International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 04
February 2018

Security Challenges and Threats in Cloud Computing Systems

G. Radha Devi
Research Scholar, Department of CSE
Sri Satya Sai University of Technology & Medical Sciences, Sehore, Bhopal, MP (India)

Abstract—*Cloud Computing has emerged as a new paradigm of computing that builds on the foundations of Distributed Computing, Grid Computing, and Virtualization. Cloud computing is Internet-accessible business model with flexible resource allocation on demand, and computing on pay-per-use as utilities. Cloud computing has grown to provide a promising business concept for computing infrastructure, where concerns are beginning to grow about how safe an environment is. Security is one of the major issues in the cloud-computing environment. In this paper we investigate some prime security attacks and possible solutions for clouds: XML Signature Wrapping attacks, Browser Security, and Vendor Lock-in.*

Keywords--Cloud Computing, Web Service Security, SOAP message, Service Oriented Architecture, XML Signature Wrapping Attacks, Browser Security, Lock in, Security Techniques.

I. INTRODUCTION

Cloud Computing has emerged as a very well-known technique to support large and voluminous data with the help of shared pool of resources and large storage area. Cloud computing is a new computing paradigm that is built on virtualization, distributed computing, utility computing and service-oriented architecture. Further it is added that cloud computing has emerged as one of the most significant paradigm of the IT industry and has attracted most of the industry and academia. “Cloud computing is a model for enabling ubiquitous, 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.”

Cloud computing, indeed, is a wide-ranging term that transmits hosted services over the Internet. These hosted services are generally separated into three broad categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). The internet is usually represented as the “Cloud”.

A cloud service is generally used by the clients as and when needed, normally on the hourly basis. This “on-demand” or “pay as you go” approach makes the cloud service flexible, where end user can have a great deal or modest of a service the way they desire at any point of time and the service is entirely administered by the provider. Noteworthy improvements in each key components included virtualization, distributed computing and also the improved access to high-speed internet facility as well as weak economy have speeded up the inflate of cloud computing rigorously.

A cloud can either be a private or a public. Public cloud exist when a third party is offering computing resources as a service, while in a private cloud a sole user will own and operate the computing resources. Thus a public cloud sells services to any person residing on the Internet. At present, Amazon Web Services is the major public cloud provider. A private cloud is an authorized network or a data centre that provides hosted services to a restricted number of individuals. When a service provider uses public cloud resources to produce their private cloud, the result is called as a virtual private cloud. For a cloud computing, the main aim is to offer a scalable and a very easy admittance to computing resources and Information Technology services.

Cloud computing has spawned a very noteworthy interest in both academia and industry, but it is still a budding theory. In essence, it aims to combine the fiscal utility model with the evolutionary expansion of various existing advances and computing technologies. It even unites various distributed services, as well as applications and information infrastructures that consist of groups of computers, storage resources and networks. Confusion exists in IT communities about how a cloud differs from existing models and how these differences affect its adoption. Some visualize a cloud as a novel technical revolution, while others consider it a natural evolution of technology, economy and culture.

As cloud computing comprehends the idea of computing as an efficacy, providers are developing a mutual-shared group of configurable resources, which clients can vigorously condition and liberate according to their varying needs. Thus, both the group providers and the users would easily benefit from the reuse of computing resources and reduction in cost.

The cloud services that are implemented or those that will be implemented will always be accompanied by several threats. Knowledge about these threats shall prove to be the first step to prevent them. Hence security is the chief concern of several clients who desire to leverage cloud services. There exist some of the basic security threats that exploit the use of Cloud Computing. An easy example of this is the exercise of bot nets to spread spam and malware. The other example is the application interfaces that are required to connect to cloud services especially that are developed by third parties. These interfaces must provide the user with highly protected authentication, authorization, encryption and movement monitoring mechanisms.

2 RELATED WORK

Agrawal et al.[1] analyzed the design choices that allowed modern scalable data management systems to achieve orders of magnitude higher levels of scalability compared to traditional databases. J. Morin et al. [2] identified Cloud Computing Security issues and their corresponding challenges, proposing to use risk and Service Level Agreement (SLA) management as the basis for a service level framework to improve governance, risk and compliance in cloud computing environments.

N. Mayer et al. [3] defined the set of concepts and relationships taking a place in the ISSRM domain within a UML class diagram. The outcome of their work is the enrichment of the class diagram with attributes representing the elicited metrics.

S. Carlin et al. [4] proved that one of the biggest security worries with the cloud computing model is the sharing of resources (multitenancy). So, new security techniques need to be developed and older security techniques needed to be radically tweaked to be able to work with the clouds architecture. Plugging in existing security technology will not work because this new delivery model introduces new changes to the way in which we access and use computer resources.

Wang et al. [5] presented a brief summary on the analysis of current gaps and new trends in cloud computing research based on extant information systems literature, industry reports, and practical experience reflections. Additionally, it highlights the significance of cloud computing and its implications for practitioner and academics.

Zissis and Lekkas [6] concluded that; firstly to evaluate cloud security by identifying unique security requirements and secondly to attempt to present a viable solution that eliminates these potential threats. This paper proposes introducing a Trusted Third Party, tasked with assuring specific security characteristics within a cloud environment. The proposed solution calls upon cryptography, specifically Public Key Infrastructure operating in concert with SSO and LDAP, to ensure the authentication, integrity and confidentiality of involved data and communications.

Kuyoro et al. [7] introduced a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing types and the service delivery types. In this paper key security considerations and challenges which are currently faced in the Cloud computing are highlighted. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future.

Mishra et al. [8] brought their own security concerns to the already large list of cloud computing. As multi-tenancy, virtualization comes with its own issues. The hypervisor provides a new attack surface to be compromised; and the virtual network enables a malicious VM to perform attacks on other VMs avoiding traditional network security controls. The movement to the Cloud could mean an improvement in security to many organizations. New robust security controls will be required in order to assure proper security with the de-parameterization, and to be compliant with the everyday more strict laws and regulations.

Finally, [9] presented a framework for web-based interactive scalable network visualization. WiNV enables a new class of rich and scalable interactive cross-platform capabilities for visualizing large-scale networks natively in a user's browser. This allows visualizing cloud security configurations and detecting potential holes.

III. SECURITY CHALLENGES IN CLOUD COMPUTING

Although cloud computing systems are capable enough for organizations to share information and services using internet without any need of physical infrastructure, it is vulnerable for security threats which must be solved. As information and services are shared on internet, there is a strong need to understand the different issues associated with it. There are following security challenges of cloud computing.

Confidentiality

Confidentiality can be defined as the ability for an authorized group of users or authorized systems to access protected data [4]. The increase in number of users of cloud computing systems helps in increasing the access points; hence the data becomes more exposed to external entities and more likely to be compromised [4].

1) Data Confidentiality: Data confidentiality is all about to provide access control to the data, memory and devices. It is the property that data contents are not made available or disclosed to illegal users. Therefore, we need to provide a strong secure

verification system which may leads to secured access within Cloud services [4].

2) Application Confidentiality: Cloud services also provide access for software applications eliminating the needs of installing them at every system. Hence, application security can be another important factor for providing a secure cloud system [4].

Privacy

Privacy is the ability of individual user/system or group of users/systems to control the sharing of data to other users or systems. Individuals are required to follow rules set by governments concerning user's personal data privacy and confidentiality. Because, data is stored on multiple locations in cloud network, they are vulnerable to security breaches [4].

Integrity

Data integrity can be defined as the means to protect data, services and application from unauthorized modification and deletion in cloud computing systems. Data integrity can be divided into following two categories:

1) Data Integrity: Data integrity is protecting data from unauthorized deletion and modification. The cloud service provider should ensure the users that personal data are not manipulated in between. Data integrity is very important factor in order to achieve a high level of confidentiality in data and system integrity. As number of users increase, number of access points to access cloud services increases, which, in turn, requires authorized access [4].

2) Software Integrity: Software integrity is basically restricting the unauthorized access and modification in software applications provided by cloud systems. The software application owner or administrator is responsible for software integrity from unauthorized modification [4].

Availability

Availability refers to the ability of an authorized user to access a cloud system and use it to share information, use cloud resources and application even with a security interruption or a system malfunction [4]. Availability includes the availability of data, applications and physical components on request of end user [4].

IV.POSSIBLE SECURITY APPROACHES

In this section we discuss possible solutions/ countermeasures for the three most probable technical security threats in cloud computing: XML Signature Wrapping attacks, browser security, lock in.

XML Signature Wrapping attacks We would suggest use of other protocols, like use of Representational State Transfer (REST) instead of SOAP. REST provides encryption of data using many formats, unlike SOAP, which offers only the use of XML. In addition, companies can consider educating cloud computing developers on how they can best preempt XML attacks while they are designing cloud services. The rapid adoption of cloud computing services indicates a positive step towards reducing capital cost and increasing efficiency of service delivery. However, there is a need for companies providing cloud services to strengthen their security mechanisms because successful cloud computing attacks such as XML signature wrapping could be detrimental.

A. Browser Security

The browser security issue can be handled and counter measured by the following possible solutions: 1- Using Web Services Security (WS-security) concept on web browsers because WS-security works within message level as M. Jensen has shown [4] [10]. In this case, web browsers can use XML Encryption to have end-to-end encryption (Fig 8) in SOAP messages where there is no need for decryption at intermediated hosts. Therefore, attackers can't sniff and get the decrypted SOAP messages (plaintext of SOAP messages) at the intermediary hosts. In other words, SOAP messages get encrypted and decrypted one time, unlike point-to-point communications process encryption where they get encrypted and decrypted many times.

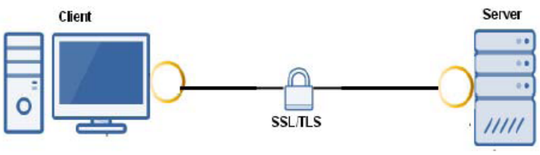


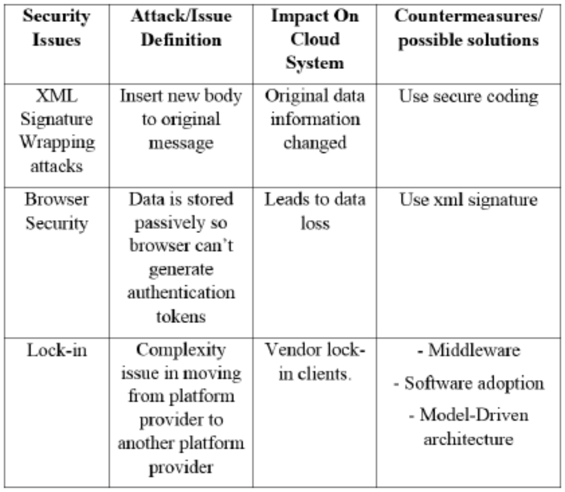
Fig 1.The SOAP message will be encrypted and decrypted one time during the supports end-to-end communications process

Fig 1.The SOAP message will be encrypted and decrypted one time during the supports end-to-end communications process 2- Steve Kirsch [12] states that in his opinion, the potential solution to solve the problem is that the user should have single identity that must allow for numerous levels of assurance that can be accomplished by getting certain requirements to obtain approvals digitally such as a PIN code or out of-band approval. He thinks that the user doesn't need to manage different identities but a single identity is enough to satisfy the security needs of both the provider and user.

B. Lock-in

One of the preferred solutions for avoiding vendor lock-ins lies in software adaptation. Software adaptation is a process of defining and arranging existing third-party application elements, and components or services with the view of removing mismatch when used in new systems. Adaptors for every cloud platforms mismatching parts are made to interoperate successfully, hence, eradicating vendor lock-ins. Adaptors are designed on four levels: signature, behavioral, service level, and semantic level. In signature interoperability, problems such as names, parameters and frameworks are streamlined. Behavioral interoperability target protocol mismatch and service level interoperability deals with service requirements such as QoS and security. Finally, semantic interoperability solves conceptual issues of what every component or service needs to do. Another proposed technique that follows this solution is Model-Driven Architecture. According to Model-Driven Engineering to Program Transformation, software to be migrated from one platform to the other goes through a number of phases including discovery, transformation and migration. The discovery stage involves recognizing the discovery sources that need to be worked. The transformation phase involves adaptation of the software platform to be transferred to. The migration phase involves testing the transformed component to establish suitability in the new platform before final deployment.

Another approach that follows the same technique is the Refactoring Approach. Refactoring is the process of altering software components in a way that does not affect external workings. The software is refurbished without changing the external behavior of the code while enhancing its structure to the new platform. Of the three proposals, Model-Driven architecture is the best. This is because the model provides developers with authority to choose which cloud framework to choose from and derive cloud specific settings. The source codes resulting from the tool will create a preconfigured cloud characteristic with the metadata in it. The model does not require adaptations that impact performance and QoS. After identifying and evaluating the solutions for risks and issues that affect the security of the web application in the cloud, we have come up with the following countermeasures. See in Table 1.



Security Issues	Attack/Issue Definition	Impact On Cloud System	Countermeasures/ possible solutions
XML Signature Wrapping attacks	Insert new body to original message	Original data information changed	Use secure coding
Browser Security	Data is stored passively so browser can't generate authentication tokens	Leads to data loss	Use xml signature
Lock-in	Complexity issue in moving from platform provider to another platform provider	Vendor lock-in clients.	- Middleware - Software adoption - Model-Driven architecture

Table 1: Common technical security issues in Cloud Computing and their highly efficient possible solutions

V.CONCLUSIONS

As described in the paper, you can see there are many advantages and benefits of using a cloud system, yet there are numerous issues that still have loose ends that might scare away certain users. These issues have to be solved.

In this paper, we presented a selection of issues of Cloud Computing security, such as XML Signature Wrapping attack, Browser Security, and Lock in. We identified the issues and evaluated existing possible solutions to those issues to choose the best one of them, as shown in Table 1.

References

[1] D. Agrawal, A. El Abbadi, S. Antony, and S. Das. Data Management Challenges in Cloud Computing Infrastructures. In DNIS, 2010.

[2] Morin, J. H., Gateau, B.: Towards Cloud Computing SLA Risk Management: Issues and Challenges. In 45th Hawaii International Conference on System Sciences, 2012

[3] N. Mayer, E. Dubois, R.Matulevicius, and P. Heymans. Towards a Measurement Framework for Security Risk Management. In Proceedings of Modeling Security Workshop, 2008.

[4] Carlin, S. and K. Curran, “Cloud Computing Security,” International Journal of Ambient Computing and Intelligence, Vol. 3, No. 1:14-19, 2011.

[5] Wang, W., Rashid, A., & Chuang, H.-M. (2011). Toward the Trend of Cloud Computing. Journal of Electronic Commerce Research, 12(4), 238–242.

[6] Zissis, D., and D. Lekkas (2010) “Addressing Cloud Computing Security Issues,” Future Generation Computer Systems (28)3, pp.583-592 , , doi: 10.1016/j.future.2010.12.006.

[7] Kuyoro S. O. et.al., Cloud Computing Security Issues and Challenges, International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011, 247-255.

[8] Ankur Mishra, Ruchita Mathur, Shishir Jain, Jitendra Singh Rathore, 2013 “Cloud Computing Security” International Journal on Recent and Innovation Trends in Computing and Computation, pp 36-39

[9] H. Gobjuka and K. Ahmat, WiNV: A Framework for Web-based Interactive Scalable Network

Visualization, in Proc. IEEE INFOCOM Demo Session, 2010.

About Author

G. Radha Devi
Research Scholar
Department of CSE
Sri Satya Sai University of Technology and Medical Sciences Bhopal MP (India)