Tenth LACCEI Latin American and Caribbean Conference (LACCEI'2012), Megaprojects: Building Infrastructure by fostering engineering collaboration, efficient and effective integration and innovative planning, July 23-27, 2012, Panama City, Panama.

Cloud Computing Security and Privacy

Jeffrey L. Duffany, Ph.D.
Universidad del Turabo, Gurabo, PR, USA, jeduffany@suagm.edu

ABSTRACT

Cloud computing security is comprised of elements drawn from computer security, network security and information security. It encompasses policies, technologies, and controls employed to protect data, applications, and the cloud computing infrastructure. The security aspects of cloud computing are examined from the point of view of its inherent vulnerabilities with regard to availability, user authentication and privacy and trust. Recent events such as the April 21, 2011 collapse of the Amazon Elastic Compute Cloud (EC2) are used to illustrate these vulnerabilities and to suggest measures that can be implemented to improve cloud security. This is followed by a discussion of key aspects of cloud security including data protection, physical and personnel security, application security and legal issues. This is followed by a discussion of strategies that can be employed to better manage and mitigate security risks associated with cloud computing.

Keywords: cloud computing, security, privacy

1. INTRODUCTION

In the last few years one of the most important trends in information technology has been the rapid rise of cloud computing. The idea behind cloud computing is that users have all of their data and software stored somewhere on the internet, so they can access it wherever they are, be it at work, at home or while traveling. According to news website Mashable[1], portability is only one of the many benefits of cloud computing. While 33 percent of companies surveyed worldwide listed access to information from any device as their top driver to adopt cloud computing, 82 percent of all companies reported to have saved money on their last cloud adoption project. Performance improvement has also been a cloud adoption driver according to the website.

The National Institute of Standards and Technology (NIST) defines clouds as a model for enabling convenient, on-demand network access to a shared pool of configurable resources, such as networks, servers, storage, applications, and other services, that can be rapidly provisioned with minimal management effort or service provider interaction [2]. Amazon's EC2 service and Google's Google App Engine are examples of cloud computing, which Gartner[3] defines as "massively scalable IT-enabled capabilities are delivered as a service to external customers using Internet technologies." The Cloud Security Alliance[5] is a consortium of companies that gives certifications in cloud security knowledge and establishes guidelines on cloud security.

There are inherent risks in cloud computing which can easily be underestimated. Once you move your information outside of your own control it is subject to the possibility of being compromised. Someone could take a copy of your information and you might never know it. The goal of this paper is to shed some insight on cloud security and privacy by drawing analogies to similar situations in other industries such as the public power utilities. Cloud computing is still in its infancy and the risks are not well understood. The situation bears more than a slight resemblance to the move by many manufacturing operations to move overseas. The labor cost saving is evident but there are additional costs and risks involved.

Decade	Technological Trends
60’s	Mainframe computers
70’s	Mini computers, Modems
80’s	Personal Computers
90’s	Internet, Supercomputers, Laptops
00’s	Data Centers, Clusters, Wireless, Notebooks, Virtual Machines
10’s	Cloud Computing, Tablets, Ultrabooks

Figure 1: Technological Computing Trends over the last 5 Decades

2. BACKGROUND

2.1 CLOUD COMPUTING CHARACTERISTICS

We are currently in the midst of a paradigm shift in the thinking about computing that was predicted over 50 years ago by John McCarthy of MIT (1961) who said: "Computing may someday be organized as a public utility”. Hardware and software vendors wish to create new markets. There is currently a lot of hype and what could be characterized as almost a “cloud fever” in some organizations who don’t want to be left behind. Businesses are looking for savings from cloud migration, thin clients and reducing IT staff. There are many advantages of moving into the cloud environment: reduce or eliminate server farms, save space and electricity (this is especially true in areas where electricity costs are high, for example, in Puerto Rico where electricity may cost upwards of $.29 per kWH). Most individuals who use the internet are already in the “cloud” (and have been for some time).

Cloud computing is typically virtual machine based: outsourced and off-site. It is hardware agnostic and views software as a service (SaaS). The compelling motivation for migration to the cloud is the economic benefit of cost reduction due to the reduction of IT infrastructure due to the economies of scale of the cloud service providers (CSPs). It is highly scalable which means that enterprises do not have to design for peak loads which tends to lead to idle capacity. Enterprises will benefit from always having the latest software versions, operating system patches and upgrades. CSP’s will be chosen primarily on cost comparisons for computation and storage and perhaps secondarily on availability and security. This will involve a degree of trust in the cloud service providers which must be earned over time and can be lost if the they do not deliver what the customer is expecting. Existing trust models[12] are unreliable to say the least. However it is possible to look to the past to understand what future cloud performance is likely to be. Adopters will likely choose larger more well established service providers and switch if not satisfied. This will lead to a competitive marketplace where the strong survive and the weak perish.

Other driving forces behind the cloud computing movement include hardware and software vendors looking to maintain and increase sales. This is normally through a continuous stream of technology advances which include new operating systems and faster processor chips. It might seem on the surface that these vendors are shooting themselves in the proverbial foot by actively promoting the cloud. However, from mainframe computers in the 60s to personal computers in the 80s there have always been dynamic forces that continuously influence the evolving computing landscape. As seen in Figure 1 it has taken several decades for the pendulum to swing from highly centralized computing environments of the mainframe computers to the PC and now moving back to highly centralized computing environments of the cloud service providers.

The reality of the matter is that a lot of legacy equipment exists out there already. And even if it were replaced by thin clients you would still need an IT staff and you still need a network. In fact, networking costs will likely increase because of all the traffic going into the cloud and back again (but this is rarely factored into cloud computing economics). Increased networking delays could also impact performance and productivity. Thin clients might need more powerful processors to handle the encryption. In addition, you still need to keep all of your data locally and at least some software so operations can continue even through catastrophic failures in the cloud and failures in the internet access.

3. CLOUD COMPUTING RISKS

There are three main components of network and computing security: confidentiality, integrity and availability[4]. All three of these must be evaluated to understand the risks associated with cloud computing[3][5]. The ability of cloud computing services to collect and centrally store data, combined with the ease with which such data may be shared with others, create a risk that data may be used in ways not originally intended or understood by the client. Any data that is stored in a cloud environment must be considered at risk of exposure or data mining for example as is evident with Facebook, Google, Amazon, etc[16]. Sensitive data can be copied or mined without the owner's knowledge or permission. Hackers have targeted websites of large corporations in the past and it would seem that clouds would make a very likely candidate for hacking or denial of service attacks especially since there are many attack vectors[15]. Authentication schemes can be broken and of course there is a higher potential for access by government or law enforcement agencies, possibly even without the owner's consent or knowledge.

Cloud computing decouples data from infrastructure and obscures low-level operational details, such as where your data is physically located. These differences give rise to a unique set of security and privacy issues that not only impact risk management practices, but have also stimulated an evaluation of legal issues in areas such as compliance and auditing. There is a lack of standards across different cloud providers. Users of cloud services need to spend considerable time and effort understanding and addressing security risks associated with outsourcing to the cloud.

Concerns such as data protection, operational integrity, vulnerability management, business continuity, disaster recovery are some of the main security issues for cloud computing. Privacy is another key concern as data that the service collects about the user gives the provider valuable marketing information, but can also lead to misuse and violation of privacy. However, despite the risks, it is likely that much of the computing activity occurring today entirely on computers owned and controlled locally by users will shift to "the cloud" in the future.

Not all types of cloud computing raise the same privacy and confidentiality risks. For example, one scenario where cloud computing would be almost ideal would be the case of a university giving online courses involving streaming video content. In this case the university does not have to correctly estimate in advance how many students might sign up for the classes and therefore would not need to invest heavily in adding new servers to meet the anticipated demand. In addition security is probably not a major issue. In the fall of 2011 Stanford University offered free online classes in the areas of artificial intelligence, databases and machine learning. According to the New York Times[13] 160,000 students signed up for the artificial intelligence class alone. Stanford used Amazon Web services and was able to meet the demand, with only a few glitches along the way. In addition when the semester ended the university was not stuck with a large number of underutilized servers.

For public clouds, the financial health of the provider must be considered along with the political and economic stability of the geographic region they are located in. In addition, what happens when a cloud service provider goes out of business or if the server farm is closed? Another consideration would be a plan for migrating from one cloud to another cloud, such as from one public cloud to another.

4. PRIVACY AND THE CONCEPT OF TRUST

Privacy can be defined in terms of a controlled disclosure of information[4]. The control over what information is disclosed to whom and when is the decision of the owner of the information. A major privacy concern with cloud-computing arises because the Cloud System Administrators (CSAs) are custodians of huge quantities of aggregated data about many different corporations and individuals. This data could be accidentally disclosed, with unforeseen consequences. Despite all the hype about cloud computing and all of the copy-cat behaviours it is at least partially a lack of trust[12] that is preventing enterprises from more fully adopting cloud computing. Enterprises are reluctant to move sensitive applications and data into the public cloud and for good reason. In these cases (for example in the case of banks) it may be feasible to consider yet another option, that of using a private cloud.

5. PRIVACY CONCERNS - AMAZON CLOUD DRIVE AND DROPBOX

5.1 AMAZON CLOUD DRIVE

It is possible to get 5GB of free cloud-based storage from Amazon. However, like all of these schemes (e.g., free email) there must be a catch and it is almost always some kind of advertising. Also it appears likely that Amazon may be using the offer to gain consumer confidence on speculation that they might be willing to pay for more enhanced services later on as their needs grow if you give them something free up front. One drawback is that the subscriber has to give up their privacy to use the free storage. The Amazon Cloud Drive Terms of Use states:

"You give us the right to access, retain, use and disclose your account information and Your Files: to provide you with technical support and address technical issues; to investigate compliance with the terms of this Agreement, enforce the terms of this Agreement and protect the Service and its users from fraud or security threats; or as we determine is necessary to provide the Service or comply with applicable law". This could lead to a conjecture that Amazon is using this agreement to derive revenues for example by data mining or by detecting digital rights management (DRM) violations and selling that information to third parties.

5.2 DROPBOX

Dropbox was one of the first internet companies to offer free online storage or at least it is one of the first that was successful and well known. What is not so well known is that you can pay for a premium service. However around 98% of the people who use Dropbox use the free service so Dropbox must base their business model on the non-paying subscribers. This implies that Dropbox uses advertising or other means to get revenues from third parties for information about their non-paying subscribers.

Dropbox has been criticized by independent security researchers who claim that Dropbox's authentication protocol is insecure. Software experts have said that Dropbox's claim that "Dropbox employees aren't able to access user files" is not accurate. Dropbox has been criticized for not supporting the ability for users to use their own encryption keys and for automatically signing in users. In May 2011, a complaint was filed with the US FTC alleging Dropbox misled users about the privacy and security of their files. On 20 June 2011, all Dropbox accounts could be accessed without password for 4 hours[7]. The error was caused by a code update error and was detected a few hours later and immediately corrected. In early July 2011 Dropbox revised their Terms of Service several times in a manner that appeared to give them irrevocable license to any data uploaded. They subsequently retracted those terms in response to the consumer criticism. It is in general difficult to know with any certainty whether the privacy or security of cloud service providers is what the client believes it to be or that it did not suddenly change without warning. There are many examples of e-commerce websites that have had customer data such (as credit card numbers) compromised through hacking and various security lapses[15].

6. AVAILABILITY

Recent events such as the collapse of the Amazon Elastic Compute Cloud (EC2) can be used to illustrate cloud vulnerabilities and to suggest measures that can be implemented to improve cloud performance. On Thursday morning, April 21, 2011, around 2AM Amazon suffered a major outage in one of its datacenters that services their EC2, or Elastic Cloud Computing services. A number of Amazon cloud-based services such as Reddit and FourSquare were out of service. As of 6pm, many of these services were still either down completely or operating in a degraded state. It is not clear whether any data was lost as a result of the outage but it quite possibly may have been the case. In any event, it is very probable that some cloud users will experience some loss of data during some future cloud failure event due to one cause or another.

Amazon Web Services (AWS) guarantees a level of service availabiity of 99.95% (which is around 4 hours of downtime per year) and needs to build their infrastructure to support those guarantees. This would include some level of internal redundancy to keep the service up and protect data during failures. However the outages at Amazon and Microsoft Azure, as well as security issues at DropBox reinforce the concern that cloud computing can represent risks for their clients that are difficult to quantify.

7. Cloud Security Strategic Areas

The following is a breakdown of cloud security into ten strategic areas which need to be addressed from the both cloud service provider's point of view and their client user base[9][10].

7.1 Data Security

Cloud service providers are responsible for implementing security and operational procedures to ensure customer data confidentiality, integrity and availability. This includes documenting cloud security controls and operations along with security options like encryption and extensible or multi-factor/biometric authentication. Other layers of security are required including auditing, monitoring and event logging. Issues such as location of data centers and incident response procedures need to be resolved. In addition to producing logs and audit trails, cloud service providers need to ensure that these logs and audit trails are properly secured, maintained and are accessible for forensic investigation.

7.2 Data Protection

Data must be stored securely and it must be able to move securely from one location to another. Data from one customer must be properly segregated from that of another. Cloud providers should have systems in place to prevent data leaks or access by third parties. Software should ensure that auditing and/or monitoring cannot be defeated, even by privileged users at the CSP. One problem inherent with virtualization has to do with the nature of allocating and deallocating resources such as local storage associated with virtual machines[6][7]. During the deployment and operation of a virtual machine, data is written to physical memory. If the data is not cleared before those resources are reallocated to the next virtual machine there is a potential for exposure.

7.3 Authentication

Clients may support a wide variety of identity management systems to control access to information and computing resources. Cloud providers can integrate the client identity management system into their own infrastructure or provide an identity management solution of their own. Authentication schemes can be broken if not properly designed or used. The cloud service may not be able to tell the difference between an authorized person typing in their user name and password and someone else typing in their user name and password.

7.4 Physical and Personnel Security

Cloud providers must ensure that computing facilities are secure and that physical access to these machines as well as customer data is restricted and access documented. Personnel should be trained and/or certified in security.

7.5 Data and Service Availability

Cloud providers must guarantee clients that they will have 24/7/365 access to their data and applications. Service level agreements will need to specify availability in some probabilistic terms that can be verified by observed performance. Cloud Service Providers can be evaluated on the basis of Mean Time between Failures (MTBF) and Mean Time to Repair (MTBR). It could prove difficult for the cloud providers to live up to their agreements in case of catastrophic failure or in the event of unpredictable surges in demands. One need only look at the history of major power outages in the United States and the rest of the world to get some insight into the availability concerns associated with large scale networks[14]. Significant outages typically occur several times a year while large scale outages occur once every several years. For example on August 14, 2003 some 55 million people were affected by a wide area power failure in the northeastern USA and Canada[14]. Large scale natural disasters such as hurricanes could also play a role in service outages. Unexpected peaks in demand could occur if several large clients simultaneously need to increase their computing resources and there is no limit placed on the scalability of individual clients (or if one CSP fails leading to a domino effect on the remaining CSPs).

7.6 Application Security

Cloud providers should take precautions to ensure that applications available as a service via the cloud (SaaS) are secure by implementing testing and acceptance procedures for application code. It also requires application security measures in place in the production environment.

7.7 Data Privacy

Cloud providers should require that all sensitive data such as credit card numbers are secured and that only authorized users have access to data. User information and must be protected as should any data that the provider collects or produces about customer activity in the cloud.

7.8 Business Continuity

Cloud providers have business continuity and disaster recovery plans in place to ensure that service can be maintained in case of a disaster or an emergency and that any lost data will be recovered.

7.9 Compliance

Industry and Federal regulations pertain to the storage and use of data, including the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act, the Payment Card Industry Data Security Standard and any other applicable regulations. Many of these regulations require regular reporting and audit trails. Cloud providers must enable their customers to comply appropriately with these regulations. No amount of third-party certification or on-site auditing can replace the loss of direct control

7.10 Legal and Contractual Issues

Contractual issues include end-of-service support so that when the provider-customer relationship ends, customer data and applications should be archived and delivered in their entirety to the customer. All copies of customer data should be erased from the cloud infrastructure. Contracts should cover service-level agreements, liabilities, penalties, maintenance, training, and adherence to standards. The terms of liability need to be fully understood and agreed to by the client. Other legal issues may include records-keeping requirements where enterprises may be required to retain and make available electronic records of data and transactions.

8. Risk Mitigation Strategies

Cloud Redundancy and Data Backup

Even though the client may trust the cloud there is still a possibility of catastrophic failure. For an example look at the US power grid. A few years ago a blackout in the northeast[14] resulted in 4 billion dollars of damage. The lesson to be learned here is to back up everything stored in the cloud on your local machine and have at least the basic software required to process it in case of catastrophic cloud failure or internet connectivity failure

When Amazon Web Services (AWS) experienced an outage on April 21, 2011, a number of businesses that used AWS went completely off line. However Netflix, a company providing online movie access, had spread its cloud infrastructure across multiple vendors and has designed redundancy into its platform. Technologies like Cloud Services Broker and CloudSwitch can be used to establish, maintain and manage cloud redundancy. For example, CloudSwitch can provide monitoring of cloud service availability and quality. When service quality falls below a certain threshold, CloudSwitch can send out alerts and automatically divert traffic to back-up cloud service providers. There is a price to be paid for this type of redundancy which could impact profit margins of the cloud service providers.

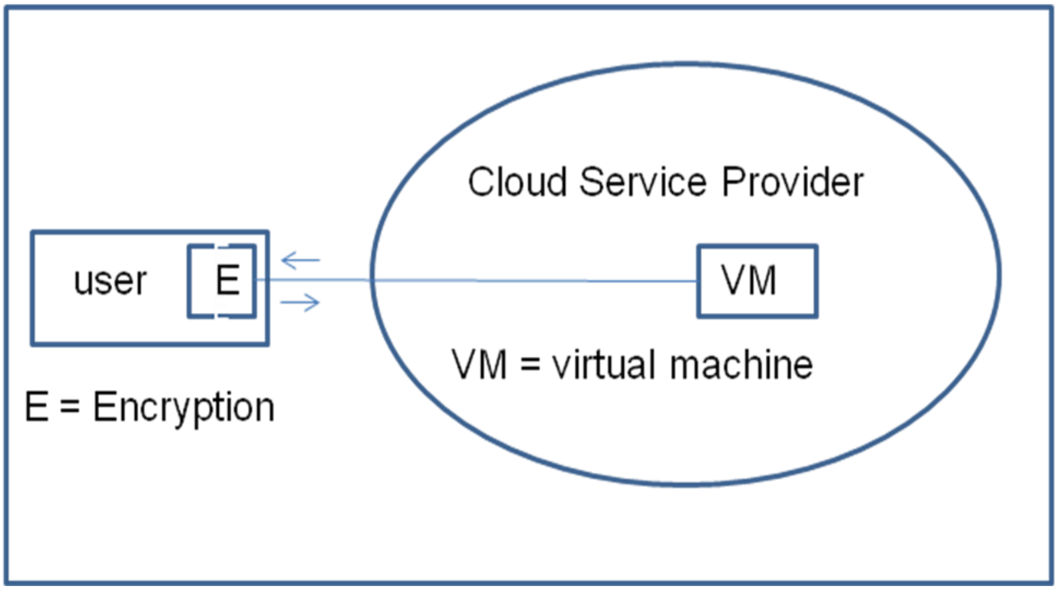

Figure 2. Complete User Control of Encryption Function (E)

Encryption and User-Based Security Controls

Amazon Web Services Simple Storage Service (SSS) encrypts user data before storing it in the cloud however this does not guarantee the confidentiality of the information. A more secure approach would be to move the encryption functionality (E) completely under user control as indicated in Figure 2. This would require keys to be managed and shared among users in a practical and efficient way. However the added security entails additional risk: loss of key could result in permanent data loss while compromise of a key could render encryption useless.

An example of this kind of technology is the cloud data gateway that encrypts and secures data before it leaves the enterprise premises. The cloud data gateway monitors data traffic to the cloud and enforces policies to block, remove, mask, or encrypt sensitive data. Using a combination of gateways at the cloud service provider and gateways on-premise, different levels of data security can be achieved. By giving customers control over data security before the data leaves the premises, customers do not have to trust the cloud service provider and need not rely on the cloud provider alone to ensure the safekeeping of its data.

Unfortunately the above approach does not work when data processing in the cloud is required. Progress has been made in encryption systems[8] that would allow users to upload encrypted data and allow the service providers to perform computations and searches on the encrypted data without giving them the possibility of decrypting it. Although such encryption has been shown possible in principle commercial implementations do not appear to be widely available at this time. A hybrid approach which uses indexing may work for certain types of searches where the index is restricted to contain only data that is not sensitive. The sensitive data is encrypted before sending it to the cloud and then decrypted only after being retrieved from the cloud via the search index.

Integration of Cloud Services with Existing Security Platforms

Enterprises have invested heavily in security infrastructure, including identity and access management, data security, and application security. These tools and processes will need to evolve and incorporate new technologies like cloud computing and mobile devices while at the same time allowing cloud services to be integrated into existing security platforms. Hardware-based security initiatives such as the Trusted Platform Module and Intel's Trusted Execution Technology are designed to allow a remote user to have confidence that data submitted to a platform is processed according to an established policy. These technologies are embedded in the server hardware and help to defend against attacks directed at the operating system. The benefit is to increase the overall level of security of the computing environment however these systems are still vulnerable to certain kinds of attack.

9. SUMMARY AND CONCLUSIONS

The economic advantages of cloud computing are undeniable. However, based on the history of other utilities such as the power grid, widespread and spectacular catastrophic failures are inevitable[14]. Trust models[12] based on past behaviour are questionable and cannot be relied upon. Any data stored in a cloud environment must be considered at risk of exposure or data mining. Sensitive data can be copied without the owner's knowledge or permission. Hackers have targeted websites of large corporations in the past and it would seem that clouds would be a likely target for hacking or denial of service attacks in the future. Once data has been copied into a cloud the owner has lost control of it, unless it is encrypted. There is also a potential for access by government or law enforcement agencies. A cloud may be good solution in cases where a low level of security is sufficient or if an enterprise is willing to accept the inherent cloud risks, given the large magnitude of potential cost savings.

One of the limiting factors in the adoption of cloud computing by enterprises is a lack of trust in cloud service providers. There are concerns over the security, integrity, and reliability of cloud-based services. Recent outages at Amazon as well as security issues at DropBox and many e-commerce websites underscore the fact that cloud computing poses significant and poorly understood risks. One partial solution is to encrypt all data that is stored in the cloud. Unfortunately, many cloud services do not work with encrypted data and the effect of bulk encryption of all data sent to the cloud would be to relegate the cloud to serving as nothing more than a large data storage device. Technologies to allow software to operate on encrypted data (e.g., search engines) are still in their infancy and viable commercial products do not appear to be on the horizon anytime soon. In the meantime, enterprises who wish to benefit from the cloud can try to separate their computing operations (data and software) into areas which either (a) can be outsourced to a cloud or (b) cannot be outsourced for security reasons. The result is that they will end up with one foot in the cloud and one foot in the traditional IT environment. This outcome is not necessarily all that bad, especially where there is a clean separation between these areas, as in the previously discussed example of Stanford University offering online courses via the public cloud.

Cloud computing holds promise for cost savings and revenue generation by introducing new and potentially disruptive technologies. However, to improve the acceptance of cloud computing many security issues remain to be resolved. In addition enterprises cannot completely eliminate their IT infrastructure. There is much that can be done to mitigate security-related failures in clouds. It is also clear that more needs to be done to place control back into the hands of the customer. In some cases where the question boils down to a matter of "whose security is better - the CSP or the enterprise?" In some cases, the CSP security may actually be better than the enterprise itself, in spite of the higher risks of the cloud data exposure.

Enterprises back up critical information and build redundancy into their mission-critical infrastructures. To date many enterprises have not put critical applications and sensitive data into the public cloud. As these enterprises look to cloud technologies for secure applications some organizations that are highly regulated (e.g., banks) or need high levels of security might have to consider the option of implementing their own private clouds. Cloud migration will be highly dependent on service level agreements and reliability strategies. There needs to be a balance that represents both consumer rights and provider obligations. The potential for failure exists, as it does in other contexts (for example the electrical grid). Failover capability is a major issue in the case of the loss of internet access as is the increased cost and delays when sending all of your computations to a cloud somewhere on the internet.

Securing sensitive data and protecting systems from intrusions are primary concerns for companies that are considering possible cloud migration. These concerns include unauthorized data access, account or session hijacking, uncertainty over data location, continuity planning, disaster recovery, and system resiliency. Both insider and outsider threats are significant concerns. Data centers of public clouds must be physically hardened and have capabilities for audits, intrusion detection, event logging, video surveillance, uninterruptible power supplies and backup generators. Software should consist of firewalls with intrusion prevention and virus, spam, and rootkit detection. Cloud service providers should conduct penetration tests and security audits. All backup data and client communications should be performed over secure encrypted channels.

REFERENCES

1. Silverman, M. “How has Cloud Computing Changed Business”, Infographic, December 11, 2011, http://mashable.com/2011/12/11/cloud-computing-business-infographic/.
2. Peter Mell and Tim Grance, "The NIST Definition of Cloud Computing", *National Institute of Standards and Technology*. October, 7, 2009, Version 15. http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf
3. "Gartner: Seven cloud-computing security risks". *InfoWorld*. 2008-07-02. http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853.
4. Pfleeger, Charles, "Security in Computing", ISBN 0-13-2390779, Prentice Hall, 4th edition, 2006.
5. “Security Guidance For Critical Areas of Focus in Cloud Computing V3.0, 2011, Cloud Security Alliance, https://cloudsecurityalliance.org.
6. Winkler, V. "Cloud Computing: Virtual Cloud Security Concerns". *Technet Magazine, Microsoft*. http://technet.microsoft.com/en-us/magazine/hh641415.aspx. December, 2011.
7. Hickey, K. "Dark Cloud: Study finds security risks in virtualization". *Government Security News*. http://gcn.com/articles/2010/03/18/dark-cloud-security.aspx. March 18, 2010.
8. Stallings, William, “Cryptography and Network Security, Fifth Edition, Prentice Hall, ISBN 0-13-609704-9, 2009.
9. "4 Cloud Computing Security Policies You Must Know". *CloudComputingSecurity*, 2011. http://cloudcomputingsec.com/268/4-cloud-computing-security-policies-you-must-know.html.
10. "Cloud Security Front and Center". Forrester Research. 2009-11-18. http://blogs.forrester.com/srm/2009/11/cloud-security-front-and-center.html.
11. Gellman, R. “World Privacy Forum Cloud Privacy Report”, http://www.worldprivacyforum.org, February 23, 2009
12. Wu, M. “Cloud Trust Model in E-Commerce”, *Proceedings of the Second International Symposium on Networking and Network Security (ISNNS ’10)*, Jinggangshan, P. R. China, 2-4, April. 2010, pp. 271-274.
13. http://www.nytimes.com/2012/03/05/education/moocs-large-courses-open-to-all-topple-campus-walls.html?pagewanted=all
14. http://en.wikipedia.org/wiki/List_of_power_outages
15. Dhanjani, N., Rios, W. and Hardin, B. “Hacking, the Next Generation”, ISBN 978-0-596-15457-8, O’Reilly Media, September 2009.
16. Russell, M. A., “Mining the Social Web: Analyzing Data from Facebook, Twitter, LinkedIn and Other Social Networking Sites”, ISBN 978-1449388345, O’Reilly Media, February 8, 2011.

Authorization and Disclaimer

Authors authorize LACCEI to publish the paper in the conference proceedings. Neither LACCEI nor the editors are responsible either for the content or for the implications of what is expressed in the paper.