Cr

Output: Cloud Source Allocation

Step 1: Route interface (Ri) layer receive a request from the client

```
Route_Interface{
If(Cr==Accept(Istrue))
  Establish the connection. Ri→Cr;
          Call cloud assistant ();
    }
```

Step 2: Cloud assistant (Ca) verify the request

```
Assistant_interface{
If(Cr==Ca.varify(Istrue))
  Check the Client request to Cloud Assistant Ca rules. $\sum_{Ca=0}^{t} Cr\ \beta(Ca)$
  Here, t=time, β(Ca)=calculate the cloud assistant verification rules between Cr.
  Call_ProcessInterface(Cr)
}
```

Step 3: calculate the client request processing size (Ps)

$$Ps^{n} = \sum_{k=0}^{n} \binom{n}{k} £^{k} {Cr_{process\_size}}^{n-k}$$

k as a variable , n=total user request,

$£ =$ User Priority

Step 4: Allocation Resource (Ar)

```
  Client processing request (Ps)
  For (Check (CCStatus =$\prod_{1}^{0} Ps$)
If (CCstatus == 0)
```

```
        Allocate the resource Ps
    End if
    Allocation Delay Time (ADT) =
$\int_{n=0}^{t} Ps -$ (CCstatus $=\prod_{1}^{0} Ps$))
  End for
```

Step 5: After work transaction, check the status of each CM (Cloud Machine), and any cloud machine is still overloaded, re-load balancing function repeatedly.

The end-users send resource requests to the data center with all possibilities and available resources. In all incoming requests active to collect the relevant information needed to further process the request. If the request is found to be feasible in terms of the required resources to generate the request ID. Then the Cloud assistance verifies user requests and evaluates the request rule to transfer to the process layer. It is calculated the user request process size and it will be managing the cloud system workload. Finally, the above all process completes the resource layer is allocate the resource in clout whenever enter the new client to cloud center the resource layer allocates the available resource based on client process size-based. In case the number of clients enters the cloud resource the resource layer creates another VM same as the previous cloud system facility and once again verify the client or user rule list. Also, ADT is a data center that is defined as the time required for the allocation of the service, and it also keeps track of the allocated delay time (ADT) records maintained by each data center for the workload.

IV. RESULT AND DISCUSSION

We assume that this ratio is evenly distributed to the tenants of the workload weight distribution where the total resources required. The tenant module and the workload required for the total amount of resources available for resource allocation simulated proportions. Simulation results show that the relative model to supply the most advanced application-independent country eVNS-PRS recommendations. It reduces to 50% utilization of computing resources in different network scenarios. This result ultimately leads to a 40% reduction in end-to-end application traffic response time, more security services provided.

Network density depends on the number of different cloud systems in the network. The routing and traffic load densities change from low to high. This method is due to the fact that it is also applicable to densities and 4m/s or 1m/s speeds of different networks. The cloud computing proposed method eVNS-PRS has been analyzed based on the results of the simulation done using the .Net.

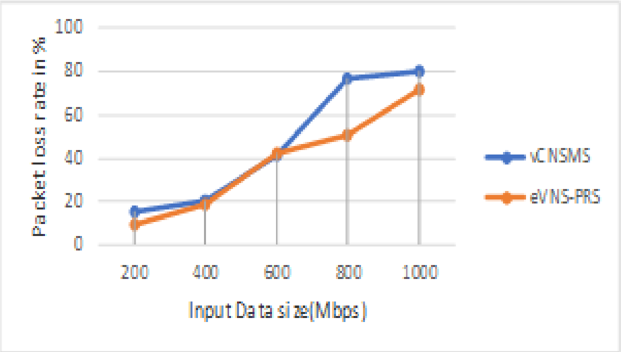

Figure 4: Analysis of packet losses

Cloud Packet Loss Analysis Performance Comparison the above method shows the vCNSMS and the proposed method eVNS-PRS. The eVNS-PRS method is 72% lower in this existing approach vCNSMS.

a. Analysis of time complexity

The time complexity parameter has been calculated by the eVNS-PRS for data from the data pool. The number of host or client connect to the server and response time to calculate time complexity. The figure given below shows the Time complexity by different comparisons as follows.

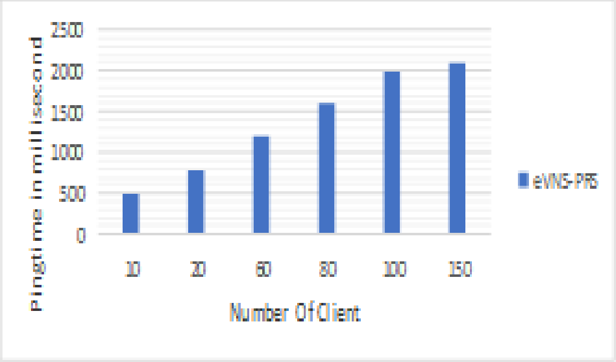

Figure 5: Time Complexity of Cloud response

The above of the graph shows the clients connecting the cloud response time in milliseconds respectively.

b. Failure rate analysis

The success of the cloud is the ability to change the allocation of resources and demand more of their use. However, this is achieved in the cloud from time to time on all system resource allocations facing overhead heaves. Therefore, the failure rate of the proposed system must be calculated to define the efficiency of the system.

The eVNS-PRS overhead does not require the following sequence of operations 200, 400, 600 and 1000 that require the retransmission resource allocation requirements of the work implementing the proposed system. The eVNS-PRS proposed system has a 1.8% very low failure rate of other methods exisiting more of the job under high resource allocation requirements.

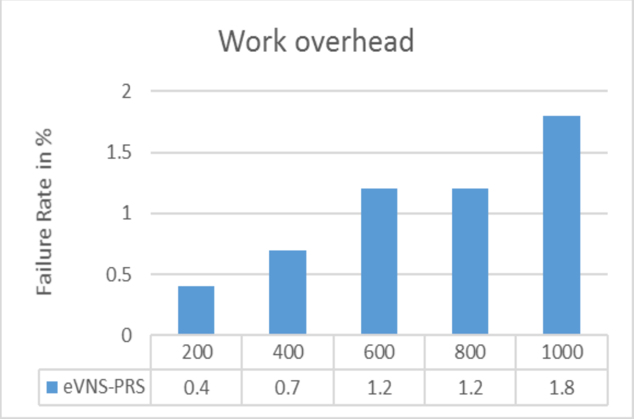

Figure 6 Failure Analysis

V. CONCLUSION

In summary, in this paper, we propose two different parameters such as security and performance of cloud, which have been simulated as a percentage of transmitted data and the overall performance of eVNS-PRS in order to evaluate security, resource availability, request failures, time complexity. Obviously in a cloud environment more eVNS-PRS is used for consumer security. However, there is still room for improvement to improve the performance of the proposed eVNS-PRS. It also identifies a number of factors that can extend the life of a data center in a stable network cloud data center and distribution of VPC security extend the lifetime of the data center within the network thus stabilizing the cloud datacenters.

REFERENCES

1. Md. Mahmud Hasan and Hussein T. Mouftah "Cloud-Centric Collaborative Security Service Placement for Advanced Metering Infrastructures" 2017 IEEE Transactions on Smart Grid, pp - (1-9).
2. Tri Gia Nguyen,Trung V. Phan, Binh T. Nguyen, Chakchai So-In,Zubair Ahmed Baig,And Surasak, Sanguanpong "SeArch: A Collaborative and Intelligent NIDS Architecture for SDN-based Cloud IoT Networks" IEEE 2019, pp - (1-18).
3. Fei Hao, Doo-Soon Park, Jungho Kang, Geyong Mi "2L-MC3: A Two-Layer Multi-Community-Cloud/Cloudlet Social Collaborative Paradigm for Mobile Edge Computing" IEEE 2018, pp - (1-11).
4. Nisrine Bnouhanna,Georg Neugschwandtner "Cross-Factory Information Exchange for Cloud-Based Monitoring of Collaborative Manufacturing Networks" IEEE 2019, pp -(1203-1206).
5. Wenjun Fan, Joanna Ziembicka, Rogério de Lemos, David Chadwick, Francesco Di Cerbo, Ali Sajjad, Xiao-Si Wang and Ian Herwono "Enabling Privacy-preserving Sharing of Cyber Threat Information in the Cloud"2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud),pp - (74-80).
6. Roberto Vasconcelos Melo,Douglas D. J. de Macedo "A Cloud Immune Security Model Based on Alert Correlation and Software Defined Network"2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), pp - (52-57).
7. Dhilip Kumar V, Vinoth Kumar V, Kandar D (2018), “Data Transmission Between Dedicated Short-Range Communication and WiMAX for Efficient Vehicular Communication” Journal of Computational and Theoretical Nanoscience, Vol.15, No.8, pp.2649-2654
8. Jin Yang, Jianmin Pang, Ning Qi,Tao Qi "On-Demand Self-Adaptivity of Service Availability for Cloud Multi-Tier Applications"2015 15th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, pp - (1237-1240).
9. Giuseppe Portaluri,Stefano Giordano "Multi-Objective Virtual Machine Allocation in Cloud Data Centers"2016 5th IEEE International Conference on Cloud Networking, pp - (107-112).
10. A-Young Son, Yeon Soo Lim ,Eui-Nam Huh "Energy-efficient VM placement scheme based on Fuzzy-AHP system for sustainable cloud computing "IEEE 2018, pp -(260-265).
11. Vincent Shi-Ming Huang,Robert Huang,Ming Chiang "A DDoS Mitigation System with Multi-Stage Detection and Text-Based Turing Testing in Cloud Computing"2013 27th International Conference on Advanced Information Networking and Applications Workshops, pp -(655-662).
12. Karthikeyan, T., Sekaran, K., Ranjith, D., & Balajee, J. M. (2019). Personalized Content Extraction and Text Classification Using Effective Web Scraping Techniques. International Journal of Web Portals (IJWP), 11(2), 41-52.
13. Janarthanan Y, Balajee J.M, and Srinivasa Raghava S. Content based video retrieval and analysis using image processing: A review."International Journal of Pharmacy and Technology 8, no.4 (2016): 5042-5048.
14. Bhanuprakash T V, N.R. Sunitha "Agent based adaptive resource allocation algorithms for cloud computing " 2018 IEEE Proceedings of the 2nd International Conference on Trends in Electronics and Informatics, pp - (845-851).
15. Gustavo de los Reyes, Sanjay Macwan, Deepak Chawla, Cristina Serban "Securing the Mobile Enterprise with Network-Based Security and Cloud Computing "IEEE 2012, pp - (1-5).
16. Ran Li,Qingqing Liu,Mingqiang Wang,Xianglin Wei "A novel framework for the application of cloud computing in wireless mesh networks "2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, pp -(448-452).
17. Vinoth Kumar, V., Arvind, K.S., Umamaheswaran, S., Suganya, K.S (2019), “Hierarchal Trust Certificate Distribution using Distributed CA in MANET” International Journal of Innovative Technology and Exploring Engineering, 8(10), pp. 2521-2524
18. Maithili, K , Vinothkumar, V, Latha, P (2018). “Analyzing the security mechanisms to prevent unauthorized access in cloud and network security” Journal of Computational and Theoretical Nanoscience, Vol.15, pp.2059-2063
19. Liu Qing,Zhu Boyu,Wan Jinhua,Li Qinqian "Research on Key Technology of Network Security Situation Awareness of Private Cloud in Enterprises"2018 the 3rd IEEE International Conference on Cloud Computing and Big Data Analysis, pp -(462-466).
20. Kouser, R.R., Manikandan, T., Kumar, V.V (2018), Heart disease prediction system using artificial neural network, radial basis function and case based reasoning, Journal of Computational and Theoretical Nanoscience, 15, pp. 2810-2817.
21. Sultana, H Parveen; Shrivastava, Nirvishi; Dominic, Dhanapal Durai; Nalini, N; Balajee, J.M. Comparison of Machine Learning Algorithms to Build Optimized Network Intrusion Detection System, Journal of Computational and Theoretical Nanoscience, Volume 16, Numbers 5-6, May 2019, pp. 2541-2549(9).
22. Wang Li, Jing Chao, Zhou Ping "Security Structure Study of City Management Platform Based on Cloud Computing under the Conception of Smart City"2012 Fourth International Conference on Multimedia Information Networking and Security, pp - (91-94).
23. Yara AlHumaidan, Lama AlAjmi, Moudhi Aljamea, Maqsood Mahmud "Analysis Of Cloud Computing Security In Perspective Of Saudi Arabia"2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), IEEE 2018, pp - (1-4).
24. Jayasuruthi L,Shalini A,Vinoth Kumar V.,(2018) ” Application of rough set theory in data mining market analysis using rough sets data explorer” Journal of Computational and Theoretical Nanoscience, 15(6-7), pp. 2126-2130
25. Anshul Kesarwani, Chandani Gupta, Manas Mani Tripathi, Vishnu Gupta, Rahul Gupta, Vijay K.Chaurasiya "Implementation of Chinese Wall Model in Cloud Computing for Enhanced Security “, IEEE 2011, pp - (411-413).

AUTHORS PROFILE

U. Udhayakumar, has received his B.Sc(CS) from Shanmuga Industries Arts and Science College, Tiruvannamlai in 2002 and M.Sc(CS) from Sengunthar arts and science college, Tiruchencode in 2004.Currently pursuing Ph.D. degree in Bharathiar university, Coimbatore. His Research area includes Big data analytics, Cloud computing and Network Security.

Dr. G. Murugaboopathi, received the Undergraduate Degree in Computer Science and Engineering from Madurai Kamaraj University in 2000, the Post Graduate degree in Digital Communication and Network from Madurai Kamaraj University in 2002 and Ph.D in Computer Science and Engineering at Bharath University, Chennai. He has more than 45 publications in National, International Conference and International Journal proceedings. He has more than 17 years of teaching experience. His areas of interest include Wireless Sensor Networks, Bioinformatics. Mobile Communication, Mobile Adhoc Networks, Mobile Computing, Cloud Computing, Network Security, Network and Data Security, Cryptography and Network security. He is currently working as an Associate Professor in the Department of Computer Science and Engineering at Kalasalingam Academy of Research and Education, Tamil Nadu, India