Security Issues Present in Cloud Computing

Paulino III Santos Crespo
Computer Science
Juan M. Ramirez, Ph.D.
Electrical and Computer Engineering & Computer Science Department
Polytechnic University of Puerto Rico

Abstract — *Cloud computing has increasingly become part of day to day operations from large government organizations to international level corporations as well as the common mobile smart phone user. The availability of high Internet connections has contributed to the growth of cloud computing. Hence, the demand for security in cloud computing has become crucial and increases as it becomes essential in business operations, services, and other uses that are provided by cloud based computing. This paper discusses the characteristics of cloud computing, main services offered by cloud computing providers, major threats and security issues that affect cloud computing environments, and some available solutions to such threats. Also, this paper proposes a method that offers data encryption and integrity in databases residing on cloud environments.*

Key Terms — *Cloud Computing, Cloud Security, Encryption, Security*

INTRODUCTION

One of the most important advances in computing has been the birth of cloud computing. The National Institute of Standards and Technology NIST, defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1]. Now days many enterprises and business have embraced the use of cloud computing services for their business operations, customer services, and information management. Also, public cloud computing services have been made available to the overall population, which has as well adopted its use.

Cloud computing has become popular given to the many different benefits it brings to its users. The most notable benefit of cloud based computing is the level of abstraction it provides between the physical infrastructure and the owner of the information [2]. Hereby, the hardware and operational costs are reduced given to such level of abstraction. Furthermore, various problems rise given to this level of abstraction. Outsourcing IT services to cloud providers will create a dependency for enterprise operations; thus, relying in third party providers will always be a risk. Most cloud computing services are well designed and strictly monitored, but no system is fully perfect and safe.

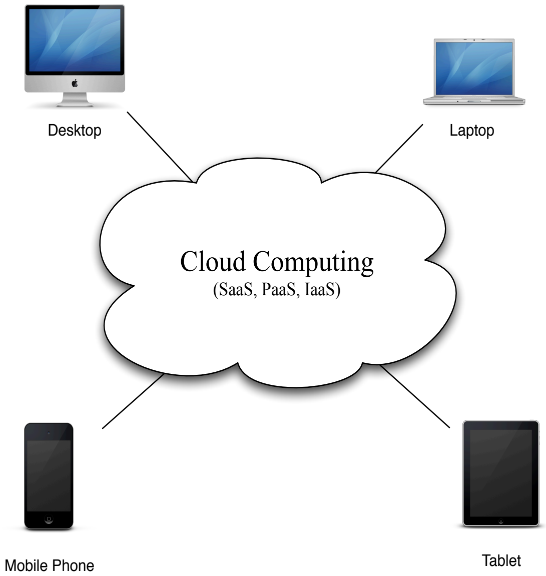

Figure 1
Cloud Computing Model

Figure 1 displays a cloud computing model showing the level of abstraction that exists between the user's devices and the different services offered by the cloud provider which mainly are: Software as a Service, Platform as a Service, and Infrastructure as a Service.

Cloud Computing Characteristics

Cloud computing is characterized by providing shared resources, on-demand-self-service, elasticity, and measured service [2]. Shared resources refers to the sharing of network, application, storage, or other computing capabilities in which resources are assigned and reassigned to customers as needed. As for on-demand-self-service, consumers can manage and upgrade their usage of resources without requiring human intervention [2]. Furthermore, elasticity allows rapid escalation of resources thus, allowing consumers increase or decrease their usage of resources depending on the workload [2]. Lastly, cloud computing is also characterize by measured service; users only pay for resource consumption excluding the provider's operational costs.

Cloud Computing Services

The three major services offered by cloud computing are: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

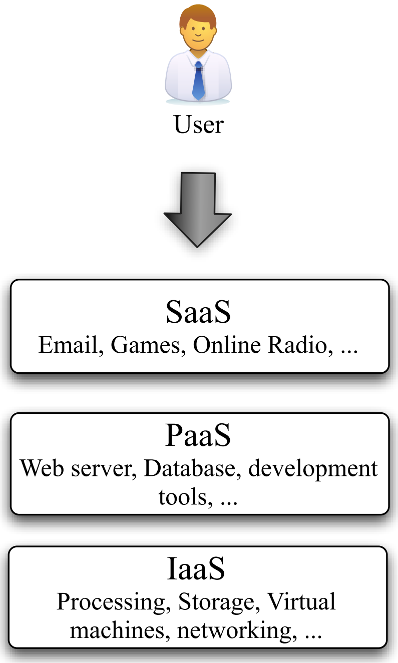
User
SaaS
Email, Games, Online Radio, ...
PaaS
Web server, Database, development tools, ...
IaaS
Processing, Storage, Virtual machines, networking, ...

Figure 2
Cloud Computing Services

Figure 2 displays somes examples of tools and resources provided by the different cloud computing service models.

Software as a Service (SaaS)

The SaaS model offers users the option of renting the use of software through the Internet instead of buying the actual software. Thus, bypassing the need to install any software or hardware in the user's system. Instead of having to buy software licenses, Software as a Service costs may be provided by pay-per-use or subscription fees [2]. One of the most notable benefits of SaaS is that software updates, fixes, and patches are entirely handled by the provider. Other benefits that SaaS provides are: abstraction of hardware specifications, software operation support, and reduced operational costs. Google Docs, Acumatica, Salesforce.com, and SAP are some examples of popular SaaS.

Platform as a Service (PaaS)

Another service model known in cloud computing environments is the Platform as a Service (PaaS) model. PaaS offers users the opportunity to make use of a development environment to code software targeting specific platforms while using libraries and other tools provided by the provider [2]. Furthermore, users have full control to deploy and configure their applications as desired. Similar to SaaS, PaaS offers the benefit of abstraction; users don't need to "manage the underlying cloud infrastructure, including servers, storage mediums and network configurations" [2]. Hence, users can develop and deploy software without acquiring servers or third party tools. Google's Apps Engine and Microsoft's Azure Platform are two examples of PaaS.

Infrastructure as a Service (IaaS)

The Infrastructure as a Service model is similar to normal hosting services. In this model the users can access various capabilities of networking, processing, storage, bandwidth, and others. Also, users can choose to run different operating systems with full management and control [2]. This is possible through the use of virtual machines, also known as hypervisors. Virtualization is the main technology that makes cloud computing possible [3]. The IaaS model is very similar to utility computing in which users pay for consumption of disk storage, processing power, and bandwidth. The difference of IaaS from utility computing relies on the advantage of IaaS to scale the service as required [2].

Cloud Computing Threats and Security Issues

Similar to the Information Assurance principles, cloud computing must provide confidentiality, integrity, and availability of information to users [4]. Confidentiality assures that only authorized users have access to the resources being accessed. Moreover, the integrity of information is kept if data hasn't been altered, modified, and remains in its correct format. Lastly, the availability principle consists of keeping resources available to the user at all times. Usually, these three principles are displayed in a triangle as shown below in Figure 3.

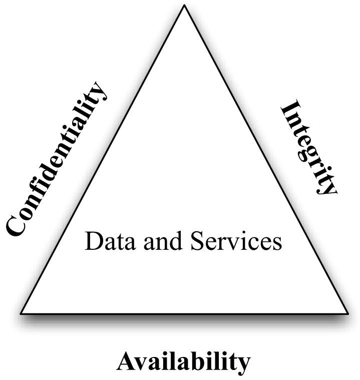

Figure 3
Information Assurance Triangle

Attacks and security risks present in cloud computer environments try to affect directly one or more of the information assurance principles. The following threats and security risks discussed are mainly generated from inside the cloud environment, the user's personal system used to communicate with the cloud, or from third persons such as the man-in-the-middle attack. Some of these security risks can affect both cloud users as well as cloud providers [3].

"Wrapper Attack" within XML Signatures

It is common for web applications to make use of XML and SOAP (Simple Object Access Protocol) to communicate with each other. These two technologies are used to create XML signatures that will "prove to the recipient that the data is authentic and has integrity" [3]. The "wrapper attack" consists of injecting or adding additional XML content to an XML, which will lead to unwanted code execution [3]. Furthermore, the attacker wraps the XML signature to the unwanted code and passes it on as if it where a genuine XML communication [3]. The paper [3] states that wrapper attacks are unlikely to happen and uncommon in business applications.

Browser Security

The use of Internet browsers for accessing cloud environments has become very common. For example, in the Google Chrome OS the browser is the main tool for I/O operations [3]. Browsers make use of SOP (Same Origin Policy) as a security measure for communication between the browser and the server. The server records the origin of the first request made by the browser and accepts further requests if they come from the same initial location [3]. The [5] paper argues that many browsers lack XML Signature and encryption capabilities and proposes that these should be included in future browsers.

The other alternative to securing communication in browsers is the use of TLS (Transport Layer Security). TLS makes use of the record layer and the TLS handshake for browser security [3]. However, such technique requires a digital certificate from the server, and not all servers possess digital certificates [3]. By servers not owning digital certificates, users may access illegitimate servers, mainly "phishing" scams, that intend to trick users to believe that they are accessing a legitimate website or server [3]. Hence, the attacker will have access to the user's data if the user, unaware of the danger, submits his credentials in such situation. In order to secure online communication the user must:

- Keep his browser up-to-date with the latest updates and patches 2 column format for the body of the document
- Make use of encryption supported browsers
- Access servers that provide TLS encryption and possess a valid security certificate
- Ensure that visited servers are legitimate

Other security measures exist, but the ones mentioned above are the most basic precautions.

Denial of Service

One type of attack known to be popular among online servers is known as flooding. The most common type of flooding attacks is considered to be the Denial of Service (DOS) attacks. Denial of Service attacks occur when "a hacker uses infected computers to all connect to a specific website" [3]. The main purpose of DOS attacks is to overload a server with high amounts of requests thus, increasing the server's performance to its limit [3]. A server with large amounts of workload will not function efficiently and could cease operations for as long as the DOS attack is active [3].

Traditional servers possess to some extent a limitation of resources [3]. However, this is not the case for cloud-based servers. When a DOS attack occurs in a cloud environment the cloud infrastructure does provide extra resources to support the wave of requests initiated by the attack. Thus, two major problems arise when a DOS attack targets a cloud environment. First, the owner of the server under attack may be charged an overwhelming amount of money given to the large quantity of resources used by his server given to the denial of service attack [3]. Secondly, other clients of the cloud provider may be affected by the attack given that shared resources will be taken away to support the demand of the DOS attack [3]. Furthermore, the amount of affected users could increase if the cloud uses resources located in other nodes or parts of the cloud.

Denial of Service attacks can be very difficult to manage. A solution to handle cloud-specific DOS attacks is to measure a client's average usage of resources. Moreover, both parts (cloud provider and client) can mutually agree on a "limit" of resources usage that if reached will serve as signal of a possible denial of service occurring. The cloud provider should then contact immediately the client and inform him that his "limit" has been reached. Consequently, the cloud provider and client decide whether to consider or not the event as a DOS attack and if necessary further action is needed.

Reputation Fate Sharing

One drawback or side effect of cloud computing is that shared hardware can affect innocent users in certain situations such as spam proliferation or criminal activity [3]. In cloud computing the behavior of a single user can affect the reputation of other users given to the shared resources principle. The following two real world examples involve victims of reputation fate sharing [3].

- **Amazon EC2:** Amazon.com, Inc. and its Amazon Elastic Compute Cloud (Amazon EC2) is one of the best-known cloud services provider in the industry. This cloud provider was forced to change and modify security policies regarding its cloud services after attackers were able to corrupt its services and release a large amount of spam proceeding from within the cloud [3]. Hence, Spamhaus, an online project that tracks Internet spam, listed various Amazon EC2 IP addresses as harmful [6]. Evidently, the reputation of many users was affected given to such event.
- **FBI Raid:** Another case of significant harm was when FBI agents raided a data center given to the fact that cyber crimes were committed using the data center's hardware. While the FBI searched for evidence and held an investigation, some companies had

unrecoverable losses due to the suspension of service [6]. “Table Caption”.

Even though these security issues are significant, data centers are still more capable than individual clients in maintaining and securing systems [3]. However, the fact that many users are affected when a security flaw is discovered in data centers that provide cloud services still exists [3].

Side Channels

Another type of attack that affects cloud environments given to its resource sharing nature is side channeling. The side channel attack occurs in virtual machines that share the same hardware [3]. In such attack the attacker can intercept data being sent or received by a neighbor virtual machine [3]. The [3] paper states that “this form of security risk has been documented and there are many methods for preventing this type of attack”. An advantage of having the cloud provider manage security measures in the cloud is that when side channel flaws are discovered in virtual machines, updates or fixes are implemented rapidly all at once [3].

Data Control

One of main concerns of using data storage services from cloud providers is the control data. On traditional computers there is control over how data is stored, who has access to the data, and what backup methods will be used [3]. However, in cloud computing user’s data is stored in a server and the cloud provider decides on how the data will be stored [3]. In order for the user to store confidential or sensitive data, a level of trust should exist between the user and the cloud provider [3].

The [3] paper conducted a research and weren’t able to find evidence of cloud providers illegally selling information to third parties. However, it is expected that the user will have to sign a user agreement that will grant the cloud provider permission to use data analytics for advertisement purposes [3]. For example, Google’s business model serves users with services in exchange of users’ information to benefit advertisers [3].

Internet Dependence

Cloud computing and its services provide many benefits to all sorts of businesses, organizations, and people. Even though, relying major business operations to cloud services will inevitably create a dependence of the Internet. Thus, in case a critical or catastrophic event such as a terrorist attack, virus, or long-term power outage occurs production will be severely affected [3]. Furthermore, if a production facility such as a water plan chooses to outsource their servers and computers to virtual machines in the cloud, in a catastrophic event they could loose control of water supplies thus, affecting the population as well [3]. Therefore, it is of great importance to analyze all the risks involved when outsourcing business operations to cloud based environments.

Other Security Issues

Other security issues that aren’t directly related to cloud environments also exist. Some external threats that may be of harm to both customer and cloud provider include man-in-the-middle attack, packet sniffing, IP spoofing, and inside threats [4]. The man-in-the-middle attack occurs when a attacker “deploys a proxy application in between a consumer and provider without them knowing and the attacker intercepts personal information” [4]. Similar to the man-in-the-middle attack, packet sniffing tries to intercept data between the user and the provider by analyzing packets. Also, an attacker can use IP spoofing to impersonate a user’s valid IP address and access information that was meant for the legitimate IP address. For this reason, it is important to use proper encryption to secure all communications between the user and the cloud environment. Lastly, another possible security issue that could be present is the existence of a malicious insider in the cloud’s data center [4]. Even though it is uncommon, a malicious insider is a major threat to consumers of cloud services [4]. Improper security procedures in the cloud’s data center can allow a malicious employee to access or modify data that could be used for corporate espionage, organized crime, or terrorism [4].

Cloud Security Awareness

Before considering cloud computing, users must be aware of various facts concerning overall security in cloud environments.

- Social Engineering is an easy way to gain access to confidential material [3]. One must review the authenticity of sources that ask for confidential information such as login credentials, and never submit login credentials from third party sources [3].
- There are security flaws present in all types of computing including cloud computing [3].
- Cloud computing is considered to be more secure that traditional computing given to the fact that security and updates are handled by experts [3].
- The users' behavior has a large impact on security. The amount of security features available don't manner if a user posts confidential data in public or non-secure places [3].
- Research on the different companies that provide cloud services and choose one that possesses good reputation [3].

CRYPTOSYSTEM FOR DATABASES

As previously noted, storing data in cloud environments bring certain security risks regarding the confidentiality, accessibility, and integrity of data. Database systems are highly used in cloud environments and are the main tool used to store information. Even though the accessibility of data relies on the cloud provider, the user can implement a cryptosystem approach to ensure confidentiality and integrity. Web services are mainly delivered through cloud computing as SaaS, which is considerably the most popular cloud service. These services require user authentication through login processes to gain access. The proposed cryptosystem is designed for such web services that require user credentials for service access offered by a cloud provider and make use of database systems for data storage. Figure 4 depicts the proposed cryptosystem with all its components.

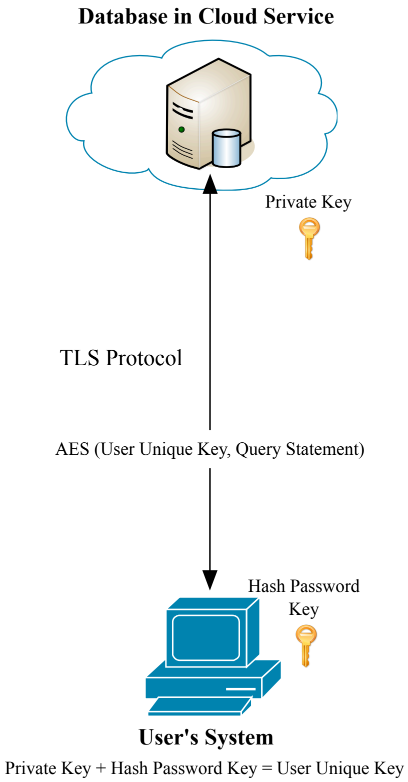
Database in Cloud Service
Private Key
TLS Protocol
AES (User Unique Key, Query Statement)
Hash Password Key
User's System
Private Key + Hash Password Key = User Unique Key

Figure 4
Cloud Database Storage Cryptosystem

Cryptosystems use various combinations of encryption algorithms, keys, and procedures to add additional data security.

Transport Layer Security

The proposed cryptosystem makes use of the TLS protocol to encrypt the direct communication with the database's server. Data is stored in database by using query statements. These query statements will travel from the user's system to the database through TLS. TLS uses "asymmetric cryptography for key exchange, symmetric encryption for confidentiality, and message authentication codes for message integrity" [7].

AES and Hash Values

Secondly, the user's query values will be encrypted using the Advanced Encryption Standard (AES) algorithm with a user unique key. The user unique key is a combination of a private key stored in the server and a hash value of the user's password. Hash values are produced by hash functions such as MD5 or SHA-1. A hash function is a mathematical algorithm that converts data to a fixed length value. Hash values are used to ensure data integrity. A hash value can't be calculated back to the original data input and if a single bit of the original data is altered the hash function will produce a different value.

Encryption Procedure

Finally, the proposed cryptosystem works in the following steps:

1. The user connects to the cloud server and initiates a connection using the TLS protocol.
2. The user inserts his credentials at login. The user's password is then converted into a hash value using Javascript or any client-side language that supports hash functions.
3. Furthermore, the hash value is concatenated at the end of the private key to create a user unique key.
4. After the user unique key is generated, query statements are constructed using AES encryption in the desired fields. An example for encrypting the password field using MySQL would be similar to "INSERT INTO user (username,password,age) VALUES ('averagejoe',AES_ENCRYPT('secretpassword','secretkey2034f6e32958647fdff75d265b455ebf'),'21')".
5. The query statement is executed and travels safely using the TLS protocol.
6. Moreover, the decrypting procedure works similarly to the encrypting procedure and can be also be done by executing a query statement. An example for decrypting a password field using a MySQL database system would be similar to "SELECT AES_DECRYPT('secretkey2034f6e32958647fdff75d265b455ebf',password) as password FROM user WHERE username = 'averagejoe' ".

Cloud Database Storage Cryptosystem Benefits

The proposed cryptosystems not only ensures integrity and confidentiality but also protects users from attacks such as man-in-the-middle, packet sniffing, and unauthorized data access. Furthermore, if an attacker possesses the username and hash value of a user's password, he still can't access the system because the non-hashed original password is never stored or transmitted to the server. Therefore, user authentication is done by comparing a password's hash value with the hash stored in the database. Note that every user will possess his own unique key thus, procedures for decryption of data will vary from user to user depending on the user's password hash value; hence, adding another layer of security to data residing in the database.

Cloud Database Storage Cryptosystem Disadvantages

There are some main disadvantages that arise when implementing the cloud database storage cryptosystem approach. First, encryption is known to require certain computational power thus, the computational usage for the client may increase when implementing such approach. Secondly, adding encryption to the query statements will affect the database's performance given to the encryption implementation; this could become a problem if many users are requesting information from the database system. Lastly, if a user wants to change his password the application must command the database to decrypt all the user's encrypted information and re-encrypt it using the user's new unique key.

Conclusion

Cloud computing security will keep becoming an important subject as long as more businesses, organizations, and people make use of cloud services. Attackers are frequently thinking of new ideas on how to penetrate systems, and with the popularity of cloud computing it will surely become a desirable target. However, cloud providers are well aware of such dangers and possess security experts and numerous tools that provide safety to cloud users.

This paper discussed security issues related specifically to cloud computing, but more security threats, which weren't covered, still exist in the client's side. Hence, cloud providers could create a user security awareness program to educate users on security good practices and secure usage of cloud services. Also, cloud providers could create an alliance with educational institutes to research on new security vulnerabilities and test their services against those threats especially those most common and harmful such as the denial-of-service attacks. Furthermore, cloud providers could investigate new ways to substitute procedures that require human intervention with automated procedures. In brief, the cloud environment does provide numerous benefits but also a handful of risks. No amount of security features is sufficient to completely secure a cloud environment from threats and vulnerabilities thus; it's the customer's choice to decide whether the use of cloud services is a viable option for him.

References

[1] NIST, "NIST.gov – Computer Security Division – Computer Security Resource Center", DOI=http://csrc.nist.gov/groups/SNS/cloud-computing/.

[2] Dahbur, K., et al., "A Survey of Risks, Threats, and Vulnerabilities in Cloud Computing", *ISWSA '11 Proceedings of the 2011 International Conference on Integlligent Semantic Web-Services and Applications*, April 2011

[3] Roberts, J., C., et al., "Who Can You Trust in the Cloud? A Review of Security Issues Within the Cloud", *InfoSecCD '11 Proceedings of the 2011 Information Security Curriculum Development Conference*, October 2011, pp. 15-19

[4] Yu, H., et al., "Cloud Computing and Security Challenges", *ACM-SE '12 Proceedings of the 50th Annual Southeast Regional Conference*, March 2012, pp. 298 – 302

[5] Jensen, M., et al., "On Technical Security Issues in Cloud Computing", *CLOUD '09 Proceedings of the 2009 IEEE International Conference on Cloud Computing*, September 2009, pp. 109 – 116

[6] Chen, Y., et al., "What's New About Cloud Computing Security?", *Technical Report No. UCB/EECS-2010-5*, January 2010

[7] Wikipedia, "Transport Layer Security - Wikipedia", DOI=http://en.wikipedia.org/wiki/Transport_Layer_Security.