Security Attacks in Stand-Alone Computer and Cloud Computing: An Analysis

K.Kavitha
Research Scholar, Bharathiar University,
Assistant Professor,
Dr.G.R.Damodaran College of Science
Coimbatore

B. Arunkumar, Ph. D.
Professor
Coimbatore Institute of Technology
Coimbatore

ABSTRACT

The data that is stored on the computer may be confidential or sensitive according to its applications or usage. The data must be protected from unauthorized users. This paper analyses the security attacks in a) stand-alone computers and b) in cloud computing. A study of existing protective mechanisms is also presented.

Keywords

stand-alone security, cloud computing, virtualization, multi-tenancy, virus.

1. INTRODUCTION

Computing is data centric. The data can be generated internally, taken from an user of the computer, accessed from a file or shared from another data storage which could be local or over the internet. There is a need to ensure that only authorized personnel have access to the data and are allowed to modify the data. An unauthorized user may snoop on the data or malign the data or add wrong data or delete the data or obstruct access to the data. Ensuring authorized data access is termed as Data security.

This paper is organized as: 1) security issues with a standalone computer 2) the approaches to handling these security issues. 3) the security issues that arise when the computer is in a network 4) security issues when the data is moved to a cloud storage. 5) The state of art of solutions for handling cloud based security issues.

2. SECURITY ISSUES IN STAND ALONE COMPUTER

2.1 Malwares:

Malware is the short form of "Malicious Software", designed to cause damage to a standalone computer or a networked computer. Once malware get into the system, they begin to damage a system's boot sector, data files, software installed in it, including the system BIOS.

2.1.1 Types of Malware:

2.1.1.1 Computer Virus and Worms:

The virus can get into the user's computers from network or Internet, through removable media such as CDs or memory sticks.

Unlike a virus, an Internet Worm does not need to attach itself to an existing program. It can spread copies of itself from one computer to another without being activated by users like

- file sharing
- By exploiting network configuration errors (for example, to copy themselves onto a fully accessible disk)
- Exploit loopholes in operating system and application security.

Other worms carry a so-called "payload", a piece of code designed to do damage the data stored in the computer. It might delete files on the PC(e.g., the ExploreZip worm) or cause damage or to retrieve sensitive information such as passwords and credit card numbers [1,2,3,4,5,6,7,8].

2.1.1.2Trojan Horse:

A Trojan horse is is another type of malware that looks as a genuine application. Unlike viruses, Trojan horses do not replicate themselves. Keylogger is a software program that is installed on a user's computer, often by a Trojan horse to capture and record user keystrokes. The data captured is then transmitted to a hacker's computer. [4,6,10].

2.1.1.3 Spyware and Adware:

The spyware will get into a computer in any one of the many methods like

- Installing a software package which automatically tries to download

- Browser add-ons, a piece of software that add enhancement to the web browser like toolbar, animated cursors, screen saver [4,9,10].

2.2 Unauthorized Access:

This attack aims in gain access of other's computer to gain some information or to modify or to delete the data. The goal of these attacks is to access some resource that the machine should not provide the attacker. Password hacking is the commonly used method in this kind of threat [11,17].

Table 1: Security Attacks in Stand-Alone Computer and Current Solutions

Intrusion Mechanisms	Intrusion Type	Consequences of Attack	Defense Mechanisms
Password Cracking and Un-authorized Access	Masquerader	Misusing computer system and doing data processing like file creation, modification and deletion	User validation. User control access. Data encryption. Statistical anomaly detection. Rule-based techniques.
Malware: Virus Worms Trojan Horse Spyware Adware	Misfeasor Clandestine users	Some malware programs delete files, reformat the hard disk or cause other damage. Others only replicate themselves & affect computer's performance. Trojan horse install "pay-loads" which capture user's keystroke process	Anti-virus software. Firewalls. Anti-spyware. Anti-keylogging technique.

2.3 Password Cracking:

Password cracking is the process of using other's password to gain data access. This is a technique attacker use to surreptitiously gain system access through another user's account [11,17].

3. SECURITY MECHANISMS FOR STAND ALONE COMPUTER SECURITY

The data which is stored in the computer can be accessed, by a malicious user or third party is known as Intrusion. Intrusion Detection System is the process of monitoring the events occurring in a computer system and intrusion prevention is the process of detecting the signs of intrusion and attempting to stop the intrusive efforts.

The intruder can be broadly divided into 3 types:

i) **Masquerader**: They are outsiders and unauthorized to use the computer system.

ii) **Misfeasor**: They are insiders and legitimate users but misuse their privileges.

iii) **Clandestine users**: They can be both insiders and outsiders.

3.1 Defense Mechanisms for Masquerader:

3.1.1User Validation:

Password is the most widely used authentication technique to validate the user. In this method, the users can access their computer system with user name (also known user id) along with password. The problem is that passwords can be hacked [11, 17].

3.1.2 User Account Control:

User Account Control (UAC) is a feature that helps to control the user in multi-user environment. This can be done using administrator-level permission. Using UAC, changes cannot be made to the computer without administrator's permission or knowledge. It can help prevent malicious software (malware) and spyware from being installed on or making changes to the computer [11, 17].

3.1.3 Data Encryption:

Data encryption is the process of converting the data into cipher text using an algorithm (mathematical formula) by use of a code. Decryption is the reverse process of it. A secret key is used to encrypt and decrypt the data. Symmetric key and Asymmetric key are current techniques used in data encryption [2].

3.1.4 Statistical Anomaly Detection:

This method involves the collection of data relating to the behavior of authorized users in a period of time. Then statistical tests are applied to observed behavior to determine that the observed behavior is not legitimate user behavior[1]. Statistical anomaly detection techniques fall into two broad categories: Threshold detection and Profile-based systems [18].

3.1.4.1 Threshold Detection:

It involves counting the number of occurrences of a specific event type over an interval of time. If the count exceeds than the reasonable number that one might expect to occur, then intrusion is assumed [18].

3.1.4.2 Profile-based Anomaly Detection:

It focuses on characterizing the past behavior of individual users or related groups of user and then detecting significant deviations. A profile may consist of a set of parameters, so that deviation on just a single parameter may not be sufficient in itself to signal an alert. Examples of metrics that are useful for profile-based intrusion detection are interval timer, resource utilization etc. Using these metrics, various tests can be performed to determine whether current activity fits within acceptable limits such as Mean, standard deviation and Multivariate. These detection systems work on audit records [18].

3.1.4 Rule-based Techniques:

It detects intrusion by observing events in the system and applying a set of rules that lead to a decision regarding whether a given pattern of activity is or is not suspicious. With the rule-based approach, historical audit records are analyzed to identify usage patterns and to generate automatically rules that describe those patterns. Rules may represent past behavior patterns of users, programs, privileges, time slots, terminals, and so on. Current behavior is then observed, and each transaction is matched against the set of rules to determine if it conforms to any historically observed pattern of behavior. These rules can be supplemented with rules generated by knowledgeable security personnel [18].

3.2 Defense Mechanisms for Misfeasor and Clandestine Users:

3.2.1 Anti Virus-Software:

An anti-virus is a software or computer program that can be used to scan files to identify and eliminate computer viruses. Anti-virus software uses two different techniques to accomplish this [4,7,11,12,13].

3.2.1.1 Virus Dictionary Signature:

In this approach, when the anti-virus software examines a file, it refers to signatures that have been identified and listed by the anti-virus software service provider. If any piece of code in the file matches signature, which is identified in the dictionary, then the anti-virus software will notify this to user and delete it [1].

3.2.1.2 Suspicious Behavior Approach:

It doesn't attempt to identify known viruses; but instead monitors the behavior of all programs. If any program tries to write data to an executable program, (for example, this is flagged as suspicious behavior) and the user is alerted to this, and asked what to do.

3.2.2 Firewall:

Firewalls are software programs or hardware which is used to protect personal computer or networked computer. Personal Firewall is one type in firewall, used in personal computer to avoid unauthorized access. There are two ways a firewall can prevent this from happening. It can allow all traffic to pass through except data that meets a predetermined set of criteria, or it can prohibit all traffic unless it meets a predetermined set of criteria. Using firewalls always helps to secure unused ports in the computer. Using these ports only the intruder gets access to the target computer [4, 5,7,12,17,19].

3.2.3 Anti-Spyware Software:

Spywares are controlled when using anti- spyware softwares. Anti-spyware programs can fight with spyware in two ways [4,16,17,18,19].

3.2.3.1 *Real-time Protection:*

These programs work just like anti-virus software. They scan all incoming network traffic for spyware software and block any threats that are detected.

3.2.3.2 Detection and Removal:

It involves periodical scanning of files and programs installed on the computer [4,7,10].

3.2.4 Anti-keylogging Techniques:

The keylogging process can be prevented, detected or removed by using a technique called "on-screen virtual keyboard". This technique will create a virtual keyboard on user's computer. On the other hand it can be detected using dedicated anti-logging tool which monitors the behavior of running applications and notify the user if any keylogging activity[4,7,20].

4. CLOUD COMPUTING AND ITS DEPLOYMENT MODELS

Cloud computing changed the trend of data storage and access from the traditional method to on-demand access. It offers the service to the users through Internet. The users make use of cloud computing for its significant benefits such as reduced infrastructure cost, reliable data access, on demand service and also security. Cloud computing provide services to the user community through three different deployment models such as Iaas, PaaS and SaaS.

- Infrastructure as a Service (IaaS) implies that clouds of hardware resources, e.g. computers, storage, networks, can be pooled and inter-operated.

- Platform as a Service (PaaS) means that users may gain access to (virtual) hardware infrastructures and already functional run-time environments where they may then develop, test, or run software etc., without needing to deal with the complexities of an operational environment or hardware in cloud.

- Software as a Service (SaaS) means that users that have gained access to the cloud in a virtual environment with on-demand functional software applications.

At the same time, there are some security threats which motivate the hackers to access others' data, stored in cloud server. Since the users do not know the exact location of their data, they cannot completely restrict their data from unauthorized usage. To avoid this, the cloud service provider should identify the threats relevant with cloud data storage and apply strong security mechanisms to protect users' data.

5. SECURITY ISSUES IN CLOUD COMPUTING

This section deals with cloud computing security issues based on deployment models.

5.1 Security Threats in SaaS

SaaS is a software deployment model where applications are remotely hosted by the vendor and made available to customers' on-demand, over the Internet. Because of this, data storage and data security are highly important for enterprise. But in cloud storage, enterprise data is stored at the SaaS provider's data center, along with the data of other enterprises [21].

5.1.1 Data Security

In cloud environment, the data storage is location independent, more exactly in a remote server. Since the enterprise's data has more weightage, the SaaS vendor must adopt additional security checks to ensure data security and prevent unauthorized data access due to security vulnerabilities in the application or through malicious employees.

Since Internet is the communication medium to access the SaaS application, web browser security is fundamentally important. Using Internet to access application may leads to more vulnerabilities when transmitting data and storing it in the cloud storage. For example, the malicious user can view/alter the data during transmission, listen to the traffic, change traffic to some malicious websites, steal information and install any malware. The security also can be given to Extendable Markup Language (XML) encryption, Secure Socket Layer (SSL) to prevent data attacks. [21,22,23,24,25].

5.1.2 Data Segregation

In cloud based environment, the same remote server is shared by all the users. As a result, multiple users can store their data in same physical location using the applications provided by SaaS. This is known as Multi-tenancy. Intrusion of data of one user by another becomes possible in this environment. This intrusion can be done either by hacking through the loop holes in the application such as misuse of user log-in credentials, internal monitoring tool for security or by injecting client code into the SaaS system. A malicious client who is the co-user of victim instance (also known virtual machine) can write a masked code and inject into the application. If the application executes this code without verification, then there is a high potential of intrusion into other's data [21].

5.1.3 Data Confidentiality and Internal Breach:

In cloud, Confidentiality refers to the customers' data and computation tasks are to be kept confidential from both vendor and other customers. Multi tenancy feature of cloud leads to more vulnerabilities. In cloud environment, the confidentiality may be violated either by malicious user or malicious employees [21,26,27].

In cloud, the data is stored virtually. Hypervisor is a tool used in virtualization to create a virtual machine (VM). In such a case, there is a chance of creating malicious VM to attack others' instances. This is the main security hole in the cloud environment. Being one of the co-user in the cloud, a malicious user can perform this kind of operations. This attack is known as Cross VM Attack [21,26,27].

The cross VM attack can be done in two stages: i) placement of malicious VM ii) Extraction.

Placement: In this stage, an adversary needs to identify the location of target VM to which he wants to perform attack. This co-resident check can be done using some network probing tools such as wget, nmap and hping. After this, a malicious instance can be created in target physical machine, by specifying the parameters of the instance such as zone, host type. There are two basic strategies used to launch a VM: i) Brute-force technique, which will create multiple instances and ii) Using hypervisor tool used by the vendor.

Extraction: After step 1, a malicious VM has placed in target machine with the victim VM. Since the malicious VM and the victim are sharing certain physical resources, such as data cache, network access, CPU branch predicators, there are many ways an adversary can employ attacks:

- Measuring a cache usage that can estimate the current load of the server

- Estimating a traffic rate that can obtain the visitor count or even the frequently requested pages

- Keystroke timing attack that can steal a victim's password by measuring time between keystrokes.

These kinds of attacks are known as internal breaches. In the same way, a privileged system administrator of the cloud provider can perform this attack by accessing the memory of a customer's VMs[21,26,27].

5.1.4 Availability

In cloud environment, the data and service availability may be violated by hardware/software failure and lack of load balancing. Any hardware failure such as network problem, disk/component failure and software failure such as malicious attack in SaaS application will leads to unavailability of data or service. In other hand the vendor also take care of server load balancing. For example Denial of Service (DDoS) attack.. This can be done by sending countless false requests to the server from a malicious VM which co-resides in the same physical location. In this case, the server will try to respond to the received requests and make all other services will be blocked by the server until it finishes the responses. This is how a malicious user can make cloud service unavailable to other cloud users. The DoS attack can be performed in two ways:

Direct DOS: In this method, the attacking target VM is determined, and the availability of the targeting cloud service will be fully lost.

Indirect DOS: In this method all services hosted in the same physical machine with the target victim will be affected; sometimes the attack is initiated without a specific target [21,24,28].

5.2. Security Threats in PaaS

PaaS is the middle layer and hosted on top of IaaS. In cloud, the PaaS models, offers a computing platform which includes operating system, programming language execution environment (run-time engine) and database. Application developers can develop and run their software solutions on a cloud platform without buying and managing the underlying hardware and software layers. In simple words, SaaS applications are depeded on PaaS. As, SaaS has high level of abstraction with PaaS, any vulnerability in PaaS, will affect the SaaS application also. In PaaS, the vulnerabilities will be addressed in two software layers [21,27,26,28].

- Security of the PaaS platform itself

- Security of customer applications deployed on a PaaS platform

5.3 Security Threats in IaaS

IaaS layers in cloud are designed to offer infrastructures such as servers, storage, networks, and other computing resources in the form of virtualized systems. The user can access these resources through the Internet [21]. Virtualization is the concept used in cloud, used to offer the services to the users in virtual form. Similar to SaaS and PaaS vulnerability, IaaS also deals with similar kinds of vulnerabilities like hardware failure, muti-tenancy, data confidentiality [21,29].

6. CURRENT SECURITY MECHANISMS

6.1 Encryption Techniques:

This can be done in three ways:

- Use server-side encryption
- Use client-side encryption
- User server side encryption with customer provided encryption key

In Server-side the vendor encrypts users' data as it writes it to disks in its data centers and decrypts it when user accesses it. Each vendor has their own encryption standard for offering security. For example Amazon Web Service provide data storage services in the name of Simple Storage Service (S3) in which server-side encryption employs strong multi-factor encryption. Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt user data.

In client-side encryption, users manage encryption/decryption of their data, the encryption keys, and related tools. In this method, the users could encrypt their data and upload the encrypted data to the cloud.

User server side encryption with customer provided encryption key is a third method, in which user has to provide the encryption key as part of the request to vendor. Using the encryption key the vendor will perform encryption/decryption process on users' data. When user wants to retrieve the data, he must provide the same encryption key as part of his request. Then vendor will verifies that the encryption key provided matches, and then decrypts the data before returning it to the user[21,30,31].

6.2 Retaining Data Control:

Encrypted VM images guarantee careful access control since only the authorized users known as key-holders are permitted access. Due to the encryption, the data cannot be mounted and modified within the cloud without an access key, assuring confidentiality and integrity. Here, VM is encrypted upon launch and stored on server where as in data security, data is encrypted and stored on instances. In this case, for malicious user, who wants to access a target VM, it is difficult to identify the VM on the server[27,31].

6.3 Trusted Third Party Auditing (TTPA):

In most enterprises there is distrust on cloud service provider and their security policies. This can be eliminated by introducing the concept of trusted third party in cloud server. This ensures that, there is no data integrity done on users' data. It will act as a additional security layer on cloud server.

TPA checks the integrity of data on the cloud on the behalf of the users, and it provides the reasonable way for the users to check the validity of data in the cloud. In TPA, there are three main participants: Third Party Auditor (TPA), User, Cloud Provider.

As the initial requirement the user and the TPA generates their own private key and public key with respect to the Asymmetric key algorithm. The public keys have been shared between them as the part of SLA or in a secured data transmission. Then the message is encrypted as well as signed in a unique way. With the generated public key sets the data gets exchanged between the user and the TPA. At first the data is signed with the user's private key then the cipher is again encrypted with the TPA's public key. This package is now sent to the Cloud and also the TPA. The TPA now decrypts the encrypted message with his private key and then de-signs the cipher with the user's public key to recognize the data. Then the same process of decryption is carried out in the cloud by the TPA to verify the correctness by comparing the data which he has with the stored one. Then as per the result the TPA indicates the user [32,33,27].

6.4 Co-Residence Detection:

Co-Residence detection is the process of restricting placing concurrent instances on the same cloud server. Cloud providers may obfuscate co-residence in two ways:

- Design DomO(host operating system, which has special privileges, like being able to access the hardware directly) not to respond in traceroute
- By providing internal IP address to VM

Traceroute is one of the vulnerability in cloud; because, to perform a malicious attack, the adversary will perform this operation. The successful response shows the availability of the VM(Dom). To avoid this, the vendor has to design the VM which must not respond to traceroute.

The second solution for malicious attack by a co-tenant is to provide dynamic IP address to each instance. This method makes the identification of VM very difficult on the cloud server [27,34].

6.5 NoHype and VM Isolation:

In cloud, all the services are in virtual form called virtualization. In this, hypervisor is a tool used to create and manage the instances. In cloud, an adversary who resides in the same cloud can use such tools to create malicious instances on the same server. The NoHype technique will eliminate such malicious VM creation. This is simply create one VM in one core exactly(also known as VM isolation).

Placing multiple instances in one core of the microprocessor, leads to some vulnerabilities such as traffic monitoring. For example, due to each core sharing common hardware, one instance's traffic may be monitored by malicious VM which resides in the same place. NoHype will guarantee that there is no traffic monitoring of any VM. [21,27,34].

6.6 Service Migration:

A Denial of Service(DOS) avoidance strategy called service migration has been developed to deal with the new flooding attack. A monitoring agent located outside the cloud is set up to detect whether there may be bandwidth starvation by constantly probing the cloud applications. When bandwidth degradation is detected, the monitoring agent will perform application migration, which may stop the service temporarily, with it resuming later. The migration will move the current application to another subnet of which the attacker is unaware [35].

6.7 Cryptographic Separation:

In cryptographic separation, computations and data are concealed in such a way that they appear intangible to outsiders. Confidentiality and integrity, but also privacy of data can be protected through encryption. Similar to encrypted VM, the cryptographic separation also restrict the malicious user in identifying the target VM on the server [36,37].

7. CONCLUSION AND FUTURE WORK

This paper has discussed the problems in enforcing data security and the current approaches to handling them. The paper notes that data security is still a problem. This problem is highlighted by the ubiquitous usage of computers and the critical nature of the data stored in them.

Current approaches to securing data fail from the fact that they do not naturally adapt to newer attack methods. There seems to be a requirement to provide a security mechanism that can learn to defend itself from newer and different attacks.

8. REFERENCES

[1] Nitesh Kumar Dixit, Lokesh mishra, Mahendra Singh Charan and Bhabesh Kumar Dey, "The New Age Of Computer Virus And Their Detection", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.3, May 2012

[2] Widiasari, Indrastanti R, "Combining Advanced Encryption Standard (AES) and One Time Pad (OTP)

Encryption for Data Security", International Journal of Computer Applications;2012, Vol. 57

[3] Peter J. Denning, "Computers Under Attack: Intruders, Worms and Viruses", ACM Press (Addison-Wesley), 1990.

[4] Simar Preet Singh, Renuka Gujral, "Security Threats", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 3, March 2014

[5] J. Aycock, "Computer Viruses and malware," Springer Science+Business Media, 2006.

[6] Lance J.Hoffman, "Rogue Programs:Viruses,Worms, and Trojan Horses", VanNostrand Reinhold, New York, NY, 1990.

[7] Jan Hruska, "Computer Viruses and Anti-VirusWarfare", Ellis Horwood, Chichester, England, 1990.

[8] Ankur Singh Bist, "A Review: Computer Worms", International journal of engineering sciences and research technology, February 2013.

[9] Thomas F. Stafford , Andrew Urbaczewski , "Spyware: The Ghost In The Machine", Communications of the Association for Information Systems, Volume 14, 2004

[10] Preeti Tuli, Priyanka Sahu, "System Monitoring and Security UsingKeylogger", International Journal of Computer Science and Mobile Computing, Vol. 2, Issue. 3, March 2013, pg.106 – 111

[11] B.A.Forouzan, Debdeep Mukhopadhyay, "Cryptography and Network Security", The McGraw Hill Companies, 2nd Edition.

[12] Sarika Choudhary, Ritika Saroha, Mrs. Sonal Beniwal, "How Anti-virus Software Works??", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 20132.

[13] G Fragkos, O Angelopoulou, K Xynos, **"**Antivirus False-Positive Alerts, Evading Malware Detection, and Cyber-security Issues", The journal of Information Warfare, Volume 12, Issue 3.

[14] M.Alshamrani and S.M.Furnell, "Internet User's Awareness and Understanding of Spyware and Anti-Spyware", Advances in Communications, Computing, Networks and Security 7

[15] Kumar Utkarsh, "System Security And Ethical Hacking", International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013

[16] Mehdi Dadkhah, Mohammad Davarpanah Jazi, "Secure Payment in E-commerce: Deal with Keyloggers and Pishings", International Journal of Electronics Communication and Computer Engineering, Volume 5,Issue 3,May 2014

[17] Security Guideline for standalone and Network computers, National Computer Board, Mauritius, September 2007, Issue No 6.

[18] Course Material on "Computer Security and Reliability",Webmaster Chapter 20

[19] Bazrafshan Z, Hashemi H, Fard S.M.H, Hamzeh A, "A survey on heuristic malware detection techniques", IEEE, 5th Conference on Information and Knowledge Technology (IKT), Shiraz, 2013

[20] Mihai Christodorescu, Somesh Jha, Douglas Maughan, "Malware Detection", Springer-verlag, 2007 Edition.

[21] S. Subashini n, V.Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications 34 (2011) 1–11

[22] PriyankRajvanshi, Varun Singh Nagar, Priyanka Chawla, "Data Protection in Cloud Computing", International Journal of Innovative Technology and Exploring Engineering (IJITEE) Volume-3, Issue-3, August 2013

[23] Sara Qaisar, KausarFiaz Khawaja, "Cloud Computing: Network/Security Threats and counter measures", Interdisciplinary Journal of Contemporary Research in Business, ijcrb.webs.com, January 2012, Vol 3, N0 9, pp: 1323 – 1329.

[24] K.L.Neela, V.Kavitha, R.K.Ramesh, "Cloud Computing: Threats and Security Issues", International Journal Of Engineering Sciences & Research Technology, August, 2013 [2070-2072]

[25] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," Proc. 16th ACM conference on Computer and communications security, 2009, pp. 199-212.

[26] Mather T, Kumaraswamy S, Latif S, "Cloud Security and Privacy", O'Reilly Media, Inc., Sebastopol, CA

[27] Zhifeng Xiao and Yang Xiao, "Security and Privacy in Cloud Computing", IEEE Communications Surveys & Tutorials.

[28] 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 2013, 4:5(A SpringerOpen Journal)

[29] Attanasio CR. "Virtual machines and data security", Proceedings of the workshop on virtual computer systems. New York, NY, USA: ACM; 1973. p. 206–9.

[30] Amazon. AmazonElasticComputeCloud (EC2),2010 (http://www.amazon.com/ ec2/S.

[31] M. Descher, P. Masser, T. Feilhauer, A. Tjoa, and D. Huemer, "Retaining Data Control to the Client in Infrastructure Clouds," Availability, Reliability and Security, 2009. ARES '09. International Conference on, 2009, pp. 9

[32] http://www.dmst.aueb.gr/dds/pubs/conf/1999-WISE-TTP/html/ttp.html

[33] Commission of the European Community. Green paper on the security of information systems, ver. 4.2.1, 1994. Alshamsi, T. Saito, A technical comparison of IPSec and SSL, Cryptology (2004).

[34] E. Keller, J. Szefer, J. Rexford, and R. B. Lee, "NoHype: virtualized cloud infrastructure without the virtualization," in Proc. 37th annual international symposium on Computer architecture, New York, NY,USA, 2010, pp. 350-361.

[35] Haeberlen. "A Case for the Accountable Cloud," 3rd ACM SIGOPS International Workshop on Large-Scale Distributed Systems and Middleware (LADIS '09), Big Sky, MT, October 2009

[36] KuiRen, Cong Wang, and Qian Wang, "Security Challenges for the Public Cloud", IEEE Press, 2012, pp. 69 – 73

[37] Yinqian Zhang, Ari Juels, Alina Oprea, Michael K. Reiter, "HomeAlone: Co-Residency Detection in the Cloud via Side-Channel Analysis", IEEE Symposium on Security and Privacy, 2011.