SECURITY THREATS ON CLOUD COMPUTING VULNERABILITIES

Te-Shun Chou

Department of Technology Systems, East Carolina University, Greenville, NC, U.S.A.

ABSTRACT

Clouds provide a powerful computing platform that enables individuals and organizations to perform variety levels of tasks such as: use of online storage space, adoption of business applications, development of customized computer software, and creation of a "realistic" network environment. In previous years, the number of people using cloud services has dramatically increased and lots of data has been stored in cloud computing environments. In the meantime, data breaches to cloud services are also increasing every year due to hackers who are always trying to exploit the security vulnerabilities of the architecture of cloud. In this paper, three cloud service models were compared; cloud security risks and threats were investigated based on the nature of the cloud service models. Real world cloud attacks were included to demonstrate the techniques that hackers used against cloud computing systems. In addition, countermeasures to cloud security breaches are presented.

KEYWORDS

Cloud computing, cloud security threats and countermeasures, cloud service models

1. INTRODUCTION

Cloud computing has been involved in everyone's life. It delivers applications and storage spaces as services over the Internet for little to no cost. Most of us utilize cloud computing services on a daily basis. For example, we use web-based email systems (e.g. Yahoo and Google) to exchange messages with others; social networking sites (e.g. Facebook, LinkedIn, MySpace, and Twitter) to share information and stay in contact with friends; on-demand subscription services (e.g. Netflix and Hulu) to watch TV shows and movies; cloud storages (e.g. Humyo, ZumoDrive, and Dropbox) to store music, videos, photos and documents online; collaboration tools (e.g. Google docs) to work with people on the same document in real time; and online backup tools (e.g. JungleDisk, Carbonite, and Mozy) to automatically back up our data to cloud servers. Cloud computing has also been involved in businesses; companies rent services from cloud computing service providers to reduce operational costs and improve cash flow. For example, the social news website, reddit, rents Amazon Elastic Compute Cloud (EC2) for their digital bulletin board service. The digital photo sharing website, SmugMug, rents Amazon S3 (Simple Storage Service) for their photo hosting service. The automaker, Mazda USA, rents Rackspace for their marketing advertisements. The software company, HRLocker, rents Windows Azure for their human resources software service.

There is no doubt that the convenience and low cost of cloud computing services have changed our daily lives; however, the security issues associated with cloud computing make us vulnerable to cybercrimes that happen every day. Hackers employ a variety of techniques to gain access to clouds without legal authorization or disrupt services on clouds in order to achieve specific objectives. Hackers could trick a cloud into treating their illegal activity as a valid instance, therefore, gaining unauthorized access to the information stored in the cloud.

DOI : 10.5121/ijcsit.2013.5306

Once the exact location of data is located, hackers steal private and sensitive information for criminal activities. According to DataLossDB, there were 1,047 data breach incidents during the first nine months of 2012, compared to 1,041 incidents during the entire year of 2011[1]. Epsilon and Stratfor were two data breach victims. In the data leakage accident, Epsilon leaked millions of names and email addresses from the customer databases. Stratfor's 75,000 credit card numbers and 860,000 user names and passwords were stolen [2]. Hackers could also take advantage of the massive computing power of clouds to fire attacks to users who are in the same or different networks. For instance, hackers rented a server through Amazon's EC2 service and carried out an attack to Sony's PlayStation Network [3]. Therefore, a good understanding of cloud security threats is necessary in order to provide more secure services to cloud users.

In this paper, section 2 presented an overview of cloud service models. Section 3 investigated the cloud security risks and threats from three various perspectives. Related real world cloud exploits were included. Section 4 introduced countermeasures to cloud security breaches. Finally, the conclusions and future work were presented in the last section.

2. CLOUD SERVICE MODELS

Cloud computing involves delivering computing resources (e.g. servers, storages, and applications) as services to end users by cloud computing service providers. End users access on-demand cloud services through web browsers. Cloud computing service providers offer specific cloud services and ensure the quality of the services. Basically, cloud computing includes three layers: the system layer, the platform layer, and the application layer.

The bottom layer is the system layer, which includes computational resources such as infrastructure of servers, network devices, memory, and storage. It is known as Infrastructure-as-a-service (IaaS). The computational resources are made available for users as on-demand services. With the use of virtualization technology, IaaS provides virtual machines that allow clients to build complex network infrastructures. This approach not only reduces the cost in buying physical equipment for businesses, it also eases the load of network administration because IT professionals are not required to continuously monitor the health of physical networks. An example of a cloud computing service provider of IaaS is Amazon's EC2. It provides a virtual computing environment with web service interfaces; by using the interfaces, users can deploy Linux, Solaris or Windows based virtual machines and run their own custom applications.

The middle layer is the platform layer and is known as Platform-as-a-Service (PaaS). It is designed to provide a development platform for users to design their specific applications. Services provided by this cloud model include tools and libraries for application development, allowing users to have control over the application deployment and configuration settings. With PaaS, developers are not required to buy software development tools, therefore reducing the cost. GoogleApps is an example of PaaS; it is a suite of Google tools that includes Gmail, Google Groups, Google Calendar, Google Docs, Google Talk, and Google Sites. It allows users to customize these tools on their own domain names. Windows Azure is another PaaS provider. It enables users to build applications using various languages, tools or frameworks. Users can then integrate the applications into their existing IT environments.

Finally, the top layer is the application layer, also known as Software-as-a-Service (SaaS). This layer allows users to rent applications running on clouds instead of paying to purchase these applications. Because of its ability to reduce costs, SaaS is popular among companies that deploy their businesses. Groupon is an example that uses SaaS. With the use of the online support solutions provided by Groupon, Zendesk processes its thousands of daily customer tickets more efficiently, thus providing a better customer service. Marathon Data Systems is

another example that offers SaaS. It provides solutions for field services such as pest control, lawn and landscaping, heating, air conditioning, plumbing, janitorial, maid, and carpet cleaning services. Table 1 shows examples of cloud computing service providers specialized on three cloud service models.

Table 1. Cloud Computing Service Providers on Cloud Service Models

Cloud Service Models	Cloud Service Providers
SaaS	Antenna Software, Cloud9 Analytics, CVM Solutions, Exoprise Systems, Gageln, Host Analytics, Knowledge Tree, LiveOps, Reval, Taleo, NetSuite, Google Apps, Microsoft 365, Salesforce.com, Rackspace, IBM, and Joyent
PaaS	Amazon AWS, Google Apps, Microsoft Azure, SAP, SalesForce, Intuit, Netsuite, IBM, WorkXpress, and Joyent
IaaS	Amazon Elastic Compute Cloud, Rackspace, Bluelock, CSC, GoGrid, IBM, OpenStack, Rackspace, Savvis, VMware, Terremark, Citrix, Joyent, and BluePoint

3. TAXONOMY OF CLOUD SECURITY THREATS

Three cloud service models (SaaS, PaaS and IaaS) not only provide different types of services to end users but also disclose information security issues and risks of cloud computing systems. First, the hackers might abuse the forceful computing capability provided by clouds by conducting illegal activities. IaaS is located in the bottom layer, which directly provides the most powerful functionality of an entire cloud. It maximizes extensibility for users to customize a "realistic" environment that includes virtual machines running with different operating systems. Hackers could rent the virtual machines, analyze their configurations, find their vulnerabilities, and attack other customers' virtual machines within the same cloud. IaaS also enables hackers to perform attacks, e.g. brute-forcing cracking, that need high computing power. Since IaaS supports multiple virtual machines, it provides an ideal platform for hackers to launch attacks (e.g. distributed denial of service (DDoS) attacks) that require a large number of attacking instances.

Second, data loss is an important security risk of cloud models. In SaaS cloud models, companies use applications to process business data and store customers' data in the data centers. In PaaS cloud models, developers use data to test software integrity during the system development life cycle (SDLC). In IaaS cloud models, users create new drives on virtual machines and store data on those drives. However, data in all three cloud models can be accessed by unauthorized internal employees, as well as external hackers. The internal employees are able to access data intentionally or accidently. The external hackers gain access to databases in cloud environments using a range of hacking techniques such as session hijacking and network channel eavesdropping.

Third, traditional network attack strategies can be applied to harass three layers of cloud systems. For example, web browser attacks are used to exploit the authentication, authorization, and accounting vulnerabilities of cloud systems. Malicious programs (e.g. virus and Trojan) can be uploaded to cloud systems and can cause damage [4]. Malicious operations (e.g. metadata spoofing attacks) can be embedded in a normal command, passed to clouds, and executed as valid instances [5]. In IaaS, the hypervisor (e.g. VMware vSphere and Xen) conducting administrative operations of virtual instances can be compromised by zero day attack [6].

It is necessary to identify the possible cloud threats in order to implement better security mechanisms to protect cloud computing environments. In the following subsections, we explored security threats presented in clouds from three perspectives: abuse use of cloud computational resources, data breaches, and cloud security attacks. Recent real world cloud attacks were also included to demonstrate the techniques that hackers used in exploiting the vulnerabilities of cloud systems.

3.1. Abuse Use of Cloud Computational Resources

In the past, hackers used multiple computers or a botnet to produce a great amount of computing power in order to conduct cyber-attacks on computer systems. This process is complicated and can take months to complete. Nowadays, a powerful computing infrastructure, including both software and hardware components, could be easily created using a simple registration process in a cloud computing service provider. By taking advantage of the prevailing computing power of cloud networks, hackers can fire attacks in a very short time. For example, brute force attacks and DoS attacks can be launched by abusing the power of cloud computing.

A brute force attack is a technique used to break passwords. The success of this attack is greatly reliant on powerful computing capability because thousands of possible passwords are needed to be sent to a target user's account until it finds the correct one to access. Cloud computing system provides a perfect platform for hackers to launch this type of attack. Thomas Roth, a German researcher, demonstrated a brute force attack in the Black Hat Technical Security Conference [7]. He managed to crack a WPA-PSK protected network by renting a server from Amazon's EC2. In approximately 20 minutes, Roth fired 400,000 passwords per second into the system and the cost of using EC2 service was only 28 cents per minute.

DoS attacks attempt to disrupt a host or network resource in order to make legitimate users unable to access the computer service. They come in a variety of forms and aim at a variety of services. Generally, they are categorized into three basic types: consumption of scarce, limited, or non-renewable resources, destruction or alteration of configuration information, and physical destruction or alteration of network components [8]. Among them, flooding is the most common way in which hackers crumble the victim's system with the use of an overwhelming number of bogus requests; therefore, the services to legitimate users are blocked. When the flooding attack is applied to cloud services, two types of DoS could happen in cloud computing systems: direct DoS and indirect DoS [9]. When a cloud server receives a large volume of flooded requests, it will provide more computational resources to cope with the malicious requests. Finally, the server exhausts its full capability and a direct DoS is occurred to all requests from legitimate users. Moreover, the flood attack could possibly cause indirect DoS to other servers in the same cloud when the servers share the workload of the victim server, which results a full lack of availability on all of the services.

Cloud computing services can be used to send a large amount of packets to companies' networks. For example, two security consultants, Bryan and Anderson, launched cloud-based DoS attacks to one of their clients in order to test its connectivity with the help of Amazon's EC2 cloud infrastructure [10]. By spending only $6 to rent virtual servers on EC2, they used a homemade "Thunder Clap" program to successfully flood their client's server and made the company unavailable on the Internet. Another DoS attack example was discussed on a Danish developer's, Jesper Nøhr [11] blog. According to his report, Bitbucket, a web-based hosting service company hosted by Amazon, was attacked by massive-scale DDoS attacks used by two flooding techniques: a flood of UDP packets and a flood of TCP SYN connection requests. The attacks caused the company to become unavailable and hence, many developers lost access to projects hosted on Bitbucket.

3.2. Data Breaches

3.2.1. Malicious Insider

Security threats can occur from both outside of and within organizations. According to the 2011 CyberSecurity Watch Survey conducted on 607 businesses, government executives, professionals and consultants, 21% of cyber-attacks were caused by insiders. 33% of the respondents thought the insider attacks were more costly and damaging to organizations [12]. The most common inside attacks were unauthorized access to and use of corporate information (63%), unintentional exposure of private or sensitive data (57%), virus, worms, or other malicious codes (37%), and theft of intellectual property (32%). The vulnerabilities of cloud computing to malicious insider are: unclear roles and responsibilities, poor enforcement of role definitions, need-to-know principle not applied, AAA vulnerabilities, system or OS vulnerabilities, inadequate physical security procedures, impossibility of processing data in encrypted form, application vulnerabilities or poor patch management [13].

While moving data and applications to cloud computing environments can expand businesses, malicious sabotage of an organization's sensitive information resources could jeopardize the entire victim organization's operation. There are three types of cloud-related insider threats: the rogue administrator, insiders who exploit cloud vulnerabilities, and the insiders who use the cloud to conduct nefarious activity [14]. Rogue administrator has privilege to steal unprotected files, brute-force attack over passwords, and download customers' data from the victim organization. Insiders who exploit cloud vulnerabilities try to gain unauthorized access to confidential data in an organization; they could make a fortune by selling the sensitive information, or use the information for their future businesses. Insiders who use the cloud to conduct nefarious activity carry out attacks against its own employer's IT infrastructure. Since the insiders are familiar with the IT operations of their own companies, the attacks are generally difficult to be traced using forensic analysis.

3.2.2. Online Cyber Theft

Cloud computing services provide users with powerful processing capability and massive amounts of storage space. With their inexpensive cost, companies could move their business into clouds so that they do not need to buy their own servers to store customers' information and handle traffic from customers and visitors. For example, Netflix leases computing space from Amazon Web Services (AWS) to provide subscription service for watching TV episodes and movies. Dropbox offers cloud storage service to customers for storing terabytes of data. Cloud-based services are now becoming a part of our daily lives. In the meantime, the sensitive data stored on clouds becomes an attractive target to online cyber theft. According to the analysis of data breaches of 209 global companies in 2011, 37 percent of data breach cases involved malicious attacks. The average cost per compromised record is $222 [15]. Online retailer Zappos (owned by cloud provider Amazon) was the victim of online cyber theft [16]. Almost 24 million client accounts might have been compromised in the breach. The compromised information includes names, email addresses, billing and shipping addresses, phone numbers, the last four digits of credit card numbers, as well as encrypted versions of account passwords.

Stealing data stored on clouds could be happening on social networking sites. Social networking sites, such as Twitter, MySpace, and Facebook, have attracted people who use them to interact with friends in their daily lives. USA Today found that 35 percent of adults Internet users have a profile on at least one social networking site [17]. These networks provide a platform for users to share information with others, e.g. personal profile (sex, birthdate, email, telephone, and education) and digital media (music, photos and videos). However, that private data can possibly be hacked by online cyber thieves, if they find a way to access the clouds. For example,

LinkedIn, the world's largest professional networking website that owns 175 million users, reported that their password database was compromised in a security breach [18]. Approximately 6.5 million hashed passwords were stolen and posted onto a Russian web forum. More than 200,000 of these passwords have been cracked.

The online cyber thieves could use stolen passwords to access users' accounts as well as to launch malicious attacks to users. Dropbox has confirmed that its users suffered from a spam attack [19]. Usernames and passwords stolen from other websites were used to sign in to Dropbox users' accounts. Furthermore, a stolen password was used to access a Dropbox employee's account containing a project document with user email addresses. Then, the hacker sent spam emails about online casinos and gambling sites to other users.

Online cyber thieves could also take the advantage of the computing power offered by cloud computing service providers to launch attacks. Amazon's EC2 cloud service was used by hackers to compromise private information. By signing up Amazon's EC2 service with phony information, hackers rented a virtual server and launched an attack to steal clients' data from Sony's PlayStation Network [3]. The hackers didn't break into the Amazon servers during the incident; however the personal accounts of more than 100 million Sony PlayStation Network subscribers were compromised.

3.3. Cloud Security Attacks

3.3.1. Malware Injection Attack

Web-based applications provide dynamic web pages for Internet users to access application servers via a web browser. The applications can be as simple as an email system or as complicated as an online banking system. Study has shown that the servers are vulnerable to web-based attacks [20]. According to a report by Symantec, the number of web attacks in 2011 increased by 36% with over 4,500 new attacks each day [21]. The attacks included cross site scripting, injection flaws, information leakage and improper error handling, broken authentication and session management, failure to restrict URL access, improper data validation, insecure communications, and malicious file execution [22].

Malware injection attack is one category of web-based attacks, in which hackers exploit vulnerabilities of a web application and embed malicious codes into it that changes the course of its normal execution. Like web-based applications, cloud systems are also susceptible to malware injection attacks. Hackers craft a malicious application, program, and virtual machine and inject them into target cloud service models SaaS, PaaS and IaaS, respectively. Once the injection is completed, the malicious module is executed as one of the valid instances running in the cloud; then, the hacker can do whatever s/he desires such as eavesdropping, data manipulation, and data theft.

Among all of the malware injection attacks, SQL injection attack and cross-site scripting attack are the two most common forms [23]. SQL injection attack increased 69% in Q2 2012 compared to Q1, according to a report by secure cloud host provider FireHost [24]. FireHost said that between April and June, it blocked nearly half-million SQLi attacks.

SQL injections target SQL servers that run vulnerable database applications. Hackers exploit the vulnerabilities of web servers and inject a malicious code in order to bypass login and gain unauthorized access to backend databases. If successful, hackers can manipulate the contents of the databases, retrieve confidential data, remotely execute system commands, or even take control of the web server for further criminal activities. Sony's PlayStation was a victim of an SQL injection attack. SophosLabs's blog reported that an SQL injection attack has been

successfully used to plant unauthorized code on 209 pages promoting the PlayStation games, "SingStar Pop" and "God of War" [25]. SQL injection attacks can be launched by a botnet. The Asprox botnet used a thousand bots that were equipped with an SQL injection kit to fire an SQL injection attack [26]. The bots first sent encoded SQL queries containing the exploit payload to Google for searching web servers that run ASP.net. Then, the bots started an SQL injection attack against the web sites returned from those queries. Overall, approximately 6 million URLs belonging to 153,000 different web sites were victims of SQL injection attack by the Asprox botnet. A scenario that demonstrates SQL injection attacking cloud systems was illustrated in [27]. An online retail SaaS application that allows multiple retailers to host their products and sell them through SaaS was used. The procedure of exploiting vulnerability and accessing to backend database was explained in details.

Cross-site scripting (XSS) attacks are considered one of the most malicious and dangerous attack types by FireHost. 27% of web attacks, cross-site scripting attack, were successfully blocked from causing harm to FireHost clients' web applications and databases during Q2 2012 [24]. Hackers inject malicious scripts, such as JavaScript, VBScript, ActiveX, HTML, and Flash, into a vulnerable dynamic web page to execute the scripts on victim's web browser. Afterwards the attack could conduct illegal activities (e.g. execute malicious code on the victim's machine and steal session cookie used for authorization) for accessing to the victim's account or tricking the victim into clicking a malicious link. Researchers in Germany have successfully demonstrated a XSS attack against Amazon AWS cloud computing platform [28]. The vulnerability in Amazon's store allowed the team to hijack an AWS session and access to all customer data. The data includes authentication data, tokens, and even plain text passwords.

3.3.2. Wrapping Attack

When a client requests services to a web server through a web browser, the service is interacted using Simple Object Access Protocol (SOAP) messages that are transmitted through HTTP protocol with an Extensible Markup Language (XML) format. In order to ensure confidentiality and data integrity of SOAP messages in transit between clients and servers, a security mechanism, WS-Security (Web Services Security), for web service is applied. It uses digital signature to get the message signed and encryption technique to encrypt the content of the message. This makes the client authenticated and the server can validate that the message is not tampered with during transmission.

Wrapping attacks use XML signature wrapping (or XML rewriting) to exploit a weakness when web servers validate signed requests [29]. The attack is done during the translation of SOAP messages between a legitimate user and the web server. By duplicating the user's account and password in the login period, the hacker embeds a bogus element (the wrapper) into the message structure, moves the original message body under the wrapper, replaces the content of the message with malicious code, and then sends the message to the server. Since the original body is still valid, the server will be tricked into authorizing the message that has actually been altered. As a result, the hacker is able to gain unauthorized access to protected resources and process the intended operations.

Since cloud users normally request services from cloud computing service providers through a web browser, wrapping attacks can cause damage to cloud systems as well. Amazon's EC2 was discovered to be vulnerable to wrapping attacks in 2008 [30]. The research showed EC2 had a weakness in the SOAP message security validation mechanism. A signed SOAP request of a legitimate user can be intercepted and modified. As a result, hackers could take unprivileged actions on victim's accounts in clouds. Using XML signature wrapping technique, researchers also demonstrated an account hijacking attack that exploited vulnerability in the Amazon AWS [28]. By altering authorized digitally signed SOAP messages, the researchers were able to

obtain unauthorized access to a customer's account, delete and create new images on the customer's EC2 instance, and perform other administrative tasks.

4. COUNTERMEASURES

A cloud computing infrastructure includes a cloud service provider, which provides computing resources to cloud end users who consume those resources. In order to assure the best quality of service, the providers are responsible for ensuring the cloud environment is secure. This can be done by defining stringent security policies and by applying advanced security technologies.

4.1. Security Policy Enhancement

With a valid credit card, anyone can register to utilize resources offered by cloud service providers. This causes hackers to take advantage of the powerful computing power of clouds to conduct malicious activities, such as spamming and attacking other computing systems. By mitigating such abuse behavior caused by weak registration systems, credit card fraud monitoring and block of public black lists could be applied [31]. Also, implementation of security policies can reduce the risk of abuse use of cloud computational power [32]. Well-established rules and regulations can help network administrators manage the clouds more effectively. For example, Amazon has defined a clear user's policy and isolates (or even terminates) any offending instances whenever they receive a complaint of spam or malware coming through Amazon EC2 [33].

4.2. Access Management

The end users' data stored in the cloud is sensitive and private; and access control mechanisms could be applied to ensure only authorized users can have access to their data. Not only do the physical computing systems (where data is stored) have to be continuously monitored, the traffic access to the data should be restricted by security techniques. Firewalls and intrusion detection systems are common tools that are used to restrict access from untrusted resources and to monitor malicious activities. In addition, authentication standards, Security Assertion Markup Language (SAML) and eXtensible Access Control Markup Language (XACML), can be used to control access to cloud applications and data. SAML focuses on the means for transferring authentication and authorization decisions between cooperating entities, while XACML focuses on the mechanism for arriving at authorization decisions [34].

4.3. Data Protection

Data breaches caused by insiders could be either accidental or intentional. Since it is difficult to identify the insiders' behavior, it is better to apply proper security tools to deal with insider threats. The tools include: data loss prevention systems, anomalous behavior pattern detection tools, format preserving and encryption tools, user behavior profiling, decoy technology, and authentication and authorization technologies [35 – 37]. These tools provide functions such as real-time detection on monitoring traffic, audit trails recording for future forensics, and trapping malicious activity into decoy documents.

4.4. Security Techniques Implementation

The malware injection attack has become a major security concern in cloud computing systems. It can be prevented by using File Allocation Table (FAT) system architecture [5]. From the FAT table, the instance (code or application) that a customer is going to run can be recognized in advance. By comparing the instance with previous ones that had already been executed from the

customer's machine, the validity and integrity of the new instance can therefore be determined. Another way to prevent malware injection attacks is to store a hash value on the original service instance's image file [4]. By performing an integrity check between the original and new service instance's images, malicious instances can be identified.

For XML signature wrapping attacks on web services, a variety of techniques have been proposed to fix the vulnerability found in XML-based technologies. For example, XML Schema Hardening technique is used to strengthen XML Schema declarations [38]. A subset of XPath, called FastXPath, is proposed to resist the malicious elements that attackers inject into the SOAP message structure [39].

5. CONCLUSIONS AND FUTURE WORK

Cloud computing is in continual development in order to make different levels of on-demand services available to customers. While people enjoy benefits cloud computing brings, security in clouds is a key challenge. Much vulnerability in clouds still exists and hackers continue to exploit these security holes. In order to provide better quality of service to cloud users, security flaws must be identified. In this paper, we examined the security vulnerabilities in clouds from three perspectives (abuse use of cloud computational resources, data breaches, and cloud security attacks), included related real world exploits, and introduced countermeasures to those security breaches. In the future, we will continue to contribute to the efforts in studying cloud security risks and the countermeasures to cloud security breaches.

REFERENCES

1. DataLossDB Open Security Foundation. http://datalossdb.org/statistics
2. Sophos Security Threat Report 2012. http://www.sophos.com/
3. Amazon.com Server Said to Have Been Used in Sony Attack, May 2011. http://www.bloomberg.com/news/2011-05-13/sony-network-said-to-have-been-invaded-by-hackers-using-amazon-com-server.html
4. D. Jamil and H. Zaki, "Security Issues in Cloud Computing and Countermeasures," International Journal of Engineering Science and Technology, Vol. 3 No. 4, pp. 2672-2676, April 2011.
5. K. Zunnurhain and S. Vrbsky, "Security Attacks and Solutions in Clouds," 2nd IEEE International Conference on Cloud Computing Technology and Science, Indianapolis, December 2010.
6. W. A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing," 44th Hawaii International Conference on System Sciences, pp. 1–10, Koloa, Hawaii, January 2011.
7. T. Roth, "Breaking Encryptions Using GPU Accelerated Cloud Instances," Black Hat Technical Security Conference, 2011.
8. CERT Coordination Center, Denial of Service. http://www.packetstormsecurity.org/distributed/denial_of_service.htm
9. M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "On Technical Security Issues in Cloud Computing," IEEE International Conference in Cloud Computing, pp. 109-116, Bangalore, 2009.
10. Thunder in the Cloud: $6 Cloud-Based Denial-of-Service Attack, August 2010. http://blogs.computerworld.com/16708/thunder_in_the_cloud_6_cloud_based_denial_of_service_attack
11. DDoS Attack Rains Down on Amazon Cloud, October 2009. http://www.theregister.co.uk/2009/10/05/amazon_bitbucket_outage/
12. 2011 CyberSecurity Watch Survey, CERT Coordination Center at Carnegie Mellon University.
13. D. Catteddu and G. Hogben, "Cloud Computing Benefits, Risks and Recommendations for Information Security," The European Network and Information Security Agency (ENISA), November 2009.
14. Insider Threats Related to Cloud Computing, CERT, July 2012. http://www.cert.org/
15. Data Breach Trends & Stats, Symantec, 2012. http://www.indefenseofdata.com/data-breach-trends-stats/

16. 2012 Has Delivered Her First Giant Data Breach, January 2012. http://www.infosecisland.com/blogview/19432-2012-Has-Delivered-Her-First-Giant-Data-Breach.html
17. A Few Wrinkles Are Etching Facebook, Other Social Sites, USA Today, 2011. http://www.usatoday.com/printedition/life/20090115/socialnetworking15_st.art.htm
18. An Update on LinkedIn Member Passwords Compromised, LinkedIn Blog, June, 2012. http://blog.linkedin.com/2012/06/06/linkedin-member-passwords-compromised/
19. Dropbox: Yes, We Were Hacked, August 2012. http://gigaom.com/cloud/dropbox-yes-we-were-hacked/
20. Web Based Attacks, Symantec White Paper, February 2009.
21. Symantec Internet Security Threat Report, 2011 Trends, Vol. 17, April 2012.
22. P. P. Ramgonda and R. R. Mudholkar, "Cloud Market Cogitation and Techniques to Averting SQL Injection for University Cloud," International Journal of Computer Technology and Applications, Vol. 3, No. 3, pp. 1217-1224, January, 2012.
23. A. S. Choudhary and M. L. Dhore, "CIDT: Detection of Malicious Code Injection Attacks on Web Application," International Journal of Computer Applications, Vol. 52, No. 2, pp. 19-26, August 2012.
24. Web Application Attack Report For The Second Quarter of 2012 http://www.firehost.com/company/newsroom/web-application-attack-report-second-quarter-2012
25. Visitors to Sony PlayStation Website at Risk of Malware Infection, July 2008. http://www.sophos.com/en-us/press-office/press-releases/2008/07/playstation.aspx
26. N. Provos, M. A. Rajab, and P. Mavrommatis, "Cybercrime 2.0: When the Cloud Turns Dark," ACM Communications, Vol. 52, No. 4, pp. 42–47, 2009.
27. S. S. Rajan, Cloud Security Series | SQL Injection and SaaS, Cloud Computing Journal, November 2010.
28. Researchers Demo Cloud Security Issue With Amazon AWS Attack, October 2011. http://www.pcworld.idg.com.au/article/405419/researchers_demo_cloud_security_issue_amazon_aws_attack/
29. M. McIntosh and P. Austel, "XML Signature Element Wrapping Attacks and Countermeasures," 2005 workshop on Secure web services, ACM Press, New York, NY, pp. 20–27, 2005.
30. N. Gruschka and L. L. Iacono, "Vulnerable Cloud: SOAP Message Security Validation Revisited," IEEE International Conference on Web Services, Los Angeles, 2009.
31. A. Tripathi and A. Mishra, "Cloud Computing Security Considerations Interface," 2011 IEEE International Conference on Signal Processing, Communications and Computing, Xi'an, China, September 2011.
32. H. C. Li, P. H. Liang, J. M. Yang, and S. J. Chen, "Analysis on Cloud-Based Security Vulnerability Assessment," IEEE International Conference on E-Business Engineering, pp.490-494, November 2010.
33. Amazon: Hey Spammers, Get Off My Cloud! http://voices.washingtonpost.com/securityfix/2008/07/amazon_hey_spammers_get_off_my.html
34. W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing," Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Special Publication 800-144, December 2011.
35. Tackling the Insider Threat http://www.bankinfosecurity.com/blogs.php?postID=140
36. "Cloud Security Risks and Solutions," White Paper, BalaBit IT Security, July 2010.
37. S. J. Stolfo, M. B. Salem, and A. D. Keromytis, "Fog computing: Mitigating Insider Data Theft Attacks in the Cloud," IEEE Symposium on Security and Privacy Workshops, pp. 125-128, San Francisco, CA, 2012.
38. M. Jensen, C. Meyer, J. Somorovsky, and J. Schwenk, "On the Effectiveness of XML Schema Validation for Countering XML Signature Wrapping Attacks," First International Workshop on Securing Services on the Cloud, Milan, Italy, September 2011.
39. S. Gajek, M. Jensen, L. Liao, and J. Schwenk, "Analysis of Signature Wrapping Attacks and Countermeasures," IEEE International Conference on Web Services, pp. 575–582, Miami, Florida, July 2009.