"SECURITY ON THE CLOUD"- A Review

[1] Mr. Ravindra Kumar Gupta(ravindra_p84@rediffmail.com)
[2] Ram Sagar Mishra(ramsagar.mishra@gmail.com)

Abstract - *Cloud computing is, through use of the Internet, the sharing of data, programs and other computer resources. In essence, cloud computing simplifies security issues for users by outsourcing them to another party, one that is supposed to be highly skilled at dealing with them [1]. However, cloud computers are susceptible to multiple vulnerabilities. In order for cloud computing to become an effective, integral part of business and consumer operation, greater security measures must be implemented in order to protect the end user's data. Our paper will discuss the technologies being developed to combat these vulnerabilities, such as fully homomorphic decryption, and will then evaluate the strengths and weaknesses of these technologies. These security measures will make cloud computing a more reliable computing platform for business and the consumer market, and will increase the efficiency of computing as a whole.*

Keywords – Cloud Computing, Data, Encryption, Fully Homomorphic Encryption, Security, etc.

CLOUD COMPUTING: ENTERING THE CLOUD

Within the last 15 years, Internet usage within the United States has exploded from 9.4% of the population to a staggering 75.8% [2]. In addition, the need for power from personal computers has grown exponentially. In 1976, the Cray-1, the world's faster computer at that time, could process 250 megaflops of data. In comparison, the IBM Roadrunner, the world's fastest computer as of 2008, processes 1.105 petaflops of data. In 32 years, the amount of data that a computer could process increased over 4.4 million percent [3]. With these new demands, the need for a more flexible computing technology arose. In response to these demands came Cloud Computing, the use of a more powerful computer system that is located offsite from the user's location. In essence, cloud computing allows users to send, receive, and interact with data stored offsite by means of the Internet. Formally, Cloud Computing is a technological service that enables users and developers to utilize services without knowledge of, expertise with, nor control over the technology infrastructure that supports them. Cloud computing has evolved into a very diverse and complex system as its demand has grown. Similar to a traditional computing model, cloud computing is susceptible to security flaws. Despite the fact that cloud computing currently faces less vulnerability than traditional computers, it is imperative that these flaws be addressed in order to ensure the adoption of cloud computing on greater scales. This paper will discuss the multiple aspects of cloud computing, the current security flaws. How these problems can be addressed, as well as the pros and cons of each security solution.

THE BASIC FRAMEWORK OF THE CLOUD

Cloud computing framework is often referred to by the acronym "SPI", which stands for the three major services of the cloud; Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) [4]. Figure 1 displays these three delivery models and some of their applications. SaaS solutions, such as Google Docs, are used to access web applications over the web. The continuous growth and expansion of the web and technology as a whole has led to a widespread adoption of these SaaS delivery models. As a result of this adoption, there is also a growing demand to protect the data that is being constantly being uploaded to the cloud. PaaS delivery solutions allow developers to create applications right in the cloud, without having to install any development tools. A recent addition to the PaaS array is the App Inventor for Android, created by Google, to allow users to create mobile applications right in the cloud. Securing PaaS delivery solutions is vital in order to ensure confidence amongst the application development community that the cloud is a safe environment in which they can create. The IaaS aspect of the Cloud Computing framework is the traditional idea of Cloud Computing in which a company provides storage, computing power, network space, and other computing resources for a user. The need to secure IaaS delivery models is imperative for those that use their services (i.e. both large and small businesses) in order to protect vital information. All three of these delivery models have several practical applications, including high performance computing and web hosting. As a result, Cloud Computing as a whole is an extremely flexible and adaptable technology whose adoption will greatly improve the lives of many users on the web [4].

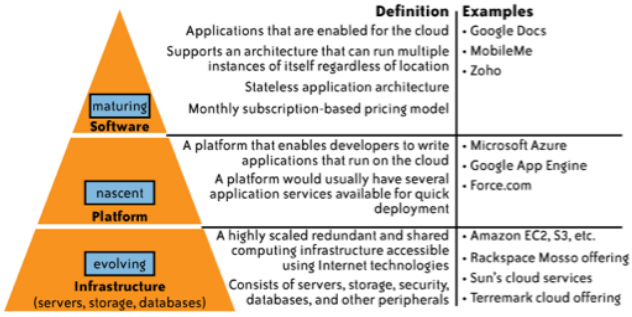

FIGURE 1
THREE ASPECTS OF THE CLOUD COMPUTING FRAMEWORK [3]

There are three subsets of cloud, public, private and hybrid. A public cloud is where resources are delegated for paying users over the Internet through a third party provider. It is extremely important that the public clouds be secure, as they house the personal information of many individual users and small business users. Should a public cloud (or clouds) be compromised, customers of the third party cloud provider can lose sensitive data, be unable to operate their small business, and/or become victims of identity theft. A private cloud is a cloud network that is privatized and often dedicated to a single entity such as a large corporation. It is imperative that private clouds be secure. Although the fact that the outage of private clouds may affect a smaller group of people immediately, on a greater scale the abrupt outage of the cloud can delay business transactions and in turn have a much larger effect. Hybrid clouds are a combination of both public and private clouds. Within a hybrid cloud, non-core applications are run within the public cloud while core applications and sensitive data are kept in a private cloud. These two clouds, the public and private, are linked together to create the hybrid cloud as a means of protection should be compromised [5]. However, considering that a hybrid cloud consists of two different types of clouds, there are two areas that can be affected. Figure 2 shows a graphical representations of the different forms of cloud, how they interact with the three delivery models, and some of their applications...

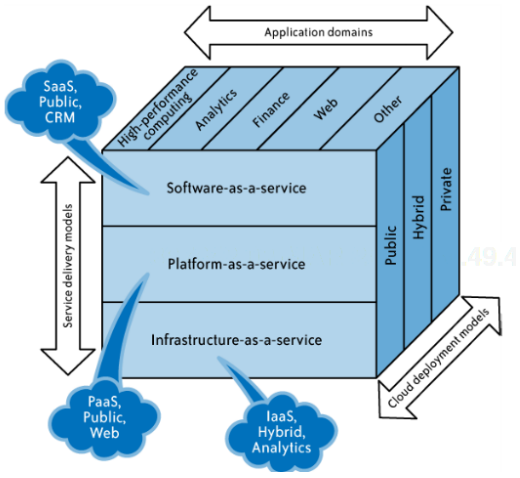

FIGURE 2
APPLICATIONS AND DEPLOYMENT MODELS OF CLOUD COMPUTING [3]

LIFE IN THE CLOUD

Several factors of Cloud Computing make it ideal for business and personal usage as opposed to traditional computing. Cloud computing operates on a pay as you go model, where the user pays for the resources that are used and the time those resources are utilized [4]. This payment model is ideal for users who only require the resources certain times of the year, such as a Tax Professionals. Especially in the months when taxpayers are scrambling to get their taxes done, Tax Professionals require more computing power and storage space for their clients' tax information. However from May to December, fewer resources are needed. As a result, by adopting Cloud Computing, the Tax Professional in this example would avoid having to pay for technology, which would be obsolete by the next tax season.

Cloud computing is both highly elastic and scalable, meaning the computer resources used can be rapidly increased/ decreased as needed [4]. These attributes can be vital to start up ventures, which cannot predict their future computing needs (or lack thereof). Thus by adopting the Cloud model, small businesses use only what they need, saving capital for future business growth. These aspects of Cloud Computing are also vital to large businesses, especially those who have offices located around the world. Utilization of Cloud Computing can allow businesses to rely on several different servers across the globe should one fail. They can reallocate resources as needed for different internal uses, wherever and whenever they are needed. These uses can include storing/accessing employee information in human resources to the collaboration of several groups of people on a new project.

THE DANGER IN THE CLOUD

Despite its clear advantages over traditional computing as a cost efficient, highly adaptable computing model, Cloud Computing has security flaws that prevent it from taking center stage. The first of these problems is misuse or abusing of the system. One of the main benefits of this type of computing is access of much stronger hardware than an average person would have. However, this also means that people can use this with malicious and/or criminal intent. Criminal misusage of the cloud can include data theft and manipulation and identity fraud. One way that hackers crack and get passwords is through brute force. This tactic involves using a computer or multiple computers to attempt every password available until the correct password is found. This method is not always viable for hackers, however, as this requires a strong computer. The use of cloud computing allows hackers to use this method because, through the cloud, they have access to ultra-powerful computers. This has, in fact, already happened. In Germany, a hacker used Amazon Elastic Compute Cloud (Amazon EC2) to obtain Wi-Fi passwords in half the time that it would have taken him if he would have used his at home system [6]. This blatant misuse of Amazon's cloud service resulted in a great deal of personal data to be compromised. In order for cloud computing to be more commonly used, the users and what they are doing must be monitored in a way so that resources are not abused.

Cloud computing is also susceptible to data theft, a concern for any computer user. Since information stored in the cloud is placed on a server somewhere other than the users' own physical location, it is left vulnerable to interception. Data is particularly vulnerable when it is at rest, in transit/being accessed, and when it is being processed. Many people leave important information "unattended" when using it on the web, in what is known as a "cyber footprint". A cyber footprint can consist of anything from credit card information or social security numbers. Often, hackers will gain access to these footprints by tricking the user into downloading a Trojan horse or some other kind of virus in order to take this information. This stagnant data is very susceptible to theft, whether the information is on a home system or stored in the cloud.

Data at rest used by a cloud-based application is generally not encrypted. Encryption is the process of transforming plaintext, the raw unprotected data, into cipher text, the data that is unusable to anyone other than those that have knowledge of how the information was transformed and can undo that process (or 'decrypt') [7]. There are two forms of encryption, symmetric and asymmetric. In a symmetric encryption scheme, the same algorithm is used to encrypt and decrypt information. In an asymmetric encryption scheme, as demonstrated in Figure 3, two different keys are used, one to encrypt the data, and one to decrypt the data. The one used to encrypt the data is said to be 'public' (denoted *pk*), that is, it is widely known and distributed. The 'private' key (denoted *sk*) is only known to the intended recipient of the data. Of the two, asymmetric encryption is much safer as compromising one of the keys doesn't necessarily lead to compromising the data [5]. As a result, it is desirable for cloud providers/customers to adopt the use of asymmetric encryption as means of stronger security. By whatever means an individual pursues in encrypting the data, actions such as indexing and searching become impossible [4]. During transit to the user's computer from the server (or vice-versa) data is susceptible to theft. One of the primary causes of data theft in this situation is the lack of a vetted encryption algorithm to protect the data during transit [3]. In order for data to be processed by any means it *must* be decrypted (with one exception, see Fully Homomorphic Encryption).

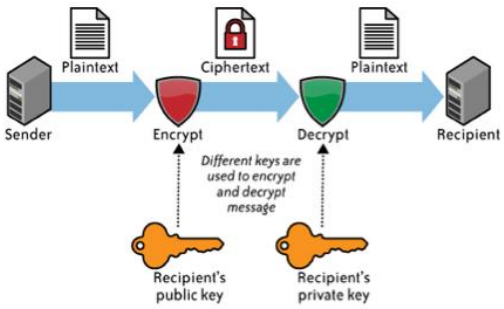

FIGURE 4
A VISUAL DEPICTION OF ASYMMETRIC ENCRYPTION [5]

FUNDAMENTALS OF SECURITY

In order for data to be safe but still useful to the user, security must follow three fundamental tenets. These tenets, known as the CIA Triad, are confidentiality, integrity, and availability. Confidentiality involves making sure other parties do not have access to the data. Integrity is the guarantee that the data has not been changed and/or altered in any way. Finally, availability is how much access the original user has to this data. All of these tenets work in conjunction with each other. If availability was not important, data could be scrambled and encrypted to a point that, while a hacker would not get information, the people that need access to the data would not be able to decipher the information. Without confidentiality and integrity, data would not be safe and no one would be able to trust information sent to them. With these pillars in place, security systems have a goal to provide these three important things to the user in the best way possible [3].

FULLY HOMOMORPHIC ENCRYPTION

The integration of cloud computing into our daily lives grows as technology becomes more adaptable and advanced. However, dependence on the cloud to store data, especially leaving it unencrypted, is as Craig Gentry states, 'to risk an Orwellian future' [7]. In this statement, Gentry, a renowned security expert, is attempting to convey the idea that a lack of encryption will lead to anyone (i.e. Government/'Big Brother') can gain unauthorized access to our data. For an encryption to scheme to be considered Fully Homomorphic, there can be not any limitations on what manipulations can be performed on the plaintext, and the scheme must be malleable. The plaintext is the original information. This has not been scrambled or changed in any way. If someone were to send data in this format, it would be highly vulnerable to theft or manipulation. Using the fundamentals of security previously mentioned, data in the original plaintext format does not follow the confidentiality or integrity tenets. In order to protect the data, plaintext is seemingly randomized by using a specially designed algorithm, or cipher. Ciphertext, in contrast to plaintext, is the changed data. The Ciphertext is the result of encrypting the data by using a cipher, in order to make it unreadable by anyone except for those who have the knowledge to decrypt it. This knowledge is often referred to as a key, and is the method of reversing the algorithm. It is necessary to change data back into the readable plaintext in a reasonable amount of time. A malleable encryption scheme in the context of Fully Homomorphic Encryption means that an encryption of dataset/plaintext *d* into another valid encryption *f(d)* (function on d) without necessarily learning the original *d* [5]. In effect, Fully Homomorphic Encryption is a very secure asymmetric form of encryption. In essence, the use of Fully Homomorphic Encryption is highly applicable and useful if a user wished to alter data by performing some function to it, but wanted to hide the data from the cloud, as demonstrated in Figure 5. In hiding the data from the cloud, the sensitive information is much less vulnerable to attack and theft.

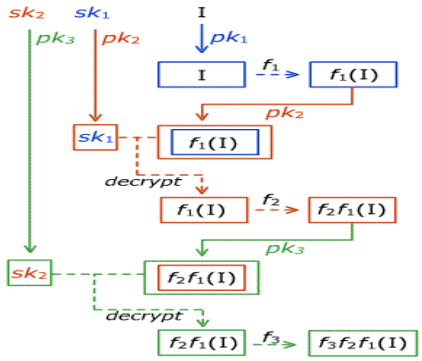

FIGURE 5
FLOWCHART OF FULL HOMOMORPHIC ENCRYPTION [3]

The reason that computers as a whole have become so widely integrated in everyday life is our ability to delegate tasks to them that are too complex or mundane to perform ourselves. That is, for a computing application such as Fully Homomorphic Encryption to become fully adopted it must be efficient despite its complexity. For an encryption scheme that acts in the cloud to be efficient as we delegate the encryption processes to the cloud, it must reach completion within a predetermined time period. This time period is defined as the time it would take a user to decrypt the cipher text, apply function *f* to it, re-encrypt it, and upload it back to the cloud [7]. Obtaining optimal efficiency is the greatest obstacle facing Fully Homomorphic Encryption since its unveiling in July 2009 [3]. However, once this obstacle is overcome, the application of Fully Homomorphic Encryption will greatly aid in the security of the Cloud.

In order for Fully Homomorphic Encryption to be viable as a type of security, it still must follow the CIA Triad. Any cipher is able to pass the first two pillars with flying colors, as properly decrypted data is unreadable and unalterable by anyone that does not have the key. Where Fully Homomorphic Encryption is revolutionary is through its accessibility. In the previous example, the third party consultant would be able to prove and check banking records without actually needing to know the actual number. As of right now, this type of encryption has not been perfected and is still relatively slow, which means that it doesn't follow the third tenet for good security. As this technology advances, however, Fully Homomorphic Encryption would be a viable security measure for those on "the cloud."

Fully Homomorphic Encryption's application to cloud computing today will vastly improve the security of the cloud. This is perhaps best exampled in applying Fully Homomorphic Encryption to confirm the integrity and provenance of a data set. Data integrity is defined as ensuring that the data has not been altered or changed. Data provenance refers not only to its integrity, but also that the data is computationally accurate [7]. Another aspect of data provenance is the process of tracing and recording the origins of data and its movement between databases or cloud [6]. In the real world, we can view this application through a company such as a third party consultant that is reviewing banking practices for a particular bank. The consultants want to make sure that the computations that the bank are performing are accurate, yet the bank cannot disclose the amounts in their customers accounts due to privacy laws. As a result, the third party consultants could apply a Fully Homomorphic Encryption algorithm to check that the banking transactions have not been incorrectly altered (integrity) and that they are computational accurate and originate from the bank (provenance).

CLOUD SECURITY: THE VIRTUALIZATION APPROACH

A different approach to ensuring the sanctity of the cloud being currently developed by Hewlett-Packard (HP) is an approach they call 'Cells-as-a-Service', with which they hope to fully automate security management in the cloud through the use of virtual machines [1]. A virtual machine is the software emulation of another computer, that is, it is to run a computer within another computer. With this security measure, several virtual machines, storage volumes (i.e. hard drives) and networks run across multiple physical machines/servers to consist of a cell. Within each cell, HP programs various detectors and sensors that detect any malicious or suspicious behavior. In particular, these cells can watch CPU activity, I/O patterns and memory usage. Spikes in CPU activity and uncommon I/O patterns (input and output signals) can be telltale signs of a security breach. They are able to compare the past activity in the cloud to real time activity in order to discern as to whether there is any suspicious activity or not [1]. This methodology for running a virtual machine is very effective in detecting and countering threats to the CPU, due to the fact that the virtual machines/agents can get very close to the action without being a part of action. In addition, this monitoring does not intrude on the user's sensitive personal data during the virtualization process. The cell, which is essentially acting as an anti-virus service, cannot be detected by any malicious code.

Another approach to cloud security currently being pursued by IBM is called "Virtual Machine Introspection". In this methodology of security, a protected virtual machine is run on the same physical machine as the guest virtual machines on the cloud [1]. The virtual machine can perform different protective measures such as whitelisting and blacklisting (allowing/disallowing) kernel functions, which are defined as processors cores or groups of cores enclosed within a secure perimeter [7]. In essence, kernels allow the execution of applications and manage a computer's resources. If the kernel were to be tampered with as a result of malicious code, not only is sensitive data at risk but also the physical computer itself (i.e. too many intensive processes can lead to overheating and damage to the CPU). By whitelisting and blacklisting kernel functions, we can regulate the processes being run. As a result, the security-based virtual machine ensures that the computers connected to the cloud are safe for themselves and others connected to the cloud [1]. Similar to HP's 'Cells as a Service' prototype, Virtual Machine Introspection cannot be detected by malicious code. It differs in the respect that if it were, for example, in charge of monitoring fifty machines, it would only need to run one virus scan for all fifty as opposed to one per machine [1]. The result is a faster, more efficient means of protection. Simultaneously, virtual machine introspection is not only excellent at preventing and resolving computer issues in the cloud, it is very unintrusive of the user's sensitive data.

Both of these security models, Virtual Machine Introspection and Cells-as-a-Service can be very befitting to virtually every type of cloud user. In addition, both follow all three tenets of the CIA Triad. The constant monitoring of the usage of the computer would show suspicious activity quickly which means that confidentiality and integrity would remain intact. The sweeps do not require a large amount of processing either, which means that is doesn't hinder the user. This would mean that the data would be readily available which is fundamental to strong security. Large businesses can efficiently sweep their thousands of employee computers for malicious code that would otherwise potentially halt business. At the same time, the high efficiency of these security methods does not put computational weight on the CPU, allowing for efficiency to stay at normal levels. In addition, the fact that both security mechanisms do not invade upon a user's personal data would prevent the company's proprietary information to be taken into the cloud without permission. Thus, cloud computing is much more secure as a result of implementing either of these security measures.

USER RECOGNITION TECHNOLOGY

As with any other computing system, it is imperative that cloud computers ensure that the individual attempting to access the system is authorized to do so. A new methodology of authorizing access to the cloud currently being used is face recognition. Face recognition technology consists of the following aspects, user initialization, computer initialization, and the private matching identification part of cloud. Figure 6 displays the user initialization process. In the user part of the identification process, the computer takes a picture of the individual attempting to access the system. It then identifies the part of the image that is the person's face, adjusts the lighting of the image, and greys the image out, converting each pixel's RGB color value to gray scale data. The grey scale data is transformed from the two-dimensional face image to a one-dimensional vector. This vector is then encrypted by means of Paillier encryption algorithm to protect the user's identity [8]. In essence, Paillier encryption is a type of homomorphic encryption scheme, but is not fully homomorphic as there are limitations in the functions used to encrypt the data [8]. However, Paillier encryption is extremely efficient, making it ideal for this application. In the cloud initialization and private matching identification aspects of authentication, the computer then compares an individual's image to a database of predetermined authorized users. In order to do so, it maps the image of the face and compares it to the one's found in the database. In order for access to be approved, the key aspects of the taken picture must match the image that is stored in the date base within a predetermined deviation from the original [8]. If it does not, the individual is denied access and the system has effectively prevented unauthorized access to the cloud.

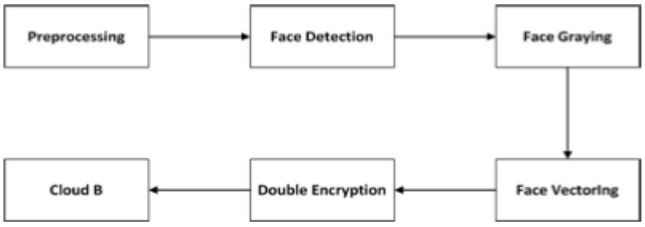

FIGURE 6
THE PROCESS OF FACE RECOGNITION ON THE USER END [8]

The utilization of Face Recognition technology would greatly compliment any security features already in place of the cloud. It is more reliable than biometrics or iris scanning means of authorization, as these two identification forms rely too heavily on hardware accuracy and consistency [8]. Face recognition technology is another means of identity verification in addition to an encrypted password that has the potential to be cracked or stolen. Implementing face recognition technology would help security considerably as those attempting to gain access to the cloud must have permission to do so. In effect, companies (whether they be cloud providers or cloud customers) can track how long a user was using/accessing the cloud and validate their identity simultaneously. A real world application for this technology is large companies using it to ensure that lower level

employees are not trying to obtain proprietary secrets to sell for profit. Face recognition technology is also applicable for the government's use. Using a private cloud(s), different branches of government can set specific levels of authorization for sensitive materials, only to viewed by authorized agents. The result of implementing this technology in the real world is a securer cloud environment [8].

ADOPTIONS OF CLOUD COMPUTING TECHNOLOGIES

Many companies are beginning to adapt and change to using cloud computing, or offering forms of it to their customers. For example, Sony is planning to offer infrastructure-as-a-service to their customers who have paid for the Playstation Plus service. These customers will be able to save their game data on an off-site server instead of on their own console [9]. Amazon is also continuing to expand the Elastic Compute Cloud, another IaaS offering, which sells server space, as previously mentioned.

The sales of cloud services across the globe are set to double from a little over 50 billion dollars in 2009 to over 100 billion dollars by 2012. Because of the potential growth, computer corporations are expanding and trying to profit. For example, HP recently bought 3Par Inc., a data storage company for just under 2.5 billion dollars [10]. Another computer giant, Apple, is planning on offering IaaS to its customers in its upcoming update of the Mac OS. Apple is planning on adding a feature with Mac OS X Lion, the next update, called the Safe Deposit Box. This safe deposit box secures any files that the user drags into the "safe." Things deposited into the safe will then be saved offsite, so that the user has a backup copy of the data, very similar to Sony's use of the cloud and video game saves [11]. One of the most interesting uses of cloud computing that is coming out in the next few years is Google's Chrome OS.

In 2009, Google announced that they were working on a new operating system that would be primarily for netbooks (tiny laptops with minimal power that are not used for much more than internet browsing). This operating system is not supposed to be used for anything other than connecting to the World Wide Web. In fact, as opposed to a classic Windows or Mac OS, the Chrome OS would only ship with the chrome internet browser loaded onto the computer. This minimalist approach leads to this computer being run completely on the cloud. Any applications that this computer would run would be on the web, and any computations or storage would have to be on the cloud [12].

The Chrome OS is an excellent example of where cloud computing is headed. While companies are now embracing the cloud through infrastructure, Chrome uses not only IaaS, but also SaaS and PaaS. Google's early embrace of the cloud through this experimental operating system has a good chance to pay off [12].

THE SUSTAINABILITY OF CLOUD COMPUTING

Sustainability has many proponents in the field of Cloud Computing. It can greatly aid in increasing the sustainability of real world projects, but at the same time its operations are detrimental to the environment if not properly managed. The use of Cloud Computing in the long run will help sustain the environment as long as several steps are taken. These steps include data center optimization and efficient energy usage.

In order for Cloud Computing to be effective in daily usage, it requires large data centers. However, these data centers use 1.5% of the country's power, with expenses of 4.5 billion dollars annually [13] and are a growing source of greenhouse emissions [14]. As a result, companies such as HP, Google, and IBM are focusing on minimizing data center energy use without compromising computing power. IBM has begun the building of a data center in Syracuse, New York that will use 50% less energy than current facilities. It contains an electrical co-generation system with water-cooled server racks and sensors that direct workloads to optimal servers, diverting energy and power from overworked servers, as exampled in Figure 7 [13]. Google's data centers also use half as much energy over traditional data centers by using cooling towers to evaporate excess heat and recycling the cooled down water back into the data center [13]. By reducing the heat of these facilities and recycling the water used in the cooling process, we reduce the energy used by these data centers. In effect, the carbon footprint of this emerging technology is reduced.

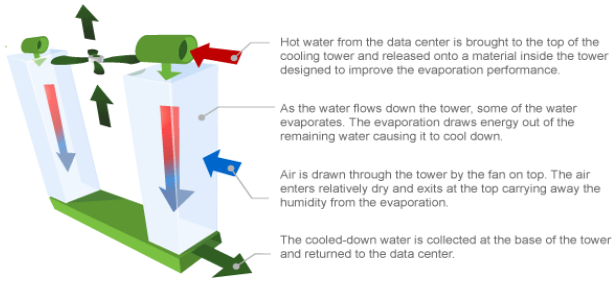

FIGURE 7
A COOLING PROCESS SIMILAR TO THAT OF GOOGLE AND IBM'S DATA CENTERS [13]

In a recent study by Accenture US, a management consulting company, moving business operations to the cloud led to significant reductions in carbon footprints. A smaller carbon footprint was achieved through optimizing four key factors: Dynamic Provisioning, Multi-Tenancy, Server Utilization, and Data Center Efficiency. In Dynamic Provisioning, resources from the cloud are provided on an as needed basis. Multi-Tenancy is the delivery of applications at the same time for multiple users of the cloud. This in turn decreases peak loads. In Sever Utilization, cloud server space is more efficiently allocated to users than an in-house server dedicated to a business. The way a data center is designed plays a great role in how efficiently it uses power. In order to increase sustainability, data center must be efficient. That is, it must be constructed with materials and equipped with IT to run to its fullest potential. As a result of these four key aspects, the goal is to minimize the amount of energy used and in turn reducing the carbon footprint [15].

Despite the fact that current innovations are needed to maximize the efficiency of Cloud Computing in terms of its operations, the technology itself is highly applicable in maximizing sustainability for structural engineering processes. By utilizing the extremely cheap computational power of cloud computing, engineers can compile large and complex sets of data in order to design buildings better suited for their geographical location and climate. With such information, engineers can then use the parameters of the datasets to increase the efficiency of water and energy use [14]. For example, a civil engineer can take several years of data for weather, climate shift, soil composition, and terrain shifts in order to design a building best suited for a predetermined building site. As a result of designing such a building, costs such as repairs and ineffectual energy use can be offset. In addition, Cloud Computing allows engineers to work from their own office, while performing computations on servers elsewhere in real time, maximizing their own work efficiency [14].

THE FUTURE OF CLOUD COMPUTING

The rapid expansion of computers is expected to continue for the next few according to Moore's Law. Gordon Moore, wrote in 1965 that the number of components in an integrated circuit has doubled every year, and he predicted that that trend would continue. Moore was correct with his assumption and the number of components has, in fact, approximately doubled every year since then. However, in a recent interview, according to Moore himself, his law will not apply within 15 years [16]. This is because there is a limit to how small things can get, as nanochips are beginning to be hindered by the "graininess of the universe." That is, the atomic nature of matter is going to eventually prevent computers from getting more powerful by shrinking the various components. This means that in order for computers to be more powerful, they will have to get bigger. As these computers grow in size, it is the responsibility of engineers to do be conscious of the environment, keeping things such as minimal power consumption in mind. As not everyone will have the ability to house or afford these future supercomputers, cloud computing will be the only answer for the majority of people.

Working on the cloud is the future of computing, not only for business, but also for use by the public sector as well. Technologies like Fully Homomorphic Encryption or cells-by-a-service may be an excellent security measure for cloud computing, but hackers and code breakers will continue to evolve. Computer engineers must continue to make new security measures in order to protect the future of computing. It is the duty of computer engineers to make the cloud a safe place for people to work.

REFERENCES

[1] G. Anthes. (2010, November). "Security in the Cloud." *Communications of the ACM*. Vol. 53, no 11. pp.16-18

[2] (2011). "Internet users as percentage of population" World Bank. [Online]. Available: http://www.google.com/publicdata?ds=wb-wdi&met=it_net_user_p2&idim=country:USA&dl=en&hl=en&q=internet+usage+statistics

[3] T. Mather, S. Kumaraswamy, S. Latif (2009). *Cloud Computing and Privacy*. Sebastopol, CA: O'Reilly Media.

[4] R. Krutz, R. Vines. (2010). Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Indianapolis: Wiley Publishing Inc.

[5] J. W. Rittinghouse, J. F. Ransome. (2010). Cloud Computing: Implementation, Management, and Security. Boca Raton: CRC Press.

[6] J C. Bagh. (2010, January 12) "Amazon EC2 helps researcher to crack Wi-Fi password in 20 minutes." International Business Times. [Online]. Available:http://www.ibtimes.com/articles/100314/20110112/amazon-ec2-password-wi-fi-hacking-cracking-brute-force-attack-wpa-psk-encryption-cloud-computing-iaa.htm

[7] C. Gentry. (2010, March) "Computing Arbitrary Functions of Encrypted Data." *Communications of the ACM*. Vol. 53, no 3. pp.97-105

[8] C. Wang, H. Yan. (2010, December 12) "Study of Cloud Computing Security Based on Private Face Recognition" *Beijing Institute of Technology*. Available: http://ieeexplore.ieee.org/search/srchabstract.jsp?tp=&arnumber=5676941&queryText%3Dcloud+computing+security%26openedRefinements%3D*%26searchField%3DSearch+All

[9] L. Plunkett. (2011) "You Can Soon Save Your PS3 Games In Thin Air" [Online] Available: Kotaku. Available: http://kotaku.com/#!5746393/save-your-ps3-games-in-thin-air

[10] J. Simpkins. (2010) "The Bright Future for Cloud Computing is Becoming Much Clearer" Morning Money. [Online] Available: http://moneymorning.com/2010/09/23/cloud-computing/

[11] (2011). "Apple in the Sky with Diamonds: A Cloud Based Safe Deposit Box" Patently Apple. [Online] Available: http://www.patentlyapple.com/patently-apple/2011/02/apple-in-the-sky-with-diamonds-a-cloud-based-safe-deposit-box.html#more

[12] N. McAllister. (2009) "Chrome OS: Cloud computing made real" InfoWorld. [Online] Available: http://www.infoworld.com/d/developer-world/chrome-os-cloud-computing-made-real-660?page=0,0

[13] A. Schwartz. (2009) "Can Cloud Computing Ever Truly Be Sustainable? " Fast Company. [Online] Available: http://www.fastcompany.com/blog/ariel-schwartz/sustainability/can-cloud-computing-ever-truly-be-sustainable

[14] E. Stewart. (2009) "The Sustainability Potential of Cloud Computing: Smarter Design" Environmental Leader. [Online] Available: http://www.environmentalleader.com/2009/07/20/the-sustainability-potential-of-cloud-computing-smarter-design/

[15] (2010) "Cloud Computing and Sustainability: The Environmental Benefits of Moving to the Cloud." Accenture US. [Online] Available: http://www.greenbiz.com/sites/default/files/Cloud Computing and Sustainability - Whitepaper - Nov 2010.pdf

ACKNOWLEDGMENTS

I would collectively like to thank **Dr. J. S. Parihar** (Principal of Aditya Engineering College of Technology and Science), my chairperson who has been helpful in providing insight and suggestions from a professional standpoint and for proofreading out paper and checking for general coherence. I would also like to thank our friend Mr. Anoop Shrivastava, for his efforts in helping improving my paper and reading this paper despite the fact that he absolutely hates cloud computing. I would also like to thank my family for their general support. I would like to thank Market Central for its tasty food and beverages, which keep him nourished during the long binges of writing and formatting this paper.