International Journal of Advanced Technology in Engineering and Science
Vol. No.5, Issue No. 03, March 2017
www.ijates.com
ijates
ISSN 2348 - 7550

ANALYSIS OF NETWORK SECURITY ISSUES IN CLOUD BASED NETWORKS AND COUNTER MEASURES WITH SOFTWARE DEFINED NETWORKS

Dr.Chinthagunta Mukundha

Associate Professor, Department of Information Technology
Sreenidhi Institute of Science and Technology, Yamnampet, Ghatakesar,
Hyderabad, Telangana (India)

ABSTRACT

Cloud computing is an emerging technology and all the areas are using cloud computing resources like infrastructure, platforms and services. Cloud is accessed by many people from different geographic locations so providing security for cloud based network is a challenge. There are so many cloud security issues like Data Protection, Contingency Planning and User Authentication .In this paper myself proposed some of the techniques to solve Data protection, Incident Planning and User Authentication security issues in the cloud networks using software defined networks. Software-defined networking is an approach to computer networking that permits network administrators to employ network administrative services through abstraction of higher-level functionality.

Keywords: Emerging Technology , Data Protection , cloud security ,software defined networks

I. INTRODUCTION

Providing cloud computing resources is a complex task in cloud environment. Cloud offers different services like Applications, Infrastructure, Monitoring, Communication and Platform. To provide security for all these resource in cloud with different locations cloud face different security issues like Data protection, Contingency and Authentication .Data protection defines different issues like Data Location , Data Segregation , Data recovery and Long term visibility of data. Data Location deals with the location of cloud server ,Cloud user has any right on taking the decision on cloud data location or not. Data Segregation is a mechanism for encrypting the data in cloud server and the techniques that are used for data segregation in the cloud .Data recovery is another issue under Data security how the data is retrieved from the data losses. Contingency is another security issue under long term viability of the cloud provider. Last and more important issue is like Authentication of cloud users , Providing access to resource to privileged users .In this paper I proposed different techniques for some of the above mentioned cloud security issues using software defined networks.

Software defined networking (SDN) is a new technology to provide automated, simple, scalable and efficient solutions for networking and cloud solutions. It is highly impossible for a rigid system that's difficult to manage, maintain, and upgrade. So to provide flexibility, simplicity, and the ability to quickly grow to meet changing IT

and business needs we need a new system .If the network is totally within the premises, cloud based, or a hybrid of both, these networks gives the vast communication links that organizations need in order to execute their services ,deliver services and be competitive. Software defined networking provides a new way of looking at how networks are controlled, Configured and operated. Software defined networks provide checking indirect security violations with open flow allows various set field actions that can dynamically change the packet headers. Software defined networks are also provide a security for the data by using security mechanism like firewalls.

By Combining the feature of software defined networks with cloud computing it is possible to generate highly secure and flexible cloud environment .software defined networks allows the cloud developers to build cloud network with easy and secure manner by implementing security measures in SDN devices like switches and routers. SDN enables you to makes use of virtualization to greatly enlarge network efficiency and thus provide solutions to the need for increased capacity without breaking the bank, and making the management easy of those consolidated resources.SDN changes that equation in a very basic way: SDN automates the organizing the processes management like provisioning, configuration, and remediation via software. Rather than need of an IT employer to physically manage and configure each piece of hardware, SDN enables you to jump from network changes by sending out software updates. One important capability of an OpenFlow network is that the controller has network-wide intelligence of the system. Certain Open Flow switches can be connected to a single controller and it is then possible to make judgment in a centralized manner. Instead of having several network devices with a limited intelligence of the network, a single controller decide to take decisions based on its knowledge of a broader part of the network.

This paper is completely organized into five sections. In the first section discussed brief introduction about Software defined network and cloud computing issues. Second part is about Literature survey, third section discuss about system model, forth section about the challenges in security issues and the last one gives the conclusion of paper.

II. LITERATURE SURVEY

There are various security problems for cloud computing as it is implemented with many technologies like operating systems, virtualization with hypervisors, networks, databases, resource scheduling, transaction management, load balancing, memory management and concurrency control. So that security issues for most of these technologies are applicable to cloud computing. For example, the network that establishes the connection with the systems in a cloud has to be secure. Furthermore, virtualization model in cloud computing concludes in several security issues. For example, mapping of the virtual machine with the hypervisor to correct physical machine carried out securely and it is a big challenge. Securing the data is by implementing encryption techniques and for sharing the data ensure that appropriate policies are implemented or not. With these, allocating the resources and memory there is a need of implementing the algorithms in a secure manner. Finally, there is a need of implementing data mining techniques for detecting the malware in clouds.

Providing security in cloud computing is the very important issue. We are placing all the things with the service providers it makes the data highly insecure. This is the main problem of adopting the cloud computing environment. IDC's held a survey on the cloud security, services concerns are number one issue facing cloud

computing. IDC's findings in the survey of 224 IT executives are shown in fig.1. Main difficulties facing with the cloud computing is the danger of-Disrupts Services, Loss of Privacy, Theft of Information and Damage of information. The companies adopting cloud computing services can prevent these problems. These security issues can be overcome by applying highly trusted security protocols. Causal Productions has used its best techniques to ensure that the templates have the same appearance.

Generally cloud computing model uses public networks and at the same time keeps the transmitting data exposed to the world, any form of cyber attacks are anticipated for cloud computing. The current implemented cloud based services have been identified to suffer from vulnerability issues with the existing security drawbacks that cloud existence of possible security loopholes that could be abused by an attacker. Privacy and security both are very important things of cloud computing because of its nature of such computing approach. Cloud computing implementation is same for both the information security and network security issues. Implementing cloud computing with third party might emerge as a problem for cloud environment along with other security threats inherent in virtual machine and infrastructural aspects. Elements like Social engineering, human errors and software bugs make the security for cloud a dynamically challenging one. It very important to implement Intrusion detection system for reduces security risks and seamless network monitoring. If the contemporary IDSs are not fit, the resultant consequence might be undetected security breach for cloud environment.

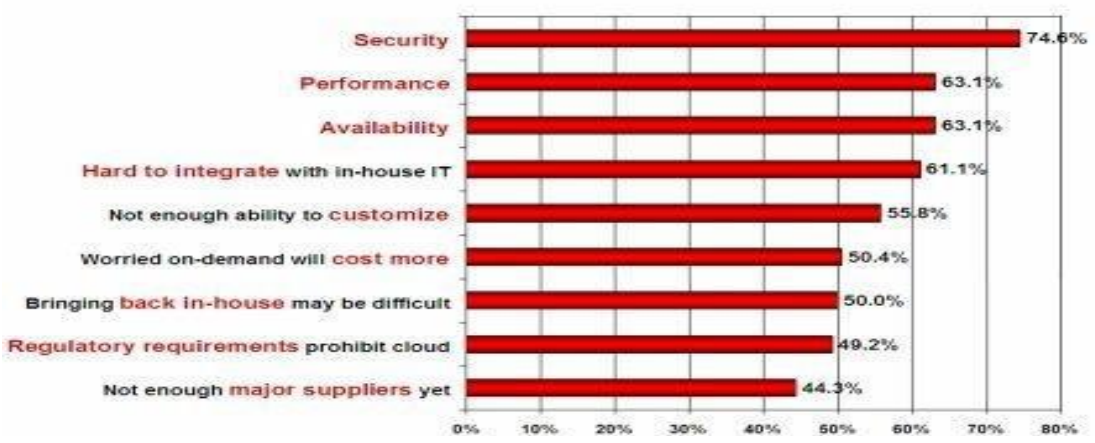

Fig: survey of 224 IT executives

The characteristics of security threat might be imported into cloud computing model are ranging from different technologies like virtual servers, database, networks, operating systems, load balancing, concurrency control and memory management. First and basic unavoidable security challenges for cloud users are Data segregation and session hijacking. Another challenge for cloud model is in its abstraction levels as well as scalability to provide resources in dynamically it tends to poorly defined security or infrastructural boundary. There is a chance to vary the Privacy and its underlying concept significantly in different regions and thus it may lead to security violations for cloud services in specific contexts and scenarios. Data loss and various botnets can come into action to violate security of cloud servers. When we discuss about security multitenancy is also an important criteria. Cloud providers are responsible for providing security in the cloud data-centers because a single server maintains a data of many clients in a single shared platform in terms of physical server or operating system. Cloud service provider is also responsible for the storage security at data centers of the cloud services. All these

conventional security risks are thus applicable with added degree of capability in a cloud infrastructure which makes the ongoing success of cloud computing a quite challenging one. All cloud environments fall under the categories like availability, confidentiality and integrity. Cloud model threats are applicable both infrastructure and data.

Normally enterprise applications are a mix of old and newly implemented cloud based services. As the network architecture evolves to support the next phase of cloud and virtual networking needed to bring these worlds together, it is important to look at the two main elements in a Software Defined Network.

OVERLAY SDN

SDN overlays utilize network virtualization to decouple and abstract the physical topology of networks from a 'logical' or 'virtual' topology by implementing the concept of encapsulated tunneling. This logical network topology is often referred to as an 'Overlay Network'. In these models some network characteristics and functions are placed into overlays to control the data, precise flow or forwarding path. This may include:

1. Software overlays to transfer management characteristics from the control plane of the switch to servers.
2. Specific network services such as access control, load balancing, visibility controllers and fire walling for SDN overlays leverage existing physical networks to deliver functions such as provisioning and visibility.

UNDERLAY SDN

Controllers do not clear up the broader set of difficult high-performance network issues that exist at L2/L3/L4. To accomplish that we need a determined wire-speed SDN data plane as the physical 'Underlay Network.' To utilize perfectly the efficiencies of an SDN overlay while providing maximum transparency and performance, the underlying physical network must increase linearly and programmatically interface in a seamless manner with new network virtualization capabilities with very limited dispute and limited end-to-end latency. The use of open standards and open APIs allows it possible to be controller skeptic and interoperable with other network infrastructure elements such as load balancers, firewalls and Wi-Fi.

At the core of every cloud, customers demand scalability, resiliency, and 24-hour business-critical uptime every day of the year. Hundreds of switches can easily be located within the same data center and need to instantaneously react to change events anywhere within the topology without dropping packets or creating congestion conditions. To deliver on these requirements, networking platforms have evolved with many of the data plane controller functions distributed and embedded. Link Aggregation Control Protocol (LACP), Open Shortest Path First (OSPF), ECMP, and Border Gateway Protocol (BGP) are primary examples of standards-based distributed controller functions (which are often referred to as traffic engineering protocols). Because the majority of change events typically occur locally, a distributed approach allows the affected network node to operate independently, reacting and resolving changes within split seconds with near-zero packet drop. This distributed approach provides the high-resiliency behavior that is required for around-the-clock every-day uptime. As a result, networks today are rarely the root cause when there are application outage conditions.

Arista SDCN can greatly enhance and automate the operations that are associated with these use cases. Integration with an external controller provides the customized intelligence for mapping, connecting, and tracing highly mobile VMs, while the distributed protocols within the networking devices provide the best-path data forwarding and network resiliency intelligence across large distributed topologies.The migration to private, public or hybrid clouds is revolutionary in technology, but evolutionary in adoption. Arista endorses a broad

spectrum of data, management and control plane capabilities to bring flexibility to customers as shown in Figure 2.

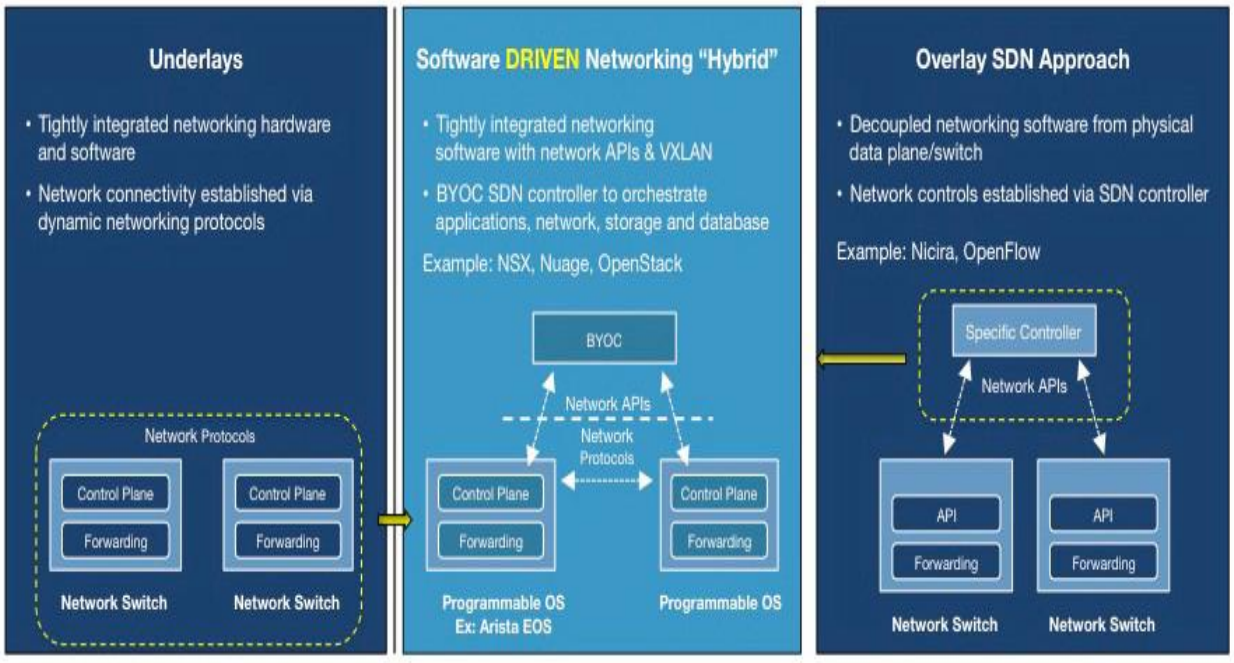

Fig 2: SDN Approaches

III. SYSTEM MODEL

Here designed a model for Secure Authentication or Threat Detection and Data Security of cloud using software defined networks.

1. Model for Secure Authentication or Threat Detection

The SDN paradigm offers a new level of visibility into the cloud networks which is ideally suited for traffic monitoring applications. The controller can program forwarding devices in the network to conduct fine-grained packet inspection on traffic passing through the devices. These statistics, periodically collected by the controller, afford a centralized real-time view of cloud network state which is exposed via open APIs, allowing for automation. Developers can write applications utilizing data mining and machine learning techniques to enable rapid intelligent identification of threats.

a) Denial-of-Service Attack Detection: Security solutions provider Radware has recently developed DefenseFlowTM , the first commercial SDN application that addresses denial-of-service (DoS) attacks. Radware has furthermore contributed a simplified open source version of DefenseFlow, Defense4All, to the OpenDaylight project. DefenseFlow directs the network controller to collect specific flow statistics from forwarding devices in the cloud network at a per second resolution. The application measures baseline traffic flows and then monitors for patterns suggestive of a DoS attack. In the event that a threat is detected, a traffic diversion mechanism programmatically redirects suspicious traffic to a dedicated scrubbing center for detailed traffic inspection, signature analysis, and threat neutralization.

b) Traffic Anomaly Detection: SDN-enabled distributed traffic inspection functionality also has application to anomaly detection solutions. Anomaly detection mechanisms running on Internet core routers cannot process

adequately the high volumes of traffic flowing through at line rates, and, additionally, these mechanisms generate a large number of false positives, which cannot be dealt with practically in the network core.

C. Threat Remediation: In traditional networks, the only possible response to a threat has been to drop offending traffic. SDN, however, with on-the-fly programmatic capabilities, makes possible a richer variety of dynamic responses, including emergency alarms, dynamic quarantine solutions, traffic redirection for forensics, and entrapment mechanisms such as tarpits and honeypots. FRESCO, proposed by Shin et. al is an application development framework facilitating design of sophisticated threat detection and mitigation modules. FRESCO provides a scripting API and basic reusable modules, which can be assigned relevant parameters and stitched together into a desired security configuration. At compilation, these modules produce flow rules which are overseen by FortNOX, a specialized security enforcement kernel which is embedded in the network controller. The author provide two case studies to demonstrate the power and range of FRESCO: first they build Reflector Net,an application to detect and entrap malicious scanners. If an attacker initiates a large number of failed TCP connections, the ScanDetector module is triggered, prompting the ActionHandler module to redirect the traffic to a remote honeypot. The attacker therefore receives valid responses from the honeypot machine, under the impression that it is still communicating with the original target. In the second example, the author demonstrate how FRESCO can be integrated with legacy security applications: monitoring tools such as BotHunter, in the event that they detect a threat, can invoke security applications written in FRESCO script to quarantine infected hosts on the network.

D. Network Verification

A popular area of research is the use of automated techniques to verify network consistency in SDNs. Human operators are prone to make errors: security professionals attending the DEF CON 18 conference recently reported encountering poorly configured networks “more than three quarters of the time” and they were in strong agreement that badly configured networks are the main cause of network breaches. A

Gartner study predicts that in the period 2010 to 2015, 80% of network outages impacting mission-critical services will be due to ‘people and process issues’, and more than 50% of these stemming from configuration modifications and updates and hand-off problems.

In software defined networks, such problems may be encountered when network controllers are shared by different users or applications, or multiple controllers operate in the same domain, leading to conflicting rules, violation of policy, or network faults, such as loops, black holes, access control violations, etc. Malicious parties may even bypass security policies by defining strategic flow rules to re-label and redirect traffic. Furthermore, in the case of large networks potentially comprising hundreds of switches, where multiple applications are able to program the network and SDN controllers have the capability to install approximately 50k new flows per second , there needs to be quick and efficient mechanisms to ensure security compliance, fault tolerance and fast failover.

The SDN paradigm simplifies the traditional network in two very important ways: first the network no longer consists of disparate elements running proprietary protocols but instead comprises uniform switching hardware with standard functionality and interfaces, communicating using a single open protocol. Second, network control is no longer purely distributed over several elements but restricted to the controller. The state and behavior of the network therefore is the logical outcome of configuration commands dispatched by the

controller, and these can easily be modeled using formal techniques. This allows administrators to fault-check networks, verify network properties, and build in failsafe mechanisms. Formal techniques are already being applied in designing 'machine-verified' network controllers, programming languages for software defined networks, and innovative abstractions with verifiable security properties such as isolated network slices and security monitoring routing protocols.

2. Data Security

Providing security for the data in the cloud is more important and very complex, because cloud is accessed by any one at any point of time so the data in the cloud is not secure. To provide the security for the data in the cloud data owner uses some encryption and decryption mechanisms to store data in the cloud environment. These encryption mechanisms are implemented in the SDN Routers data is encrypted into secure form before enter into the cloud servers.SDN Routers are implemented with Encryption standards like AES , Triple DES etc. Figure 3 shows the encrypted system on the cloud using SDN routers.

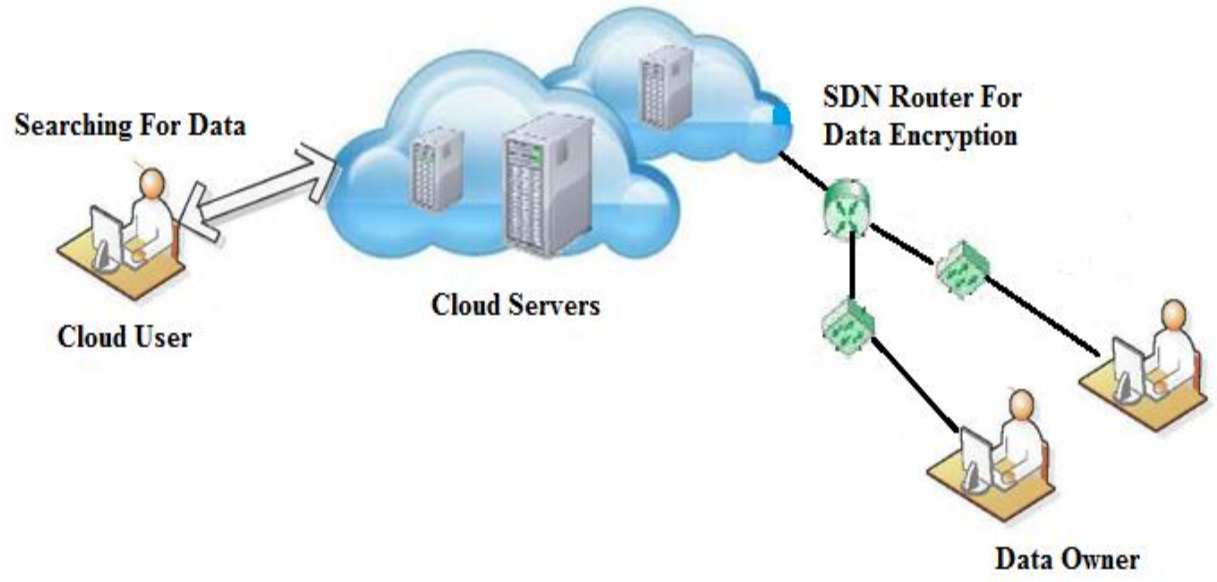

Fig 3: Encrypted System on the Cloud Using SDN

IV. CHALLENGES

a) Securing SDN: Whereas, so far I have summarized research where SDN enables greater security for networks and here discussed the major challenge of securing SDN itself. In a position paper, Kreutz et al. make a persuasive case for the need to incorporate security and dependability into SDN design from the group up. They note that threats in SDN are not only of a different nature as compared to traditional networks, but, by virtue of SDN being highly programmable, the potential impact is also far more serious. They outline certain categories of threats which may be used to attack SDN, including the following: Forged traffic flows may be used to attack network entities, including DoS attacks on switches and controllers. Switches in the network may be exploited or hijacked to launch attacks on other entities. Control plane communications may be targeted with DoS attacks or exploiting weaknesses in TLS/SSL implementations. Faulty or hijacked controllers could wreak

havoc in the whole network. Furthermore, the interface between the controller and high level applications is a potential point of attack.

b) Federating Heterogenous Networks : The SDN programmable networks vision is already being applied to unify network management in WiFi networks , to provide programmable interfaces across the wireless stack, for accessing services in IEEE 802.15.4 networks , and in coordinating services across heterogenous networks . It is anticipated that SDN will also be a key driver in the emerging Internet of Things paradigm , where the centralized control element and standardized protocols facilitate the process of federating disparate devices such as mobile phones, smart TVs, computers, household appliances, sensor devices, healthcare monitors, etc. and enable implementation of federated policies on top. How to manage privacy and trust in a seamless and efficient manner across heterogenous networks and multiple devices is a critical question.

C. Coupling Overlays and Underlays : With advancement in virtualization technologies, overlay networks have become a popular choice for managing data centers and enterprise networks, and successful recent examples include Midokura MidoNet, Nicira NVP , IBM's Distributed Overlay Virtual Ethernet (DOVE) and PLUMgrid . Overlay networks enable finer customization, differentiation in services, and remote management, but may suffer from operational issues in larger and more complex deployments such as wide-area networks due to the loose coupling between the virtual overlay and the underlying physical hardware.

V. CONCLUSION

Cloud computing is a combination of several key technologies that have evolved and matured over the years. Cloud computing has a potential for cost savings to the enterprises but the security risk are also enormous. Enterprise looking into cloud computing technology as a way to cut down on cost and increase profitability should seriously analyze the security risk of cloud computing. The strength of cloud computing in information risk management is the ability to manage risk more effectively from a centralize point using software defined networks. Although Cloud computing and software defined networks can be seen as a new phenomenon which is set to revolutionize the way use the Internet, there is much to be cautious about. There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human's lives easier. However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies. Cloud computing is no exception. In this paper key security considerations and challenges which are currently faced in the Cloud computing are highlighted. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future. Author tried to solve many issues. In future work, Author will include the developing of testing of data flow and security in cloud computing.

REFERENCES

[1] Press Release. "Hacking Habits" Survey Cites Misconfigured Networks As The Main Cause Of Breaches. Tufin Technologies, 31August, 2010. http://www.tufin.com/about-us/news-and-media/pressreleases/2010/august-31,-2010/.

[2] R. J. Colville and G. Spafford. Configuration Management for Virtual and Cloud Infrastructures. Gartner Inc., 27 October, 2010. http://www. gartner.com/id=1458131.

[3] A. Feldmann, M. Kind, O. Maennel, G. Schaffrath, and C. Werle. Network Virtualization - An Enabler for Overcoming Ossification. European Community in Information Technology (ERCIM) News, Retrieved 14 June, 2013. http://ercim-news.ercim.eu/en77/special/networkvirtualization- an-enabler-for-overcoming-ossification.

[4] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson,J. Rexford, S. Shenker, and J. Turner. OpenFlow: Enabling Innovation in Campus Networks. ACM SIGCOMM Computer Communication Review (CCR), 38(2):69–74, 2008.

[5] N. Gude, T. Koponen, J. Pettit, B. Pfaff, M. Casado, N. McKeown, and S. Shenker. NOX: Towards an Operating System for Networks. ACM SIGCOMM Computer Communication Review, 38(3):105–110, 2008.

[6] R. Tagnipes. High Availability with Dynamic Load Balancers. GoGrid Blog, 4 Feb, 2013. http://blog.gogrid.com/2013/02/04/high-availabilitywith- dynamic-load-balancers/.

[7] S. Shin, P. Porras, V. Yegneswaran, M. Fong, G. Gu, and M. Tyson. FRESCO: Modular Composable Security Services for Software-Defined Networks. In ISOC Network and Distributed System Security Symposium (NDSS), 2013.

[8] V. Mann, A. Vishnoi, K. Kannan, and S. Kalyanaraman. CrossRoads: Seamless VM Mobility Across Data Centers through Software Defined Networking. In Network Operations and Management Symposium (NOMS), 2012 IEEE, pages 88–96, 2012.

[9] OpenFlow Network Research Center, Retrieved 14 June, 2013. http: //onrc.stanford.edu/.

[10] Syed Taha Ali, Member, IEEE, Vijay Sivaraman, Member, IEEE, Adam Radford, Member, IEEE,and Sanjay Jha, Senior Member, IEEE , A Survey of Securing Networks using Software Defined Networking .

[11] Takabi H, Joshi J B D, Ahn G. Security a nd privacy challenges in cloud computing environments. IEEE Security & Privacy;2010;8(6) :24–31.

[12] Esteves, R.M. and Chunming Rong, "Social Impact of Privacy in Cloud Computing" in 2010 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom), N ov. 30-Dec. 3 ,2010, pp. 593-596

[13] Ricardo vilaca, Rui oliveira 2009. Clouder: A Flexible Large Scale Decentralized Object Store. Architecture Overview. Proceeding of WDDDM '09

[14] Michael Miller. 2009. Cloud Computing-Web Based Application that change the way you collaborate online. Publishing of QUE, 2nd print.

[15] M. Casassa-Mont, S. Pearson and P. Bramhall, "Towards Accountable Management of Identity and Privacy: Sticky olicies and Enforceable Tracing Services", Proc. DEXA 2003, IEEE Computer Society, 2003, pp. 377-382

[16] Wikipedia, 6 February 2010, http://en.wikipedia.org/wiki/Risk_management

[17] Wikipedia, 27 January 2010, http://en.wikipedia.org/wiki/Risk_assessment

[18] A. Nakao, L. Peterson, and A. Bavier. A Routing Underlay for Overlay Networks. In Proceedings of the Annual Conference of the ACM Special Interest Group on Data Communication (SIGCOMM), pages 11–18, 2003.