A SURVEY ON LAYERED SECURITY IN CLOUD COMPUTING: ISSUES,THREATS, AND SOLUTIONS

Henna Abdul Jaleel[1], Rahul P[2]

[1] *(Mtech Cyber Security,Department Of Computer Sceience And Engineering,Met's School Of Engineering,Mala)*

[2] *(Assistant Professor,Department Of Computer Sceience And Engineering,Met's School Of Engineering,Mala)*

ABSTRACT

Over the internet, the cloud computing reveals a remarkable potential to provide on-demand services to consumers with greater flexibility in a cost effective manner. While moving towards the concept of on-demand service, resource pooling, shifting everything on the distributive environment, security is the major obstacle for this new dreamed vision of computing capability. This survey present a comprehensive overview of the security issues for different factors affecting cloud computing. Furthermore, a detailed discussion on several key topics regarding embedded system, application, storage system, clustering related issues and many more. This paper works on some public cloud and private cloud authorities as well as related security concerns. Additionally, it encompasses the requirements for better security management and suggests 3-tier security architecture. Open issues with discussion in which some new security concepts and recommendations are also provided.

***Keywords* : -** *Cloud Computing,Resource Pooling,Embedded System,Clustering,Security Architecture .*

1. INTRODUCTION.

During the primary years of the 60s, computers needed large rooms and consumed large amounts of electricity, had,expensive electronic parts and produced little or no processing output. However, smaller computers eventually replaced those roomsize computers. At the top of the last century, the magnitude of computing and infrastructure nodes to be organized to make a distributed system, which provided a rise in efficiency [1]. In recent years, when the demand of knowledge and online users has vastly increased, the normal computing infrastructure is becoming costlier and harder to manage. Traditional computing isn't suitable for accessing data anywhere and at any time. so as to try to to so, we'd like to save lots of the info on anexternal storage system. Additionally, the rise of online users on networking sites, online surfing, video conferencing,and such can't be handled by traditional computing [1]. This rapid increase in global internet usage needs new ways of managing the quantity , variety and availability of knowledge , therefore, we are moving towards cloud computing.Cloud computing is one among the most well liked core technical topics within the era . it's emerged with broad ranging effects across IT, businesses, software engineering and data storage. one among the most effects is that the increase of their capability. This Increase in capability doesn't necessarily mean a rise in expenses in hardware, software, and training of private to mention a couple of . consistent with the National Institute of Standards and Technology (NIST) definition , "the cloud computing is a model for enabling convenient, resource pooling, ubiquitous, on-demand access which may be easily

delivered with different types of service provider interaction" [5]. The cloud computing follows simple "pay as you go (PAYG)model,where you buy the services you've used [2]. one among the main benefits of PAYG model is that we will reduce our expenditure by provisioning a particular amount of resources. The user can select processor,

memory, hard disk, operating system, networking, access control and any additional new software as needed to their Service(SaaS) [4]. NIST defines four-development model of the cloud: public, private, hybrid and community. Cloud computing uses cloud server stack where the client or user is on the front and server on the rear end. Services reside in middlewareof stack as shown in . At the highest level resides the appliance , which directly delivers the outsourced software to the clients and eliminates sophisticated software. Customers do no got to expend money to put in software, only they buy their usage.Cloud service delivery models.As internet technology and large data cloud computing grow, they raise a replacement concept of services. This new services are able to interconnect the growing number of online activities.

creates many issues, as we don't know where the resources are located or who owns them, increasing the problem of protecting them from attack [1].

• Community cloud: Cloud infrastructure of the organizations shared concerns (mission, security requirements, policy, and compliance considerations) of consumers a special provision has been made for exclusive use by the community model. It is owned, managed, and community organizations, a 3rd party, or some combination of them is driven by one or more, and that could also be present on or off campus. In simple words, a community cloud is being shared and controlled by multiple organizations [39]. It also reduces the safety risk within the public cloud and reduces the value of personal cloud.

• Hybrid cloud: it's the mixture of two or more clouds (public, private, community). Usually, the info and application are bound together by standardized and propriety technology. Hybrid cloud offers the benefits of various clouds deployment models. However, it's well organized and safer than public cloud while accessing the entities over the internet.

• Virtual private cloud: it's a semi-private cloud, which is fewer resources, and it consists of virtual private network (VPN). It is on demand configurable pool of shared resources allocated within the cloud environment. Cloud computing basic component In this section, we'll discuss the essential components on which cloud computing deployed. These components contains a wide range of services that we will use everywhere the web . Here we discuss some important component:

• Virtualization: It plays a crucial role in deploying the cloud. it's the strategic component within the cloud, which allows the physical resources by multiple consumers. It creates the virtual instance of resource or device like OS , servers, network resources and storage devices wherein the framework utilize the resources into quite one execution environment [2].

• Multi-tenancy: Multi-tenant environment can have multiple customers or users who doesn't see or share each other's data but can share resource or application in an execution environment, albeit they'll not belong to an equivalent organization. Multi-tenancy results the optimal utilization of hardware and data storage mechanism.

• Cloud storage: it's a component, which maintained, managed, and protected remotely and it is also made available over the network where the users can access data .

• The hypervisor: The So called virtual machine monitor or manager may be a key module of virtualization. It allows multiple Virtual Machines (VMs) to run on one hardware host. It manages and monitors the varied operating systems, which run during a shared physical system [13].

• Cloud Network: It can operate quite one conventional data centers; a typical data center contains hundreds or thousands of servers. To efficiently build and manage the storages the cloud requires a secure network infrastructure called cloud networking. It requires an online connection and similar with a virtual private network which enables the user to securely access printers, applications, files etc. Cloud computing security concept Nowadays, cyber warfare is arguably the foremost complex challenge during a distributed and multi- tenant environment. It is a complex job within the client-server architecture. When the info transfer to the cloud services, the wants of security should be the foremost important. the ecu Network Information Security Agency (ENISA) enumerated the risks, recommendations and benefits for cloud computing . It also lists the infection on confidential document, loss of governance, malicious insider, and insecure incomplete data. The Elastica 2015 shadow data report it focuses on 4 unauthorized apps discovered in a corporation . It examines which sort of knowledge typically found in sharing apps, riskiest exposure, and what steps fancy mitigate these security problems. The CSA and ElasticaQ2 2015 also examine the way to build an effective cloud app security architecture, which provides control, visibility, and remediation. during this section, we briefly introduce about the main security concerns of cloud computing.

• Software security: It provides basic idea of software security come from the engineering software department that it continues to function correctly under the malicious activities. to create a cloud environment a central and important problem is software security problem. It defects with security including implementation bugs, buffer overflow, designed flaws, error handling promises and far more . • Infrastructure security: the foremost common and

fundamental challenges is to demonstrate that the virtual and physical infrastructure of the cloud are often trusted. The attestation of the third party isn't enough for the critical business process. It's absolutely essential for the organization to be ready to verify business requirements that the underlying infrastructure is secure.

• Storage security: In cloud storage system, user stores the info within the cloud and not owns the info and where it's stored. This always has been a crucial aspect of quality of service. It ensures the correctness of user's data within the cloud and by utilizing the homomorphic token along with distributed verification of erasure-coded data. Storage security concerns about data sanitization, cryptography, data-Remanence, data leakage, snooping of knowledge availability and malware.

• Network security: In cloud computing, communication is via the web and it's the backbone of the cloud environment. Network security concerns about both internal and external attacks. These attacks within the network can either occur within the virtual or physical network. Hanqian W., et al.focuses on the virtual network during a Xen platform by discussing and analyzing its security problems. Flavio L., and Robert D. P., present a completely unique virtual network in the framework that is aimed to regulate intercommunications and provide high-security level . Some attacks like DoS or DDoS, DNS, ARP spoofing, IP spoofing phishing attack and port scanning are aimed to realize access to the resources during a cloud network we've discussed cloud computing and its characteristics, which are well understood, but still the safety state of it's still puzzling. Security is that the biggest concerns for IT businesses who are considering to hitch the cloud computing. Currently, security is one among biggest obstacles for cloud computing service adoption. Security issues within the cloud environment are caused by its essential characteristics like resource pooling, virtualized nature, elasticity, and a few measured services. There was a rise of 70% Advance Persistence Threat (APT) attacks, 68% suspicious activities, and 56% brute force attacks on a cloud environment in 2015. APT attack is network attack during which an unauthorized identity gain access to a network and remain undetected for an extended period. The International Data Center (IDC) is an analysis and research firm that takes the opinion of companies' security. **is most concerned topic for 87% of respondents.**

Watermarking technique is employed in case of secret and top secret data to spot the leaker responsible for leaking the sensitive data.

2. CLOUD SECURITY ISSUES AND CHALLENGES

This chapter discusses the safety state of cloud environments thoroughly by describing its security issues. Each section of this chapter represents a category of cloud computing environment as shown in figure 3. Moreover, each section is further divided to some topics that group security issues common in some property. It elaborates the various security issues while developing on cloud computing environment. The classification discusses embedded security issue during which property of virtual machine arises many security issues like Cross-VM attack misconfiguration, in programmability single point failure. additionally , this chapter also focuses on application level issue. The service with utility relies on web services and technology. There are many lines of code in software application and many developing languages to make an interface, which may cause many security vulnerabilities. Data in rest or in communication has issues due to flaws in cryptographic techniques. Sometimes a drag arises from client experience its authentication policy of customer relationship management. Clustering issue also affects the cloud, some flaws within the physical cluster, and virtual cluster brings attack within the network cloud. there's much vulnerability within the operating system of desktops, network servers and smartphones that are hospitable some serious attacks. Embedded security issues Security in cloud computing environment may be a crucial concern in lately . the safety in embedded systems has several challenges that caused by the unique features of those systems. The advancement of embedded system is because of improved tools working with them. the straightforward thanks to debug an embedded device is to attach it to an area network. An embedded system associated with the ever present computing. the most security issues for cloud computing in embedded systems are caused by virtualizations [5]. Different areas of security issues in embedded systems are as following;

• Virtual machine isolation: the first advantage of virtualization is isolation. If it doesn't deploy correctly then it are often a threat to the environment. The workload is separated amongst the VMs is one among the important issues in implementing the cloud. It can cause data leakage and cross-VMs attack. therefore the isolation process should be configured carefully while deploying virtual machine in cloud infrastructure.

• VM Monitoring: during a virtual environment, the host machine considered as an impact point and designed for monitoring the application running on the VMs. generally , all the traffic data is passing through the monitor host. There are many techniques that influence the host monitor machine, for instance , the host can restart or shutdown the VMs, it cannot monitor the traffic during this span of your time . differently is that the host itself can sniff, alter, change, copy or delete the resources that are available in VMs [13].

• Programmability: during a cloud environment, commercial routers use advanced functionality (e.g., accounting, blocking, anomaly detection, etc.) for programmable processor packet on each port. The key challenge of using this device in network processor is to implement packet monitoring functionality for developing software. Many software environments in network processing use a coffee level of abstraction to realize high throughput performance .
• Electronic access control system: Information of client transmitted over the cloud network. EACS negotiates the authentication system and perimeter security by providing the support of Security Assertion terminology (SAML). It is a federation protocol, which contains authentication credentials [14]. SAML wont to exchange the knowledge associated with subject or authentication between the cooperating domains, and therefore the request and response mapped in Simple Object Access Protocol (SOAP) counting on XML. However, by using signature-wrapping attack, it's possible to change an eavesdropped message despite being it digitally signed. meaning an attacker allowed to execute random machine act as legitimate users.
• SNMP Server: it's simple network management protocol, which designed to supply a low-overhead mechanism to collect the info from network devices.

Security in a software application is the most vulnerable area. Most of the applications have a front end, back end, different types of platforms, frameworks, parallelism, which have different types of vulnerabilities. The basic security issue in a software application is that it has a million lines of programming code. Different programmers in a different language write the software and many of the programming languages have vulnerabilities. In this section, we will discuss different varieties of application issues in cloud computing.
• User front end: The security of front end should be like an onion structure but there is the very high probability of an authorized access and deficient configuration in the software application. A programmer needs to know the security aspects of the web developing language like HTML/CSS/PHP/JS. Subhasini and Kavita stated that the isolation barrier can breach by loophole or injection masked code. Suppose that if an intruder has already compromised the database, there should be a proper front end to prevent the error.
• User back end: SQL injection attack takes advantage of backend application weaknesses. and visit the post, we will find that the script gets injected and executed .OWASP project aimed for backend security and it focuses on three fields like development, hardening, and testing. However, in these three fields have already many security issues, which need to be concerned.
• Platform: It is important to discuss what kinds of security issues are present while deploying the platform as service model such as windows Azure. The shared environment includes some unique challenges involving authentication, authorization, and access control. Isolation,
rapid elasticity, and resource accounting are also big challenges in a multi-tenant cloud system environment . To isolate the running programs, java implements sandbox bytecode to check the integrity and cryptography for secure communication APIs. Still, this is not secure enough and it does not prevent information leakage.
• Framework: The major security issue in cloud computing is found on the framework. IBM cloud framework proposed the strength and weakness of security functionalities. IBM defined five functional security subsystems that are: audit & compliance, access control, flow control, identity management and solution integrity [21]. The framework has designed in java and .net for isolation and resource accounting but they failed with thread termination. Multitasking Virtual Machine (MVM) provided generic API.
• License: While moving in the cloud, the major issue is the licensing of the applications. It is a very complex problem and vendors still have not found a proper solution. The Copy, Sell, Sharing or Distribution of software illegally is called software piracy. Dynamically change the number of servers hosting a variety of application demand uptime, elastic scaling, reliability, performance, and stability. Even today, in the world of personal computer users use 57 % pirated software, this is a big issue from a security point of view. There are many possible attacks on this unauthorized pirated software.
• Service Availability: Technically, there are so many ways to achieve high availability in the cloud. Cloud services categorized as SaaS, PaaS, and IaaS. Because of the fluctuation in the cloud environment, application and infrastructure level need high availability and scalability. On the contrary, there is a chance of availability attack like DoS or Botnet DDoS. Subhashini S. et al. discussed multi-tier architecture to adopt and providing ‘security as a service’ framework.
• Parallel application: Parallel application improved the performance of the system, but there are some challenges while deploying it. While executing many applications parallel there is a problem of mutual authentication among them and due to this vulnerability some attacks are possible. Due to high non-uniform data distribution, the parallel algorithm is troubled by catastrophic load imbalances.

3. SECURITY THREAT IN THE CLOUD COMPUTING

. Many researchers have studied and discussed the safety problems with cloud computing. Fernandes et. suggested making comprehensive reviews on cloud security issue, it addresses many several key topics namely threats, vulnerability, attacks proposing and taxonomy for his or her classifications given. Mazhar explained the safety survey highlighted the communication, architectural, contractual and legal aspects. It also discussed the countermeasure for communication issues, it also surveyed on the vulnerability of virtual machine like VM migration, VM image, hypervisor, and discusses security in future direction. Flavio Lombardi et al. gave the detailed knowledge on critical infrastructure for the secure cloud. Moreover, Subashini S., et al. [2] emanated the safety issue in commission delivery models of cloud computer system and provide solution to counter these issues. Saripalli P., et al. surveyed the foremost relevant privacy and trust issue and analyzing privacy, security and trust threats. The author provide solution within the paper to realize a secure trustworthy and dependable cloud computing. This paper provides the safety requirements for effective governance, personal requirements, some better encryption techniques, disaster and backup recovery management and scheme for secure virtualization within the cloud system. Security concerns privately cloud providers Popular service vendors for 2015 said that cloud security platform helps organizations mitigate the danger using cloud-based services. The group of vendors provides strong data protection, encryption, and good access management. Others have good monitor based cloud system for suspicious activity that gives reporting and alerting, and policy enforcement . Mr. Gray Hall, the chairman, and CEO of Alert Logic may be a SaaS-based platform organization that concerns about log management, vulnerability scanning, intrusion detection and monitoring via managed service provider partner. Many major vendors and little cloud providers have a personal cloud offering that are available for on-premises deployment or available as a secure hosted offering [2].Microsoft Windows Azure adopts firewall, filtering routers, security patch management of software, physical security, cryptography algorithm for encryption of knowledge , SSL-128 bit encryption. Force.com uses SAML for authentication on login, session security, and auditing. It also provides security at various levels like logical network, host security, database security, and communication security. Meanwhile Rackspace protects against spam and provides SSL security. Rightscale and Apple cloud have security monitoring technique and key chain technique for password and authentication respectively [1].

4. REQUIREMENTS AND THE LITERATE SOLUTIONS

Cloud computing offers both unique advantage and challenges to non-public and government users. Advantages include greater efficiency, flexibility, and economy, which may help enterprises to satisfy rapidly changing computing needs, and cheaply while being environmentally friendly. Among the various challenges, security is that the commonly cited concerns in moving mission-critical services or sensitive information to the cloud. Organizations are ready to manage dozens to thousands of employees and users who can access their cloud applications and services, each with varying roles and privileges. Cloud service providers must allow the cloud consumer to assign and manage the roles and allied levels of authorization for every of their users in accordance with their security policies. For example, a cloud consumer, consistent with our security policies, an employee whose role is to allow them to be to get a purchase request, but during a different role and powers of the authority to approve the request of another employee is to be responsible for. Most organizations, which have established security, compliance policies and procedures, protect their intellectual property and company assets used exclusively in IT space. These policies and procedures for the organization to think about the impact of those assets compromising on basis of risk analysis are developed. A controls framework and further procedures established to mitigate risk and function a typical for the execution and validation of compliance. These principles and policies, enterprise security planning improves the standard of the method surrounding enterprise security governance, risk management, and compliance represents models. In Liu B., et al. [19], a risk framework presents security risks in terms of six key categories for security objectives (i.e., confidentiality, integrity, audibility, multiparty trust, mutual auditability and usability) during a cloud platform. The advantage of this approach of risk assessment is that it allows customers, vendors, and regulation agencies to assess comparatively the relative robustness of various cloud vendors with their offerings during a defensible manner. Afghan et. al. shows that the knowledge security principles of integrity, confidentiality and availability are most relevant to the cloud related scenarios. the knowledge risk ratings performed shows the loss of confidentiality rated because the highest level of risk followed by availability and integrity. for every of the threat categories the common research issues identified are:

• Scalable fine granular access control and data confidentiality in cloud computing scenarios.

• Using an intrusion detection system (Identification of user behavior) to stop data leakage at infrastructure provider level.
• Detection of malware on virtual machines, from the hypervisor level by performing the static and dynamic analysis.
• Identification of vulnerabilities at the hypervisor when giving API level access to the introspective layer of the hypervisor to the programs.
• Security architecture for a hypervisor using the Usage control model.

5. SECURITY SUGGESTIONS AND THE DISCUSSIONS

During this chapter, we propose 3–tier security architecture as shown in figure 4, where security is interdependent on each other. The proposed security classification is consists of three levels: application level, cloud-service middle level, and infrastructure level. Organizations that are keen to use cloud computing to run their in-house applications got to review and potentially modify their software development approach. The organizations should concern about the key points that help to design programming standards, and adopt multi-tenancy and most vital the safety capabilities. Here we'll discuss the security issues on each level of the cloud security architecture. To secure our cloud system, we use one among the simplest anti-spam sniffing tools, Heluna plus and Heluna standard, which block 99% of spam message with approximately zero false positive rates. We also use a protocol and standard called Cloud Trust Protocol (CTP) for establishing digital trust between end-users and providers. User and repair authentication is verified through the login process. The cloud customers of USA or Canada follow the service regulations very securely and trustful to follow the confidential property. Legal requirements and regulations create a replacement relationship between information of the organization and therefore the third party, which describe how the knowledge must be handled and stored by the cloud providers. For the middleware trust and repair credibility, many approaches are recently proposed. These approaches provide the trust management in cloud environments; still, not much attention has been given to work out the credibility of trust feedbacks. Credibility service checking is liable for user credibility verification. It authorizes a device by providing a interface that's the sole single legal entry point. Regarding protocol standards, the TCP/IP protocol model or WAP (Wireless Application Protocol) are the foremost common ways of communication over the web system. Nevertheless, they need much vulnerability to be exploited. Dynamic Host Control Protocol (DHCP), Hypertext Transfer Protocol (HTTP), Wireless terminology (WML), and straightforward Mail Transfer Protocol (SMTP) are well-known vulnerable protocols also utilized in the cloud. Therefore, the safety of protocols is necessary to secure Middleware level. additionally to the cryptographic solution we already discussed in chapter IV, to secure middleware level we should always develop good authentication scheme between user and middleware, improve data sharing security and improve better spam management.

5. CONCLUSION

The hype of cloud paradigm is changing the IT industry; it brings many benefits to companies, organizations and even countries. Despite bringing several advantages, the cloud still is susceptible to many security challenges. this is often why security is the major challenge within the adoption of the cloud. The customer and vendors are cognizant of security threats. This research attempted to point out various security challenges, vulnerabilities, attacks and threats that hamper the adoption of cloud computing. Our paper provided a state-of–art survey on cloud security issues and challenges that arise from unique characteristics of the cloud just like the sharing and virtualization of resources, resource pooling and therefore the public nature of the cloud. We explored various cloud services and what they supply also as analyzed the safety concern on each provider. In addition, governments also are getting to develop the cloud technology to extend the performance, quality, innovation and security within the services they supply to the citizens. Subsequently, we've surveyed existing schemes that counter the security issues in an efficient, and price saving manner. we've proposed the 3-tier security architecture for better security enhancement of cloud security. The model discussed the three level of cloud service system and important security considerations of every level. To conclude, we also discussed open issues and suggested future work.

6. ACKNOWLEDGEMENT

First I thank the almighty, without whose blessings, I would have never been able to complete my paper work. Our gratitude also goes to Mr. SUNIL S.S., the Head of the department of computer science for his constant guidance and helping hand. My sincere thanks to our Project Coordinator Mr. RAHUL P, M.TECH., faculty of computer science for having supported the work related to this Project. His contributions, constant support and encouragement in preparing this paper are greatly acknowledged. And faculty of computer science for helped me in the development of my paper to what it is now. I thank my parents for the mental support provided during the course of the project at the times when my energies were the lowest.

7. REFERENCES

[1] Chirag Modi, Dhiren Patel, Bhavesh Borisaniya, Avi Patel, Muttukrishnan Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing", Journal of Supercomputing, Vol. 63, Issue 2, pp.561-592, 2013.

[2] Subashini, Subashini, and Veeraruna Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of network and computer applications, Vol. 34, Issue 1, pp. 1-11, 2011.

[3] Nikos Fotiou, Apostolis Machas, George C Polyzos, George Xylomenos, "Access control as a service for the Cloud", Journel of Internet Service and Application, ISSN 1869-0238, 2015.

[4] Keiko Hashizume, David G. Rosado, Eduardo Fernández-Medina, and Eduardo B. Fernandez, "An analysis of security issues for cloud computing", Journal of Internet Services and Applications Vol 4, Issue 1, pp 1-13, 2013.

[5] Dimitrios Zissis, and Dimitrios Lekkas, "Addressing cloud computing security issues." Future Generation Computer Systems, Vol. 28, no. 3 pp. 583- 592, 2012.

[6] Yingjie Xia,, Fubiao Xia, Xuejiao Liu, Xin Sun, Yuncai Liu, and Yi Ge, "An Improved Privacy Preserving Construction for Data Integrity Verification in Cloud Storage", KSII Transactions on Internet and Information Systems (TIIS), Vol. 8, Issue 10, pp.3607-3623, 2014.

[7] Haolong Fan, Farookh Khadeer Hussain, Muhammad Younas, and Omar Khadeer Hussain, "An integrated personalization framework for SaaS-based cloud services", Future Generation Computer Systems, Vol. 53, pp.157-173, 2015.

[8] Behl, Aseem, and Kanika Behl, "An analysis of cloud computing security issues," Information and Communication Technologies (WICT), 2012 World Congress on, pp. 109-114. IEEE, 2012.

[9] Wang, Bin, Zhengwei Qi, Ruhui Ma, Haibing Guan, and Athanasios V. Vasilakos. "A survey on data center networking for cloud computing." Computer Networks Vol. 91 pp.528-547, 2015.

[10]Jansen, Wayne. "Cloud hooks: Security and privacy issues in cloud computing", In System Sciences (HICSS), 2011 44th Hawaii International Conference on, pp. 1-10. IEEE, 2011.

[11]Booth, Gehana, Andrew Soknacki, Anil Somayaji, "Cloud Security: Attacks and Current defenses", Annual Symposium on Information Assurance (ASIA'13), pp. 56, 2013.

[12] Le Xu, Dijiang Huang, Wei-Tek Tsai, "Cloud-based virtual laboratory for network security education", Education, IEEE Transactions, Vol. 57, Issue 3, pp.145-150, 2014.

[13]Jianxin Li, Bo Li, Tianyu Wo, Chunming Hu, Jinpeng Huai, Lu Liu, and K. P. Lam., "CyberGuarder: A virtualization security assurance architecture for green cloud computing", Future Generation Computer Systems, Vol. 28, Issue 2, pp.379-390, 2012.

[14] Volokyta Artem, Kokhanevych Igor, Dmytro Ivanov,"Secure virtualization in cloud computing", 2012.

[15] Khorshed, Md Tanzim, ABM Shawkat Ali, Saleh A. Wasimi. "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing." Future Generation computer systems, Vol. 28, Issue 6, pp.833-85, 2012.

[16] Shiraz Muhammad, Saeid Abolfazli, Zohreh Sanaei, Abdullah Gani,"A study on virtual machine deployment for application outsourcing in mobile cloud computing", The Journal of Supercomputing, Vol. 63, Issue 3, pp.946-964, 2013.

[17] Sultan Nabil, "Making use of cloud computing for healthcare provision: Opportunities and challenges", International Journal of Information Management, Vol. 34, Issue 2, pp.177-184, 2014.

[18]Jinpeng Wei, Xiaolan Zhang, Glenn Ammons, Vasanth Bala, Peng Ning, "Managing security of virtual machine images in a cloud environment", In Proceedings of the 2009 ACM workshop on Cloud computing security, pp.91-96, 2009.

[19]Bingwei Liu, Yu Chen, Ari Hadiks, Erik Blasch, Alex Aved, Dan Shen, Genshe Chen, "Information fusion in a cloud computing era: a systems-level perspective", Aerospace and Electronic Systems Magazine, IEEE, Vol. 29, Issue 10, pp.16-24, 2014.

[20] Xiangjian He, Thawatchai Chomsiri, Priyadarsi Nanda, Zhiyuan Tan, "Improving cloud network security using the Tree-Rule firewall", Future Generation Computer Systems, Vol. 30, pp.116-126,2014.

[21] Tianyi Xing, Dijiang Huang, Le Xu, Chun-Jen Chung, Pankaj Khatkar, "Snortflow: A openflow-based intrusion prevention system in cloud environment," In Research and Educational Experiment Workshop (GREE) IEEE, pp. 89-92, 2013. International Conference on, pp.109-116. IEEE, 2009.

[22] Yizeng Chen, Xingui Li, Fangning Chen, "Overview and analysis of cloud computing research and application," International Conference on EBusiness and E-Government (ICEE),pp.1-4.IEEE,2011.