A COMPREHENSIVE SURVEY ON SECURITY IN CLOUD COMPUTING

Anil Lamba¹, Satinderjeet Singh², Natasha Dutta³, Sivakumar Sai Rela Muni⁴
Department of Computer Science, Charisma University, Turks and Caicos Islands

Abstract: According to a Forbes’ report published in 2015, cloud-based security spending is expected to increase by 42%. According to another research, the IT security expenditure had increased to 79.1% by 2015, showing an increase of more than 10% each year. International Data Corporation (IDC) in 2011 showed that 74.6% of enterprise customers ranked security as a major challenge. This paper summarizes a number of peer-reviewed articles on security threats in cloud computing and the preventive methods. The objective of our research is to understand the cloud components, security issues, and risks, along with emerging solutions that may potentially mitigate the vulnerabilities in the cloud. It is a commonly accepted fact that since 2008, cloud is a viable hosting platform; however, the perception with respect to security in the cloud is that it needs significant improvements to realise higher rates of adaption in the enterprise scale. As identified by another research, many of the issues confronting the cloud computing need to be resolved urgently. The industry has made significant advances in combating threats to cloud computing, but there is more to be done to achieve a level of maturity that currently exists with traditional/on-premise hosting.

Keywords: Cloud computing; Security in cloud; Security Threats, cloud computing; deployment model; service level agreement; utility computing; privacy; platform as a service; software as a service; infrastructure as a service; Denial of service attack; Cyber Security; Cloud Security; Network; Cyber; Cyber Threats; Threat Analysis; Information Security; Data security.

Citation: Anil Lamba. 2017."A COMPREHENSIVE SURVEY ON SECURITY IN CLOUD COMPUTING". International Journal for Technological Research in Engineering, International Conference on Emerging Technologies in Engineering, Biomedical, Medical and Science (ETEBMS - 2016), pp.31-34,2347-4718.

I. INTRODUCTION
Cloud computing is increasingly being adapted by a wide range of users starting from commercial entities to consumers. A survey by Right Scale³ found that an average user runs at least four cloud-based applications and at any point in time is evaluating another four. The survey also found that 41% of commercial entities run significant workload on public clouds. With so much of our workload moving to cloud, security in cloud computing is under increased scrutiny. This assessment is also supported by the 2017 report by Forbes⁵, which says that in 15 months, while 80% of all IT budgets will be committed to cloud solution, 49% of the businesses are delaying cloud deployment due to security skills gap and concerns. The problem appears to be multi-dimensional, with lack of skilled resources, lack of maturity, conflicting best practices, and complex commercial structures to name a few. Adaption of cloud has reached a tipping point and it is expected that more workloads will move from traditional local storage to cloud from not just average Internet users, but also from most if not all commercial entities. While there are many problems that need identifying, analyzing, and addressing, this document attempts to survey the security in cloud computing and reports on various aspects of security vulnerabilities and solutions. Some questions that need urgent answers are: (a) Privileged User Access Management, (b) Regulatory Compliance, (c) Data Location, (d) Data Segregation, (e) Data Protection and Recovery Support, (f) Investigative Support, and (g) Long-term Viability.

It is highly recommended that these questions, along with other risks, are assessed and addressed. Some of the assessments could be as follows:

- Organization capability and maturity
- Technology & data risks
- Application migration and performance risk
- People risks
- Process risks
- Policy risks
- Extended supply chain risks

This article consolidates various works that address the risks, vulnerabilities, and potential controls in cloud computing. It also provides information on leading cloud architectures and frameworks. Moreover, the article identifies potential future research areas related to security in cloud computing.

The remainder of the paper is organized as follows: The cloud architecture is discussed in section 2. Section 3 discusses the security implications based on deployment and delivery models. General vulnerabilities, attacks, and threats are explained in section 4, whereas section 5 gives insights into countermeasures and controls. Finally, section 6 concludes the paper with potential future directions.

II. CLOUD ARCHITECTURE
Before we dive into the security issues, it is important to understand the cloud definition and architecture. According to Sharma and Trivedi3, cloud computing is a set of resources that can scale up and down on-demand. It is available over the Internet in a self-service model with little
to no interaction required with the service provider. Cloud enables new ways of offering products and services with innovative, technical, and pricing opportunities.

As per NIST’s Cloud Computing Reference Architecture4, there are five major factors that influence and are impacted by cloud computing, along with its security implications. This document focuses on cloud consumer and cloud provider’s threat and risk perceptions.

Table 1: Actors in NIST Cloud Computing Reference Architecture

<table>
<thead>
<tr>
<th>Actor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Consumer</td>
<td>A person or Organization that maintains a business relationship with another service from Cloud Provider</td>
</tr>
<tr>
<td>Cloud Provider</td>
<td>A person, organization, or entity responsible for making service available to an interested party</td>
</tr>
<tr>
<td>Cloud Auditor</td>
<td>A party that can conduct independent assessment of service security, information system operations, performance, and security of the cloud implementation</td>
</tr>
<tr>
<td>Cloud Broker</td>
<td>An entity that manages the use, performance, and delivery of cloud services and implements service assurance policies between Cloud Providers and Cloud Consumers</td>
</tr>
<tr>
<td>Cloud Carrier</td>
<td>A mechanism that provides connectivity and transport of cloud services from Cloud Providers to Cloud Consumers</td>
</tr>
</tbody>
</table>

Figure 1 is a complete reference architecture for cloud computing. It is important to note that the figure represents an end-to-end reference architecture that addresses all the seven layers of the Open Systems Interconnection (OSI) model, and extends to include the business, commercial, and governance aspects. As it is evident, cloud computing is a comprehensive and complex solution with many areas of vulnerabilities.

II. SECURITY IMPLICATIONS BASED ON DEPLOYMENT AND DELIVERY MODELS

The two most important aspects that determine the level of vulnerability in a cloud-computing platform is the choice of deployment and delivery model. According to Modi et al.6& NIST4, there are three deployment and three delivery models that are considered as industry standards. Each of these three deployment and delivery models have unique security implications. The following sub-sections briefly discuss each of these models and their security implications:

3.1. Cloud Deployment Model

The three most common types of cloud deployment models7 are Private Cloud, Public Cloud, and Hybrid Cloud.

Table 2: Cloud Deployment Model

<table>
<thead>
<tr>
<th>Deployment Model</th>
<th>Description</th>
<th>Implications</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private Cloud</td>
<td>In a private cloud, the cloud service provider exists as an isolated resource and virtual applications and resources are available to the cloud consumer. Service delivery model, the services are dedicated to a single or set of interconnected service instances or on-demand instances. The billing model is one of service consumption or shared resources management.</td>
<td>Insider security implications are relatively high and the organization has significant influence on the architecture and process used to implement and/or offload data and services.</td>
<td>Security/sharing loophole: high cost of infrastructure and management, anti-competitive, and vulnerability management in third-party suppliers, cost and financial risk assessment, software vendors, data confidentiality, and security breach.</td>
</tr>
<tr>
<td>Public Cloud</td>
<td>In a public cloud, resources are dynamically and physically provisioned to a virtual or physical environment. The cloud service provider has relatively low control over the infrastructure on which the service is deployed.</td>
<td>Insider security implications are relatively high and the organization has significant influence on the architecture and process used to implement and/or offload data and services.</td>
<td>Security/sharing loophole: high cost of infrastructure and management, anti-competitive, and vulnerability management in third-party suppliers, cost and financial risk assessment, software vendors, data confidentiality, and security breach.</td>
</tr>
<tr>
<td>Hybrid Cloud</td>
<td>Hybrid cloud is a deployment model where private cloud services are installed on public cloud resources.</td>
<td>Insider security implications are relatively high and the organization has significant influence on the architecture and process used to implement and/or offload data and services.</td>
<td>Security/sharing loophole: high cost of infrastructure and management, anti-competitive, and vulnerability management in third-party suppliers, cost and financial risk assessment, software vendors, data confidentiality, and security breach.</td>
</tr>
</tbody>
</table>

3.2. Cloud Delivery Model

The three cloud delivery models proposed by NIST and adapted by the industry are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

Table 3: Cloud Delivery Model

2.1. Advantages of Cloud

According to Avram5, there are some unique advantages to cloud computing. Some of the key advantages are:

- Cost of entry for all organizations including small firms
- Almost immediate access to the resources
- Reduction in IT barriers to innovation
- Easy to scale the services
- Implement and/or offer new class of application and delivery services
Changes to Business Model – cloud computing can be a significant change to a cloud consumer’s business model. IT department, and business needs to adapt or face exposure to risk.

Abusive use – certain features of cloud computing can be used for malicious attack purposes such as the use of trail period of use to launch zombie or DDoS attacks.

Malicious Insider – a malicious insider is always a major risk, however, a malicious insider at the cloud provider can cause significant damage to multiple consumers.

Availability – the probability that a system will work as required and when required.

4.2. Attack Vectors

According to a recent research8, the three major vectors of attack are network, hypervisor, and hardware. These vectors are mapped to attacks such as external, internal, and cloud provider or insider attack respectively.

V. COUNTERMEASURES & CONTROLS

The vulnerabilities and threats in the cloud are well documented. Each cloud service provider and cloud consumer have to devise countermeasures and controls to mitigate the risks based on their assessment. However, the following are some of the best practices in countermeasures and controls that can be considered:

End-to-end encryption – the data in a cloud delivery model might traverse through many geographic locations; it is imperative to encrypt the data end-to-end.

Scanning for malicious activities – end-to-end encryption while highly recommended, induces new risks, as encrypted data cannot be read by the Firewall or IDS. Therefore, it is important to have appropriate controls and countermeasures to mitigate risks from malicious software passing through encryption.

Validation of cloud consumer – the cloud provider has to take adequate precautions to screen the cloud consumer to prevent important features of cloud being used for malicious attack purposes.

Secure Interfaces and APIs – the interfaces and APIs are important to implement automation, orchestration, and management. The cloud provider has to ensure that any vulnerability is mitigated.

Insider attacks – cloud providers should take precaution to screening employee and contractors, along with strengthening internal security systems to prevent any insider attacks.

Secure leveraged resources – in a shared/multi-tenancy model, the cloud provider has secure shared resources such as hypervisor, orchestration, and monitoring tools.

Business Continuity plans – Business continuity plan is a process of documenting the response of the organization to any incidents that cause unavailability of whole or part of a business-critical process.

VI. CONCLUSION

Security in cloud computing is evolving in step with risks as they are discovered often too late to prevent incidents. Cloud
computing due to its disruptive nature, complex architecture, and leveraged-resources pose a unique and severe risk to all actors. It is critical to all stakeholders and actors to understand the risk and mitigate it appropriately. Security needs to be built at every layer in a cloud-computing platform by incorporating best practices and emerging technologies to effectively mitigate the risk. In the cloud, consumer, provider, broker, carrier, auditor, and everyone else has to take the necessary precautions against risks to truly secure the cloud-computing platform or be exposed to significant and sometimes business critical risk. According to a recent survey, the industry recognizes that security engineering provides best practices, methods, and techniques for developing systems and services, which are built for security, sustainability, and resiliency. It is important to take this research forward to provide such best practices to more applications and use cases. It is also essential to conduct further research in systems development life cycle (SDLC) for cloud consumers to incorporate various development and technological advancement models and container systems such as Docker to improve security at a fundamental level. Additionally, there is very limited research on training and people impact on security. Work can be done to understand the challenges, requirements, and impact of effective security training for consumers and other providers.

REFERENCES