IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Security for Virtual Machines in Cloud Services using VMM

Naveen Kumar A. N.[1], Udaya Kumar N.L.[2]
[1]Research Scholar, Sri Siddhartha Academy of Higher Education, Agalakote, Tumakuru, naveenkumaran@ssit.edu.in
[2]Associate Professor, Dept of CSE, SSIT, Tumkur, msgraceuk@gmail.com

Abstract : Cloud computing is the on-demand delivery of the IT resources over the internet on Pay-as-you use system. Since Virtualization is the key player of Cloud computing, it is necessary to have more knowledge on Virtualization environment to avoid attacks, intrusions and system failures. Virtualization enables the creation of virtual resources (instances) by consuming existing physical resources. Here we introduce an approach to provide the security for the Virtual machines and their required resources by allowing them to work normally without problems. This approach checks each and every request coming from Virtual machine for its authentication and validity and make them to work normally if they are valid requests otherwise stop allocating resources to Virtual machines.

Key words: cloud services; Hypervisor (VMM: Virtual Machine Manager/Monitor); security; vulnerability; virtual instance, Security Supervisor (SS);

INTRODUCTION

Computational power, server capacity, applications, platforms, softwares etc are the IT resources, which are available to customers whenever they need, from cloud service providers through the internet. The virtualization logically partitions these resources to create a pool of logical resources by reducing the initial investment and increases the rate of utilization.

Generally, the cloud models are divided into two types. Deployment models and Service models. In Deployment models, we have three basic types of clouds, Public, Private and Hybrid cloud. There are three basic types of clouds in service models, Infrastructure as a service (IaaS), Platform as a service (PaaS) and Software as a service (SaaS). Iaas is the base, over which PaaS will run and above that SaaS will run. Hypervisor plays very important role in both the models in creation of logical resources. Hypervisor is also called as Virtual Machine Manager (VMM). Cloud computing becomes a new way of computing, which plays an important role in both IT companies and academics. To make services possible in cloud computing, it requires some promising techniques such as Service Oriented Architecture (SOA), Service Oriented Modelling and Architecture (SOMA) and other open architectures to develop the cloud applications, that are platform independent, portable and easily usable. Though the use of virtualization in cloud computing has many benefits, it is suffering from security problems, when sharing the logical resources. In addition, data security is the biggest issue of cloud computing. It is necessary to have the suitable security mechanisms to protect both logical and physical resources.

Hypervisor enables provision of resources based on customer demand and allow the resources to share among many customers, this enables cloud computing to have the property called multi-tenancy, there by reduces cost of using those resources. The presently available security mechanisms may not fulfill the needs of security in cloud computing. Here we focus on challenges of virtualization security, vulnerabilities, impact of virtualization on cloud services and propose an approach to overcome these problems.

VIRTUALIZATION

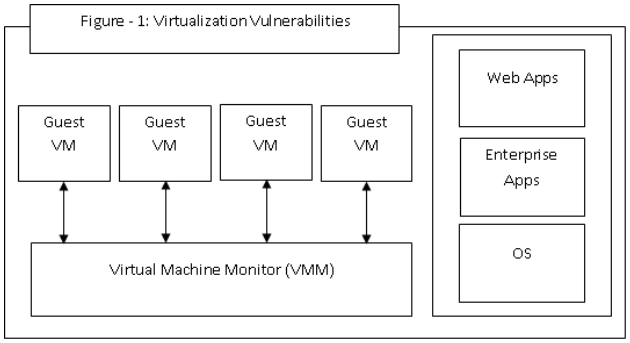
Virtualization is the process of separating the logical resources from physical resources there by fulfill the multiple requests coming from different users. For example, by using logical memory, the processes can allocate more memory than available physical memory with the help of exchanging the data and information from main to secondary and vice-versa, Though the physical resources are partitioned and allocated to different users, each user has a feel that they have their own resource and work like as if they work with physical resource. This technique is also work with various layers of resources like networks, server, desktop, platform, application etc.,

A Hypervisor is a piece of software, whose main function is to create virtual resources from the existing physical resources. For example, multiple virtual machines can be created by one existing physical machine, after creating the machines or instances, it is the responsibility of the hypervisor to take care of those machines. It has to allocate the resources such as compute power, storage, server etc., required by the machines to make them work according to user requirements. It is the responsibility of the hypervisor to de-allocate the resources from that virtual machine after the work is over and release the instance. The important factor is, the creation of required number virtual resources depends on the available size of the physical resource. There are two types of hypervisors, Type1 and Type2 hypervisors. Type1 is also called as Bare metal or Native hypervisor, Type2 is also called as Hosted hypervisor. Virtual machines are called as Guest machines and physical machines are called as Host machines. The Operating system running in guest machines are called as Guest operating systems and operating systems running in host machines are called as Host operating systems. Type1

hypervisor directly runs on the physical hardware but Type2 hypervisor runs on host operating system. Type1 has direct control of hardware whereas type2 has to interact hardware via host operating system. Bare metal hypervisor uses high-level resource management policies to compute a target memory allocation for each virtual machine based on the current infrastructure load and parameter settings for each of the virtual machines.

SECURITY RISKS

The machine where the Hypervisor is running is the one, who acts as central control point for the purpose of allocating the resources to the virtual instances created before processing starts and de-allocating the same resources from those instances after the processing is over, there by releases the virtual instances. Since it is in the position of creating, allocating and de-allocating of resources, it may be vulnerable to attacks. As shown in figure below, the Virtual Machine Monitor become the weak point. The virtual instances of some other physical machine may try to resources from this VMM and it may try to inject the attacks to the virtual environment by breaching the security measures.



Authorised users and accesses: The authorised users have more rights than the ordinary users. The chances of injecting the attacks and involving in problematic access to the resources are usually more with the authorized users only, because the ordinary users are usually avoided at the basic level of security thereby avoiding the serious attacks at the initial stage itself. The main problem is identifying the authorized users who are involving in problematic activities, because they have authorization to access the resources and enter into the virtual environment and easily involve in such activities, which is one of the main issue.

Protection: Service on request and Dynamic elasticity are two important characteristics of cloud computing. When there is a request from customers for IT resources, the same has to be provisioned by the cloud service providers without fail. These resources are provided with some level of protection mechanisms, whenever the customers' requests for the resources which are different from previous requests, the protection mechanisms must identify these changes in the requests and intimate the cloud service providers and try to provide the required level protection to changed requests. These requests dynamically change according to the needs of the users. As cloud computing gaining importance day by day, the quality and level of service and protection should be increased so that the customer safely and securely use resources which may lead to increase in the cloud business and help providers to involve in implementing high level of protection and security systems to satisfy more customers. This is one of the issues of cloud computing.

Resource availability: This is one of the benefits facilitated by the concept virtualization. It also helps to track and leverage the resource pool under the same umbrella of resource units. Availability is not just a technology issue; it is a business issue as well. When it is working, you don't know it is there, so it is easy for management to assume it always will be. Achieving very high level of resource availability usually requires substantial investment by the cloud owners on infrastructure and other resources and virtualization concept to make logical resources with adequate security mechanisms to protect both physical and logical resources.

Veracious data: Originality of data and information is very important. If the original data is not received by the receiver, it is of no use. It is very much necessary to maintain and retain the original data without contamination and corruption. During the transmission of data over the internet, to or from the storage devices or servers, it may be affected by attackers or intruders because internet is open to all and nobody owns it. The restricted users can contaminate and inject the attacks to the original data during transmission so that the destination may not receive the data in original form. If such corrupted data is used in IT companies to run their business and to take the important decisions, which helps to improve their businesses. This is one of the issues of cloud computing.

Service Secrecy: The cloud service users requests for the required resources such as softwares, applications, infrastructures, platforms or storage from the cloud service providers. In this scenario the customer has to interact with the cloud service provider and their cloud services. During this interaction, exchange of data and confidential information with respect to cloud services will be happened using network transactions. In this situation, it is necessary to maintain customers information and their status safely and securely. The restricted users can try to hack customer's confidential information. This may create serious problems to customers. In addition, when many customers are sharing the common resources among them, it is necessary to avoid each customer from using or knowing the usage or status of other customers to avoid the problems. This is one of the issues of cloud computing.

Migrating instances: Generally, the virtual machines or instances which are created from the physical machines are available in the form of files. These files can go from one physical machine to another physical machine. During this movement of instances, they may vulnerable to attacks and problems. When they affected by the malwares or viruses they can create the problems to other virtual instances and also to physical machines by changing their settings, configurations and corrupting the files and folders of other virtual instances. This may tend leakage of data and information and in turn virtual instances may behave improperly. Sometimes this may create the problems to the operating systems running in physical machines. When these physical machine's operating systems are corrupted, these corrupted operating systems can create the problems to virtual instances. They may not allocate the required resources to the virtual instances, or they may de-allocate the resources from the virtual instances early before they complete the processing. It is the responsibility of OS to allocate and de-allocate the resources required by the virtual instances after their creation. This is also one of the serious issues.

Service Level Agreement: It is the agreement or contract made between cloud service provider and service user before resources are provisioned to the user after their

request. It plays very important role in cloud service business. It is very essential to make the cloud service business possible. It defines the level of service availability, response time, how reliable the resource components are, responsibilities of both customer and service user and other warranties with respect to service components. It specifies how the service user has to utilize the resources without breaching the SLA by maintaining the resources in the proper condition and specifies how the service provider has to provision the resources to the user, quality of services, replacement of resources when something happens, maintaining the uptime and backups, providing the quality of service, decreasing the response times etc. Tailoring the separate SLA for each and every customer is one of the biggest issues of cloud service business. When virtual instances created from physical machines, usually different operating systems are installed on virtual instances to make them to run compatible applications. After creation of instances, managing, maintaining and providing protection to those instances is the tedious task. Since they have different operating systems and applications running, it should be mentioned in agreement so that both service provider's and service user's responsibility in taking care of instances or virtual machines. The provider must neatly configure and settings should be made to those instances and attach security mechanisms. The service user must maintain this virtual instance by proper handling with proper updates and compatible patches which are received from service provider. This is the reason to say that stitching a separate SLA for every customer is the tedious task.

In addition, virtual instances which are created from same physical machine must be isolated properly to make them run independently to process by running the compatible applications without any dependency. But sometimes it is possible that the virtual instances that are malicious, may attack neighbour instances or disrupt their normal routines by stealing the resources from them or by corrupting the data required to process by them or by injecting the malwares to the guest operating systems so that the guest operating systems should not work properly to handle the processing required by the customers. This leads to the serious problem to the virtual machine resources such as network bandwidth, memory, computational power that are shared among multiple users. This is one more situation where Service Level Agreement has to define the clear-cut isolation policies among the virtual instances created from the same physical machine, which is a serious issue.

PROPOSED APPROACH

We are proposing an approach where a virtual machine enters Cloud environment and send requests to VMM for receiving the resources. That request pass through the **Security Supervisor (SS)**. The Security Supervisor checks the virtual machines details and its requests for validation. This provides the result in distinguishing malicious machine identification from non malicious one. If the virtual machine does not satisfy the Security Supervisor, then it will be treated as infected or malicious and it will be disconnected from environment. It will not get the permission to access the resources. If it is recognized as a valid virtual machine, then it will be registered and allow it to access the resources based on the control policy. This method will provide security to virtualization environment by avoiding infected virtual machines resource requests.

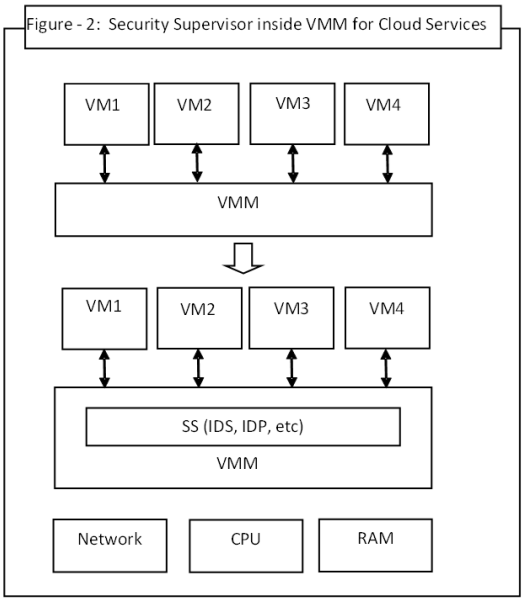


Figure - 2: Security Supervisor inside VMM for Cloud Services

Algorithm (shows the function of Security Supervisor):

1. Virtual machines (VMs) are created from available physical resources.
2. VMs Sends request to Virtual Machine Manager to get resources to run the applications.
3. That request will be sent to the Security Supervisor.
4. Check for Authentication and validity.
5. If Invalid, stop allocating resources and disconnect that VM from the environment.
6. If valid, check for access control policy.
7. Allow it to access resources.

A different types of security mechanisms, problem identification functions, problem correction methods, avoiding restricted users and accesses, process of hiding the originality of data mechanisms, methods of identifying and avoiding intruders, attackers, malwares, viruses should be included in Security Supervisors.

In addition, it may contain some updates and patches required by the virtual machines and softwares. It should have the flexibility of including the latest techniques and other solutions which may work very well in future. It should have the routine of redesigning its methods and solutions and keep updating at regular intervals so that it should always contain latest, adequate and effective security solutions.

- It may give the flexibility that, some security solutions can directly be injected to the virtual machines itself.
- Performance issues may exist when implementing such type of security solutions inside the Security Supervisor.

Overall Response Time Summary (When SS, IDS and IPS absent and all VMs are normal)

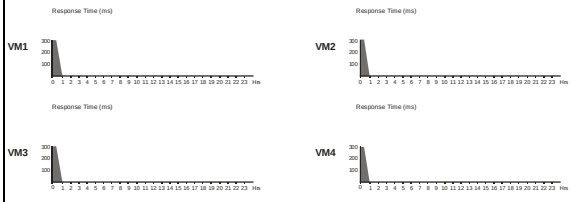
Export Results

	Average(ms)	Minimum(ms)	Maximum(ms)
Overall Response Time:	300.382	235.986	364.619
VMM Processing Time :	0.35	0.02	0.64

Response Time:

Virtual Machine	Avg (ms)	Min (ms)	Max (ms)
VM1	300.110	232.612	360.113
VM2	301.165	232.615	375.110
VM3	300.461	237.111	360.119
VM4	299.795	241.608	363.137

VMM Hourly Average Response Times



Memory Used:

Virtual Machine	Avg (ms)	Min (ms)	Max (ms)
VM1	410	390	426
VM2	410	393	432
VM3	407	387	440
VM4	409	380	430

Total Virtual Machine Cost: $ 0.50
Memory Allocated for each VM: 512 Mb

VM Request Servicing Time:

Avg	Min	Max
0.46	0.071	0.76

Overall Response Time Summary (When SS, IDS and IPS absent and VM1 is infected)

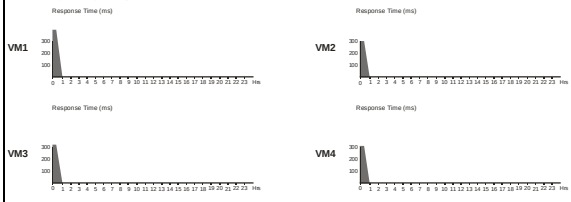
Export Results

	Average(ms)	Minimum(ms)	Maximum(ms)
Overall Response Time:	315.623	290.889	349.586
VMM Processing Time :	0.49	0.06	0.78

Response Time:

Virtual Machine	Avg (ms)	Min (ms)	Max (ms)
VM1	358.617	312.307	418.732
VM2	300.423	279.412	320.608
VM3	302.338	280.360	331.117
VM4	301.117	291.480	327.889

VMM Hourly Average Response Times



Memory Used:

Virtual Machine	Avg (ms)	Min (ms)	Max (ms)
VM1	482	413	560
VM2	412	387	429
VM3	408	380	430
VM4	408	382	426

Total Virtual Machine Cost: $ 0.50
Memory Allocated for each VM: 512 Mb

VM Request Servicing Time:

Avg	Min	Max
0.69	0.082	0.92

Overall Response Time Summary (When SS, IDS and IPS absent and VM1 is infected and affects VM4)

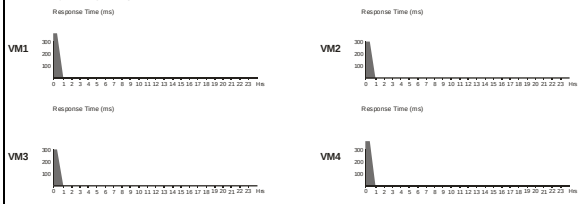
Export Results

	Average(ms)	Minimum(ms)	Maximum(ms)
Overall Response Time:	329.649	298.269	374.653
VMM Processing Time :	0.51	0.08	0.81

Response Time:

Virtual Machine	Avg (ms)	Min (ms)	Max (ms)
VM1	362.581	317.062	427.102
VM2	301.234	272.128	326.860
VM3	300.361	283.776	327.430
VM4	354.420	320.113	417.221

VMM Hourly Average Response Times



Memory Used:

Virtual Machine	Avg (ms)	Min (ms)	Max (ms)
VM1	487	412	568
VM2	411	378	419
VM3	409	387	428
VM4	476	427	579

Total Virtual Machine Cost: $ 0.50
Memory Allocated for each VM: 512 Mb

VM Request Servicing Time:

Avg	Min	Max
0.72	0.12	0.96

Overall Response Time Summary (When SS, IDS and IPS present and VM1 is infected)

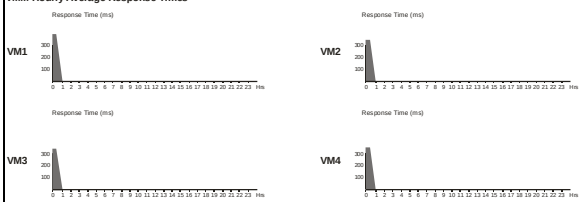
Export Results

	Average(ms)	Minimum(ms)	Maximum(ms)
Overall Response Time:	359.219	302.574	404.727
VMM Processing Time :	0.33	0.039	0.66

Response Time:

Virtual Machine	Avg (ms)	Min (ms)	Max (ms)
VM1	392.461	340.318	470.641
VM2	348.806	278.189	367.460
VM3	346.342	287.874	383.366
VM4	349.268	303.918	397.442

VMM Hourly Average Response Times



Memory Used:

Virtual Machine	Avg (ms)	Min (ms)	Max (ms)
VM1	476	410	530
VM2	409	379	432
VM3	411	383	441
VM4	409	381	430

Total Virtual Machine Cost: $ 0.60
Memory Allocated for each VM: 512 Mb

VM Request Servicing Time:

Avg	Min	Max
0.481	0.087	0.83

Overall Response Time Summary (When SS, IDS and IPS present and VM1 is infected and affects VM3)

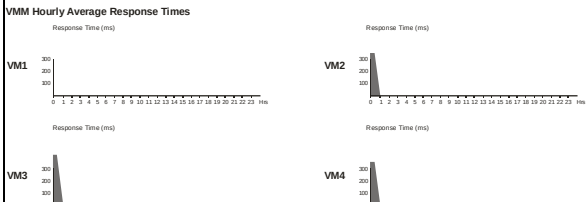
Export Results

	Average(ms)	Minimum(ms)	Maximum(ms)
Overall Response Time:	278.256	243.044	322.607
VMM Processing Time :	0.31	0.023	0.63

Response Time:

Virtual Machine	Avg (ms)	Min (ms)	Max (ms)
VM1	0	0	0
VM2	349.903	282.918	376.110
VM3	412.573	382.114	502.160
VM4	350.611	307.147	412.160

VMM Hourly Average Response Times



Memory Used:

Virtual Machine	Avg (ms)	Min (ms)	Max (ms)
VM1	0	0	0
VM2	410	382	431
VM3	492	412	570
VM4	408	387	428

Total Virtual Machine Cost: $ 0.60
Memory Allocated for each VM: 512 Mb

VM Request Servicing Time:

Avg	Min	Max
0.46	0.086	0.81

Overall Response Time Summary (When SS, IDS and IPS present and all VMs infected and VM1 recovered)

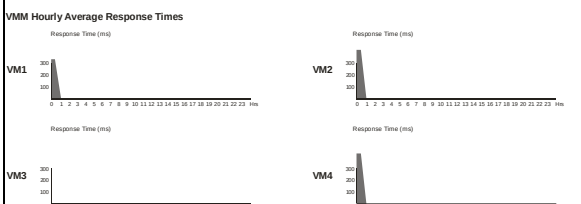
Export Results

	Average(ms)	Minimum(ms)	Maximum(ms)
Overall Response Time:	296.150	268.272	343.621
VMM Processing Time :	0.29	0.022	0.64

Response Time:

Virtual Machine	Avg (ms)	Min (ms)	Max (ms)
VM1	343.416	293.437	369.471
VM2	413.690	387.421	498.603
VM3	0	0	0
VM4	427.496	392.230	506.412

VMM Hourly Average Response Times



Memory Used:

Virtual Machine	Avg (ms)	Min (ms)	Max (ms)
VM1	408	387	432
VM2	462	408	517
VM3	0	0	0
VM4	457	398	506

Total Virtual Machine Cost: $ 0.60
Memory Allocated for each VM: 512 Mb

VM Request Servicing Time:

Avg	Min	Max
0.53	0.12	0.94

RESULT ANALYSIS & CONCLUSION

We used Cloudsim Simulator to simulate various scenarios by applying different inputs and injecting malwares to test how the VMs in the Cloud environment will behave for inputs and how they work when malwares are present and impact of malwares on normal VMs.

In the first case, the Intrusion Detection System, Intrusion Prevention System and other security mechanisms are not introduced i.e. Security Supervisor is absent. In this case, all virtual machines are in normal condition, its response times, memory consumptions (Allotted and consumed) and service times are recorded. In the second case, VM1 is infected and the results are

recorded, we can observe that the memory consumption and Overall response time of VM1 is varied (much difference) when compared with other normal VMs. In case three, impact of infected VM1 is shown and results are recorded, here infected VM1 disturbed VM4, so that VM4 also behaves like VM1 by consuming more memory and increasing Overall response time. In case four Security Supervisor (SS) is introduced, and make VM1 infected and results are recorded.

In the fifth case we observe that infected VM1 make VM3 to work abnormally by consuming more memory and increasing its Overall response time and at the same time we observe that SS directs VMM to deallocate all the resources given to VM1 and make VM1 no more, to avoid further disturbance by the VM1 to other VMs.

In the last case, we can observe that, VM1 is recovered, VM3 is stopped by deallocating resources from it and remaining VMs are infected and results are recorded.

REFERENCES

[1] N. L. Udayakumar and Dr M.Siddappa, 2010, "Meeting the challenge of Virtualization impact on Cloud services", *In International Journal for Engineering Research & Technology* (IJERT), 2010.pp.55-57

[2] Yamini B & selvi D V, 2010, "Cloud virtualization: A potential way to reduce global warming", *In recent advances in space Technology services and Climate change* (RSTSCC), 2010.pp.55-57

[3] Szefer, J., et al. 2011, "Eliminating the hypervisor attack surface for a more secure cloud", *Proceedings of the 18th ACM conference on computer and communication security, Chicago, Illinois, USA*, ACM:401-412.

[4] K.Owens, "Securing virtual computer infrastructure in the cloud", *white paper, savvis communications corp.*, 2009.

[5] A.Jasti et al., "Security in Multi-tenancy cloud", *proc. IEEE Int Carnahan Conf. security technology (ICCST 10)*, IEEE Press, 2010.

[6] T.Ristenpart et al., "Hey you Get off my cloud: Exploring information leakage in third-party compute cloud", *proc 16th ACM conf. computer and communication security* (CCM 09).

[7] T.Garfinkel and M Rosenblum, "When virtual is harder than Real: security challenges in Virtual machine based computing environments", *proc. 10th workshop on hot topics in Operating systems.*

[8] J.Oberheide, E. Cooke, and F.Jahanian, "Empirical exploitation of live virtual machine migration", *proc. Black Hat DC 2008 convention, 2011*; *www.net-security.org/dl/articles/migration.pdf.*

[9] Salesforce.com, Force.com, http://www.salesforce.com/platform/

[10] https://apps.gov/cloud/advantage/main/start page.do

[11] CloudSecurityAlliance,http://www.cloudsecurityalliance.org/

[12] G. J. Popek and R. P. Goldberg, "Formal requirements for virtualizable third generation architectures," *Comm. ACM*, vol. 17, no. 7, pp. 412– 421.

[13] Hassan Takabi, James B.D. Joshi, Gail-Joon AHN, "Security and Privacy Challenges in Cloud Computing Environments", *IEEE Security & Privacy, 2010*, 10(6): 24-31.

[14] Siani Pearson, Azzedine Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing", *Proceedings of IEEE International Conference on Cloud Computing Technology and Science*, 2010, 693-702.

[15] Prasad Saripalli, Ben Walters, "QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security", *Proceedings of IEEE 3rd International Conference on Cloud Computing (ICCC)*, 2013, 280-288.

[16] Gunnar Peterson, "A Security Architecture Stack for the Cloud", *IEEE Security & Privacy*, 2010, 10(5): 83-86.

Dr. Udaya kumar N. L. received B. E. degree in Computer Science & Engineering from University of Bangalore, Karnataka, India in 1993 and M.Tech degree in Computer Science & Engg from VTU, Belgaum, Karnataka in 2007. He has teaching experience of 16 years. He published 03 Technical Papers in National, International Conference and Journals. He is a Life member of ISTE. He is working in the field of Cloud Computing, Virtualization, Storage Networks and Computer Networks. He is working as an Associate Professor in Department of Computer Science & Engineering from 2004 in Sri Siddhartha Institute of Technology, Tumkur.

Naveen Kumar A. N. received the Bachelor of Engineering Degree in Computer Science and Engineering from Bangalore University, Bangalore, Karnataka, India in 1998 and the Master of Technology degree in Computer Science and Engineering from Visveswaraiah Technological University, Belgaum, Karnataka, India in 2001.

Mr. Naveen Kumar Adalagere Nemirajaiah is a Life Time member of Indian Society for Technical Education, New Delhi, India. He is currently pursuing the Ph.D. degree in Computer Science and Engineering at Sri Siddhartha Academy of Higher Education, Agalakote, Tumakuru, Karnataka, India.

He is having teaching experience of 19 years, 1 year as a Computer Operator Trainee at IISc, Bangalore, Karnataka, India and another 1.1 years as a Nodal Officer (Under Computerization Programme of Govt. of Karnataka, India for District Urban Development Cell - Tumakuru Urban and Bangaluru Rural), Karnataka, India. He is currently working as an Associate Professor in Department of Information Science & Engineering from 2018 in Sri Siddhartha Institute of Technology, Tumkuru, Karnataka, India.