An Analysis On Identifying Various Security Issues And Threats In Cloud Security

Nasreen Sultana Quadri, Kusum Yadav, Yogesh Kumar Sharma

Abstract: Cloud Computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer Information Technology (IT) services over the Internet. However, cloud Computing presents an added level of risk because essential services are often outsourced to a third party, which makes it harder to maintain data security and privacy, support data and service availability, and demonstrate compliance. This rapid change of storage towards the clouds has increased the concerns various threats and security issue for the success of this cloud storage. From the perspective of cloud storage security, a number of threats and challenges have been introduced which needs an effective mechanism for protection. As a result, this paper aims to analyses and various security issues and potential threats present in the cloud storage. This paper also analyses the most important security components that should be included in the design of cloud storage systems. This study also provides us to understand all the current and future, security and privacy challenges with cloud computing and its storage.

Index Terms: Keywords: Cloud Computing, Security, Deployment, Adoption, Data Analysis, Security Threat

1. INTRODUCTION

In the history of Computer science, various actions have been done to disengage the users from needs of computer hardware, from sharing of time and other utilities etc. These drawbacks leads to the growth of various academic and business leaders in this cloud computing. Cloud computing is an innovative Information System (IS) architecture, which leads to understand the operating systems, architectures client–server, and browsers etc. Cloud computing has changed the users from hardware requirements, while reducing complexity in client side requirements. Since the cloud computing is getting popularity among the users, various concerns are being noticed about the security issues when this this new model is being adopted. The effectiveness and efficiency of traditional mechanisms on cloud security are being reconsidered, as the basic characteristics of this cloud computing based architecture model widely differs from the existing architectures. In this paper, various challenges cloud security and also classify various threats that causes the security issues are discussed.

The main objectives of this paper are to analyses the security in cloud computing, threats in security and at last the specific security requirements were documented. This paper proposes a security solution, which is based on the combination of two already available security models such as the Infrastructure as a Service and the Platform as a Service which leverages all the clients from the security burden, by trusting the proposed security model. The proposed security model is tasked with assuring specific security characteristics within a distributed information system, while forming a distribution of a trust mesh between involved entities, forming combination of clouds. The proposed methodology is a framework based and it is expected to achieve the main goal of this work as to analyze the various threats and security issues which are present in the cloud Security Models in Cloud Computing. The available security models in cloud computing is as follows:

- **Infrastructure as a Service (IaaS)**
  This service provides the user with the capability to process, storage, perform networks, and other fundamental computing resources within the cloud architecture. It also allows the user to apply arbitrary based software, which can include operating systems and various applications.

- **Platform as a Service (PaaS)**
  Provides the consumer with the capability to deploy onto the cloud infrastructure, consumer created or acquired applications, produced using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

- **Software as a Service (SaaS)**
  Provides the consumer with the capability to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices, through a thin client interface, such as a web browser (e.g. web-based e-mail). The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings. Four deployment models have been identified for cloud architecture solutions, described below:

- **Private cloud**
  The cloud infrastructure is operated for a private organization. It may be managed by the organization or a third party, and may exist on premise or off premise.

- **Community cloud**
  The cloud infrastructure is shared by several organizations and supports a specific community that has communal concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party, and may exist on premise or off premise.

- **Public cloud**
  The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
Hybrid cloud
The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology, that enables data and application portability (e.g., cloud bursting for load-balancing between clouds) [2]. Cloud computing is viewed as one of the most promising technologies in computing today, inherently able to address a number of issues. A number of key characteristics of cloud computing have been identified [6,7].

2 FACTORS FOR CLOUD ADOPTION
Security in cloud computing has always been a top concern for most organizations and that’s the reason why most researches are on security in cloud computing. For this paper we reviewed several researches but here we will be mentioning some most recent and relevant ones. In [7] trusted third party model is proposed to secure the confidentiality and integrity of data, 8 only focuses on Identity and access management (IAM) security issues, 9 explains about securing documents in third party environment and security in Hadoop environment etc. Similarly, [10, 11, 12, 13, 14] have also shed some light on security concerns and with few solutions too, in different areas of cloud in terms of services and models, but none of these researches have given a solution of identified security concerns in regards to ease up cloud adoption by incorporating it in a framework. The security threats and vulnerabilities mentioned in this paper is one of the parts of the stage 1 of the cloud framework which focuses on the readiness of the organization by making them aware of all the risks and preparedness associated with cloud computing [32] as shown in figure 1. The contribution of this paper and eventually a cloud framework is in cloud computing adoption among small organizations and enhancing cloud security [15].

Figure 1. Cloud Computing Adoption Factors

3 METHODOLOGY AND DATA ANALYSIS
The research methodology consisting appropriate techniques and steps was vital for this research program. The main stages of the methodology are outlined underneath:

• Reviewing previous literature and relevant cloud computing issues: In this step, previous relevant literature, surveys and studies have been reviewed to identify issues with cloud adoption.

• Identify and define the research problem: To do so, a qualitative research method has been adopted as a primary approach and following this; a number of semi-structured interviews were conducted with SMEs, cloud providers and developers to gather relevant information.

• Analyzing data collected from interviews: The collected data from the interview is then analyzed by applying the content analysis approach.

• Preparing a road map for SMEs: A structured guideline will then be designed in order to mitigate the cloud adoption barriers among SMEs.

• The fifth step of the research methodology concentrates on verification and validation of the proposed framework and gathers a feedback from SMEs and Cloud Service Providers (CSPs). For this, reflexivity workshops will be held.

• The feedback from the workshop will then be used to modify the framework to rectify and increase the efficiency of the framework.

• Finally, the proposed framework will then be prepared for use by SMEs in cloud adoption.

3.1 Security in Cloud Computing
Trust is not a new research topic in computer science [31], spanning areas as diverse as security and access control in computer networks, reliability in distributed systems, game theory and agent systems, and policies for decision making under uncertainty [15]. Perhaps the most notable example was the development of the Trusted Computer System Evaluation Criteria (TCSEC) [16] in the late 70s and early 80s. Here, trust was used in the process of convincing observers that a system (model, design or implementation) was correct and secure [17]. The concept of trust, adjusted to the case of two parties involved in a transaction, can be described as follows: “An entity A is considered to trust another entity B when entity A believes that entity B will behave exactly as expected and required” [18]. Thereinafter, an entity can be considered trustworthy, if the parties or people involved in transactions with that entity rely on its credibility. In general, the concept described above can be verbally represented by the term reliability, which refers to the quality of a person or entity that is worthy of trust. Trust in the information society is built on various different grounds, based on calculus, on knowledge or on social reasons [19]. The notion of trust in an organization could be defined as the customer’s certainty that the organization is capable of providing the required services accurately and infallibly. A certainty which also expresses the customer’s faith in its moral integrity, in the soundness of its operation, in the effectiveness of its security mechanisms, in its expertise and in its abidance by all regulations and laws, while at the same time, it also contains the acknowledgement of a minimum risk factor, by the relying party. The notion of security refers to a given situation where all possible risks are either eliminated or brought to an absolute minimum [20].

3.2 Requirements for Security in Cloud Storage
One of the first steps in the design of any secure system is to discover the security requirements. These requirements will help not only to identify which security components have to be developed (e.g. authentication), but also to describe various requisites that affect the design of those components (e.g. performance). In order to obtain the security requirements, we have followed a methodology known as the Asset Table [1]. This methodology firstly identifies the different assets that belong to the infrastructure such as the devices, networks, protocols and services, users, information and secondly
creates a table describing how those assets should be protected and how they should be attacked by means of use cases.

**TABLE 1. SECURITY REQUIREMENTS IN CLOUD STORAGE SYSTEMS**

<table>
<thead>
<tr>
<th>Category</th>
<th>Applied for Particular Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Protocol Interoperability, Scalability, Performance / Availability, Extensibility, Updating</td>
</tr>
<tr>
<td>Management</td>
<td>Accountability (logging protection), Policy Management (usability), Simple Administration (constraints), Auditing (intrusion detection systems)</td>
</tr>
<tr>
<td>Data</td>
<td>Secure Storage (privacy), Migration, Redundancy, Retirement (zeroing), Authorization (minimal permissions, flexibility), Proof of Operations</td>
</tr>
<tr>
<td>Credential</td>
<td>Creation (randomness), Storage, Rekeying, Maintenance</td>
</tr>
<tr>
<td>Network</td>
<td>CIAA (Confidentiality, Integrity, Authentication, Availability, Robustness)</td>
</tr>
<tr>
<td>User</td>
<td>Authentication (flexibility), Usability, Trust in the platform (perception) Authentication (flexibility), Usability, Trust in the platform (perception)</td>
</tr>
<tr>
<td>External (Perimetral)</td>
<td>Perimetral Security (software, hardware, physical)</td>
</tr>
</tbody>
</table>

4 RISK ANALYSIS AND MAJOR SECURITY THREATS IN CLOUD STORAGE

The list of requirements presented in Section 2 can help designers and architects to be aware of the main security issues that can affect a cloud storage infrastructure. To identify the most important security requirements, we can perform a risk management process, deriving the risk from the likelihood and the impact (cf. [3]). Firstly, we used the asset table (cf. Section 2) to analyze the likelihood (i.e. probability of the anomalous event to occur) and impact (i.e. effect on the system and its services) of every attack use case. Second, after assigning a score to every factor (from ‘very low’ to ‘high’), we calculated the severity of the attacks following a risk combination table (cf. [4]). These values, once combined, provided a list of the most dangerous attacks and in turn the most important security requirements. As a result of the previous analyses, we can provide an ordered list of the most important security components that should be included in the design of cloud storage systems. The list is shown below:

1) Logging System and Auditing System. These two components can help administrators to understand the actual (and past) state of the system.
2) User Authentication and User Authorization. As a cloud storage platform deals with user data, it is essential that only those who are authorized can access it.
3) Device Authentication/Authorization and Secure Communications. Not only the elements of the system must prove that they belong to the same infrastructure, but also all communications must be protected as well.
4) Data Protection. The system should protect the data at all times, even when it is stored in the storage nodes.
5) Credentials Storage. The credentials stored within all devices must be managed securely.
6) Extended Services. The storage system should provide an open interface where diverse mechanisms (e.g. proof of storage) can be integrated.
7) Policy Administration. The management of all the policies of the storage system, as well as other management tasks such as user administration, should be simple and usable.

**TABLE 2: CLASSIFICATIONS OF VARIOUS THREATS IN CLOUD COMPUTING**

<table>
<thead>
<tr>
<th>Threat ID</th>
<th>Threat Name</th>
<th>Description of the Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>T01</td>
<td>Hijacking the Account or Services</td>
<td>An account theft can be performed by different ways such as social engineering and weak credentials. If an attacker gains access to a user’s credential, he can perform malicious activities such as access sensitive data, manipulate data, and redirect any transaction [21].</td>
</tr>
<tr>
<td>T02</td>
<td>scavenging of Data</td>
<td>Since data cannot be completely removed from unless the device is destroyed, attackers may be able to recover this data [22,23,24]</td>
</tr>
<tr>
<td>T03</td>
<td>Leakage of Data</td>
<td>Data leakage happens when the data gets into the wrong hands while it is being transferred, stored, audited or processed [21,23,27,28].</td>
</tr>
<tr>
<td>T04</td>
<td>Service Denial</td>
<td>It is possible that a malicious user will take all the possible resources. Thus, the system cannot satisfy any request from other legitimate users due to resources being unavailable.</td>
</tr>
<tr>
<td>T05</td>
<td>Manipulating Customer’s data</td>
<td>Users attack web applications by manipulating data sent from their application component to the server’s application [27,29]. For example, SQL injection, command injection, insecure direct object references, and cross-site scripting</td>
</tr>
<tr>
<td>T06</td>
<td>Escaping the Virtual Machine</td>
<td>It is designed to exploit the hypervisor in order to take control of the underlying infrastructure [31,5].</td>
</tr>
<tr>
<td>T07</td>
<td>Hoping the Virtual Machine</td>
<td>It happens when a VM is able to gain access to another VM (i.e. by exploiting some hypervisor vulnerability) [23,8].</td>
</tr>
<tr>
<td>T08</td>
<td>Malicious creation of Virtual Machine</td>
<td>An attacker who creates a valid account can create a VM image containing malicious code such as a Trojan horse and store it in the provider repository [27].</td>
</tr>
<tr>
<td>T09</td>
<td>Insecure migration of Virtual machine</td>
<td>Live migration of virtual machines exposes the contents of the VM state files to the network. An attacker can do the following actions: a) Access data illegally during migration [8] b) Transfer a VM to an untrusted host [9] c) Create and migrate several VM causing disruptions or DoS</td>
</tr>
</tbody>
</table>

5 CONCLUSION AND FUTURE ENHANCEMENTS

Cloud Computing is a relatively new concept for storing huge data. It presents a good number of benefits for its users. However, the security threats and various issues present in this cloud storage make it un-trustable to some users. Understanding the types of issues and vulnerabilities present in this Cloud storage will help organizations and various users to make the shift towards the Cloud. Since many technologies have been used in this storage based on the cloud computing, the security issues will also be inherited towards these technologies. This paper focused on various security issues for the existing cloud based models such as the IaaS, PaaS, and SaaS, which varies depending on the respective model. As described in this paper, storage, virtualization, and networks are the biggest security concerns in Cloud Computing. Various surveys have been discussed security issues about clouds by...
past researchers without making any difference between vulnerabilities and threats. This paper focuses on various security issues and potential threats present in the cloud storage. This paper also analyses the most important security components that should be included in the design of cloud storage systems. This study also provides us to understand all the current and future, security and privacy challenges with cloud computing and its storage. Future works could be the design of model to overcome for the security threats in the cloud storage.

REFERENCES
APSEC, Sydney, Australia
