Survey on Security Attacks in Virtual Organization

Khalid Saeed
University of Engineering &
Technology Peshawar, Pakistan
khalid_saeed102@yahoo.com

Wajeeha Khalil
University of Engineering &
Technology Peshawar, Pakistan
wajeeha.khalil@uetpeshawar.edu.pk

Sheeraz Ahmed
IQRA National University
Peshawar, Pakistan
sheerazahmed306@gmail.com

Arbab. Waseem Abbas
University of Engineering &
Technology Peshawar, Pakistan
aristocratarbab@yahoo.com

Muhammad Naeem Khan Khattak
University of Engineering &
Technology Peshawar, Pakistan
khattak1962@yahoo.com

Madeeha Ishtiaq
Abdul Wali Khan University
Mardan, Pakistan
madeehaishtiaq@gmail.com

***Abstract*— Virtual Organization (VO) involves workers from different organizations. These workers work together to achieve a common task. The workers of VO communicate and perform activities using the cyber infrastructure. Since VO involves the use of cyber infrastructure which is vulnerable to different security attacks. This research identifies the possible vulnerabilities to VO, evaluates different security attacks as well as their consequences and mitigation plan. Moreover there are some proposed guidelines to VO administrators and users to improve the overall security of VO.**

Keywords—Virtual Organization; Security attacks; Vulnerabilities.

I. Introduction

Virtual Organization (VO) involves sharing of geographically dispersed resources for achieving a common goal. A VO involves group consist of individuals whose resources and members may be spread both institutionally and geographically, yet who work as a logical unit by using the cyber infrastructure [1]. Since VO relies on the underlying cyber infrastructure which is vulnerable to different security attacks. If the resources of VO are compromised due to security attacks then the traditional organizations are least likely expected to use the resource or become part of the VO.

Trust Management is the limitation in the success of VO. Since VO involves worker from different organizations and usually face to face communication is very rare among these workers therefore building trust in VO is a challenging task for the managers of VO.

Three main goals of security are confidentiality, availability and integrity as shown in figure 1. There should be a good balance between these three goals of security. Absolute secure systems do not exist. The important aspect in securing a system is to minimize the chances of loopholes to be exploited by an attacker by using different security mechanism. For this purpose loopholes will have to be identified which can be exploited by an attacker. The best security solutions should be used and as a result the consequences of an attack can be minimized up to a great extent.

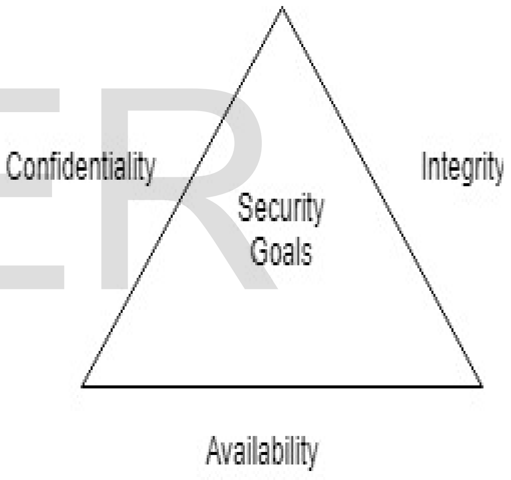

Figure 1. Goals of security

A) Security concern a barrier for adoption of virtual environment

There are many barriers for adoption of Virtual Environment (VE) and due to these barriers the users are reluctant regarding adoption of the VE environment. According to the survey conducted about different barriers towards adoption of VE, data security is among the top three concerns of the users as reflected in figure 2 [2]. According to [3] the security requirement of VE is more as compared to traditional environment because the virtual environment is susceptible to all attacks which are possible in traditional environment and moreover it also requires security management of several virtual computers which are providing services to the users. Attackers are actively developing different malware programs for VE. The attacks which are unique for the VE are low level hypervisor attacks and malicious virtual system deployment.

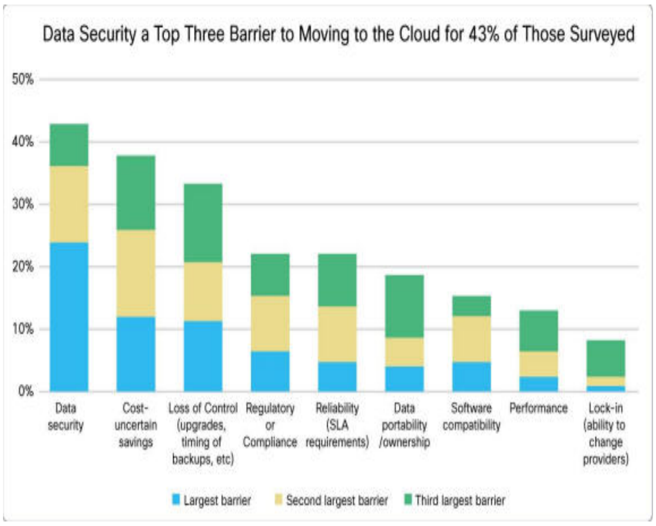

Figure 2. Barriers towards virtualization [2]

B) Motivation

There are different security issues in VO such as the collaboration of different security mechanism in a single VO, need of security management system for supervising the security of all applications deployed in VO etc. Making the VO secure is a challenging task. The major research contribution in this area so far is the development of security framework and security architecture for VO. This research work addressed the security loopholes in VO because very little attention has been given to address this issue by the research community. Moreover general guidelines for improving the security of VO need to be developed.

C) Objectives of Research

The objectives of this research are as follows:

- To identify security loopholes in VO.
- To analyze the consequences of identified loopholes.
- To recommend guidelines to overcome the identified loopholes.

II. Related work

The research conducted in [4] presented security framework for VO which consisted of four elements or layers such as protected resources layer, recovery layer, detection layer and prevention layer as shown in figure 3 but, their main focus was on the security issues related or experienced in the four projects named E-COLLEG, EXTERNAL, PRODNET and TeleCAREe follow. Moreover they focused more on the technical aspect of the VO and thereby skipping the organizational and legal aspect of VO.

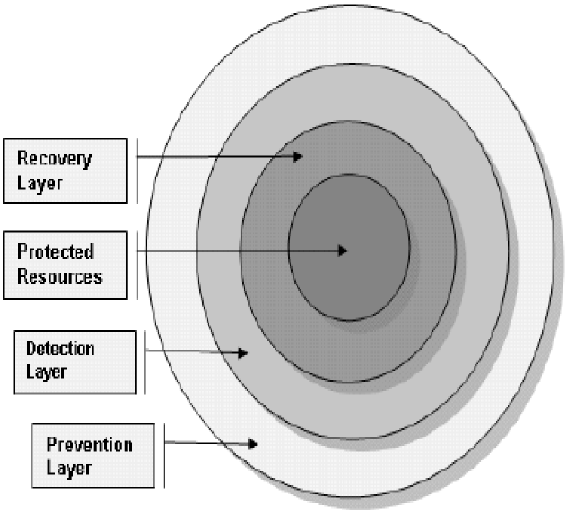

Figure 3. Multiple layer security model [4]

The research conducted in [5] discussed how to use Role Based Access Control (RBAC) model in VO. The standard RBAC is usually applied to single large domain with centralized role management. The use of RBAC in VO is a challenging task. The advantages and disadvantages of both centralized and de-centralized approach of role management in VO has been discussed in this research work. The advantage of centralized approach is its widely acceptance in the grid community and need of single VO administrator. The disadvantage of centralized approach is single point of failure. The advantage of de-centralized approach is that it allowed dynamic collaboration. The disadvantage of de-centralized approach is association of roles with VO are scattered across different locations.

The research conducted in [6] proposed security architecture for addressing the requirements of business oriented applications. Components of the proposed architecture are web service, policy generator, policy enforcement point, policy decision point, lifecycle manager and membership manager. Since business application users use web services therefore this architecture can be used to secure interaction involved in web services.

The research conducted in [7] developed a new service known as Virtual Organization Membership Service (VOMS). The purpose of VOMS system is to manage authorization information in the VOs. The VOMS system consist of the following four parts such as i) user server ii) user client iii) administration client iv) administration server. According to VOMS resource provider has the ability to override the permissions granted by VO. Moreover user can be a participant of different groups and different roles can be assigned to users.

According to [8] the number of users increase and decrease in VO and the need of processing capabilities of users also increases and decreases therefore, to address such issues a Grid Information Retrieval (GIR) System using VO and security mechanism has been proposed in this research. The major advantage of GIR System is efficient management of security information in VO, when different information retrieval system each having changed security policies are combined in a VO. It means that the organizations can distribute secure information to other organizations by applying multilevel security policies.

According to [9] cloud computing are used to provide services on Internet but some applications require the services of many clouds together which can be achieved with the help of VO. This research work proposed a framework such as CloudVO. The proposed framework provides secure management of VO across multiple clouds. CloudVO provides flexible in nature and dynamic VO protocol for the clouds. Therefore Inter-cloud collaboration can be achieved without disturbing the local polices of clouds. The CloudVO framework addresses the challenge of dynamic, autonomous and distributed cloud environments.

According to [10] **w**ith the help of VO the collaboration among different administrative domains is possible and, the VO applies joint security policies on different administrative domains. This research work proposed Open Stack Keystone service which can be used to act as VO management system. This application can be used to use the services of VOs. The services can be either Infrastructure level services or application level services.

The research conducted in [11] proposed a model such as grid security model based on VO. The model consists of both physical model as well as logical model. The logical model contains 5 layers and physical model is used to implement the logical model. Using this model a security mechanism can be established in grid environment.

According to [12] VO comprises of people from dissimilar organizations and usually they do not have a trust on each other. Due to the open nature of VOs the security concerns of people increases. This research work examines the existing negotiation protocols and enhances one protocol among them.

III. Research Contribution on Security in VO

The section consists of the following three phases.

- Identifying possible vulnerabilities in VO.
- Possible security attacks in VO.
- Recommended guidelines for both VO users and administrators for improving the security of VO.

A) Possible vulnerabilities in VOs

The following are some of the possible vulnerabilities in VO.

1) Since VO relies on web based system therefore the attacker can divert the traffic of VO towards a fake website and can obtain the credentials of users.

2) VO requires authentication for all users therefore the authentication system can by compromised by different means.

3) VO offer Internet based services which require web services therefore different attacks can be launched against web servers.

4) VO includes workers from different organizations therefore any worker can launch attack against VO. Such type of attack lies under the category of insider attack.

5) If the security of a VO is compromised there is no possible means for user to know about such incident because the organizations usually do not share such information with users.

6) The hypervisor has comparatively more access to the base system hardware resources than application. If the attacker hijacks the hypervisor than the base system as well as multiple VM which are running on the same system can be accessed [13].

B) Possible security attacks on VO

There are different security attacks possible on VOs. Some of these attacks are discussed in this section.

1) DNS cache poisoning

The purpose of this attack is to poison the cache of DNS server in order to divert the traffic towards a fake website hosted by attacker. The attacker first share updates with the DNS server in order to poison the DNS cache. Such type of attack can be launched against VO and the attacker can divert the traffic towards a bogus website in order to obtain the credentials of the user. The process is shown in figure 4. To avoid such type of attack the user should look at the browser address and should use certification authority.

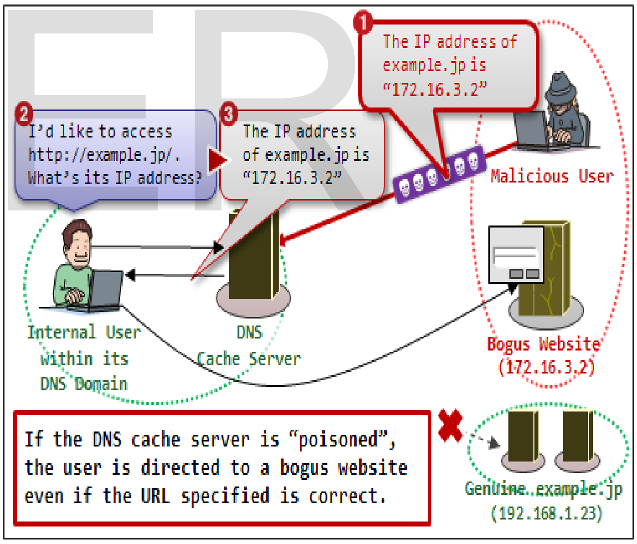
1
The IP address of example.jp is "172.16.3.2"
2
I'd like to access http://example.jp/. What's its IP address?
3
The IP address of example.jp is "172.16.3.2"
Malicious User
Internal User within its DNS Domain
DNS Cache Server
Bogus Website (172.16.3.2)
If the DNS cache server is "poisoned", the user is directed to a bogus website even if the URL specified is correct.
Genuine.example.jp (192.168.1.23)

Figure 4. DNS cache poisoning procedure [16]

2) Phishing attack

The purpose of phishing attack and DNS cache poisoning attack is same but phishing attack is easy to launch. In phishing attack the attacker sends a malicious file to user which contains a link to malicious website so that the traffic diverts towards a fake website and the attacker fools the user to input user name and password. If the user inputs credentials than the attack is considered successful. Such type of attack can be stopped by looking at the browser address, using certification authority and restraining from opening malicious files.

3) Attack on hypervisor

The main aim of attack on hypervisor is to access the virtual machine and base system. Such type of attacks can be minimized by using a SHype a secure hypervisor proposed by IBM. In this software based solution security policies are bind to the VE.

4) DOS attack

This attack can be launched against VO in which one user uses all the resources and as a result the resources are not available to the actual clients. To overcome such type of attack proper virtualization technology should be used in VO in order to control the access of all users.

5) DDOS attack

This attack is the more severe form of DOS attack. In such type of attack the VO resources are not available to the actual users. The genuine users are not able to access the web servers of VO. To mitigate the chances of this attack ping command should be disabled on the servers and moreover manual codes should be used in order to stop machine attacks.

6) Attack on authentication system

VO includes authentication system in order to allow only VO users to access the system. Therefore attacker can attack the authentication system of VO by using different means such as brute force attack, dictionary attack etc. In order to minimize the chances of such attack maximum number of login attempts should be 3 and after 3 failed login attempts account should be locked for some specific period of time. Log files should be frequently checked to identify suspected activities.

7) Attack on authorization system

In VO different level of access is provided to the users. In this attack the VO user access the resources for which the user is not authorized. Such type of attack can be handled by using role base access control mechanism.

8) Eavesdropping

When VO user is communicating with VO servers then attacker can capture the traffic communicated between user and server. To minimize the effect of such attack best encryption algorithm should be used so that if the attacker captures traffic then it will be of no use for the attacker because attacker can't decrypt the coded data.

9) TCP session hijacking

Such type of attack can be launched against VO user. The attacker can hijack an established session between VO user and servers. The process of this attack is shown in the figure 5. In order to avoid this attack encryption should be used because attacker will not be able to decrypt cipher text and won't be able to find the sequence number which is required for launching this attack.

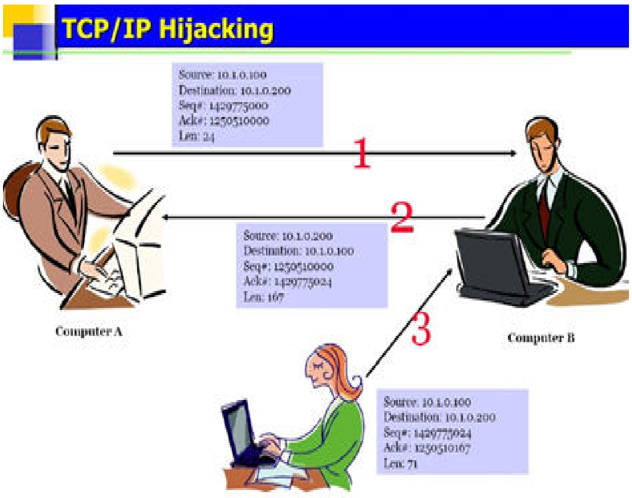

Figure 5. TCP Session Hijacking [17]

10) ARP cache poisoning

The purpose of this attack is to poison the cache of switch used in a LAN so that the attacker can capture the traffic intended for the genuine user. The process to poison the cache of switch is shown in figure 6. To avoid such type of attack port number to MAC address mapping should be used and moreover the use of intrusion detection system detects suspicious activities in the network.

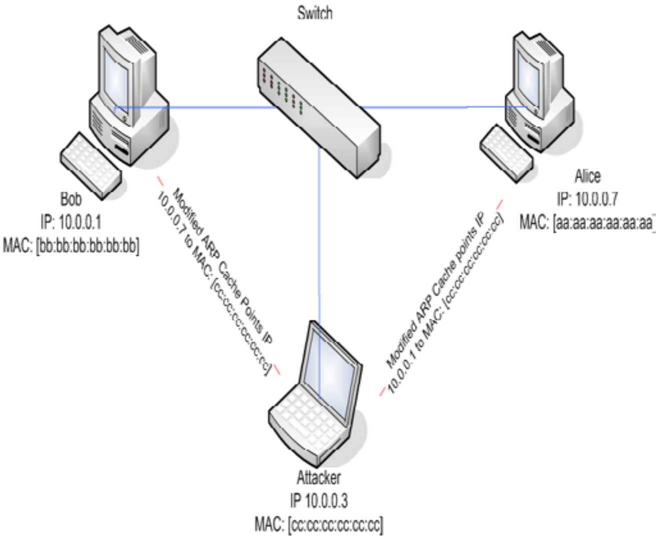
Switch
Bob
IP: 10.0.0.1
MAC: [bb:bb:bb:bb:bb:bb]
Alice
IP: 10.0.0.7
MAC: [aa:aa:aa:aa:aa:aa]
Modified ARP Cache Points IP 10.0.0.7 to MAC: [cc:cc:cc:cc:cc:cc]
Modified ARP Cache points IP 10.0.0.1 to MAC: [cc:cc:cc:cc:cc:cc]
Attacker
IP 10.0.0.3
MAC: [cc:cc:cc:cc:cc:cc]

Figure 6. ARP cache poisoning [18]

11. ARP spoofing

The purpose of this attack is to use the spoofed MAC address and start communication with host and impersonating as a legitimate user. The process of ARP spoofing is shown in the figure 7. To avoid such type of attack port security and IDS should be used.

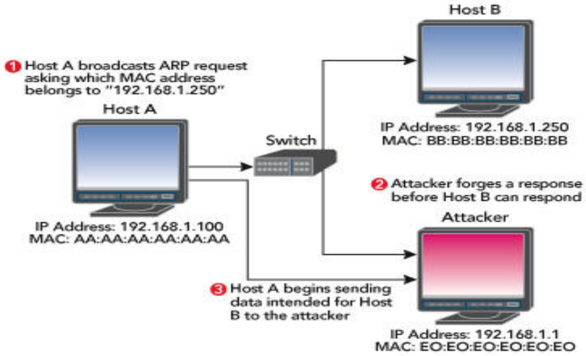
Host B
❶ Host A broadcasts ARP request asking which MAC address belongs to "192.168.1.250"
Host A
Switch
IP Address: 192.168.1.250
MAC: BB:BB:BB:BB:BB:BB
❷ Attacker forges a response before Host B can respond
Attacker
IP Address: 192.168.1.100
MAC: AA:AA:AA:AA:AA:AA
❸ Host A begins sending data intended for Host B to the attacker
IP Address: 192.168.1.1
MAC: EO:EO:EO:EO:EO:EO

Figure 7. ARP spoofing [19]

12. Attack on virtual machine

The attacker can attack the specific virtual machine by exploiting the loop holes in the virtual machine. If the configuration is not properly done then the application on one virtual machine can access the applications running on other virtual machines. The break in the one virtual machine can be exploited by providing access to the other virtual machines in the same environment [20].

C) Recommended guidelines

Guidelines for improving the security of VO are divided into two categories such as guidelines for VO administrators and guidelines for VO users.

1) Recommended guidelines for VO administrators

The following are some recommended guidelines which can be used by VO administrators in order to handle security related issues.

1) The users of VO can access the resources online and usually the users are authenticated on the basis of user name and password. The problem in this scenario is user share their authentication credentials with other people who can use the resources of VO. The solution to such type of problems is to authenticate user by username and password as well as by typing pattern [21].
2) A role based access control mechanism should be used for user authorization [5] which will minimize the chances of insider attacks.
3) Use best encryption algorithms such as AES.
4) Passwords should be stored in salted form on servers so that the password can't be recovered but can be changed.
5) For trust management a third party monitoring system should be used which will monitor the security of VO and if the VO is under attack than it will send alert to the VO administrator as well as VO users.
6) Limit the cache size of DNS.
7) Use certification authority.
8) Use licensed version of firewall, antivirus and Intrusion Detection System (IDS).
9) Ping should be disabled on web servers.
10) Automated queries should be stopped.
11) Use VPN for establishing secure connection so that users can securely access VO resources [10].

2) Recommended guidelines for VO users

The following are some recommended guidelines which can be used by VO users in order to handle security related issues.

1) DNS cache poisoning is extremely difficult attack to launch and it is also very difficult attack to detect because maximum users do not look at the browser address while using web applications. The users should look at the web browser addresses and if any suspected website address found than administrator should be informed immediately.
2) Do not open suspected files on the computer because if the user's computer security is compromised by Trojan then the attacker can access the resources of VO by using the account of user.
3) Do not install suspected software on system because such software usually includes back door channel which transfers the sensitive information to attackers.
4) Users should not share authentication credentials with others.

Table 1: Possible attacks and their countermeasures in VO

Possible attacks	**Consequences of each attack**	**Mitigation plans**
DNS cache poisoning	Misguide user and divert traffic towards a fake website.	User should look at the browser address and use digital certificates.
Phishing attack	Misguide user and divert traffic towards a fake website	User should check the browser address before entering credentials.
Attack on hypervisor	Attacker access the VM and base system.	Use SHype, in which security policies are binded to the VE[3]
DOS attack[14]	One user consumes all resources in VE due to which resources are not available to other users.	Properly configure virtualization technology for controlling access of users[15]
DDOS attack	More severe form of DOS attack	Disable ping command on servers, use manual codes.
Attack on authentication system [4]	Illegally login to the system	Max no. of attempts should be 3, frequently check logs.
Authorization attack [4]	Use resources for which the user is not authorized	Use role base access control mechanism.
TCP session hijacking	Hijack an established session between client and server	Use secure socket layers (SSL) port no. 443.
Eavesdropping [4] such as using packet sniffers	Captures traffic	Use best encryption algorithm (AES). Should use VPN to create a private tunnel using public network [13].
ARP cache poisoning	Attacker poisons the cache of switch and receives data of target system.	Use port based security such as port no. to mac address mapping, use intrusion detection system [4].
ARP spoofing	Attacker receive data of the target system.	Use port based security such as port no. to mac address mapping, use intrusion detection system [4].

Attack on virtual machine	Application running on one VM can access applications running on other VMs, break-in one VM provide access to the VMs in the same environment.	The resources in the environment should be carefully deployed. Configuration should be carefully done [20].

IV. CONCLUSION

VO allow user to work from different locations using cyber infrastructure to achieve a common goal therefore traditional organization can move towards VO to get advantages from it. This research paper evaluates the possible security vulnerabilities in VO, possible attacks as well as their consequences and mitigation plan are also discussed. At the end there are some recommendations for VO administrators and users to make the environment more secure.

According to survey conducted [2] which identified different barriers towards adoption of VE, data security was the concern of 43% users participated in the survey. VO administrators need to focus more on security concerns of the users and should use the best available security mechanisms.

REFERENCES

[1] Cummings, J., Finholt, T., Foster, I., Kesselman, C., & Lawrence, K. A. (2008). Beyond being there: A blueprint for advancing the design, development, and evaluation of virtual organizations.

[2] Securing Virtual Applications and Servers. Retrieved from http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/unified-network-services-uns/white_paper_c11-652663.pdf on March 17, 2016.

[3] K. J. Higgins. Vm’s create potential risks. Technical report, darkREADING, 2007. http://www.darkreading.com/document.asp?doc_id=117908.

[4] Magiera, J., & Pawlak, A. (2005). Security Frameworks for virtual organizations. In *Virtual Organizations* (pp. 133-148). Springer US.

[5] Sinnott, R. O., Chadwick, D. W., Doherty, T., Martin, D., Stell, A., Stewart, G., ... & Watt, J. (2008, May). Advanced security for virtual organizations: The pros and cons of centralized vs decentralized security models. In*Cluster Computing and the Grid, 2008. CCGRID'08. 8th IEEE International Symposium on* (pp. 106-113). IEEE.

[6] Kerschbaum, F., & Robinson, P. (2009). Security architecture for virtual organizations of business web services. *Journal of Systems Architecture*,*55*(4), 224-232.

[7] Alfieri, R., Cecchini, R., Ciaschini, V., dell’Agnello, L., Frohner, A., Gianoli, A., ... & Spataro, F. (2004). VOMS, an authorization system for virtual organizations. In *Grid computing* (pp. 33-40). Springer Berlin Heidelberg.

[8] Kim, Y. P., Lee, S., Lee, P., & Newby, G. B. (2006, October). Grid Information Retrieval Management System for Dynamically Reconfigurable Virtual Organization. In *Grid and Cooperative Computing, 2006. GCC 2006. Fifth International Conference* (pp. 301-306). IEEE.

[9] Li, J., Li, B., Du, Z., & Meng, L. (2010, June). Cloudvo: Building a secure virtual organization for multiple clouds collaboration. In *Software Engineering Artificial Intelligence Networking and Parallel/Distributed Computing (SNPD), 2010 11th ACIS International Conference on* (pp. 181-186). IEEE.

[10] Lee, C. A., Desai, N., & Brethorst, A. (2014, December). A Keystone-Based Virtual Organization Management System. In *Cloud Computing Technology and Science (CloudCom), 2014 IEEE 6th International Conference on* (pp. 727-730). IEEE.

[11] Xiuying, W. U., Geng, Y. A. N. G., Jiangang, S. H. E. N., & Quan, Z. H. O. U. (2005, December). A novel security model based on virtual organization for grid. In *null* (pp. 106-109). IEEE.

[12] Darko-Ampem, S., Katsoufi, M., & Giambiagi, P. (2006, October). Secure negotiation in virtual organizations. In *Enterprise Distributed Object Computing Conference Workshops, 2006. EDOCW'06. 10th IEEE International* (pp. 48-48). IEEE.

[13] Vaughan-Nichols, S. J. (2008). Virtualization sparks security concerns.*Computer*, *41*(8), 13-15.

[14] Abdulla, P. (2012). Understanding the Impact of Denial of Service Attacks on Virtual Machines.

[15] J. Kirch. Virtual machine security guidelines. *The center for Internet Security*, September 2007.

[16] IPA/ISEC ︰ Vulnerabilities ︰ Security Alert for DNS Cache Poisoning Vulnerability. Retrieved from http://www.ipa.go.jp/security/english/vuln/200809_DNS_en.html on August 17, 2018.

[17] Session Hijacking. Retrieved from http://www.slideshare.net/leminhvuong/module-6-session-hijacking on March 17, 2016.

[18] Sniffing Networks Part 2 – MAC addresses, IP. Retrieved from http://securitymusings.com/article/tag/arp-spoofing on March 17, 2016.

[19] Lam, K., LeBlanc, D., & Smith, B. (2005). Theft on the web: Prevent session hijacking. *Technet Magazine: Microsoft.*

[20] Reuben, J. S. (2007). A survey on virtual machine security. *Helsinki University of Technology*, *2*(36).

[21] Kumar, A., Patwari, A., & Sabale, S. User Authentication by Typing Pattern for Computer and Computer based devices.