International Journal of Computer Science and Engineering Open Access
Review Paper Volume-2, Issue-2 E-ISSN: 2347-2693

# Cloud's SaaS Security by Biometric Concept

Dharamjeet Singh[1*], Surabhi Shukla[2]

[1*]*Dept. of CS, S.H.I.A.T.S., Allahabad, Uttar Pradesh*
[2]*Dept. of Engineering, SRITS Datia, RGPV,Bhopal, Madhya Pradesh*

**www.ijcseonline.org**

Received: 06 Feb 2014 Revised: 12 Feb 2014 Accepted: 27 Feb 2014 Published: 28 Feb 2014

*Abstract-* Personal privacy is of utmost importance in the global networked world. Some vital information that are disseminated within an office, across offices ,between branches, of an organization and other external bodies and establishments at times get into the hands of the unauthorized persons who may tamper with that contents of the information. And if no security measures are taken, there is no doubt that such data and other sensitive information will be exposed to threats such as impersonation, in-secrecy, corruption, repudiation, break-in or denial of services that may cause serious danger on the individual or organization. A secure system should maintain the integrity, availability, and privacy of data. Data integrity usually means protection from unauthorized modification, resistance to penetration and protection from undetected modification.

*Keywords-* Cloud Computing, Security, SLA, VPN, Biometric Security

## INTRODUCTION

Cloud computing is an evolving paradigm with tremendous momentum, but its unique aspects exacerbating security and privacy challenges. Cloud computing is a subscription-based service where you can obtain networked storage space and computer resources. One way to think of cloud computing is to consider your experience with email. Your email client, if it is Yahoo!, Gmail, Hotmail, and so on, takes care of housing all of the hardware and software necessary to support your personal email account. When you want to access your email you open your web browser, go to the email client, and log in. The most important part of the equation is having internet access. Your email is not housed on your physical computer; you access it through an internet connection, and you can access it anywhere. If you are on a trip, at work, or down the street getting coffee, you can check your email as long as you have access to the internet. Your email is different than software installed on your computer, such as a word processing program. When you create a document using word processing software, that document stays on the device you used to make it unless you physically move it. An email client is similar to how cloud computing works. Except instead of accessing just your email, you can choose what information you have access to within the cloud.

*How can you use the cloud?*

The cloud makes it possible for you to access your information from anywhere at any time. While a traditional computer setup requires you to be in the same location as your data storage device, the cloud takes away that step. The cloud removes the need for you to be in the same physical location as the hardware that stores your data. Your cloud provider can both own and house the hardware and software necessary to run your home or business applications. This is especially helpful for businesses that cannot afford the same amount of hardware and storage space as a bigger company. Small companies can store their information in the cloud, removing the cost of purchasing and storing memory devices. Additionally, because you only need to buy the amount of storage space you will use, a business can purchase more space or reduce their subscription as their business grows or as they find they need less storage space.

One requirement is that you need to have an internet connection in order to access the cloud. This means that if you want to look at a specific document you have housed in the cloud, you must first establish an internet connection either through a wireless or wired internet or a mobile broadband connection. The benefit is that you can access that same document from wherever you are with any device that can access the internet. These devices could be a desktop, laptop, tablet, or phone. This can also help your business to function more smoothly because anyone who can connect to the internet and your cloud can work on documents, access software, and store data. Imagine picking up your smartphone and downloading a .pdf document to review instead of having to stop by the office to print it or upload it to your laptop. This is the freedom that the cloud can provide for you or your organization.

*Types of clouds*

There are different types of clouds that you can subscribe to depending on your needs. As a home client or small business owner, you will most likely use public cloud services.

1. Public Cloud - A public cloud can be accessed by any subscriber with an internet connection and access to the cloud space.
2. Private Cloud - A private cloud is established for a

*Corresponding Author: Dharamjeet Singh*

 

specific group or organization and limits access to just that group.
3. Community Cloud - A community cloud is shared among two or more organizations that have similar cloud requirements.
4. Hybrid Cloud - A hybrid cloud is essentially a combination of at least two clouds, where the clouds included are a mixture of public, private, or community.

*Choosing a cloud provider*

Each provider serves a specific function, giving clients more or less control over their cloud depending on the type. When you choose a provider, compare your needs to the cloud services available. Your cloud needs will vary depending on how you intend to use the space and resources associated with the cloud. If it will be for personal home use, you will need a different cloud type and provider than if you will be using the cloud for business. Keep in mind that your cloud provider will be pay-as-you-go, meaning that if your technological needs change at any point you can purchase more storage space (or less for that matter) from your cloud provider.

There are three types of cloud providers that you can subscribe to: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). These three types differ in the amount of control that you have over your information, and conversely, how much you can expect your provider to do for you. Briefly, here is what you can expect from each type.

1. Software as a Service - A SaaS provider gives subscribers access to both resources and applications. SaaS makes it unnecessary for you to have a physical copy of software to install on your devices. SaaS also makes it easier to have the same software on all of your devices at once by accessing it on the cloud. In a SaaS agreement, you have the least control over the cloud.
2. Platform as a Service - A PaaS system goes a level above the Software as a Service setup. A PaaS provider gives subscribers access to the components that they require to develop and operate applications over the internet.
3. Infrastructure as a Service - An IaaS agreement, as the name states, deals primarily with computational infrastructure. In an IaaS agreement, the subscriber completely outsources the storage and resources, such as hardware and software, that they need.

As you go down the list from number one to number three, the subscriber gains more control over what they can do within the space of the cloud. The cloud provider has less control in an IaaS system than with an SaaS agreement.

What does this mean for the home client or business looking to start using the cloud? It means you can choose your level of control over your information and types of services that you want from a cloud provider. For example, imagine you are starting up your own small business. You cannot afford to purchase and store all of the hardware and software necessary to stay on the cutting edge of your market. By subscribing to an Infrastructure as a Service cloud, you would be able to maintain your new business with just as much computational capability as a larger, more established company, while only paying for the storage space and bandwidth that you use. However, this system may mean you have to spend more of your resources on the development and operation of applications. As you can see, you should evaluate your current computational resources, the level of control you want to have, your financial situation, and where you foresee your business going before signing up with a cloud provider.

If you are a home client, however, you will most likely be looking at free or low-cost cloud services (such as web-based email) and will not be as concerned with many of the more complex cloud offerings.

After you have fully taken stock of where you are and where you want to be, research into each cloud provider will give you a better idea of whether they are right for you.

## CLOUD COMPUTING SECURITY

The information housed on the cloud is often seen as valuable to individuals with malicious intent. There is a lot of personal information and potentially secure data that people store on their computers, and this information is now being transferred to the cloud. This makes it critical for you to understand the security measures that your cloud provider has in place, and it is equally important to take personal precautions to secure your data.

The first thing you must look into is the security measures that your cloud provider already has in place. These vary from provider to provider and among the various types of clouds. What encryption methods do the providers have in place? What methods of protection do they have in place for the actual hardware that your data will be stored on? Will they have backups of my data? Do they have firewalls set up? If you have a community cloud, what barriers are in place to keep your information separate from other companies?

Cloud computing security is an evolving sub-domain of computer security, network security and more broadly, information security.it refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.

1. Traditional Data Security- (VM level attacks, Cloud provider vulnerabilities, Phishing Cloud Provider, Expanded Network attack surface, Authentication and Authorization, Forensic in Cloud.) These concerns

  

involve computer and network intrusions or attacks that will be made possible or at least easier by moving to the cloud. Cloud providers respond to these concerns by arguing that their security measures and processes are more mature and tested than those of other company.
2. Availability-(Uptime, Single Point of Failure, Assurance of computational Integrity.) These concerns centre on complex application data being available.
3. Third party control- (Due Diligence, Auditability, Contractual Obligations, Cloud Provider Espionage, Data Lock-in, Transitive Nature.) The legal implication of data and application being held by a Third Party are complex and not well understood. There is also a potential lack of control and transparency when a Third Party holds the data.

## PROBLEMS IN CLOUD

We now describe some elements of our vision. The core issue is that with the advent of the cloud, the cloud provider also has some control of the cloud client's data. We aim to provide tools supporting the current capabilities of the cloud while limiting cloud provider control of data and enabling all cloud clients to benefit from cloud data through enhanced business intelligence.

1. Information Centric Security- Data needs to be self-describing and defending, regardless of its environment. Data needs to be encrypted and packaged with a usage policy. When accessed, data should consult its policy and attempt to re-create a secure environment using virtualization and reveal itself only if the environment is verified as trustworthy.
2. High-Assurance Remote Server Attestation- we have noted that lack of transparency is discouraging business from moving their data to the cloud. Data owners wish to audit how their data is being handled at the cloud, and in particular, ensure that their data is not being abused or leaked, or at least have an unalterable audit trail when it does happen.
3. Privacy- Enhanced Business Intelligence – A different approach to retaining control of data is to require the encryption of all cloud data. The problem is that encryption limits data use. In particular searching and indexing the data becomes problematic.

## PROBLEM SOLVING STARTEGY

When we are talking about sensitive data in cloud, then we should be more careful. When we are using the virtual private network then. Cloud is a type of virtual network, which is somewhere but the actual location of that is undistinguishable for us. In cloud architecture there are three service model namely SaaS (Software-as-a Service),PaaS (Platform-as-a Service) and Iaas (Infrastructure-as-a Service). They all tackle different type of security issues with them. But we are focusing on SaaS, how SaaS faces different security issues regarding databases.

Actually in this layer only client and provider interact with each other. Nobody else is required as the mediator. When client stores its data on cloud, then it should be sure with provider's policy because with the full trust client stores its important data on cloud. The client should check the SLA of the cloud provider. SLA stands for Service Level Agreement, an agreement which has to be signed between the client and the provider.

The provider should make sure that the faith of client should never be broken. This is the provider's responsibility that data residing in should be safe and in any case the data should not be modified or updated. What we have studied so far is that there are several techniques by which the data can be encrypted. The data can be encrypted while in transmit and in rest, so we should not talk about this. We are here to give a concept of data security while receiving the data from cloud. When the client creates its account on the provider's website, the website should focus on the general information required for an account as well as on the concept of biometric recognition i.e. voice recognition, finger-print recognition, retina recognition etc… whenever the client transmits its data to cloud this recognition is not needed, but when client needs the data back from the provider's cloud it should be needed. This approach will make sure that the data is being approached to a right person. The client who passes the recognition test may have the access to data. Via this approach we will definitely not trouble the client by asking for biometric recognition at each time the data is transmitted into the cloud. This will trouble the client and will consume the much time as it can. This can be a drawback in the upcoming future. So to overcome this problem of data breach and access of time this concept has been suggested by us.

Approximately all the problems in cloud which we have declared earlier can be overcome with this. Client can get the authority of audit trail of his logs, and can update the logs whenever it is required. Client should be aware of this that their data is not abusing or leaked at any moment. This will give the High-Assurance Remote Server Attestation to the client. Another problem was Information Centric Security, the data centre where the data is stored, a place where data has been put in the encrypted format. This is so called a secure environment because the data residing in is encrypted format so that intruder can't attack the data. These all properties regarding to the security should be mentioned in the SLA. Third problem was Privacy-Enhanced Business intelligence, an approach for encryption of data residing in the cloud. The data which is their in the cloud is in encrypted format so access to it is limited and it is very complex while using.

Biometric concept will overcome all the issues regarded to the data, either stored in hardware or stored in cloud. When the data is transmitted to hardware from cloud it should require the biometric card via which it can be

make sure that the data which is retrieving from the cloud is retrieved by the original client, nor by attacker. If the recognition results false then the Denial of Service attack should take place, and send error message to the original client that there an attack has been attempted to audit his/her data. Both the data terminals shall be strong enough to download the safe data.

## CONCLUSION

Cloud fears largely stem from the perceived loss of control of sensitive data. Current control measures do not adequately address cloud computing third party data storage and processing needs. In our vision, we propose to extend control measures from the enterprise into the cloud through the use of Trusted Computing and applied cryptographic techniques. These measures should alleviate much of today's fear of cloud computing, and we believe, has the potential to provide demonstrable business intelligence advantage to cloud participant.

Our vision also relates to likely problems and abuses arising from a greater reliance on cloud computing, and how to maintain security in the face of such attacks. Namely the new threats require new construction to maintain and improve security. Among these are tools to control and understand privacy leaks, performs authentication and guarantee availability in the face of cloud Denial-of –Service attacks.

## REFERENCES


[1]. Zirra Peter Buba, Gregory Maksha Wajiga,"Cryptographic Algoriths for Secure Data Communication";International Journal of Computer Science and Security(IJCSS), Volume(**5**) :Issue(**2**) :**2011**.

[2]. www.wikipedia.com

[3]. Hassan Takabi, James B. D. Joshi, Gail-Joon "Security and Privacy Challenges in Cloud Computing Environments"1540-7993/**10**/IEEE.

[4]. Richard Chow, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessica Stanndon, Ryusuke Masuoka, Jesus Molina"Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Cloud ".

[5]. Alexa Huth and James Cebula"The Basics of Cloud Computing"USCERT **2011**.