# Cloud Computing Demands Security Advancements

Chen-Chi Shing, David Martin, and Lee Hur Shing

***Abstract*—This paper will serve to explain how Cloud Computing will increase the rate at which new security measures will be required. Cloud Computing is a new technology, and is advancing at a rapid pace. Its advancement is changing cyber security and exposing the weakest links within current security. Through careful observation, this study of Cloud Computing services and security issues will explain why the malicious applications provided by Cloud Computing services are of great importance. The conclusion is attained by showing how quickly Cloud Computing resources can eliminate many current security measures with purely brute force methods. The careful piecing together of many studies and their results, as well as the logical assessment of ideas, all led to the conclusion that cyber security will require new, innovative security technology and increased Government investment in the future.**

***Index Terms*—Cloud vulnerabilities, cyber security, FREAK.**

## I. Introduction

The term *Cloud Computing* was originally coined by Google CEO Eric Schmidt in a 2006 press conference [1]. Cloud Computing, due to its benefits, has become extremely popular, with up to 96% of all major companies using Cloud services and millions of normal users interacting with the services every day. To fully understand the security aspects of the Cloud, the Cloud's basic functions will need to be outlined. The Cloud will be defined, explaining how it is used, then its advantages and disadvantages will be discussed. After this, the Cloud will have some of its current and previous security problems addressed. Last but not least, the malicious applications of the Cloud will be brought to light, and finally, the conclusion will follow.

### A. Defining "Cloud"

Cloud Computing is one of the largest growing fields. The United States Health Care cloud market is projected to reach $3.5 billion by 2020 [2]. Just about anyone can create a Cloud Computing service. Cloud Computing is essentially advanced networking by connecting multiple computers together and sharing their resources. On a corporate level, Cloud Computing services can incorporate hundreds if not tens of thousands of computers all interconnected together for users to interact with using a variety of methods over the Internet from practically anywhere.

### B. Types of Cloud Services

Most companies offering Cloud services offer it in a variety of ways, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). IaaS and PaaS make connections with the Cloud over the Internet, usually connecting with Transport Layer Service (TLS), and most commonly using a software application developed by the company to interact with the Cloud. SaaS, which is the most common type of connection for the average user, is also connected to over the Internet, but unlike the previously mentioned services, connects using Hypertext Transfer Protocol (HTTP) instead of a TLS application protocol designed by the company [3].

#### 1) Infrastructure as a service (IaaS)

IaaS is mainly used for virtual machines, servers, storage space, or networks. This Cloud Computing method is essentially renting the computational resources of the Cloud. The user pays for processing power as it is used, or the amount of disk space currently being used as storage. IaaS also allows companies to have many users connect to their databases at the same time by increasing Cloud networking and processing loads as more users use the service, and decrease when it is not being used. IaaS also allows users to run programs and applications much faster than a single computer could. An example would be an extremely advanced physics engine which performs millions of calculations to predict movement and collisions of different types of objects.

#### 2) Platform as a service (PaaS)

PaaS is generally used for applications such as databases, web servers, or development tools. Instead of buying hundreds of software license keys, companies may instead choose to use the Cloud and let all their employees use the software through copies on the Cloud. The Cloud charges the company much less than cost of purchasing the individual applications. PaaS removes the company's need to buy new computers if the software is updated which may require greater computational power. It also helps unify documents used by businesses. Instead of having each employee with their own separate computer, with different operating systems and versions of software, all employees would be using the same operating systems and software, reducing sharing problems between them.

#### 3) Software as a service (SaaS)

SaaS is a model where users use applications and access user data in the cloud [4]. SaaS connects to the Cloud services with HTTP. It is the most common Cloud Computing resource used by the average user. HTTP is not secure, but through the use of Secure Socket Layer (SSL) encryption when validating and authenticating the user, the connection remains secure between the user computer and the Cloud even if there are potential eavesdroppers. SaaS is widely used for email, video game, and communication services.

### C. Advantages

Manuscript received May 18, 2015; revised November 26, 2015.

Chen-Chi Shing and David Martin are with Radford University, USA (e-mail: cshing@radford.edu, dmartin15@radford.edu).

Lee Hur Shing is with Virginia Tech., USA.

The Cloud offers many advantages which set it apart from basic computing. Scalable growth is probably the most important and widely observed advantage of the Cloud. An additional advantage provided by the Cloud is that of being a green technology. Finally the additional security benefits offered by the Cloud are of great importance.

*1) Scalable growth*

Scalable growth is the most frequently observed advantage of Cloud Computing. The potential of the user to only pay for resources as used and expand the amount of resources used at any time makes the Cloud extremely cost efficient, especially for large companies. The Cloud provides an effectively infinite amount of storage space and computing power without the need to purchase new computers and additional storage whenever software requires more powerful computers, or more disk space is needed. The Cloud offers global access through the Internet, allowing companies to let employees work from anywhere, access data from anywhere, and collaborate together.

Cloud Computing is especially attractive to new businesses. It permits the nascent company to pay for storage and processing power as needed, instead of making large up-front investments which may depreciate quickly. The Cloud technically allows for unlimited growth computationally. Most companies can save a great deal of money switching to the Cloud; utilizing the Cloud is cheaper than paying to maintain a computer after considering electricity, bandwidth, and upgrade costs.

*2) Green technology*

Cloud Computing is referred to as a "Green Technology", meaning it saves potential power. By sharing computers, the need to purchase new computers and dispose of old computers decreases. Computers purchased to use software on the Cloud also do not need to contain state-of-the-art components, which are wasted when idle. Instead, users can use an inexpensive terminal to connect to the Cloud. The Cloud is constantly sharing resources between many connected users instead of wasting power sitting idle.

*3) Increased security*

The use of Cloud Computing resources potentially increases the security of a company. It reduces their vulnerability to Denial of Service (DoS) attacks due to the Cloud providing more processing and networking power as needed. The Cloud provider can also provide additional security by providing data backups, managing employee privileges, and much more.

### *D. Disadvantages*

Due to being a relatively new field, Cloud Computing has developed many potential and unforeseen problems as well. These problems are similar to all problems faced with regular computers, but the Cloud expands them to a much greater scale. Some common problems include that Cloud services are attractive targets to "hackers", downtime, negligence, and government interference [5], [6].

*1) Prone to attack*

First and foremost Cloud servers are available to be seen by everyone, due to their public nature. This means they are a prime target for the attacks of malicious users because they are not only accessible from anywhere with an Internet connection, but also because the Cloud stores data from multiple clients, not just a single person or company.

*2) Downtime*

Potential downtime is another disadvantage associated with the Cloud. Although it is seldom, downtime does occur with Cloud Computing services. The power grid can go down at their location, or there could be an Internet outage. If the user is without Internet and relies on the Cloud to work, they cannot be productive. This risk can be mitigated by having the Cloud computers hosted in multiple locations.

*3) Negligence*

The dramatic increase in the use of Cloud Computing has created a strong incentive for many new companies to offer Cloud Computing services. Instead of having their computers sitting around unused, letting other users use them and receiving income can generate additional income. This also increases the risk, if a company enters into this new field without properly addressing security concerns, it can lower the reputability for all Cloud providers, which is seen all too frequently.

*4) Government interference*

A disadvantage to note is that Cloud providers may be required to provide data or data logs pursuant to a court issued warrant. This not a likely threat to many regular users, however, it could be a threat for major corporations and companies that use the Cloud to store high value files or data. This leads to major corporations having decreased privacy within the Cloud, and the risk of potential seizure of files which they, otherwise, might have been able to protect.

## II. Security Problems

The Cloud is a great resource for companies who wish to save money and expand in the future, but there are a few security problems and concerns which must be addressed. Some of these problems are authentication and identity verification, virtual networks, data disks, and user passwords.

### *A. Connection Security*

Security with the Cloud is provided differently depending on which kind of service is being used. IaaS and PaaS use Transport Layer Security (TLS) while SaaS uses Secure Sockets Layer (SSL). TLS is an advanced form of SSL and is used for applications. SSL and TLS perform a three-way handshake with a server from a client, which can be a browser or another application. When the application performs the handshake with the server, it tells the server what cipher suites it is running. The server then compares the cipher suite received and will select the highest level suite they have in common. After the server is finished choosing the cipher suite, it will send its certificate to the user. Then, if the user decides to trust the server, public keys are exchanged, which will be used to encrypt all further communication.

### *B. Authentication*

One of the most challenging problems facing Cloud Computing is authentication. Since one user can log in using

multiple computers it is difficult to verify their identity and authenticate them. This challenge is currently overcome by encrypting the login information, but if SSL is not used in SaaS applications the login information packets could be intercepted and read. If the Cloud provider tries to make authentication more secure, it may reduce the usability for the users. Even with the most secure connections, with the most secure encrypted information, this method is still poses risks due to the weakest link in the Cloud which will be discussed later.

### C. Virtual Networks

If the virtualized network provided by the Cloud is not implemented securely, malicious users of the Cloud could potentially infiltrate or attack other computers on the same physical network and cause havoc. This was seen when Microsoft Azure was released. Users could see all the other users using the Cloud Computing resources through the virtual computer networks [7]. Users could then target attacks on networked computers. It is important to note that this was not used maliciously. The best way Cloud companies can combat this is by distinctly separating users, not letting any resources overlap, and removing users that are trying to run malicious applications.

### D. Hard Disks

Sharing computer hardware is an amazing idea if implemented correctly. Cloud users are not only sharing processing power, RAM, network cards and graphics cards, but they are also sharing hard disks. As seen in one of the security problems Rackspace and a few other providers experienced, due to how all operating systems delete and store files, customers could view other customers' deleted data [8]. When computers "delete" files, they just delete the reference to the data. The remedy to this problem was applied eventually, by overwriting all the used sectors of the hard disk with 0's, therefore; the previously written data would be unreadable by other users, even if they used the same disk sectors.

Cloud computers are the same as regular computers, and disks can be corrupted and break like any other hardware. Many Cloud providers backup user information in multiple locations to ensure its safety, but this also increases the cost to the user.

### E. Distributed Denial of Service Attacks

As stated previously, many Cloud companies are prime targets of Distributed Denial of Service (DDoS) attacks because they are publicly available. Cloud companies handle DDoS attacks on the system by distributing the incoming packets amongst multiple computers with the same IP address. Because the incoming packets are shared amongst many computers, instead of a single one, it is much harder to overwhelm the Cloud company with swarms of incoming packets.

### F. User Passwords

A system's security is only as strong as its weakest link, and most Cloud providers and security professionals will agree that the weakest link is typically the users. The concept of making passwords with many letters, symbols, uppercase, and lowercase has been considered best practice for years, but many users still make simple, easy to crack passwords. Many malicious users targeting legitimate users are simply trying to crack the users' passwords instead of attempting to break into the Cloud. The only way Cloud companies could remedy this is by making authentication use more than just a password, only allowing a few submissions of failed passwords. However, even if these enhanced authentication measures are implemented, many users may still use the same password for multiple devices, and if those devices are not secure, the password could still be at risk.

## III. Malicious Applications

If the Cloud allows companies to reduce costs and increase performance, it can do the same for malicious users. The Cloud has decreased the opportunity cost for hackers. A user with malicious intent, using the effectively limitless resources of the Cloud, can crack a password, code or key quickly and for very little cost. In the past it may have taken days, weeks, or months to crack a password using a single computer. The time to crack passwords decreases dramatically when using hundreds or thousands of computers. The Cloud has also enabled the FREAK exploit to be exposed, which will be explained later.

### A. Password Cracking

Just as the Cloud increases a company's resources, the resource available to malicious applications is increased as well. Computers are constantly becoming faster and more affordable. Cloud providers are also trying to decrease their costs to attract additional potential customers.

Unlimited inexpensive processing power is very attractive for a user who is trying to use the Cloud for malicious purposes. Instead of cracking passwords with a single computer, they now have access to something exponentially more powerful some examples will be shown in later sections.

### B. FREAK

FREAK stands for Factoring Attack on Encrypted RSA Keys [9]. FREAK surfaced around March 2015 and targets users who use weak export grade RSA encryption keys, specifically 512 bit encryption RSA keys. Many applications use greater than 512 bit keys, but, in the 1990's, the National Security Agency (NSA) required companies which were exporting cryptography software overseas to use weaker encryption, 512 bit keys were deemed sufficient enough for commercial use. Although the NSA eventually removed the requirement for weaker encryption, there are still many applications using 512 bit RSA keys.

FREAK surfaces when a browser tries to communicate with the secure server. The browser asks the server for the RSA cypher suite, and it is intercepted by a user in between. This is known as a Man in the Middle Attack. The interceptor now asks the server for export grade RSA keys, which the server supplies. The interceptor now has a RSA export key, which is only 512 bits. Amazon EC2 Cloud Computing can "crack" a 512 bit RSA export key in less than 7 hours, and only costs the user approximately 100 USD. The malicious user can now use the cracked RSA key to decrypt the server's

master key, because the export key is a derivative of the master key, and now has the key which can decrypt all packets from the server.

### C. Denial of Service Attacks

Denial of Service (DoS) is done by sending a multitude of packets to a targeted computer from spoofed IP addresses. Because the receiving computer is trying to process the incoming packets, it cannot process the actual legitimate packets it should be. This prohibits users from connecting to the server quickly, if at all. If a malicious user has hundreds of computers, which are very cheap to operate, the user could potentially shut down any server he chooses to, if they are vulnerable to DoS attacks, for very little cost, and still be able to use his computer for other purposes. Some Cloud providers address this problem by removing users who initialize a DoS attack from their network.

### D. How Secure Is Secure Enough

Most, if not all, passwords and encryption methods are chosen because they are considered infeasible to crack, meaning in order to crack them, it will either cost the attacker more than the contents are worth, or it is impossible for the average person to ever crack in their lifetime. With the massive expansion of Cloud services, and the constantly decreasing cost, many current encryption methods may no longer be infeasible to the average hacker who is merely using Cloud Computing services for brute force attacks. For example, three years ago (in 2012) cracking 256 bit Advanced Encryption Standard (AES) key cost 26,700 machine hours, at 2.60 USD an hour using Amazon EC2, with a total cost of 70,000 USD [10] by just brute force attacking the file password. This might seem like a lot, but the encrypted files could be holding something worth a lot more than 70,000 USD, not to mention that it is even cheaper now than in 2012, with additionally increased GPU speeds. With CPU and GPU speeds constantly increasing while their cost decreases, it is not too farfetched to say Cloud Computing will become much cheaper, while its threat to our security increases.

## IV. Future of the Cloud

The continuing growth Cloud will not only lead to an increase in security, it will also require an increase in the minimum level of security for basic privacy and protection. Government investment in Cloud providers will lead the way to better future improvements.

### A. Shift to Stronger Security

With an exponential increase of available computational power to any user who wants it, for a relatively cheap cost, companies will be required to use stronger security to protect their resources. This includes changing passwords more often, and allowing the time for passwords to remain valid to be reduced. Even if a company uses a single use authentication ticket or short time period authentication ticket, if a malicious user is able to decrypt the login information fast enough and request the information before the user, it would be very insecure. Cloud companies might even consider using something besides a password system, for example many applications now let a user log in with a phone. Cloud providers might support that as well, but an entire slew of vulnerabilities come with every new method.

### B. Minimum Level of Security

The best way to address the problems with Cloud security would be to make all companies who offer such services adhere to a minimum level of security for all services offered. Because it is a new field, there are still very few requirements for companies to create a legitimate Cloud Computing resource, which lets many companies offer insecure Cloud options to their users due to simple negligence or sheer lack of basic security practices and procedures. When these companies fall prey to security problems the reputation for all Cloud providers takes a nose dive.

### C. Government Investment

The Federal Government is currently trying to support Cloud companies which offer secure services by creating the FedRAMP program. FedRAMP allows companies to join Compliant Cloud Service Providers (CSP) [11]. Providers whose Cloud services take extra steps to provide more secure platforms that are federally authorized can join this group. Being certified as a CSP can be an extra selling point to many customers.

## V. Conclusion

In conclusion, after a brief overview of Cloud Computing, its advantages, disadvantages, security threats, and malicious applications; the threat to current computer security is very apparent. The average user now has access to what would otherwise be impossible and impractical to previously attain, for very little upfront cost. This, coupled with the ability to render many currently employed security measures useless, will require other users and companies to increase the level of security they currently employ to maintain the same level of security much faster than they would previously need to. The increase in required security will undoubtedly change cyber security, but could even evolve it into a system which removes security's weakest link: the user. Security measures might be made by which users will no longer be authenticated by their password, but by something else entirely. Government investment coupled with the shift to the Cloud by companies and users is triggering this change; this is not speculation, it is already happening.

## References


[1] R. Oppenheim. "A match made in heaven," *Searcher*, vol. 17, no. 7, pp. 14, July 2009.

[2] U. S. health care cloud market projected to reach $3.5B by 2020, *Financial Services Monitor Worldwide*, 2014.

[3] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50-58. 2010.

[4] K. Jammsa, *Cloud Computing*, 1st ed., Burlington, MA: Jones & Bartlett learning, 2013, ch. 2, pp. 17.

[5] M. A. Bamiah and S. N. Brohi, (2011). The seven deadly threats and vulnerabilities in cloud computing. *IJAEST*. [Online]. *9(1)*. pp. 88-90. Available: http://www.academia.edu/4877213/Seven_Deadly_Threats_and_Vulnerabilities_in_Cloud_Computing

[6] S. Ostrowski. (November 3, 2014). As cloud computing barriers fall, new challenges arise for organizations, new comptia study concludes. *CompTIA.* [Online]. Available: http://web.archive.org/web/20150417181303/http://www.comptia.org/about-us/newsroom/press-releases/2014/11/03/as-Cloud-computing-barriers-fall-new-challenges-arise-for-organizations-new-comptia-study-concludes

[7] D. Z. Stinson. (2013). Cloud computing may not be as secure as you would like to believe. *Vulnerabilities in Azure Part 1*. [Online]. Available: http://web.archive.org/web/20140818234744/http://danielzstinson.wordpress.com/Cloud-computing-may-not-be-as-secure-as-you-would-like-to-believe-vulnerabilities-in-azure-part-1/

[8] (April 27, 2012). Rackspace resolves 'dirty disk' vulnerability. [Online]. Available: http://web.archive.org/web/20141121161340/http://www.itnews.com.au/News/298608,rackspace-resolves-dirty-disk-vulnerability.aspx

[9] C. Schrader. (May 1, 2015). What small businesses need to know about FREAK Attacks. *National Cyber Security Institute.* [Online]. Available: http://web.archive.org/web/20150315020611/http://www.nationalcybersecurityinstitute.org/what-small-businesses-need-to-know-about-freak-attacks/

[10] K. Rozario. (August 2012). Cracking passwords with the cloud. [Online]. Available: http://web.archive.org/web/20140907010008/http://www.keithrozario.com/2012/08/cracking-passwords-with-the-Cloud-vertical-vs-horizontal.html

[11] FedRAMP. (2015). [Online]. Available: http://web.archive.org/web/20150503234018/https://www.fedramp.gov/

**Chen-Chi Shing** holds a B.S. degree (physics) from the Chen-Kung University, Taiwan and the M.S. (physics) and M.S. (computer science) degrees from Virginia Tech, an M.S. (statistics) degree from the Ohio State University and a PhD (experimental design) degree from Virginia Tech, USA. Dr. Shing also earned a graduate certificate in information assurance (supported by NSA) from Purdue University in the summer of 2004. He is an associate professor teaching in the computer science concentration at the Department of Information Technology (ITEC) at Radford University, Radford, Virginia. His research interests are related to modeling and simulation in security, security assurance, digital forensics, cloud security, data analytics, web survey tool development, repeated measurement designs, course outcome assessment and interface between computer science and statistics. He has been serving as the Editor-In-Chief for the International Journal of Computer Science and Security since June 2012.

**David Martin** was born on January 14th, 1992 in Washington D.C. He is a current full-time student at Radford University. His research interests include Japanese and Chinese language and culture, and computer programming.

**Lee Hur Shing** was a business information technology student at Virginia Tech. His research interests include cloud computing, big data and information security.