Volume 2, Issue 5, May 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Security and Privacy Concerns in Cloud Computing

Anuj Kumar Yadav
Asst Proff CSE Dept.
DIT,Dehradun,

Ravi Tomar
Asst Proff CSE Dept.
DIT,Dehradun,

Deep Kumar
Asst Proff CSE Dept.
DIT,Dehradun,

Himanshu Gupta
Asst Proff CSE Dept.
DIT,Dehradun,

Abstract— **Nowadays cloud computing can be viewed as a Buzzword. Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. It extends Information Technology's (IT) existing 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 IT industry.**

But as more and more information on individuals and companies are placed 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 reluctant to deploy their business in the cloud. Security is one of the major issues which reduces the growth of cloud computing and complications with data privacy and data protection continue to plague the market. In this paper, a survey of the different security risks that pose a threat 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,TLS

I. INTRODUCTION

This document is a template. An electronic copy can be downloaded from the conference website. For questions on paper guidelines, please contact the conference publications committee as indicated on the conference website. Information about final paper submission is available from the conference website.

Cloud Computing has been envisioned as the next generation architecture of IT enterprise, 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 information technology would have found it virtually impossible to avoid coming across the term 'cloud computing' in recent times. 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 control of the user;
- Some of the resources on which the service depends are 'virtualised', 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;
- The security of the data provided;

- The legality (under the consumer's local law) 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 future needs; and
- Violating 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:

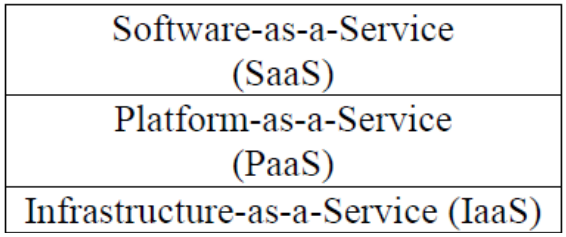

Figure 1: Service types of cloud computing.

A. 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.coms offering in the online Customer Relationship Management (CRM) space. Other examples are online email providers like Googles gmail and Microsofts hotmail, Google docs and Microsofts online version of office [4].

B. 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 interfaces (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.

C. 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 MODELS OF CLOUD COMPUTING

While cost 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 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

A. *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.

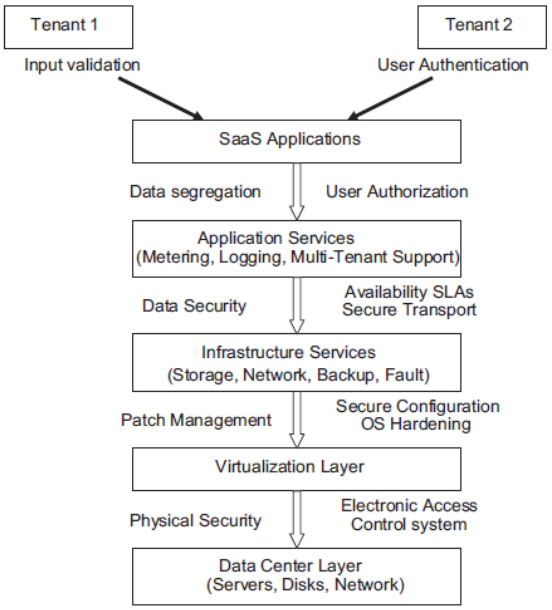

Figure 2. Security for the SaaS

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.

- ***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.

- ***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.

- ***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 utmost importance in many enterprise architecture[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.

- ***Back up***

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 in S3 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.

- ***Data Breaches***

Since data from various users and business organizations lie together in a cloud environment, breaching into the cloud environment will potentially attack the data of all the users. Thus the cloud becomes a high value target [11]. In the Verizon Business breach report blog it has been stated that external criminals pose the greatest threat (73%), but achieve the least impact (30,000 compromised records), resulting in a Psuedo Risk Score of 67,500. Insiders pose the least threat (18%), and achieve the greatest impact (375,000 compromised records), resulting in a Pseudo Risk Score of 67,500. Partners are middle in both (73.39% and 187,500) resulting in a Pseudo Risk Score of 73,125. Though SaaS advocates claim that SaaS providers can provide better security to customers' data than by conventional means, Insiders still have access to the data but it is just that they are accessing it in a different way. Insiders do not have direct access to databases, but it does not reduce the risk of insider breaches which can be a massive impact on the security. The SaaS providers' employees have access to a lot more information and a single incident could expose information from many customers. SaaS providers must be compliant with PCI DSS (Payment Card Industry—Data Security Standards) [12] in order to host merchants that must comply with PCIDSS.

- ***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.

B. *Security issues in PaaS*

In PaaS, the provider might give some control to the people to build applications on top of the platform. But any security below the application level such as host and network intrusion prevention will still be in the scope of the provider and the provider has to offer strong assurances that the data remains inaccessible between applications. PaaS is intended to enable developers to build their own applications on top of the platform. As a result it tends to be more extensible than SaaS, at the expense of customer-ready features. This tradeoff extends to security features and capabilities, where the built-in capabilities are less complete, but there is more flexibility to layer on additional security.

Applications sufficiently complex to leverage an Enterprise Service Bus (ESB) need to secure the ESB directly, leveraging a protocol such as Web Service (WS) Security. The ability to segment ESBs is not available in PaaS environments. Metrics should be in place to assess the effectiveness of the application security programs. Among the direct application, security specific metrics available are vulnerability scores and patch coverage. These metrics can indicate the quality of application coding. Attention should be paid to how malicious actors react to new cloud application architectures that obscure application components from their scrutiny. Hackers are likely to attack visible code, including but not limited to code running in user context. They are likely to attack the infrastructure and perform extensive black box testing. The vulnerabilities of cloud are not only associated with the web applications but also vulnerabilities associated with the machine-to-machine Service- Oriented Architecture (SOA) applications, which are increasingly being deployed in the cloud.

C. *Security issues in IaaS*

With IaaS the developer has better control over the security as long as there is no security hole in the virtualization manager. Also, though in theory virtual machines might be able to address these issues but in practice there are plenty of security problems . The other factor is the reliability of the data that is stored within the provider's hardware. Due to the growing virtualization of 'everything' in information society, retaining the ultimate control over data to the owner of data regardless of its physical location will become a topic of utmost interest. To achieve maximum trust and security on a cloud resource, several techniques would have to be applied. The security responsibilities of both the provider and the consumer greatly differ between cloud service models. Amazon's Elastic Compute Cloud (EC2) infrastructure as a service offering, as an example, includes vendor responsibility for security up to the hypervisor, meaning they can only address security controls such as physical security, environmental security, and virtualization security. The consumer, in turn, is responsible for the security controls that relate to the IT system including the OS, applications and data [13].

IV. IMPACT OF DEPLOYMENT MODEL IAAS

IaaS is prone to various degrees of security issues based on the cloud deployment model through which it is being delivered. Public cloud poses the major risk whereas private cloud seems to have lesser impact. Physical security of infrastructure and disaster management if any damage is

incurred to the infrastructure (either naturally or intentionally), is of utmost importance. Infrastructure not only pertains to the hardware where data is processed and stored but also the path where it is getting transmitted. In a typical cloud environment, data will be transmitted from source to destination through umpteen number of third-party infrastructure devices .

Although cloud architecture is an improvised technology, the underlying technologies remain the same. The cloud is just built over the internet and all the concerns related to security in internet are also posed by the cloud. The basis of the cloud technology makes the consumer and provider reside at different location and virtually access the resources over the Internet. Even if enormous amount of security is put in place in the cloud, still the data is transmitted through the normal underlying Internet technology. So, the security concerns which are threatening the Internet also threaten the cloud. But, in a cloud, the risks are overwhelmingly high. This is because of its vulnerability and the asset value of the resources and their nature of them residing together. Cloud systems still uses normal protocols and security measures that are used in the Internet but the requirements are at a higher extent. Encryption and secure protocols cater to the needs to a certain extent but they are not context oriented. A robust set of policies and protocols are required to help secure transmission of data within the cloud. Concerns regarding intrusion of data by external non users of the cloud through the internet should also be considered. Measures should be set in place to make the cloud environment secure, private and isolated in the Internet to avoid cyber criminals attacking the cloud.

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/for um/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.htmlS

[11]./http://www.cio.com/article/ 492695/Defining_Private_Clouds_Part_OneS

[12].https://www. pcisecuritystandards.org/security_standards/download.html?id=pci_dss_v1-2. pdfS

[13]. 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.).

