Analysis of Privacy Challenges and Security Concerns in Cloud Computing

Varun Shukla
Department of EC, PSIT

Abstract— *Cloud computing is a method to enhance the capacity dynamically without investing in new infrastructure, training new personnel, or licensing new software. It can be viewed as a cost effective solution to various security threats. It extends the existing capabilities of Electronics and Communication world and its ongoing capabilities. In the last few years, cloud computing has grown from being a promising business concept to one of the fast growing segments of the Communication industry at large. But as more and more information on individuals and companies are added in the cloud, concerns are beginning to grow about just "how safe" an environment it is. Despite of all the hype surrounding the cloud, enterprise customers are still hesitating to deploy their business in the cloud. Security is one of the major concern which curbs the growth of cloud computing and complications with data privacy/security and data protection continue to plague the market. In this paper, a survey of the different security risks that pose a concern to the cloud is presented. This paper is a survey more specific to the different security issues that has emanated due to the nature of the service delivery models of a cloud computing system.*

Keywords— Iaas, Paas, Saas, SSL

I. INTRODUCTION

Cloud Computing has been envisioned as the next generation architecture of Communication industry at large, due to its long list of unprecedented advantages in the IT history: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk [1]. As a disruptive technology with profound implications, Cloud Computing is transforming the very nature of how businesses use information technology. From users‟ perspective, including both individuals and IT enterprises, storing data remotely into the cloud in a flexible on-demand manner brings appealing benefits: relief of the burden for storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc [2]. Nowadays anyone with an interest in communication or information technology must look towards cloud computing. Cloud computing refers to a service that satisfies all of the following conditions [3].

- Users rely on the service for access to and/or processing of data;
  - The data is under the legal/ authentic control of the user;
  - Some of the resources on which the service depends are „virtualized‟, which means that the user has no technical need to be aware which server running on which host is delivering the service, nor where the hosting device is located; and
  - The service is acquired under a relatively flexible contractual arrangement, at least as regards the quantum used.

- While hailed as a new era, cloud computing has gained only a limit amount of attention from a legal regulator Perspective. Yet cloud computing is associated with a range of obvious privacy and consumer risks, such as risks relating to:
- How data provided to a cloud computing operator will be used by that operator;
- How such data will be disclosed by the cloud computing operator, and subsequently used by third parties-a big concern
- The security of the data provided;
- The legality (law for data security in that particular judiciary) of using cloud computing products;
- Disruptions of the cloud computing service;
- Getting locked into a contractual arrangement that does not cater for the consumer's/organization's future needs; and
- Manipulating privacy laws by the use of cloud computing products.

We can only enjoy the full benefits of Cloud computing if we can address the very real privacy and security concerns that come along with storing sensitive personal information in databases and software scattered around the Internet. In this paper, we discuss those, and related, risks.

II. SERVICE TYPES

Based upon the services offered, clouds are classified in the following ways:

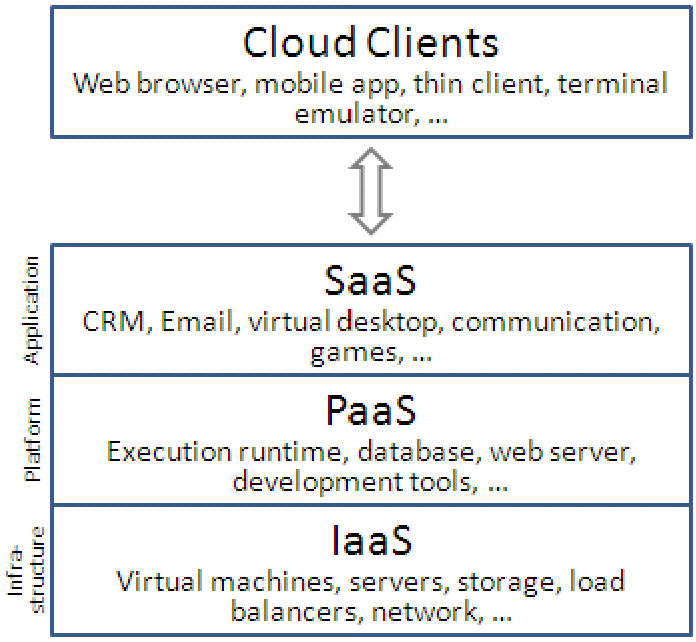
Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...
SaaS
CRM, Email, virtual desktop, communication, games, ...
PaaS
Execution runtime, database, web server, development tools, ...
IaaS
Virtual machines, servers, storage, load balancers, network, ...
Application
Platform
Infra-structure

Figure 1: Service types of cloud computing.

1. Software-as-a-Service (SaaS)

This model is designed to provide everything and simply rent out the software to the user. The service is usually provided through some type of front end or web portal. While the end user is free to use the service from anywhere, the company pays a per use fee. It includes a complete software offering on the cloud. Users can access a software application hosted by the cloud vendor on pay-per-use basis. This is a well established sector. The pioneer in this field has been Salesforce.com offering in the online Customer Relationship Management (CRM) space. Other examples are online email providers like Google's Gmail and Microsoft's hotmail, Google docs (storage) and Microsoft's online version of office [4].

2. Platform-as-a-Service (PaaS)

In this model of cloud computing, the provider provides a platform for client use. Services provided by this model include all phases of the system development life cycle (SDLC) and can use application program interface (APIs), website portals, or gateway software. Buyers do need to look closely at specific solutions, because some providers do not allow software created by their customers to be moved off the provider‟s platform. An example of PaaS is GoogleApps.

3. Infrastructure-as-a-Service (IaaS)

Infrastructure as a service delivers a platform virtualization environment as a service. Rather than purchasing servers, software, data centre space or network equipment, clients instead buy those resources as a fully outsourced service [5].

III. SECURITY ISSUES IN SERVICE MODEL OF CLOUD COMPUTING

While cost effectiveness and ease of use are two great benefits of cloud computing, there are significant security concerns that has to be taken into consideration while moving the data across the network.[6] Cloud computing utilizes three delivery models SaaS, PaaS and IaaS as discussed earlier which provide infrastructure resources, application platform and software as services to the consumer. IaaS is the foundation of all cloud services, with PaaS built upon it and SaaS in turn built upon it. Just as capabilities are inherited, so are the information security issues and risks. There are significant trade-offs to each model in the terms of integrated features, complexity vs. extensibility and security. If the cloud service provider takes care of only the security at the lower part of the security architecture, the consumers become more responsible for implementing and managing the security capabilities [7].

Security issues in different cloud service models are following:

1. Security issues in SaaS

In SaaS, the client has to depend on the vendor for proper security paradigms. The provider must do the work to keep multiple users‟ from seeing each other's data. So it becomes difficult to the user to ensure that right security measures are in place and also difficult to get assurance that the application will be available when needed [8]With SaaS, the cloud customer will by definition be substituting new software applications for old ones. Therefore, the focus is not upon portability of applications, but on preserving or enhancing the security functionality provided by the application [9]. The SaaS software vendor may host the application on its own private server or deploy it on a cloud computing infra-structure service provided by a third-party provider (e.g. Amazon, Google, etc.).

Enterprises today view data and business processes (transactions, records, pricing information, etc.) themselves as strategic and guard them with access control and compliance policies. However, in the SaaS model, enterprise data is stored at the SaaS provider‟s data center, along with the data of other enterprises. Moreover, if the SaaS provider is leveraging a public cloud computing service, the enterprise data might be stored along with the data of other unrelated SaaS applications. The cloud provider might, provide replicas of data on multiple locations across countries for the purposes of maintaining high availability. Most enterprises are familiar with the traditional on- premise model, where the data continues to reside within the enterprise boundary, subject to their policies.

Consequently, there is a great deal of discomfort with the lack of control and knowledge of how their data is stored and secured in the SaaS model. There are strong concerns about data breaches, application vulnerabilities and availability that can lead to financial and legal liabilities. The layered stack for a typical SaaS vendor and critical aspects that must be covered across layers in order to ensure security of the enterprise data is illustrated in Figure. 2.

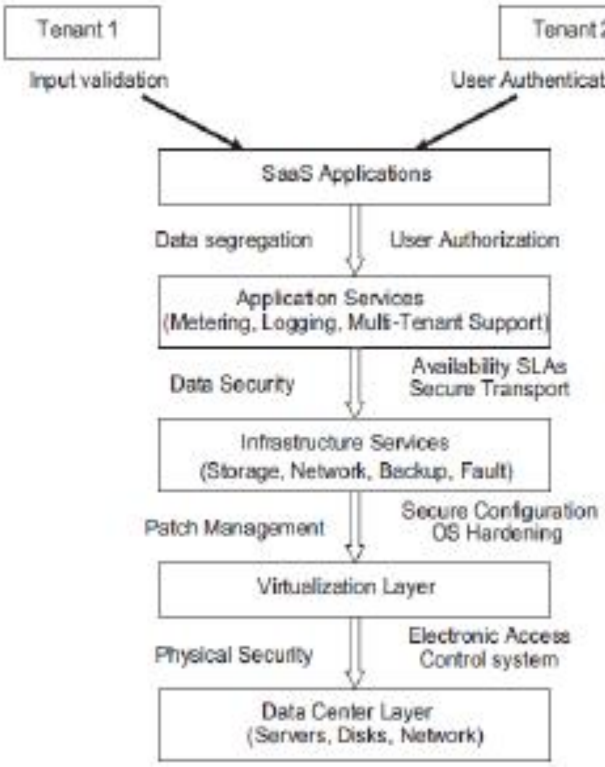

Figure 2: Security for the SaaS

The following key security elements should be carefully considered as an integral part of the SaaS application development and deployment process:

- Data security
- Network security
- Data locality
- Back up

- Data Breaches
- Identity management and sign-on process.

2. Data security

In a traditional application deployment model, the sensitive data of each enterprise continues to reside within the enterprise boundary and is subject to its physical, logical and personnel security and access control policies. However, in the SaaS model, data is stored outside the enterprise, at the SaaS vendor location. Consequently, the SaaS vendor must adopt additional security checks to ensure data security and prevent breaches due to security vulnerabilities in the application or through malicious employees. This involves the use of strong encryption techniques for data security and fine-grained authorization to control access to data.

In cloud vendors such as Amazon, the Elastic Compute Cloud (EC2) administrators do not have access to customer instances and cannot log into the Guest OS. EC2 Administrators with a business need are required to use their individual cryptographically strong Secure Shell (SSH) keys to gain access to a host. All such accesses are logged and routinely audited. While the data at rest in Simple Storage Service (S3) is not encrypted by default, users can encrypt their data before it is uploaded to Amazon S3, so that it is not accessed or tampered with by any unauthorized party. Apart from these many security techniques also used to provide security to the user data.

3. A Very Important Aspect for Cloud Computing Security-SSL

SSL Security for Cloud Computing has proven to be of great help in several aspects. It is considered as the best security protocol for Cloud users. As we know, an SSL certificate is used to create a safe channel between a web browser and web server for avoiding any type of data tampering in between. Even in the case of cloud computing, an SSL certificate effectively secures data stored or shared by establishing an encrypted session.

The significance of integrating an SSL certificate with Cloud Computing can bring forth several advantages, which can ensure the security of customers' data stored or in-transit on the cloud.

4. Data Monitoring

Sure, the ability of accessing data from anywhere sounds pretty awesome, but have you ever wondered about the server location or where exactly the data is stored on the cloud?

However, if an SSL certificate is used to encrypt the stored data by Cloud providers, they can assure the customers that their data is closely monitored, even during the transmission. Also, trusted certificate issuing authorities will avoid issuing an SSL certificate to the servers located in banned countries like Iran, North Korea, etc.

5. Regulatory Compliance

Any enterprise intending to secure data on the cloud is required to comply with certain rules and regulations that are set by the government and trusted industry authorities like Sarbanes-Oxley (SOX) Act, Payment Card Industry Security Standard (PCI-DSS), Health Insurance Portability & Accountability Act (HIPAA). And before outsourcing and trusting cloud providers with all sensitive data, enterprises must also ensure that the providers seek some compliance with industry standards. Here, SSL encryption helps in avoiding any type of disclosure of private data to third parties trying to intercept or steal it.

6. Ensure Data Segregation & Encrypted Access

In Cloud Computing, the storage location of all data coming from users across the world, and the respective server location remains unknown to the users. It is controlled by cloud providers. And the shared environment in cloud storage may not guarantee the segregation of that data and the subsequent multi-tenancy. However, using an SSL certificate can easily secure the data on the cloud. The cloud provider needs to ensure this by providing

- **Encryption**: Cloud-users should ensure they are being provided the industry-standard levels of encryption, the minimum session encryption strength of 128-bit or the preferable 256-bit encryption.
- **Authentication**: There should be an authentication of the server's ownership before the data is transferred. It is advisable to rely on certificates issued by trusted third party CAs as in that case, the servers are already authenticated by them.
- **Certificate Validity**: An SSL certificate comes with certain validity periods. In case of an unlikely event where the certificate is compromised a fail-safe check needs to be there to make sure the certificate has not been revoked since

its issuance. At present, Online Certificates Status Protocol (OCSP) and Certificate Revocation List (CRL) are the two standards popularly used to check the certificate validity.

7. **Securing Back-Up Repositories**: Users store their data on the cloud with an intention to retrieve when needed. However, if there is an unlikely event of the cloud experiencing a total crash for some unforeseen reason, then providers should be able to recover users' data from their backup repositories. An SSL certificate assures about the legitimacy of the duplicate servers that are used to retrieve the backup and also provides an encrypted channel for its transfer.

   An SSL certificate is chosen by many providers for establishing cloud security. Cloud users should also be vigilant while selecting a cloud provider based on the security they furnish. Along with other attributes like space being provided, users should also consider security aspects that are selected by the providers. To avoid security breaches or data loss, cloud providers should use SSL certificates that are issued after undergoing rigorous vetting procedures conducted by trusted authorities and offer encryption strength of 128- to 256-bit for exceptional security.

IV. NETWORK SECURITY

In a SaaS deployment model, sensitive data is obtained from the enterprises, processed by the SaaS application and stored at the SaaS vendor end. All data flow over the network needs to be secured in order to prevent leakage of sensitive information. This involves the use of strong network traffic encryption techniques such as Secure Socket Layer (SSL) and the Transport Layer Security (TLS) for security. However, malicious users can exploit weaknesses in network security configuration to sniff network packets. The following assessments test and validate the network security of the SaaS vendor:

- Network penetration and packet analysis
- Session management weaknesses
- Insecure SSL trust configuration.
- Any vulnerability detected during these tests can be exploited to hijack active sessions, gain access to user credentials and sensitive data.

1. Data locality

In a SaaS model of a cloud environment, the consumers use the applications provided by the SaaS and process their business data. But in this scenario, the customer does not know where the data is getting stored. In many a cases, this can be an issue. Due to compliance and data privacy laws in various countries, locality of data is of very important in various enterprise architectures [10]. For example, in many EU and South America countries, certain types of data cannot leave the country because of potentially sensitive information. In addition to the issue of local laws, there's also the question of whose jurisdiction the data falls under, when an investigation occurs. A secure SaaS model must be capable of providing reliability to the customer on the location of the data of the consumer.

2. Backup

The SaaS vendor needs to ensure that all sensitive enterprise data is regularly backed up to facilitate quick recovery in case of disasters. Also the use of strong encryption schemes to protect the backup data is recommended to prevent accidental leakage of sensitive information. In the case of cloud vendors such as Amazon, the data at rest is not encrypted by default. The users need to separately encrypt their data and backups so that it cannot be accessed or tampered with by unauthorized parties.

3. Identity management and sign-on process

Identity management (IdM) or ID management is a broad administrative area that deals with identifying individuals in a system (such as a country, a network or an organization) and controlling the access to the resources in that system by placing restrictions on the established identities. Identity management can involve three perspectives

- **The pure identity paradigm**: Creation, management and deletion of identities without regard to access or entitlements.
- **The user access (log-on) paradigm**: For example: a smartcard and its associated data used by a customer to log on to a service or services.
- **The service paradigm**: A system that delivers personalized role- based, online, on-demand, multimedia (content), presence- based services to users and their devices.

V. CONCLUSION

Cloud computing offers real benefits to companies seeking a competitive edge in today's economy. Many more providers are moving into this area, and the competition is driving prices even lower. Attractive pricing, the ability to free up staff for other duties, and the ability to pay for "as needed" services will continue to drive more businesses to consider cloud computing. As described in the paper, though there are extreme advantages in using a cloud-based system, there are yet many problems which have to be solved. Several outstanding issues exist, particularly related to service-level agreements (SLA), security and privacy, and power efficiency. Every element in the cloud should be analyzed at the macro and micro level and an integrated solution must be designed and deployed in the cloud to attract the potential consumers. This paper has highlighted that cloud computing is associated with serious risks to privacy and consumer rights, and that current privacy law may struggle to address some of those risks. It has also highlighted that consumers using cloud computing products, like other cloud computing users, need to be cautious. This would be more like storing related data in different locations based on the meta-data information which would make information invaluable if a malicious intent user recovers it. Another piece of the framework would be providing Security as a Service to the applications by providing security as a single-tier or a multi-tier based on the application's requirement and addition to it, the tiers are enabled to change dynamically making the security system less predictable.

REFERENCES

[1] P. Mell and T. Grance, "Draft nist working definition of cloud computing," http://csrc.nist.gov/ groups/SNS/cloud-computing/index.html.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski,G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia,"Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep. UCB-EECS-2009-28, Feb 2009.

[3] Roger Clarke,"User Requirements for Cloud Computing Architecture", Proc. 2nd Int"l Symposium on Cloud Computing, Melbourne, IEEE CS Press, May 2010.

[4] http://thecloudtutorial.com/cloudtypes.html

[5] http://www.qualitytesting.info/group/cloudcomputing/forum/topics/infrastructu reasaservice-iaas.

[6] http://www.informit.com/articles/article.aspx?p=1234970

[7] Subashini S, Kavitha V." A survey on security issues in service delivery models of cloud computing. J Network Comput Appl" (2010), doi:10.1016/j.jnca.2010.07.006

[8] Choudhary V. Software as a service: "implications for investment in software development. In: International conference on system sciences", 2007, p. 209.).

[9] Seccombe A, Hutton A, Meisel A, Windel A, Mohammed A, Licciardi A, et al. "Security guidance for critical areas of focus in cloud computing", v2.1. CloudSecurityAlliance, 2009, 25 p.

[10] http:// www.softlayer.com/sla.html