Security Challenges in Cloud Computing

L. Ertaul[1], S. Singhal[2], and G. Saldamli[3]
[1]Mathematics and Computer Science, CSU East Bay, Hayward, CA, USA
[2]Mathematics and Computer Science, CSU East Bay, Hayward, CA, USA
[3]MIS, Bogazici University, Istanbul, TURKEY

Abstract - *Cloud Computing is one of the biggest buzzwords in the computer world these days. It allows resource sharing that includes software, platform and infrastructure by means of virtualization. Virtualization is the core technology behind cloud resource sharing. This environment strives to be dynamic, reliable, and customizable with a guaranteed quality of service. Security is as much of an issue in the cloud as it is anywhere else. Different people share different point of view on cloud computing. Some believe it is unsafe to use cloud. Cloud vendors go out of their way to ensure security. This paper investigates few major security issues with cloud computing and the existing counter measures to those security challenges in the world of cloud computing..*

Keywords: Cloud Computing Security, Distributed Networks Security, Network Security

1 Introduction

Cloud computing is a pay-per-use model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction [1][4][5]. Typically there are three types of resources that can be provisioned and consumed using cloud: software-as-a-service, platform-as-a-service, and infrastructure-as-a-service [1][2][3][5].

Cloud computing services themselves fall into three major categories. The first type of cloud computing service is known as Software-as-a-service (SAAS). This service provides capability to the service subscribers to access provider's software applications running on a cloud infrastructure. The service providers manage and control the application. Customer does not have to own the software but instead only pay to use it through a web API [1] [2]. For example, Google Docs relies on JAVA Script, which runs in the Web browser [3].

The second type of cloud service is called Platform-as-a-service (**PaaS**). It is another application delivery model. PaaS lets the consumer to deploy their applications on the providers cloud infrastructure using programming languages and tools supported by the provider. The consumer does not have to manage the underlying cloud infrastructure but has control over the deployed application [1] [2]. A recent example is the Google App Engine, a service that lets developer to write programs to run them on Google's infrastructure [3].

The third and final type of cloud computing is known as Infrastructure-as-a-service (**IaaS**). This service basically delivers virtual machine images as a service and the machine can contain whatever the developers want [3]. Instead of purchasing servers, software, data center resources, network equipment, and the expertise to operate them, customers can buy these resources as an outsourced service delivered through the network cloud [2]. The consumer can automatically grow or shrink the number of virtual machines running at any given time to accommodate the changes in their requirement. For example, host firewalls [1] [2] [3].

There are different kinds of cloud deployment models available. We will discuss three major types of cloud. The first one is Private cloud. This is also known as internal cloud.

This paper is organized as follows. In section 2, we briefly describe the cloud computing architecture. In section 3, we briefly describe the applications of cloud computing. In section 4, we discuss the major security challenges in cloud computing environment and their existing counter measures. In section 5, we briefly discuss the cloud related working groups. In section 6, we discuss the security standards in cloud computing. Finally, in section 7, we conclude.

2 Cloud Computing Architecture

Cloud computing system is divided into two sections: the front end and the back end. Theses two ends connect to each other usually through Internet. The front end is the user side and back end is the "cloud" section of the system. The front end includes the client's computer and the application required to access the cloud computing system. As shown in figure 1, on the back end of the system are the various computers, servers and data storage systems that create the "cloud" of computing services [2][5][6]. A central server administers the system, monitoring traffic and client demands to ensure everything runs smoothly. It follows a set of rules called protocols and uses a special kind of software called middleware [2][5].

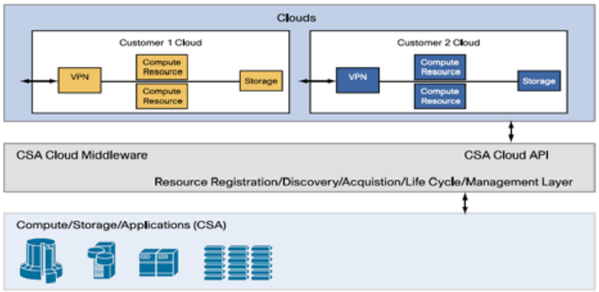

Figure 1. High-Level Cloud Middleware Architecture Example

Cloud middleware also referred to as cloud OS, is the major system that manages and controls services. Middleware allows networked computers to communicate with each other [6]. Google App Engine and Amazon EC2/S3 are examples of cloud middleware [20]. An Application Programming Interface (APIs) for applications, acquisition of resources such as computing power and storage, and machine image management must be available to make applications suitable for network clouds [2][5][13].

In a simplified vision of the cloud computing architecture, as shown in figure 2, first of all, Client sends service requests. Then system management finds correct resources. After that, system provisioning finds correct resources. After the computing resources are found then the client request is executed. Finally, results of the service requests are sent to the clients [2][6][13].

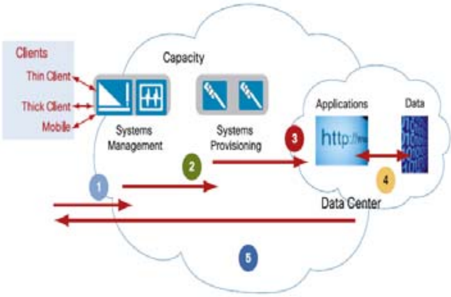

Figure 2. Cloud computing Workflow

In the next section we discuss different applications of cloud computing environment and how using cloud can be so beneficial for organizations of all the sizes.

3 Cloud Computing Applications

The applications of cloud computing are practically limitless. With the right middleware, a cloud computing system can practically run all the applications a personal computer can run.

- Clients will be able to access their applications and data at any time from anywhere using any computer linked to Internet [6].

- Traditionally, Organizations that rely on computers for their operations have to buy all the required software or software licenses for every employee. Cloud computing system gives an option to these organizations to get access to all the required computer applications without even buying those applications. Instead, company can pay a pay-per-use fee to a cloud service provider [4] [6].

- Cloud computing system will reduce the hardware costs on client side. User will not have to buy the computer with most memory, nor has he to buy the large hard drive to store his data. Cloud system will take care of this client's need. Client just have to buy a computer terminal with a monitor, input devices with just enough processing power to run the middleware necessary to connect to the cloud system [4][6][[18].

- In most of the companies servers and digital storage devices take up a huge space. Some companies do not have a large physical apace available on-site so they rent space to store their servers and databases. Cloud computing system gives these companies an option to store their data on someone else's (cloud service providers) hardware thus freeing these companies of requirement to have their own physical space on the client side [6] [17].

- Client can make use of cloud system's huge processing power. Like in grid computing, client can send huge complex calculations on cloud for processing. Sometimes complex calculations can take years for individual computer to compute. The cloud system in this case will use the processing power of required number of available computers on the back end to speed up the calculation [1][6][8].

Cloud computing offers significant advantage over the traditional computing system but it has its own issues.

In the next section we discuss about the major security challenges in cloud computing environment and their existing counter measures.

4 Cloud Computing Challenges

Security and privacy are the two major concerns about cloud computing. In the cloud computing world, the virtual environment lets user access computing power that exceeds that contained within their physical world. To enter this virtual environment a user is required to transfer data throughout the cloud. Consequently several security concerns arises [4] [7] [8] [16].

4.1 Information Security

It is concerned with protecting the confidentiality, integrity and availability of data regardless of the form the data may take [9].

- Losing control over data: Outsourcing means losing significant control over data. Large banks don't want to run a program delivered in the cloud that risk compromising their data through interaction with some other program [3][10]. Amazon Simple Storage Service (S3) APIs provide both bucket- and object level access controls, with defaults that only permit authenticated access by the bucket and/or object creator. Unless a customer grants anonymous access to their data, the first step before a user can access data is to be authenticated using HMAC-SHA1 signature of the request using the user's private key [9][15][16]. Therefore, the customer maintains full control over who has access to their data. [13].

- Data Integrity: Data integrity is assurance that data changes only in response to authorized transactions. For example, if the client is responsible for constructing and validating database queries and the server executes them blindly, the intruder will always be able to modify the client-side code to do whatever he has permission to do with the backend database. Usually, that means the intruder can read, change, or delete data at will [3]. The common standard to ensure data integrity does not yet exists [8]. In this new world of computing users are universally required to accept the underlying premise of trust. In fact, some have conjectured that trust is the biggest concern facing cloud computing [7].

- Risk of Seizure: In a public cloud, you are sharing computing resources with other companies.. Exposing your data in an environment shared with other companies could give the government "reasonable cause" to seize your assets because another company has violated the law. Simply because you share the environment in the cloud, may put data at risk of seizure [4][8]. The only protection against the risk of seizure for user is to encrypt their data. The subpoena will compel the cloud provider to turn over user's data and any access it might have to that data, but cloud provider won't have user's access or decryption keys. To get at the data, the court will have to come to user and subpoena user. As a result, user will end up with the same level of control user have in his private data center [4][16].

- Incompatibility Issue: Storage services provided by one cloud vendor may be incompatible with another vendor's services should you decide to move from one to the other. Vendors are known for creating what the hosting world calls "sticky services" – services that an end user may have difficulty transporting from one cloud vendor to another. For example, Amazon's "Simple Storage Service" [S3] is incompatible with IBM's Blue Cloud, or Google, or Dell [4][8][13]. Amazon and Microsoft both declined to sign the newly published Open Cloud Manifesto. Amazon and Microsoft pursue interoperability on their own terms [11][12][14].

- Constant Feature Additions: Cloud applications undergo constant feature additions, and users must keep up to date with application improvements to be sure they are protected. The speed at which applications will change in the cloud will affect both the SDLC (Software development life cycle) and security [4][8]. Updates to AWS infrastructure are done in such a manner that in the vast majority of cases they do not impact the customer and their Service use [9][13]**.** AWS communicates with customers, either via email, or through the AWS Service Health Dashboard when there is a chance that their Service use may be affected [9].

- Failure in Provider's Security: Failure of cloud provider to properly secure portions of its infrastructure – especially in the maintenance of physical access control – results in the compromise of subscriber systems. Cloud can comprise multiple entities, and in such a configuration, no cloud can be more secure than its weakest link [3][7]. It is expected that customer must trust provider's security. For small and medium size businesses provider security may exceed customer security. It is generally difficult for the details that help ensure that the right things are being done [3][7].

- Cloud Provider Goes Down: This scenario has a number of variants: bankruptcy, deciding to take the business in another direction, or a widespread and extended outage. Whatever is going on, subscriber risk losing access to their production system due to the actions of another company. Subscriber also risk that the organization controlling subscriber data might not protect it in accordance with the service levels to which they may have been previously committed [4]. The only option user have is to chose a second provider and use automated, regular backups, for which many open source and commercial solutions exist, to make sure any current and historical data can be recovered even if user cloud provider were to disappear from the face of the earth [4].

4.2 Network Security

Network security measures are needed to protect data during their transmission, between terminal user and computer and between computer and computer [21][22].

- Distributed Denial of Service (DDOS) Attack: In DDOS attack servers and networks are brought down by a huge amount of network traffic and users are denied the access to a certain Internet based Service. In a commonly recognized worst-case scenario, attackers use botnets to perform DDOS. In order to stop hackers to stop attacking the network, subscriber or provider face blackmail [21][14]. Amazon Web Service (AWS) Application Programming Interface (API) endpoints are hosted on large, Internet-scale, world-class infrastructure that benefits from the same engineering expertise that has built Amazon into the world's largest online retailer. Proprietary DDOS mitigation techniques are used. Additionally, Amazon's networks are multi-homed across a number of providers to achieve Internet access diversity [9].

- Man in the Middle Attack: This attack is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the attacker [21]**.** All of the AWS APIs are available via SSL-protected endpoints which provide server authentication. Amazon EC2 AMIs automatically generate new SSH host certificates on first boot and log them to the instance's console. Customers can then use the secure APIs to call the console and access the host certificates before logging into the instance for the first time. Customers are encouraged to use SSL for all of their interactions with AWS [9].

- IP Spoofing: Spoofing is the creation of TCP/IP packets using somebody else's IP address. Intruder gain unauthorized access to computer, whereby he sends messages to a computer with an IP address indicating that the message is coming from a trusted host. [21][22]. Amazon EC2 instances cannot send spoofed network traffic. The Amazon-controlled, host-based firewall infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own [9].

- Port Scanning: If the Subscriber configures the security group to allow traffic from any source to a specific port, then that specific port will be vulnerable to a port scan. Since a port is a place where information goes into and out of the computer, port scanning identifies open doors to a computer [21]**.** There is no way to stop someone from port scanning your computer while you are on the Internet because accessing an Internet server opens a port which opens a door to your computer [8]. Port scans by Amazon Elastic Compute Cloud (EC2) customers are a violation of the Amazon EC2 Acceptable use Policy (AUP). Violations of the AUP are taken seriously, and every reported violation is investigated. Customers can report suspected abuse. When port scanning is detected it is topped and blocked. Post scans of Amazon EC2 instances are generally ineffective because, by default, all inbound ports on Amazon EC2 instances are closed and are only opened by the customer [9].

- Packet Sniffing: Packet sniffing by Other Tenants: Packet sniffing is listening (with software) to the raw network device for packets that interest you. When that software sees a packet that fits certain criteria, it logs it to a file. The most common criteria for an interesting packet is one that contains words like "login" or "password" [21][22]**.** It is not possible for a virtual instance running in promiscuous mode to receive or "sniff" traffic that is intended for a different virtual instance. While customers can place their interfaces into promiscuous mode, the hypervisor will not deliver any traffic to them that is not addressed to them [9]**.** Even two virtual instances that are owned by the same customer, located on the same physical host, cannot listen to each other's traffic. Attacks such as ARP cache poisoning do not work within Amazon EC2. While Amazon EC2 does provide ample protection against one customer inadvertently or maliciously attempting to view another's data, as a standard practice customers should encrypt sensitive traffic [9]

4.3 Security Issues

They are more complex in a virtualized environment because you now have to keep track of security on two tiers: the physical host security and the virtual machine security. If the physical host server's security becomes compromised, all of the virtual machines residing on that particular host server are impacted. And a compromised virtual machine might also wreak havoc on the physical host server, which may then have an ill effect on all of the other virtual machines running on that same host [23].

Instance Isolation: Isolation ensuring that different instances running on the same physical machine are isolated from each other. Virtualization efficiencies in the cloud require virtual machines from multiple organizations to be co-located on the same physical resources. Although traditional data center security still applies in the cloud environment, physical segregation and hardware-based security cannot protect against attacks between virtual machines on the same server [18]. Administrative access is through the Internet rather than the controlled and restricted direct or on-premises connection that is adhered to in the traditional data center model. This increase risk of exposure will require stringent monitoring for changes in system control and access control restriction [8]. Different instances running on the same physical machine are isolated from each other via Xen hypervisor. Amazon is active in the Xen community, which ensures awareness of the latest developments. In addition, the AWS firewalls reside within the hypervisor layer, between the physical network interface and the instance's virtual interface. All packets must pass through this layer, thus an instance's neighbors have no more access to that instance than any other host in the Internet and can be treated as if they are on separate physical hosts. The physical RAM is separated using similar mechanisms [9].

Host Operating System: Administrators with a business need to access the management plans are required to us multi-factor authentication to gain access to purpose-built administration hosts. These administrative hosts are systems that are specifically designed, built, configured, and hardened to protect the management plane of the cloud. All such access is logged and audited. When an employee no longer has a business need to access the management plane, the privileges and access to those hosts and relevant systems are revoked [18].

Guest Operating System: Virtual instances are completely controlled by the customer. Customers have full root access or administrative control over accounts, services, and applications. AWS does not have any access rights to customer instances and cannot log into the guest OS. AWS recommends a base set of security best practices including: customer should disable password-based access to their hosts, and utilize some form of multi-factor authentication to gain access to their instances, or at a minimum certificate-based

SSH Version 2 access [9][13][15]. Additionally, customers should employ a privilege escalation mechanism with logging on a per-user basis. For example, if the guest OS is Linux, After hardening their instance, they should utilize certificate-based SSHv2 to access the virtual instance, disable remote root login, use command-line logging, and use 'sodu' for privilege escalation. Customers should generate their own key pairs in order to guarantee that hey are unique, and not shared with other customers or with AWS [9]. AWS Multi-Factor Authentication (AWS MFA) is an additional layer of security that offers enhanced control over AWS account settings. It requires a valid six-digit, single-use code from an authentication device in your physical possession in addition to your standard AWS account credentials before access is granted to an AWS account settings. This is called Multi-Factor Authentication because two factors are checked before access is granted to your account: customer need to provide both their Amazon email-id and password (the first "factor": something you know) AND the precise code from customer authentication device (the second "factor": something you have).

4.4 General Security Issues

In addition to the above mentioned issues there are few other general security issues that are delaying cloud computing adoption and needs to be taken care of.

Data Location: When user uses the cloud, user probably won't know exactly where his data is hosted, what country it will be stored in [3][4][8]? Amazon does not even disclose where their data centers are located. They simply clam that ach data center is hosted in a nondescript building with a military-grade perimeter. Even if customer know that their database server is in the us-east-1a availability zone, customer do not know where that data center9s0 behind that availability zone is located, or even which of he three East Coast availability zones us-east-1a represents [4].

Data Sanitization: Sanitization is the process of removing sensitive information from a storage device. In cloud computing users are always concerned about, what happens to data stored in a cloud computing environment once it has passed its user's "use by date" [18]. When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that ensures customer data are not exposed to unauthorized individuals. AWS uses the technique DoD 5220.22-M as per National Industrial Security Program Operating manual to destroy data, as part of the decommissioning process [9][13]. When item and attribute data are deleted within a domain, removal of the mapping within the domain starts immediately, and is also generally complete within seconds. Once the mapping is removed, there is no remote access to the deleted data. The storage area is then made available only for write operations and the data are overwritten by newly stored data [9].

Job Starvation due to some virus or worm: It is where one job takes up a huge amount of resource resulting in a resource starvation for the other jobs. Customer can reserve the resources in advance. Customer can also reduce the priority of the affected tasks/job [16] [18].

In the next section of our paper we discuss about the various cloud related working groups and their contribution in the cloud computing environment.

5 Cloud Related Working Groups

A working group is an assembled, cooperative collaboration of researchers working on new research activities that would be difficult for any one member to develop alone. Working groups generally strive to create an informational document a standard, or find some resolution for problems related to a system or network. Most often, the working group attempts to assemble experts on a topic. Working groups are sometimes also referred to as task groups or technical advisory groups.

The Open Cloud Consortium (OCC) is organized into several different working groups [8]. For example, the working group on Standards and Interoperability for Clouds. The purpose of the OCC is to support the development of standards for cloud computing and to develop framework for interoperability among various clouds [19]. There is also a working group on wide area clouds and the impact of network protocols on clouds. The focus of this working group is on developing technology for wide area clouds, including creation of methodologies and benchmarks to be used for evaluating wide area clouds. This working group is tasked to study the applicability of variants of TCP and the use of other network protocols for clouds.

The working group on information sharing, security and clouds has a primary focus on standards and standard-based architectures for sharing information between clouds. This is especially true for clouds belonging to different organizations and subject to possibly different authorities and policies. This group is also concerned with security architectures for clouds. Finally, there is an Open Cloud Test-bed working group that manages and operates the open cloud test-bed [19].

Another very active group in the field of cloud computing is Distributed management Task Force (DMTF) [8]. According to their web site, the distributed management task force enables more effective management of millions of IT systems worldwide by bringing the IT industry together to collaborate on the development, validation and promotion of systems management standards [24][25].

This group spans the industry with 160 member companies and organizations, and more than 4,000 active participants crossing 43 countries. The DMTF board of directors id led by 16 innovative, industry- leading technology companies.

The DMTF started the Virtualization Management Initiative (VMAN). The VMAN unleashes the power of virtualization by delivering broadly supported interoperability and portability standards to virtual computing environments. VMAN enables IT managers to deploy preinstalled, pre configured solutions across heterogeneous computing networks and to manage those applications through their entire life cycle [20][25].

In the next section we discuss about the major security standards for cloud computing and their application in cloud computing environment.

6 Standards for Security in Cloud Computing

Security standards define the processes, procedures, and practices necessary for implementing a security program. These standards also apply to cloud related IT activities and include specific steps that should be taken to ensure a secure environment is maintained that provides privacy and security of confidential information in a cloud environment. Security standards are based on a set of key principles intended to protect this type of trusted environment. A basic philosophy of security is to have layers of defense, a concept known as defense in depth. This means having overlapping systems designed to provide security even if one system fails. An example is s firewall working in conjunction with intrusion-detection system (IDS). Defense in depth provides security because there is no single point of failure and no single entry vector at which an attack can occur. For this reason, a choice between implementing network security in the middle part of a network (i.e., in the cloud) or at the endpoints is a false dichotomy [8]. No single security system is a solution by itself, so it is far better to secure all systems. This type of layered security is precisely what we are seeing develop in cloud computing. Traditionally, security was implemented at the endpoints, where the user controlled access. An organization had no choice except to put firewalls, IDSs, and antivirus software inside its own network. Today, with the advent of managed security services offered by cloud providers, additional security can be provided inside the cloud [8][9].

Security Assertion Markup Language (SAML): SAML is an XML-based standard for communicating authentication, authorization, and attribute information among online partners. It allows businesses to securely send assertions between partner organizations regarding the identity and entitlements of a principal. SAML standardizes queries for, and responses that contain, user authentication, entitlements, and attribute information in an XML format. This format can then be used to request security information about a principal from a SAML authority. A SMAL authority, sometimes called the asserting party, is a platform or application that can relay security information. The relying party or assertion consumer or requesting party is a partner site that receives the security information. The exchanged information deals with a subject's authentication status, access authorization, and attribute information. A subject is an entity in a particular domain by an email address is a subject, as might be a printer [8]. SAML is built on a number of existing standards, namely, SOAP, HTTP and XML. SAML relies on HTTP as its communications protocol and specifies the use of SOAP.

Open Authentication (OAuth): OAuth is an open protocol, initiated by Blaine Cook and Chris Messina, to allow secure API authorization in a simple, standardized method for various types of web applications. OAuth is a method for publishing and interacting with protected data. For developers, OAuth provides users access to their data while protecting account credentials. It also allows users to grant access to their information, which is shared by the service provider and consumers without sharing all of their identity. OAuth is the baseline, and other extensions and protocols can be built on it. By design, OAuth Core 1.0 does not provide many desired features, like automated discovery of endpoints, language support, support for XML-RPC and SOAP, standard definition of resource access, OpenID integration, signing algorithms, etc [8]. The core deals with fundamental aspects of the protocol, namely, to establish a mechanism for exchanging a user name and password for a token with defined rights and to provide tools to protect the token. It is important to understand that security and privacy are not guaranteed by the protocol. In fact, OAuth by itself provides no privacy at all and depends on other protocols such as SSL to accomplish that.

OpenID: It is an open, decentralized standard for user authentication and access control. It allows users to log onto many services using the same digital identity. It is a single-sign-on (SSO) method of access control. OpenID replaces the common log-in process, i.e. a log-in name and a password, by allowing users to log in once and gain access to resources across participating systems. An OpenID is in the form of a unique URL and is authenticated by the entity hosting the OpenID URL [9]. The OpenID protocol does not rely on a central authority to authenticate a user's identity. Neither the OpenID protocol nor any websites requiring identification can mandate that a specific type of authentication be used; nonstandard forms of authentication such as smart cards, biometrics, or ordinary password are allowed [8].

SSL/TLS: Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographically secure protocols designed to provide security and data integrity for communications over TCP/IP. TLS and SSL encrypt the segments of network connections at the transport layer. The TLS protocol allows client/server applications to communicate across a network in a way specifically designed to prevent eavesdropping, tampering, and message forgery [21]. TLS provides endpoint authentication and data confidentiality by using cryptography. TLS authentication is one way- the server is authenticated, because the client already knows the server's identity. In this case, the client remains unauthenticated [12] . TLS also supports a more secure bilateral connection mode whereby both ends of the connection can be assured that they are communicating with whom they believe they are connected. This is known as mutual (assured) authentication. TLS involves three basic steps. The first step deals with peer negotiation for algorithm support. During this phase, the client and server negotiate cipher suites, which determines which ciphers are used. In the next step, key exchange and authentication is decided. During this phase, a decision is made about the key exchange and authentication algorithm to be used, and determine the message authentication codes. The key exchange and authentication algorithms are typically public key algorithms. The finals step is about the symmetric cipher encryption and message encryption. The message authentication codes are made up from cryptographic hash functions. Once these decisions are made, data transfer may begin [9][12].

7 Conclusions

The cloud computing phenomenon is generating a lot of interest worldwide because of its lower total cost of ownership, scalability, competitive differentiation, reduced complexity for customers, and faster and easier acquisition of services. While cloud offers several advantages, people come to the cloud computing topic from different points of view. Some believe that cloud to be an unsafe place. But few people find it safer then their own security provisioning, especially small businesses that do not have resources to ensure the necessary security themselves. Several large financial organizations and some government agencies are still holding back. They indicate that they will not consider moving to cloud anytime soon because they have no good way to quantify their risks. To gain total acceptance from all potential users, including individuals, small businesses to Fortune 500 firms and government, cloud computing require some standardization in the security environment and third-party certification to ensure that standards are met.

8 References

[1] http://csrc.nist.gov/groups/SNS/cloud-computing/index.html.

[2] Cisco White Paper, http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/white_paper_c11-532553.html, published 2009, pp. 1-6.

[3] John Viega, McAffee, Cloud Computing and the Common Man," published on the IEEE Journal ON Cloud Computing Security, pp. 106-108, August 2009.

[4] George Reese, "Cloud Application Architectures", First edition, O'Reilly Media, April 2009, ISBN 9780596156367, pp. 2-4, 99-118.

[5] http://en.wikipedia.org/wiki/Cloud_computing.

[6] http://communication.howstuffworks.com/cloud computing1.htm.

[7] John Harauz, Lori M. Kaufman, Bruce Potter, "Data Security in the World of Cloud Computing," published on the IEEE Journal on Cloud Computing Security, July/August 2009, Vol. 7, No.4, pp. 61-64.

[8] John W. Rittinghouse, James F. Ransome, "Cloud Computing Implementation, Management, and Security", CRC Press, August 17, 2009, ISBN 9781439806807, pp. 147-158, 183-212.

[9] Amazon White Paper, http://aws.amazon.com/about-aws/whats-new/2009/06/08/new-aws-security-center-and-security-whitepaper/ , published June 2009.

[10] Marco Descher, Philip Masser, Thomas Feilhauer, A Min Tjoa, David Huemer, " Retaining Data Control to the Client Infrastructure Clouds", published on the IEEE, 2009 International Conference on Availability, Reliability and Security, pp. 9-15.

[11] David Bernstein, Erik Ludvigson, Krishna Sankar, Steve Diamond, Monique Morrow, "Blueprint for the Intercloud – Protocols and Formats for Cloud Computing Interoperability, submitted to IEEE, 2009 Fourth International Conference on Internet and Web Applications and Services, pp. 328-335.

[12] Liang-Jie Zhang, Qun Zhou, "CCOA: Cloud Computing Open Architecture", published on IEEE, 2009 IEEE International Conference on Web Services, pp. 607-615.

[13] Amazon White Paper, "Introduction to Amazon Virtual Private Cloud", Available: http://aws.amazon.com/about-aws/whats-new/2009/08/26/introducing-amazon-virtual-private-cloud/ , published Aug 26, 2009, pp. 6-8.

[14] Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, "Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities", grid Computing and Distributed Systems and Software Engineering, The University of Melbourne, Australia.

[15] Jinesh Varia, Amazon Web Services, "Building GrepTheWeb in the Cloud, Part 1: Cloud Architectures", Available: http://developer.amazonwebservices.com/connect, July 2008, pp. 1-7.

[16] Jon Brodkin, " Gartner: Seven Cloud-Computing Security Risks", Available: http://www.infoworld.com, published July 2008, pp. 1-3.

[17] IBM CIO White Paper, " Staying aloft in tough times", April 2009, pp. 3-19.

[18] Steve Hanna, Juniper Networks, "Cloud Computing: Finding the Silver Lining", published 2009, pp. 2-30.

[19] Manifesto, "Open Cloud Manifesto, Dedicated to the belief that the cloud should be open", Available: www.opencloudmanifesto.org, published Spring 2009, pp-1-7.

[20] Peter Fingar, " Dot.Cloud: the 21st century business platform built on cloud computing", First edition, Meghan-Kiffer Press, February 18, 2009, ISBN 9780929652498, pp. 81-99.

[21] William Stallings, "Network Security essentials", Third edition, Prentice Hall, July 29,2006, ISBN 9780132380331, pp-2.

[22] http://en.wikipedia.org/wiki/Network_security

[23] http://searchservervirtualization.techtarget.com/news/column/0,294698,sid94_gci1217705,00.html

[24] http://www.service-architecture.com/xml/articles/distributed_management_task_force_dmtf.html.

[25] http://www.dmtf.org/about/cloud-incubator/CloudIncubatorCharter2009-04-16.pdf