Analysis of Virtualization Issues and Security Enhancement Strategies for Cloud Computing

Surya Narayana Murthy Nalam

School of Computer Science and Engineering, Lovely Professional University, Phagwara, India

suryanalam3011@gmail.com

Abstract: Cloud computing is a rapidly evolving computing paradigm that enables users to access shared computing resources over the Internet with the help of virtualization. However, the adoption of cloud computing has also introduced new security challenges that need to be addressed because there may possibility of encountering problems due to virtualization. In this paper, a systematic literature review is performed to find out the vulnerabilities and risks of virtualization in cloud computing and to identify threats, and attacks that result from those vulnerabilities. Furthermore, discovered and analyzed the effective mitigation techniques and strategies that are presented by some researchers to ensure the protection of data and proper management of cloud computing environments.

Keywords - Virtualization, cloud computing, mitigating, threats, VMware, Virtualization, cloud computing, mitigating, threats, VMware.

I. INTRODUCTION

Approximately 50 years ago, a time-sharing computation server supported a wide range of users in a similar condition. Applications and data were stored in local resources in huge before personal computers arrival occurred. The Cloud computing model is not a history repeating currently. Due to the unavailable of enough resources for computing 50 years ago, we had no choice but to use time-sharing servers. Because of the need to develop sophisticated Information technology (IT) infrastructures, cloud computing has been uncommon in past years. A variety of program installations, upgrades, and configurations are to be managed by users.

As the usage of cloud computing increased due to its characteristics, Cloud computing has revolutionized the way computing resources are delivered and consumed, providing users with on-demand access to a range of IT services. It provides users with on-demand access to a range of IT services, including computing, storage, and networking. The adoption of cloud computing has been driven by several factors, including the need for scalability, cost savings, and flexibility as shown in Fig.1.1. The pay-as-you-go model of cloud computing is one of the most fantastic models which offers computing as a resource.

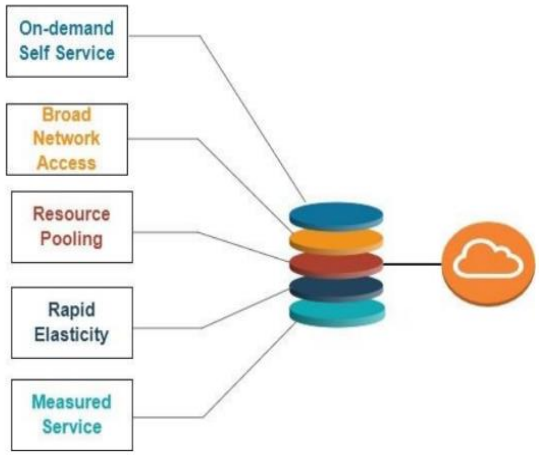


Fig.1.1 – Characteristics of Cloud Computing

Due to this fast-paced evolution, the risk of data theft and security issues can also increase which opens a door for hackers to attack and stole the data. Nearly 63 percent of the 761 data breaches probed by the US Secret Service in 2010 happened at businesses with 100 or fewer workers. A 2011 survey of medium and small 2,000+ businesses by security systems supplier Symantec Corp investigated that over 73% of businesses had been compromised by a cyber-attack.

Towards this end, it is essential to further investigate on attacks such as side channel attacks, VM migration attacks and hypervisor attacks. ENISA recommends that enterprises must conduct a risk assessment, compare various cloud services providers, choose a few cloud computing service providers to obtain the level of service guarantee. Microsoft Company analyzes the cloud computing facing the security challenges, and based on Microsoft company's cloud computing architecture gives the corresponding security

protection recommendations including: (a) between service providers and users establish a mutually dependent relationship under the cloud computing model, (b) application mode of diversification and the growing size of the user, (c) attack to cloud computing system and illegal access to or use of information, (d) the complex compliance needs. Our contributions in this paper include reviewing relevant literature to bring about useful insights and make note on significant research gaps to inspire further research in this area.

II. LITERARTURE REVIEW

Privacy becomes a major concern among cloud users' data which is stored in the data center of cloud service providers physically located in different places. In cloud, there are some circumstances which lead to the privacy threats. First, the storage issues that surface when user store data in multiple storage locations which are hidden from the user and have the possibilities of transferring data without owner's permission. Second major concern is to ensure the destruction time policy among cloud provider, broker and user once the data reach their expiration period. Third concern is data breaches which studies on how data breaches occur and who are going to take responsibility if data breach occurs in cloud. When a user opts for using cloud services, the user should read the terms and conditions thoroughly before prompt to cloud. The fourth concern is on regular auditing and monitoring policies. Cloud clients should constantly monitor / audit the activities of cloud service provider to ensure their stakeholder personal information will not be leaked while cloud resources are sharing with others.

The security challenges of cloud computing infrastructure that can be considered in detail as follows: Integrity, Confidentiality, Availability.

A. Integrity

Data integrity in cloud computing is the preservation of data that is stored in cloud server to verify the data is not modified or lost by employing the services of the third party. Organizations can achieve more confidence to prevent system and data integrity from unauthorized access . The data integrity involves the three main entities: (1) a cloud storage provider to whom outsourced the data, (2)owner of data outsources his data, (3)auditor who ensures the data integrity. The auditor may be the owner of data, or he can assign responsibility to a third party.

The process of data integrity scheme defined as in two phases as shown in Fig. 2.1.

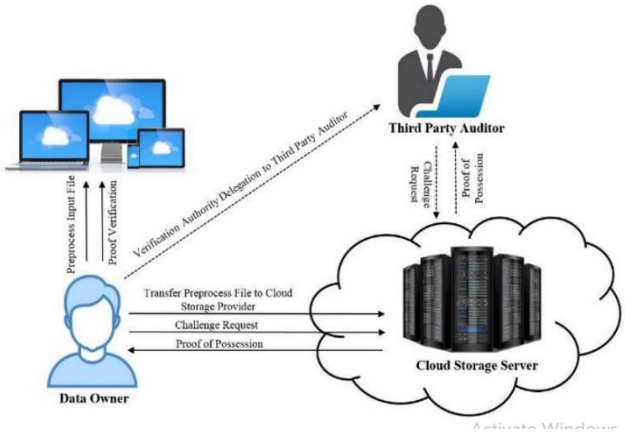


Fig. 2.1 Data Integrity Schema

B. Confidentiality

Confidentiality refers to keeping the customer's data secret in the cloud computing system and only the authorized customers or systems can be able to access the data. Cloud computing provides (e.g., applications and its infrastructures) are basically in the public clouds have more threads on the systems or applications are exposed as compare the hosted in the private data centers. So, it is the fundamental requirement to keep the customer data secret ever the increasing number of applications, customers and devices involved. The vendors of cloud computing are extensively adopted the two basic approaches such as cryptography and physical isolation to achieve the confidentiality. The cloud computing provides services and data that are transmitted through the public network, and it cannot achieve physical isolation. hybrid cloud data center ecosystems. Vertica offers VPN and firewall to secure its database and deploys on the Amazon EC2.

C. Availability

Availability in cloud computing including applications and its infrastructure is to ensure that the authorized customers can always access the property of system on demand. Cloud computing models (IaaS, PaaS and SaaS) allows its customers to access the services and applications from anyplace at any time. Vendors of cloud computing offers the cloud platform and infrastructure that is based on VM. The Amazon web services offer S3, EC2 that is based on VM called Skytap and Xen provides virtual lab management application depends on the hypervisor (Xen, VMware and Microsoft Hyper-V). For example, Xen virtual machine offered by Amazon can provide separated storage

virtualization, memory virtualization, machine/CPU virtualization etc. where the large number of commodity PCs hosted.

D. Placement Strategy for Security Enhancement

Based on the placement strategy generation algorithm shown in Table 1, we have acquired the possibility of being attacked for each VM. Next, we will design a placement strategy to reallocate guest VMs before the attack succeeds. The principle of new strategy is isolating the VMs with high security risks from VMs with low security. In order to reduce the performance overhead, connected VMs with similar security risk will be assigned in the same node. When design the placement algorithm, we assume the node will have enough resources capacity (e.g., CPU, memory and disks etc.) to hold all guest VMs. In each attack step, DTMC and CVSS will predict the attack possibility for each VM. The algorithm will sort the possibility and find the most "dangerous" VM which is most likely to be compromised. The algorithm will assign the most dangerous VM to a dedicated node and allocate other VMs to different node. Therefore, even if the most dangerous VM is compromised, other VM will not be exploited by the attacker. When migrating a VM, the VM is usually shut off first, hence, migration time is one of the most significant factors we should consider in order to improve the system performance.

Require:

1. Virtual machine set V = {V1, V2,…, Vn) Dependent VMs set for each VM set Dependent VMs, where dependent VMi is the set which represents the

2. Dependent VMs for VMi (i ≤n)

3. The Physical machine (Node) set N = {N1, N2, …, Nk}

4. The compromised possibility for each VM is Pi(i ≤ n)

Ensure: Placement Strategy

1: Sort VMs in ascending order of attack possibility Sort {V1, V2, …, Vn) .

2: dangerous VM = find Most Dangerous ( ) will find the most dangerous VM index by comparing compromised possibility of VMs in set V

3: dangerous Node = find Random Node ( ) will find a random node to store the dangerous VM.

4: Mapv (dangerous VM, dangerous Node) will assign dangerous VM to dangerous Node

5: while! V.empty ( ) do

6: node = find Random Node ( ) will return a new node

7: new VM = V.pop ( ) find a safe VM

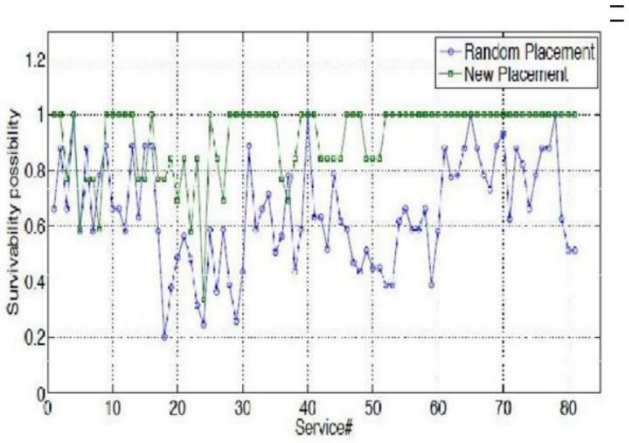
8: Map (NewVM, node) assign new VM to safe node

9: Map (Dependent new VM, node) assign the connected VMs into same node.

10: update V

11: end while

According to our experimental results shown in Fig. 2.2, the 91.4% services obtained improved survivability. The maximum survivability enhancement is 74.3% and the average improvement of survivability possibility is 27.2%. In our experiment, we can find there are 20 VMs will be compromised at attack step 1 in random placement plan. However, in our new placement plan, the number of compromised VMs is only 4. Moreover, according to our statistics, the average compromised VM number is 4 in our plan, but in random placement, this average number of compromised VMs is 11.



Fig, 2.2 Result Analysis of Placement Strategy Approach

E. Zero Trust Strategy

The Zero-Trust approach as shown in Fig. 2.3 is a strategic initiative, rooted in the principle of "never trust, always verify". It refers to a security threat model with no assumption that the users, devices, data, applications and services that operate from within the security limit of an

organization should be automatically trusted, instead before granting access, the system must verify each and every entity that requests for a connection to its resources, each and every time the user attempts to interact with the system thereby, asserting all the network traffic to be considered as untrusted. More importantly, Zero-Trust model benefits to prevent effective data breaches caused due to exploitation of privileged credentials by stamping out the concept of trust from an organization's network architecture. Furthermore, it is intended to safeguard modern digital environments by leveraging network micro-segmentation, simplifying granular user-access control, and preventing lateral movements. However, zero Trust model is all about eliminating trust from a system rather than deeming a system as trusted.

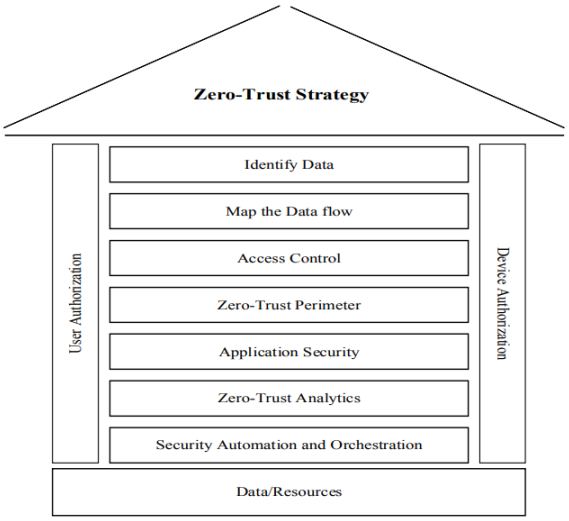


Fig. 2.3 Zero Trust Strategy Model

In this section, we propose Zero-Trust security model for cloud computing environment to address the modern security challenges that come up with cloud infrastructure. As a matter of fact, cloud-based services have changed the technology landscape for the modern enterprises. Also, security is the major challenge in deploying new infrastructure into the cloud. However, traditional security strategies (perimeter centric) failed to make available the satisfactory control, visibility, and protection of user and application traffic. Therefore, Zero-Trust is proposed as the best fit for cloud deployments because cloud environment cannot be trusted so easily due to its dynamic and sharable landscape. To advance cloud security, the Zero-Trust strategy creates a record of what it has in the cloud and accordingly implements strong access control.

However, Zero-Trust strategy begins with an assumption that all the data and transactions are required to be deemed as untrusted from the inception. With this, a new problem gets countered as how to gain sufficient trust? Furthermore, based on the organizational requirements and key focuses, trust is bound to alter. Therefore, to manage the trust worthiness of all transactions in an organization, Zero-Trust environment involves integration of control for data, users, devices and applications as shown in Fig. 2.4.

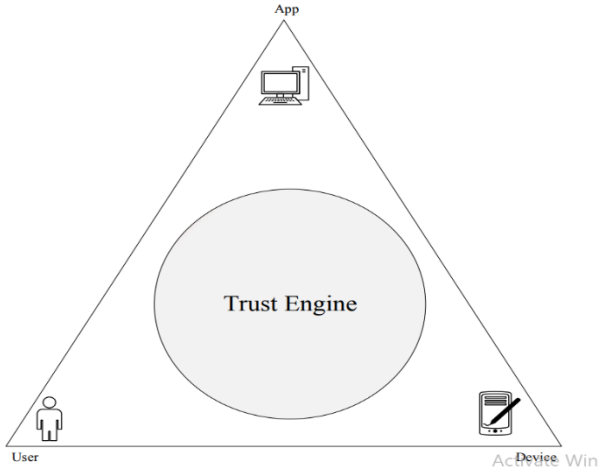


Fig. 2.4 Trust Engine Structure

Trust Engine dynamically computes the consolidated trust of a user, device, or application by giving it a trust score in a particular network. For every transaction request, the trust engine practices the evaluated trust score to make policy-based authorization conclusions.

F. Homomorphic Encryption

A fully homomorphic encryption strategy is computationally intensive and in terms of security recognized for their efficiency. Decipherment is no longer possible only a restricted number of processes can be implemented. In real-world applications, this noticeably limited their usability. Features like computations take part in numerous levels of magnitude slower than the plaintext corresponding parts gathered noise which restricted all computations being applied in modulo N and the total number of processes that can be completed, for the collaboration of data analysis and deep learning this act a big barrier. Presently no existing

strategies can handle rational numbers where improvements in HE led to modifications of encryption techniques.

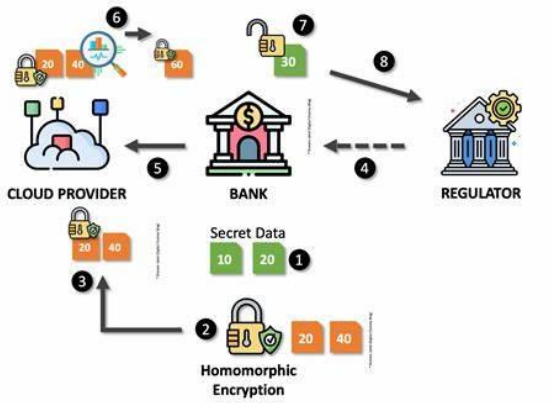


Fig.2.5 Homomorphic Encryption

In recent years numerous open source, HE techniques have developed, based on the involved encryption strategy each one with different characteristics. Simple Encrypted Arithmetic Library (SEAL) of Microsoft strategy, with sustenance for the Cheon-Kim-Kim-Song (CKKS) strategy, the Brakerski/Fan-Vercauteren strategy Fan and Vercauteren (2012) based on the Brakerski Gentry-Vaikuntanathan strategy and HELib of IBM are two most extensive used HE techniques. The absence of support for floating-point numbers is an observable limitation of HELib is SEAL takes benefit of a specific property of the CKKS strategy, computation allows to be implemented on rational numbers, without altering the encrypted value, rescaling can be implemented.

Various security concerns originating from existing and new threats affect the infrastructure of cloud computing with many hardware and software components, refer in the fig.2.6.

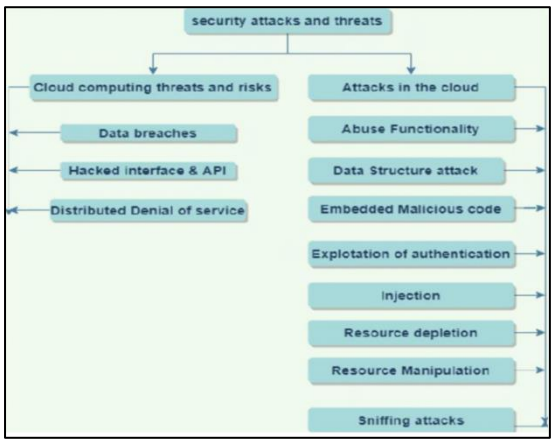


Fig. 2.6 Infrastructure of Cloud

1) Effective Governance and Risk Analysis:

Most firms with security, conformity policies and processes are responsible, and are completely responsible for IT protection of intellectual property and corporate assets. These policies and procedures are designed based on the risk analysis for the organization to assess the impact of these compromise assets. A control framework and other risk mitigation procedures set up and act as a standard for compliance execution and validation. The quality of the process around corporate security governance, and compliance is improved by these principles and policies, company security plans.

2) Backup and Disaster Recovery (DR):

Disaster recuperation in IT platforms is a definite challenge. This is vital in cloud computing because, although the data center has been shut down due to a disaster, CSPs have to supply their consumers with the services. In a system lifespan, a disaster is an unforeseen incident. Table 1 describes three different types of DR levels. It can be done by nature (such as the tsunami and the earthquake), hardware/software failure (for instance Heroku's failure VMs hosted on Amazon EC2 in 2011) or human failure (human error or sabotage). Due to its capacity to handle andachieve reliability and rapid availability the cloud-based DR solution strategy continues to evolve. An organization engine for carrier networks has been launched in Nakajima.

3) Fault Tolerance and Exception Handling:

The system decides that during the execution of distributed cloud applications an exception has been made. The serial exception happened when a computer scheme recognizes and translates when the distributed environment is running.

4) The Algorithm for Cryptography:

The popularity of cloud computing is exponential, leading to developer hazards and a number of cloud security challenges as we grow online technologies. The cryptographical technique to addressing these challenges is one of the typical methods. In this section, we offer a powerful encryption technology that tackles cloud security issues.

5) Digital Forensics Technique:

Digital crime is also expanding with the growing usage of cloud applications and devices. In an organization and structure, digital forensics plays an important function. The

forensic digital toolbox aids to examination of logs and network indexing, file interpretation, and analysis.

G. BCBF Framework for Securing Data

To address the issues with the current system, we implemented the system with a BCBF framework in the proposed work. The BCBF framework has been illustrated diagrammatically in Fig. 2.7, where the users successfully exchange secret data. The Advanced Encryption Standard (AES) technique and a 192-bit key length are used in the proposed work to first encrypt the secret data, which is raw data. The first and primary step in the proposed work is encryption, and the key size is crucial to the BCBF framework. Once the encryption process has been successfully completed, the recipient must be informed of two different pieces of information: encrypted data, often known as cypher text, and the encryption key. Here, the cloud data storage is used to transmit the encrypted cypher text. The recipient can obtain the encrypted data from the cloud. If the recipient is approved, he will possess the decryption key. This key will enable the recipient to decrypt the encrypted data and ultimately obtain the sender's original data. Essential sharing is therefore a key component of secure data exchange. Anyone who obtains the encryption key is permitted to decrypt the data.

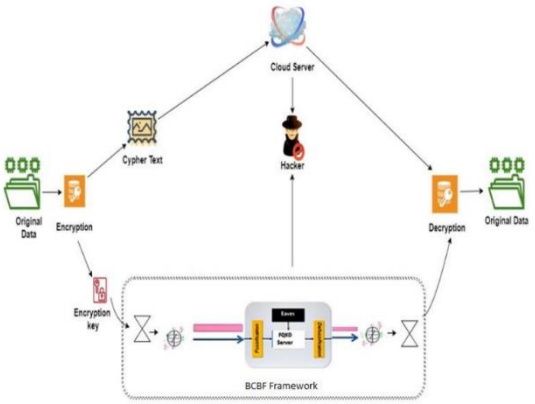


Fig. 2.7 - BCBF Framework Model

The BCBF framework employs three different security measures to protect the encryption key. These include the SBC (Shifting and Binary Conversion with parity bit) algorithm, the core (Block-Re-ordering) algorithm, Polarization and the fuzzification technique. In the first illustration, the SBC strategy is used to modify the secret key, which is the traditional data's value. In this case, the input to the SBC algorithm is the encryption key. The parity bit verification method is executed after the secret key. If the parity is even, the secret key is shifted one bit left; if it is odd, the secret key is shifted one bit right, and one bit is added at the right end. The block reordering algorithm is then used to reorder the blocks according to the type of shifting operation after dividing the encryption key into a few blocks. That data has already been sent to the receiver, followed by the polarization operation that turns the rearranged data into a Q-bit. To entangle photons, the polarization process uses one of the two polarizers. Another task is to finally turn the qubits into a fuzzy bit.

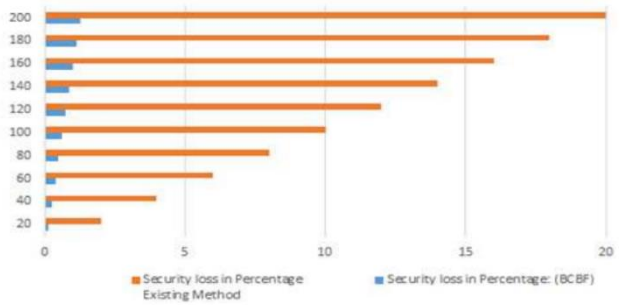


Fig.2.8 - The difference in security losses between the BCBF framework and the current key sharing mechanism is shown in the graph above.

III. CONCLUSION

Virtualization plays a crucial role in cloud computing, by replicating resources like data centers, servers, storage, and many more to efficiently use them. As every coin has 2 sides, even virtualization also have pros and cons too. There are several benefits which provided by virtualization although, we must look into the cons like data security, isolation, maintenance etc. and have to mitigate them as possible as we can by framing strategies and implementations to ensure the security in virtualization. As a result of this, our cloud security will increase.

In the view of security issues, we can say virtualization is directly proportional to cloud computing because most of the security issues that rises at level of virtualization layer. However, the researchers were working on this and enhancing the security mechanisms to ensure the CIA trait which includes characteristics like confidentiality, Integrity, and Availability. In this paper we have discussed few of them mechanism to reduce the risk related to cloud computing.

As the technology updates, the security of the data has to be improvised so that, one can enjoy the leverage of benefits from cloud computing and many other technologies that will take place in future.

IV. REFERENCES

[1]. Ahmad Mateen, Amir Waheed - *The Role of Virtualization Techniques to Overcome the Challenges in Cloud Computing,* International Journal of Computer Applications (0975 – 8887) Volume 143 – No.9, June 2016.

[2] Ahmad Mateen, Amir Waheed - *The Role of Virtualization Techniques to Overcome the Challenges in Cloud Computing,* International Journal of Computer Applications (0975 – 8887) Volume 143 – No.9, June 2016.

[3] Ahmad Mateen, Amir Waheed - *The Role of Virtualization Techniques to Overcome the Challenges in Cloud Computing,* International Journal of Computer Applications (0975 – 8887) Volume 143 – No.9, June 2016.

[4] Ahmad Mateen, Amir Waheed - *The Role of Virtualization Techniques to Overcome the Challenges in Cloud Computing,* International Journal of Computer Applications (0975 – 8887) Volume 143 – No.9, June 2016.

[5] Ahmad Mateen, Amir Waheed - *The Role of Virtualization Techniques to Overcome the Challenges in Cloud Computing,* International Journal of Computer Applications (0975 – 8887) Volume 143 – No.9, June 2016.

[6] Ahmad Mateen, Amir Waheed - *The Role of Virtualization Techniques to Overcome the Challenges in Cloud Computing,* International Journal of Computer Applications (0975 – 8887) Volume 143 – No.9, June 2016.

[7] Ahmad Mateen, Amir Waheed - *The Role of Virtualization Techniques to Overcome the Challenges in Cloud Computing,* International Journal of Computer Applications (0975 – 8887) Volume 143 – No.9, June 2016.

[8] Ahmad Mateen, Amir Waheed - *The Role of Virtualization Techniques to Overcome the Challenges in Cloud Computing,* International Journal of Computer Applications (0975 – 8887) Volume 143 – No.9, June 2016.

[9] Ahmad Mateen, Amir Waheed - *The Role of Virtualization Techniques to Overcome the Challenges in Cloud Computing,* International Journal of Computer Applications (0975 – 8887) Volume 143 – No.9, June 2016.

[10] Ahmad Mateen, Amir Waheed - *The Role of Virtualization Techniques to Overcome the Challenges in Cloud Computing,* International Journal of Computer Applications (0975 – 8887) Volume 143 – No.9, June 2016.