American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-4, Issue-9, pp-188-191
www.ajer.org
Research Paper Open Access

Security and Architectural Patterns for Securing the Cloud Architecture

Golajapu Venu Madhava Rao[1], Venu Madhav Kuthadi[2], Rajalakshmi Selvaraj[3]
[1]Department of Network and Infrastructure, Faculty of Computing, Botho University, Botswana
[2]Department of Applied Information Systems, University of Johannesburg, South Africa
[3]Department of Information Systems, BIUST, Botswana

ABSTRACT: *Operating a cloud securely and efficiently entails a great deal of advanceplanning. A data center and redundant internet connection is required at the beginning to connect to cloud. This can constitute the technology portion of an information security and some network devices that safely and securely serve the communication. National Institute of Standards and Technology states that the process of uniquely assigning the information resources to an information system will define the security boundary for that system. A massive amount of gear that is racked and cabled following defined patterns is enabled inside this boundary. Need for the infrastructure that is used to manage the cloud and its resources as it operates the cloud. Each component like server, network and storagerequires some degree of configuration. While designing or planning a complex systemit is important to look ahead the process and procedures required for operation of the system. Small cloud systems can be build without much of planning. But any Cloud system substantially bigger size needs significant planning and design. If we fail to plan it leads to higher cost due to inefficiency in design and process. In this paper we study on the architectural components that can be used to build a cloud with security as a priority. This can be achieved by identifying requirements for secured cloud architecture along with key patterns and architectural elements. This paper first discusses on security patterns and an architectural element required and also focuses on several different cloud architectures and secure cloud operation strategies.*

***KEYWORDS*:** Cloud, Security, Architecture, network, process.

I. INTRODUCTION

Implementing a cloud computing architecture ultimately is the next generation in cost management -- a shifting of traditional IT platforms to a resource-efficient, dynamic, hosted framework. Although this cost-based view of the cloud dominates the dialogue on cloud adoption, it falls short of the complete picture [1].Beyond cost organizations are looking to implement a cloud computing architecture to enhance worker productivity. To these organizations, the biggest benefit of implementing a cloud computing model is the model's ability to apply IT tools faster and more flexibly. Organizations want flexibility in presenting application services to users and in assigning applications to resources based on cost and other metrics. This means looking at the overall IT architecture specifically the network in a whole new way.

All cloud computing models have three key components: access, resource pools and address mapping[2]. The access component lets users connect with the applications they need. Resource pools support the servers and storage that users can draw on to run those applications. The address mapping component links elastic resource locations with such references as URLs; these allow users to access applications no matter where they run. Access networks typically are built on routing and VPNs. Resource pools typically are supported on data center networks built on the Ethernet and virtual local area networks, or VLANs. The technologies of these two areas will expand as the private cloud is built, but the real change will be in address mapping. This is what will connect users to the applications that now are running in a dynamic resource pool. Address mapping demands a level of network flexibility that's beyond the typical needs of static internal IT hosting or even Internet hosting. Without network flexibility, a cloud computing model's dynamism is lost.

In fact, it's the network that builds the cloud. Enterprise networks include data center LANs; storage area networks; Internet tunnels; and WANs built on switching, routing and a VPN or Virtual Private LAN Service. These network components are more costly than cloud software stacks, and making a mistake in the network part of cloud-building could be absolutely fatal to security and availability. What we call the private cloud computing model is the one that will guide all future IT investment. It's the first model that recognizes the fusion of business and IT, public and private resources, networks and software. It's a model that's very different from the Internet or from the current enterprise data center, but it's also a model that can be built from current infrastructure components and can provide both immediate and sustainable benefits in IT return on investment and worker productivity.

II. SECURITY REQUIREMENTS FOR CLOUD ARCHITECTURE

This section focus on the key architectural requirements for a cloud implementation [3]. The main aim of the cloud architecture is shown in fig.1andshould be appropriate to meet the needs of the cloud.

(1) Costs and Resources: The investment on technology and security controls will depend on cloud providers financial resources towards its implementation. The motivation factor for the customer towards the cloud services is cost. This constraint in the development and operation of the services will not be ideal to all the customers.

(2) Reliability: The underlying technology which provide delivery of services to a certain degree.

(3) Performance: This refers to usefulness of the system that includes responsiveness to the input and throughput the system can handle[4]

(4) Security: Confidentially, Integrity and Availability security principles are applicable to most of the systems and the responsibility is to match with the security requirements which must be derived from reliability performance and cost.

(5) Legal and regulatory constraints: Legal and regulatory constraints can lead to need for many additional requirements having to do with technical security controls, access polices, and retention of data among many others.

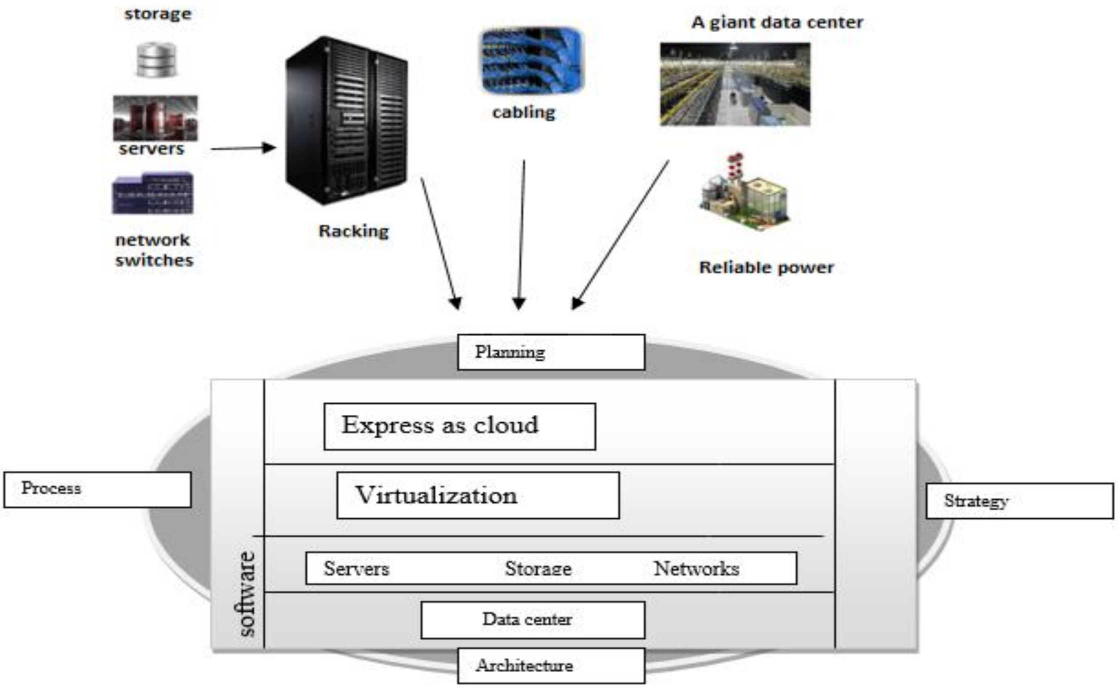

Fig 1: Cloud architecture and implementation

2.1 Cloud Security Standards and Policies

Requirements for cloud security should be consistent with appropriate standards such as International Organization for Standardization (ISO). All security requirements should derive from standard security policies. The policy should explain the need for the standard encryption methods should be used. The security policy should also have several supporting documents like guidelines for enabling security in development of infrastructure software, management processes and operational procedures. It should also contain an acceptable use policy for each category of user. A set of security standards for cloud should includes : Access controls, Incident Response and management, System and network configuration backups, security testing, data and communication encryption, password standards and continuous monitoring.

2.2Requirements of Cloud Security

Security architecture of the cloud should be consistent as per the security policies mentioned in above section. A security policy for the cloud is one of the security requirements. A separate set of activities will revolve around identifying granular requirements that are preliminary in developing the cloud security architecture. On cloud architecture there are certain representative security requirements which are likely to apply are given below.

2.3 Cloud-Wide Time service

All systems must be synchronized to the same time source by using Network Time Protocol (NTP). When communicating computers reside in different locations correct and synchronized time is very important. The records and event time-stamps synchronized to a single source. A cloud infrastructure us subjected to all manner of errors and made difficult to diagnose failuresif the clock drift between network devices or computers. Correct time information comes from authoritative national time standards through various paths which will include radio, satellite, cellular and hard-wired transmission to primary time servers. It is distributed through NTP subnets to millions of secondary servers and from there to end-clients. NTP provides coordinates Universal Time(UTP) all times zones or daylights saving time information must be provided separately. Some of the best practices to be followed for managing NTP are configure clients to reference at least two time servers to provide redundant time. Accurate time synchronization depends on how frequently clients update their time from time servers.Limit input network or radio broadcast signals to authoritative and legal ones.

2.4 Identity Management

Identity is key element in the security of operating the cloud. The information must be correct and available to cloud components that have a validated need for access.Requirements include controls to protect confidentiality, integrity and availability of identity information. Implement an identity management system that will support needs for authenticatingcloud personal, support the larger scale needs for authenticating cloud tenants and users.

2.5 Access Management

Access controls use identity information to enable and constrain access to an operating cloud and its supporting infrastructure. Cloud personnel shall have restricted access to customer data in general. Cloud personnel may require access to a hypervisor on a customer allocated machine or to storage devices that host customer VMs or customer data but such access shall be tightly constrained and limited to specific operations that are well defined by security policy and SLAs.We can implement multifactor authentication for highly privileged operations with additional security controls. Authorization mechanism for cloud management are constrained and do not allow for cloud wide access.

2.6 Requirements of Key Managements

In a cloud encryption is a primary means to protect at rest and between storage and processing phases. Ensure that appropriate controls are in place to limit access to keying material that the cloud provider maintains control over. Ensure that root level and signing keys are managed appropriately.

2.7 System and Network Auditing

To manage the ongoing security of any system in cloud audit evens will be generated at different trust zones like infrastructure system and network components. All security relevant events must be recorded and generated audit events must be logged in a near-real-time manner. All audit events logs shall be continually and centrally collected to make sure the integrity and to support timely altering and monitoring.

III. SECURITY MONITORING

Security monitoring[5] shall include the generation of alerts based on automated reorganization that critical security event or situation has taken place or is detected. Delivery of critical alerts in timely manner. Implement a cloud wide intrusion and anomaly detection capability and consider this as a service for tenants or users. The fig. 2shows the overview of security event management and relativity to security monitoring.

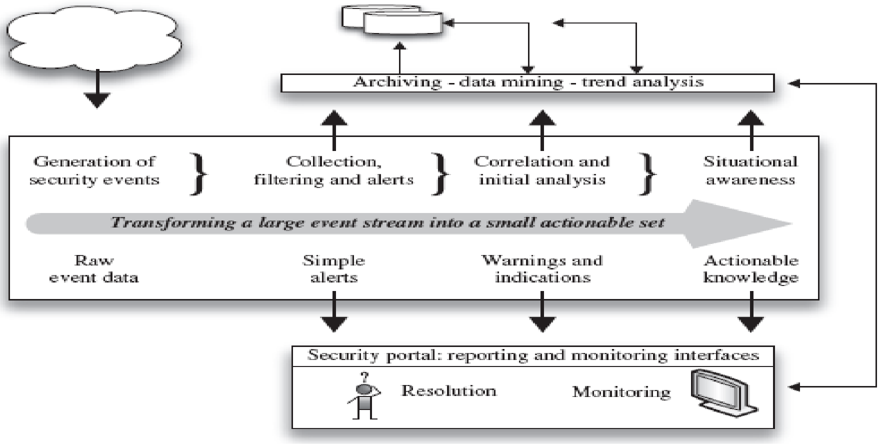
Archiving - data mining - trend analysis
Generation of security events
Collection, filtering and alerts
Correlation and initial analysis
Situational awareness
Transforming a large event stream into a small actionable set
Raw event data
Simple alerts
Warnings and indications
Actionable knowledge
Security portal: reporting and monitoring interfaces
Resolution
Monitoring

Fig2: Security event management and monitoring

The requirements for system and network controls are to ensure proper isolation, configuration and security for security components. Implementation of network isolation between functional areas in the cloud computing infrastructure. Implement completely separate networks which include use of physical separation and network virtualization for public accessible components. Use other network controls and also software firewalls on machines.

IV CLOUD OPERATION STRATEGIES

The technique for honeypot[6][7][8]can be applied for cloud computing. A honeypots virtual machinecan be deployed and then used to monitor and report on any attempt to access it. Sandboxes isused at the software layer. It is a form of virtualization or abstraction between the software and code executed between the operating system.As per the cloud architecture [3] it is wise to design for mutually reinforcing controls to increase assurance. For defense in-depth for access control mechanisms it might require to use VPN for remote administrative access. A VPN connection attempt may be shunned by the ingress router for source IP. The use open system access control for remote administrative users could require use of a dynamically changing code that is owned by remote administrator.

The various types of private, public, SaaS, PasS, IaaS, providers and technologies associated with all these types of architectures are Amazon Web Services, Amazon virtual private cloud, RackSpace cloud Hosting, GoGrid, Salesforce.com, Google Apps engine. VMware, Microsoft Hyper-V. The key strategies for cloud secure operations can be achieved by classifying data and systems and defining the valid roles for cloud personal and customers[9].

V CONCLUSION

The key architectural requirements for cloud implementation are discussed in the initial sections. Cloud security standards and policies should meet the ISO standards. All policies should derive from ISO. Security policy itself is one of the key security requirements in cloud. Security techniques like honeypots and sandboxes can be implemented in cloud computing architecture to monitoring and reporting. The key strategy for secure cloud operation can be achieved by classifying data and systems and defining the valid roles for cloud personal and customers.

REFERENCES

[1] R. Schwarzkopf, M. Schmidt, Ch. Strack, S. Martin and B. Freisleben . Increasing virtual machine security in cloud environments.*Journal of Cloud Computing: Advances, Systems and Applications*, Springer, 2012, 1–12.

[2] K. Hashizume, Nobukazu Yoshioka, and E. B. Fernandez . Three Misuse Patterns for Cloud Computing. *Security Engineering for Cloud Computing: Approaches and Tools*, IGI Global, 2013, 36–53.

[3] Vic (J.R) Winkler, *Securing the cloud, cloud computer security techniques and tactics*, (Elsevier, 2011).

[4] Dieter Gollmann, *Computer security*(Wiley, 2006).

[5] E. B. Fernandez, *Security Patterns in Practice, Designing secure architectures using software patterns*. (Wiley Series on Software Design Patterns, 2013)

[6] Selvaraj, R., Kuthadi, V.M. & Marwala, T. An Effective ODAIDS-HPs approach for Preventing, Detecting and Responding to DDoS Attacks. *British Journal of Applied Science & Technology*, Vol.5 (5), 2015, 500-509.

[7] J. Wei, X. Zhang, G. Ammons, V. Bala, and P. Ning. Managing security of virtual machine images in a cloud environment. *In Proceedings of the 2009 ACM Workshop on Cloud Computing Security (CCSW09),* Chicago Illinois, USA, ACM 2009, 91–96.

[8] Selvaraj, R., Kuthadi, V.M. & Marwala, T. Enhancing Intrusion Detection system Performance using Firecol Protection Services based honeypot system. *Proceedings of the International conference on Communication, Computing and Information Technology*. India, 2014.

[9] M. Okuhara, T. Shiozaki, and T. Suzuki. Security architectures for cloud computing. *Fujitsu Sci. Tech. Journal*, 46(4), 2010, 397–402.