International Journal of Information Technology and Management

Vol. VII, Issue No. IX, August-2014, ISSN 2249-4510

SECURING THE E-WORLD THROUGH CLOUD COMPUTING A REVOLUTIONARY TECHNIQUE AND APPLICATIONS

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

International Journal of Information Technology and Management
Vol. VII, Issue No. IX, August-2014, ISSN 2249-4510

Securing the E-World through Cloud Computing a Revolutionary Technique and Applications

G. A. Patil[1]* Dr. V. A. Athavale[2]

[1] Research Scholar, Singhania University, Jhunjhunu, Rajasthan

[2] Director, Gulzar Group of Institutes, Ferozepur

Abstract – This paper presents securing the E-world through Cloud Computing. Cloud computing has rapidly become one of the most famous buzzwords in the IT world due to its revolutionary model of computing as a usefulness. It promises greater than before suppleness, scalability, and reliability, while talented decreased operational and hold up costs. Cloud computing is a revolutionary concept that has brought a paradigm shift in the IT world. This has made it likely to manage and run businesses with no even setting up an IT infrastructure. It offers multifold benefits to the users moving to a cloud, while posing unknown security and privacy issues. User verification is one such on the increase anxiety and is greatly needed in order to make sure privacy and security in a cloud computing environment. The paper also discusses the security at different levels viz. network, application and virtualization, in a cloud computing surroundings. A security framework based on one-time pass key mechanism has been proposed. The individuality of the future security protocol lies in the fact, that it provides security to both the service providers as well the users in a highly conflicting cloud environment

Keywords: Cloud Computing, Security, Revolution, Authentication, Network, Cloud Environment

----------♦----------

INTRODUCTION

The Cloud, as it is often referred to, involves using computing resources – hardware and software – that are delivered as a service over the Internet. Organizations are no longer required to build their own IT infrastructure. Instead, they are presented with an alternative to host their data on a third party system such that they would be able to access the same by means of Internet. Cloud computing is gaining popularity due to the features that include scalability, multi-tenancy and reduced hardware and maintenance cost. Cloud technologies are enabling the users with multifold facilities but at the same time, they bring additional security and privacy issues. The rate at which cloud technologies are being adopted, it has become imperative to analyze the service offerings from different cloud service providers (CSPs) and then decide their suitability based on the organization's needs and requirements.

Cloud computing can be defined as one of the most popular trends in the history of online computing that has taken the world by a surprise. It offers a flexible IT architecture, enabling its users to be able to use services which would have been considered impossible in case of standard IT based solutions.

A cloud based architecture can be defined as a set of resources - hardware and software, which combine together to deliver the aspects of computing as a service. Services in such a scenario are charged on a usage based pricing model and the users are no longer required to care about the intricacies which are needed to be taken care in a traditional on-premise computing model.

Data mining technology and services refer to yet another interesting domain that has caught the attention of researchers in the recent times. It is the process of analyzing data from different perspectives and summarizing it into useful information. It finds a great deal of use in business and economics.

Cloud sculpt

Scaffold for investigate security in the cloud

Beginning in the 1980s, governmental initiatives were established around the world to define requirements for evaluating the effectiveness of security functionality built into computer systems. In 1996, initiatives from the US, Europe, and Canada were combined into a document known as the Common Criteria. The Common Criteria document was approved as a standard by the International Organization for Standardization in 1999 and has opened the way for worldwide mutual recognition of product security solutions [4].

The Common Criteria, however, serve primarily as a benchmark for security functionality in products [4]. For this reason, IBM consolidated and reclassified the criteria into five functional security subsystems. I have used these subsystems as the framework within which I assess the security issues present in cloud computing and evaluate solutions proposed.

The five functional security subsystems defined by IBM are as follows:

a. Audit and Compliance: This subsystem addresses the data collection, analysis, and archival requirements in meeting standards of proof for an IT environment. It captures, analyzes, reports, archives, and retrieves records of events and conditions during the operation of the system [4].

b. Access Control: This subsystem enforces security policies by gating access to processes and services within a computing solution via identification, authentication, and authorization [4]. In the context of cloud computing, all of these mechanisms must also be considered from the view of a federated access control system.

c. Flow Control: This subsystem enforces security policies by gating information flow and visibility and ensuring information integrity within a computing solution [4].

d. Identity and Credential Management: This subsystem creates and manages identity and permission objects that describe access rights information across networks and among the subsystems, platforms, and processes, in a computing solution [4]. It may be required to adhere to legal criteria for creation and maintenance of credential objects.

e. Solution Integrity: This subsystem addresses the requirement for reliable and proper operation of a computing solution [4].

SECURITY IN THE CLOUD

Security in a cloud environment can be broadly classified into three categories:

- Network level security
- Application level security and
- Virtualization security

It has been observed at multiple instances that the active cloud virtual machine instances are accessible through public cloud and allow hackers to leverage this opportunity to carry out DoS attacks. Cloud instances running on public cloud are most prone to these types of attacks and hence require a network level access control solution that would enable the delivery of cloud services in a highly protected environment. A detailed analysis of network level attacks has been carried out in [2]. The authors have gone on to propose a network based access control solution that provides additional security against such types of attacks. A few of the security threats that could be classified as network level attacks include: DoS attacks, DDoS attacks, Sniffer attacks, BGP prefix hijacking, DNS attacks, Man in the Middle attacks etc. A detailed analysis of these types of attacks has been carried out in [1].

Application level security refers to securing applications from any type of security attack in a cloud computing environment. Application security is important in the sense that it can be exploited to extract sensitive information or nefariously used to make inappropriate changes to important data. An evaluation model that can be used to assess the risks in moving a service to the cloud has been presented in [3]. The authors have focused on integrating end to end services in a secure manner in a cloud computing model.

Virtualization security refers to securing a VM or a hypervisor in a highly virtualized and distributed cloud environment. In a virtualized environment, hypervisor is defined as a virtual machine monitor that allows many VMs to be deployed on a single OS or multiple operating systems to run on a system at the same time.

DELIVERY MODELS:

- **Cloud Software as a Service (SaaS)**: Customers rent software hosted by the vendor;
- **Cloud Platform as a Service (PaaS)**: Customers rent infrastructure and programming tools hosted by the vendor to create their own applications;
- **Cloud Infrastructure as a Service (IaaS)**: Customers rent processing, storage, networking and other fundamental computing resources for all purposes.

DEPLOYMENT MODELS:

- **Private cloud**: The cloud infrastructure is owned or leased by a single organization and is operated solely for that organization.
- **Community cloud**: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations).
- **Public cloud**: The cloud infrastructure is owned by an organization selling cloud services to the general public or to a large industry group.
- **Hybrid cloud**: The cloud infrastructure is a composition of two or more clouds (internal, community, or public) that remain unique entities but are bound together by standardized or proprietary technology).

CONCLUSION

In this paper we have analyzed that the cloud providers exist in the market today, so the cloud paradigm has already overcome its initial security hurdles and moved from theory into reality. However, current cloud providers have provided extremely proprietary solutions for dealing with security issues. Experienced business managers know that Cloud Computing, like most trends and new concepts in the industry, has a tendency to be overhyped. That can create unrealistic expectations and disappointing results from early adopter and first implementations. The best way to prevent this at network, application and virtualization level to have a realistic plan for Cloud Computing adoption, one that assures the applications being targeted are the ones with the best potential for generating benefits.

REFERENCES

[1] Rohit Bhadauria, Sugata Sanyal, “Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques”, Intl. Journal of Computer Applications, Vol. 47, No. 18, pp. 47-66. Published by Foundation of Computer Science, New York, USA

[2] Kirk Beaty, Ashish Kundu, Vijay Naik, Arup Acharya, “ Network-level Access Control Management for the Cloud,” Cloud Engineering (IC2E), 2013 IEEE International Conference on , vol., no., pp.98,107, 25-27 March 2013

[3] George Mathew, “Elements of Application Security in the Cloud Computing Environment,”. Open Systems (ICOS), 2012 IEEE Conference on, pp. 1-6. IEEE, 2012.

[4] IBM Corporation, *Enterprise Security Architecture Using IBM Tivoli Security Solutions*, Aug 2007.

[5] An Essential Guide to Possibilities and Risks of Cloud Computing-A Pragmatic Effective and Hype Free Approach for Strategic Enterprise Decision Making by By Maria Spinola June 2009 http://www.mariaspinola.com

[6] Rohit Bhadauria, Rajdeep Borgohain, Abirlal Biswas, Sugata Sanyal “Secure Authentication of Cloud Data Mining API”

[7] Survey of Security Issues in Cloud Computing by Uttam Thakore

Corresponding Author

G. A. Patil*

Research Scholar, Singhania University, Jhunjhunu, Rajasthan