Information Security Using Multicloud

Miss. Komal P Gadekar & Mr. Shankarwar M.U
1M.E. First year, Department of Computer science, Anuradha Engineering College, Chikhli
2Asst. prof, Department of Computer science , Anuradha Engineering College, Chikhli

Abstract—Cloud computing usage has increased rapidly in many companies. Cloud computing offers many benefits in terms of low cost and accessibility of data. Ensuring the security of cloud computing plays a major role in the cloud computing, as customers often store important information with cloud storage providers but these providers may be unsafe. Customers are wondering about attacks on the integrity and the availability of their data in the cloud from malicious insiders and outsiders, and from any collateral damage of cloud services. These issues are extremely significant but there is still much room for security research in cloud computing. Dealing with “single cloud” providers is predicted to become less popular with customers due to risks of service availability failure and the possibility of malicious insiders in the single cloud. A movement towards “multi-clouds”, or in other words, “interclouds” or “cloud-of-clouds” has increased recently. The purpose of this paper is to survey recent research related to single and multi-clouds security and to address possible solutions. It is found that the research into the use of multi-cloud providers to maintain security has received less attention from the research community than has the use of single clouds. This work aspires to promote the use of multi-clouds due to its ability to reduce security risks that affect the cloud computing consumer.

Index Terms—Cloud computing, single cloud, multi-clouds, data confidentiality, data integrity, service availability.

I. Introduction

The use of cloud computing has increased rapidly in many organizations. Subashini and Kavitha [1] argued that small and medium companies use cloud computing services for various reasons, including because these services provide fast access to their applications and reduce their infrastructure costs. Cloud providers should address privacy and security issues as a matter of high and urgent priority. Dealing with “single cloud” providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud. In recent years, there has been a move towards “multiclouds”, “intercloud” or “cloud-of-clouds”. This paper focuses on the issues related to the data security aspect of cloud computing. As data and information will be shared with a third party, cloud computing users want to avoid an untrusted cloud provider. Protecting private and important information, such as credit card details or a patient’s medical records from attackers or malicious insiders is of critical importance. In addition, the potential for migration from a single cloud to a multi-cloud environment is examined and research related to security issues in single and multi-clouds in cloud computing are surveyed. The remainder of this paper is organized as follows. Section 2 describes the beginning of cloud computing and its components. In addition, it presents examples of cloud providers and the benefits of using their services. Section 3 discusses security risks in cloud computing. Section 4 analyses the new generation of cloud computing, that is, multi-clouds and recent solutions to address the security of cloud computing, as well as examining their limitations. Section 5 presents suggestions for security issue.

II. RELATED WORK

Cloud computing concept is relatively new concept but it is based on not so many new technologies. Many of the features that makes cloud computing attractive, however has to meet certain basic security criteria. In our paper, we have briefed on various measure ion cloud computing security challenges from single to multi clouds. While making a cloud secure, the following objectives are to be met: Understanding the cloud computing environment provided by the cloud service provider. The cloud computing solution should meet the basic security and privacy requirements of any firm deploying it. Maintain an account of the privacy of the cloud and data security and applications that are deployed in cloud computing environment. Data Integrity, Service Availability. The user runs customer applications using the service provider’s resources.

III. WHAT IS CLOUD COMPUTING

Because data is stored in the Cloud instead of on employee computers, Cloud computing enhances multiple users to access and contribute to projects simultaneously without worrying about using the same operating system, software, or browser. For example, instead of collaborating on a document by sending back and forth revision after revision as attachments, documents are stored in the cloud.
Coworkers can access the web-based document simultaneously in their browsers, and even make changes that other authorized users can see in real time. Eliminating attachment round-trips by storing data in the cloud saves time and reduces frustrations for teams who need to work together efficiently. Through synchronous replication, data and user actions are mirrored in nearly real-time across multiple data centers. If one data center becomes unavailable for any reason, the system is designed to instantly fall back to a secondary data center with non-perceptible interruption in service. Cloud provides extensive flexibility and control. Nevertheless, moving to the cloud doesn't mean that businesses lose control of their data or their technology. For example, the Google Apps Terms of Service explicitly state that customers retain ownership of their data in Google Apps. Further more, cloud providers give controls so administrators can manage which applications their users can access and how employees can use each service. They also allow administrators build custom functionality and integrations with other technologies. Going detailed in the topic of Cloud Computing we must mention that Cloud Computing is split in three different categories according to 1) IaaS - Infrastructure as a Service: Virtual provision of computing power and/or memory. Source [2] mentions a prominent example of an IaaS service the Amazon WS service.

2) PaaS – Platform as a Service: Provision of a runtime environment, like application servers, databases, In this area, paper [2] provides Google’s App Engine as probably the most prominent example.

3) SaaS – Software as a Service: Provision of usually browser based applications that can directly be used. Google Docs or the Customer Relationship Management software of salesforce.com might serve as examples.

IV. Cloud computing security

Emphasis is given to the distinction between services in the form of software (SaaS), platform (PaaS) and infrastructure (IaaS), which are commonly used as the fundamental basis for cloud service classification [3]. Aiming to concentrate and organize information related to cloud security and to facilitate future studies, in this section we identify the main problems in the area and group them into a model composed of seven categories, based on the aforementioned references. Namely, the categories are: network security, interfaces, data security, virtualization, governance, compliance and legal issues. Each category includes several potential security problems, resulting in a classification with subdivisions that highlights the main issues identified in the base references:[4],[5]

1. **Network security**: Problems associated with network communications and configurations regarding cloud computing infrastructures.

2. **Authentication**: Mechanisms required to enable access to the cloud. Most services rely on regular accounts consequently being susceptible to a plethora of attacks whose consequences are boosted by multi-tenancy and resource sharing. [6]

3. **Data security**: Protection of data in terms of confidentiality, availability and integrity (which can be applied not only to cloud environments, but any solution requiring basic security levels).[7] Cryptography: Most employed practicto secure sensitive data, thoroughly required by industry, state and federal regulations.[8]

5. **Redundancy**: Essential to avoid data loss. Most business models rely on information technology for its core functionalities and processes and, thus, mission-critical data integrity and availability must be ensured.

6. **Isolation**: Although logically isolated, all VMs share the same hardware and consequently the same resources, allowing malicious entities to exploit data leaks and cross-VM attacks.

7. **Data leakage**: Exploit hypervisor vulnerabilities and lack of isolation controls in order to leak data from virtualized infrastructures, obtaining sensitive customer data and affecting confidentiality and integrity.

8. **Loss of service**: Service outages are not exclusive to cloud environments but are more serious in this context due to the interconnections between services (e.g., a SaaS using virtualized infrastructures provided by an IaaS), as shown in many examples. This leads to the need of strong disaster recovery policies and provider recommendations to implement customer-side redundancy if applicable.

V. SECURITY ISSUES

Although cloud service providers can provide benefits to consumers, security risks play a major role in the cloud computing environment [65]. Users of online data sharing or network facilities are aware of the potential loss of privacy [18]. According to a recent IDC survey [23], the top challenge for 74% of CIOs in relation to cloud computing is security. Protecting private and important
information such as credit card details or patients’ medical records from attackers or malicious insiders is of critical importance [45]. Moving databases to large data centers involves many security challenges [67] such as virtualization vulnerability, accessibility vulnerability, privacy and control issues related to data accessed from a third party, integrity, confidentiality, and data loss or theft. Subashini and Kavitha [61] present some fundamental security challenges, which are data storage security, application security, data transmission security, and security related to third-party resources. In different cloud service models, the security responsibility between users and providers is different. According to Amazon [58], their EC2 addresses security control in relation to physical, environmental, and virtualization security, whereas, the users remain responsible for addressing security control of the IT system including the operating systems, applications and data. According to Takabi et al. [63], the way the responsibility for privacy and security in a cloud computing environment is shared between consumers and cloud service providers differs between delivery models. In SaaS, cloud providers are more responsible for the security and privacy of application services than the users. This responsibility is more relevant to the public than the private cloud environment because the clients need more strict security requirements in the public cloud. In PaaS, users are responsible for taking care of the applications that they build and run on the platform, while cloud providers are responsible for protecting one user’s applications from others. In IaaS, users are responsible for protecting operating systems and applications, whereas cloud providers must provide protection for the users’ data [63]. Ristenpart et al. [53] claim that the levels of security issues in IaaS are different. The impact of security issues in the public cloud is greater than the impact in the private cloud. For example, any damage which occurs to the security of the physical infrastructure or any failure in relation to the management of the security of the infrastructure will cause many problems. In the cloud environment, the physical infrastructure that is responsible for data processing and data storage can be affected by a security risk. In addition, the path for the transmitted data can be also affected, especially when the data is transmitted to many third-party infrastructure devices [53]. As the cloud services have been built over the Internet, any issue that is related to internet security will also affect cloud services. Resources in the cloud are accessed through the Internet; consequently even if the cloud provider focuses on security in the cloud infrastructure, the data is still transmitted to the users through network which may be insecure. As a result, internet security problems will affect the cloud, with greater risks due to valuable resources stored within the cloud and cloud vulnerability. The technology used in the cloud is similar to the technology used in the Internet. Encryption techniques and secure protocols are not sufficient to protect data transmission in the cloud. Data confidentiality of the cloud through the Internet by hackers and cybercriminals needs to be addressed and the cloud environment needs to be secure and private for clients [61]. We will address three security factors that particularly affect single clouds, namely data integrity, data intrusion, and service availability.

### A. Data Integrity

The most important issues related to cloud security risks is data integrity. The data stored in the cloud may suffer from damage during transition operations from or to the cloud storage provider examples of the risk of attacks from both inside and outside the cloud provider, [12] such as the recently attacked Red Hat Linux’s distribution servers [16] Another example of a risk to data integrity recently occurred in Amazon S3 where users suffered from data corruption. Further examples giving details of attacks can be read in One of the solutions that they [12] propose is to use a Byzantine fault-tolerant replication protocol within the cloud. Hendricks et al.[12],[3] state that this solution can avoid data corruption caused by some components in the cloud. However, Cachinet al. claim that using the Byzantine fault tolerant replication protocol within the cloud is unsuitable due to the fact that the servers belonging to cloud providers use the same system installations and are physically located in the same place.[2] It is not an easy task to securely maintain all essential data where it has the need in many applications for clients in cloud computing. To maintain our data in cloud computing, it may not be fully trustworthy because client doesn’t have copy of all stored data. We have to begin new proposed system for this using our data reading protocol algorithm to check the integrity of data before and after the data insertion in cloud. Here the security of data earlier than and following is checked by client with the help of CSP using our “effective automatic data reading protocol from user as well as cloud level into the cloud” with truthfulness.

### B. Data Intrusion:

The importance of data intrusion detection systems in a cloud computing environment, We find out how intrusion detection is performed on Software as a Service, Platform as a Service and Infrastructure as Service offerings, along with the available host, network and hypervisor based intrusion detection options. Attacks on systems and data are a reality in the world we live in.[14] Detecting and responding to those attacks has become the norm and is considered
due diligence when it comes to security. Another security risk that may occur with a cloud provider, such as the Amazon cloud service, is a hacked password or data intrusion. If someone gains access to an Amazon account password, they will be able to access all of the account’s instances and resources. Thus the stolen password allows the hacker to erase all the information inside any virtual machine instance for the stolen user account, modify it, or even disable its services.[2]

C. Service Availability

Service availability is most significant in the cloud computing security. Amazon previously mentions in its authorizing agreement that it is possible that the service might be unavailable from time to time.[14],[18] The user’s web service may conclude for any reason at any time if any users files break the cloud storage policy. In accumulation, if any damage occurs to any Amazon web service and the service fails, in this casing there will be no charge to the Amazon Company for this failure. Companies seeking to protect services from such failure need measures such as backups or use of multiple providers.[15]

VI. Multi-Clouds Computing Security

This section will discuss the migration of cloud computing from single to multi-clouds to ensure the security of the user’s data.[2]

A. Multi-Clouds: Preliminary

The term “multi-clouds” is similar to the terms“interclouds” or “cloud-of-clouds” that were introduced by Vukolic [54]. These terms suggest that cloud computing should not end with a single cloud. Using their illustration, a cloudy sky incorporates different colors and shapes of clouds which leads to different implementations and administrative domains. Recent research has focused on the multi-cloud environment [3],[8],[10],[11] which control several clouds and avoids dependency on any one individual cloud. Cachin et al. [11] identify two layers in the multicloud environment: the bottom layer is the inner-cloud, while the second layer is the inter-cloud. In the intercloud, the Byzantine fault tolerance finds its place. We will first summarize the previous Byzantine protocols over the last three decades.

B. Introduction of Byzantine Protocols

In cloud computing, any faults in software or hardware are known as Byzantine faults that usually relate to inappropriate behavior and intrusion tolerance. In addition, it also includes arbitrary and crash faults [54]. Much research has been dedicated to Byzantine fault tolerance (BFT) since its first introduction [28], [38]. Although BFT research has received a great deal of attention, it still suffers from the limitations of practical adoption [27] and remains peripheral in distributed systems [54]. The relationship between BFT and cloud computing has been investigated, and many argue that in the last few years, it has been considered one of the major roles of the distributed system agenda. Furthermore, many describe BFT as being of only “purely academic interest” for a cloud service [9]. This lack of interest in BFT is quite different to the level of interest shown in the mechanisms for tolerating crash faults that are used in large-scale systems. Reasons that reduce the adoption of BFT are for example difficulties in design, implementation, or understanding of BFT protocols [54]. As mentioned earlier, BFT protocols are not suitable for single clouds. Vukolic [54] argues that one of the limitations of BFT for the inner-cloud is that

C. DepSky System: Multi-Clouds Model

This section will explain the recent work that has been done in the area of multi-clouds. Bessani et al. [8] present a virtual storage cloud system called DepSky which consists of a combination of different clouds to build a cloud-of-clouds. The DepSky system addresses the availability and the confidentiality of data in their storage system by using multi-cloud providers, combining Byzantine quorum system protocols, cryptographic secret sharing and erasure codes [8].

i. DepSky Architecture

The DepSky architecture [8] consists of four clouds and each cloud uses its own particular interface. The DepSky algorithm exists in the clients’ machines as a software library to communicate with each cloud (Figure 2). These four clouds are storage clouds, so the particular inner-cloud infrastructure [54] there are no codes to be executed. The DepSky library permits reading and writing operations with the storage clouds.

Fig-DepSky Architecture
ii. DepSky Data model.

As the DepSky system deals with different cloud providers, the DepSky library deals with different cloud interface providers and consequently, the data format is accepted by each cloud. The DepSky data model consists of three abstraction levels: the conceptual data unit, a generic data unit, and the data unit implementation.

iii. DepSky System model.

The DepSky system model contains three parts: readers, writers, and four cloud storage providers, where readers and writers are the client’s tasks. Bessani et al. [8] explain the difference between readers and writers for cloud storage. Readers can fail arbitrarily (for example, they can fail by crashing, they can fail from time to time and then display any behavior).

iv. Cloud storage providers in the DepSky system model.

The Byzantine protocols involve a set of storage clouds \( n \) where \( n = 3f + 1 \), and \( f \) is maximum number of clouds which could be faulty. In addition, any subset of \( (n - f) \) storage cloud creates byzantine quorum protocols [8].

VII. Cloud computing solution methodology

Cloud customers may form their expectations based on their past experiences and organizations’ needs. They are likely to conduct some sort of survey before choosing a cloud service provider. Customers are expected also to do security checks that are centered on three security concepts: confidentiality, integrity and availability. On the other hand, cloud service providers may promise a lot to entice a customer to sign a deal, but some gaps may manifest later as overwhelming barriers to keep their promises. Many potential cloud customers are well aware of this, and certainly, still sitting on the sidelines. They will not undertake cloud computing unless they get a clear indication that all gaps are within acceptable limits. All relevant information are visualized into cloud computing security in a snapshot which is presented in Figure 1 [7]. We organized cloud computing security into three sections: security categories, security in service delivery models and security dimensions. Security in cloud services is based on the following:

1. Strong network security is possible around the service delivery platform.
2. Data encryption: for data in transit (particularly over wide area networks), and sometimes stored data, but it cannot be applied to data in use.
3. Access controls to ensure that only authorized users gain access to applications, data and the processing environment and is the primary means of securing cloud-based services.

![Fig.—Graphical view of cloud computing image](image-url)

Service providers are able to inspect activity in their environment and provide reports to clients. Logs need to be carefully constructed to appraise the Actions of their system administrators and other restricted users or risk producing reports that mix events relating to different customers of the service. Both the organizations seeking cloud solutions and the service providers have to ensure cloud security is addressed [8]. Some of the measures to ensure security in cloud are good governance, compliance, privacy, Identity and Access Management (IAM), Data protection, Availability, Business Continuity and Disaster Recovery plans etc.

VIII. Conclusion

It is clear that although the use of cloud computing has rapidly increased, cloud computing security is still considered the major issue in the cloud computing environment. Customers do not want to lose their private information as a result of malicious insiders in the cloud. In addition, the loss of service availability has caused many problems for a large number of customers recently. Furthermore, data intrusion leads to many problems for the users of cloud computing. The purpose of this work is to survey the recent research on single clouds and multi-clouds to address the security risks and solutions. We have found that much research has been done to ensure the security of the single cloud and cloud storage whereas multiclouds have received less attention in the area of security. We support the
migration to multi-clouds due to its ability to decrease security risks that affect the cloud computing user

IX. REFERENCE


