RESEARCH ARTICLE OPEN ACCESS

A Novel Approach to Cloud Computing Security over Single to Multi Clouds

I. Sapthami [1], P. Srinivasulu[2], B. Murali Krishna[3]
1, 3 M.TECH Scholars, VEC, Kavali
2, Assistant Professor, VEC, Kavali

ABSTRACT
The usage of cloud computing has increased speedily in the society. Cloud computing presents many benefits in terms of accessibility of data and low cost. A main characteristic of the cloud services is that users' data are usually processed remotely in unknown machines that users do not operate. It can be converted into a significant roadblock to the wide adoption of cloud services. Make sure that the security of cloud computing is a main factor in the environment of cloud computing, as users repeatedly store perceptive information with cloud storage providers but these providers may be untrusted. Dealing with "single cloud" providers is expected to become less accepted with customers due to risks of service accessibility collapse 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 come into view recently. The growing popularity of cloud storage space services has show the way companies that handle critical data to think about using these services for their storage space needs. However the reliability and security of data stored in the cloud still remain main concerns. It is found that the investigation into the use of multi-cloud providers to maintain security has acknowledged less thought from the research community has the use of single clouds. My work aims to support the use of multi-clouds due to its capability to decrease security risks that affect the cloud computing user.
Index Terms: Cloud computing, DepSky Architecture single cloud, multi-clouds, cloud storage, data integrity, data intrusion, service availability.

I. INTRODUCTION

Cloud sources should address privacy and security issues as a matter of high and vital priority. Dealing with "single cloud" providers is becoming less popular with customers due to potential problems such as service availability failure and the opportunity that there are malicious insiders in the single cloud. In current years, there has been a move towards "multiclouds", "intercloud" or "cloud-of-clouds". As data and information will be shared with a third party, cloud computing users want to keep away from an untrusted cloud provider. Defending private and significant information, such as customer details and a patient's medical records from attackers or malicious behaviors is of serious 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 is surveyed.

II. RELATED WORK

National Institute of Standards and Technology(NIST) describes cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources like networks, storage, servers, applications, services and that can be rapidly provisioned and released with minimal management effort or service provider interaction".

2.1 Cloud Computing Components

The cloud computing model consists of three delivery models, five characteristics, and four deployment models. The five input characteristics of cloud computing are: location-independent resource pooling, on demand self service, rapid elasticity, deliberate service and broad network access. These five characteristics represent the first layer in the cloud environment architecture.

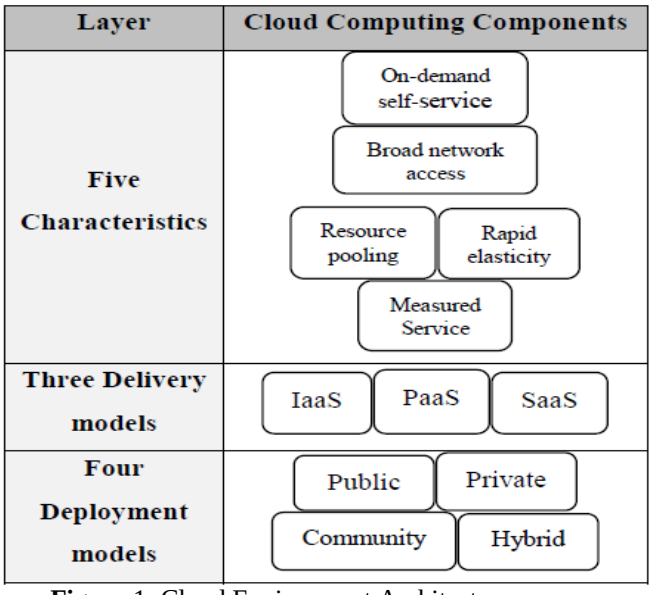

Figure 1: Cloud Environment Architecture.

The three key cloud delivery models are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). In IaaS, the user can benefit from networking infrastructure facilities, information storage space and computing services. It is the delivery of computer infrastructure as a service. A model of IaaS is the Amazon web service. In PaaS, the user runs custom applications using the service provider's resources. It is the delivery of a computing platform and solution as a service. An example of PaaS is GoogleApps. Running software on the provider's infrastructure and providing licensed applications to users to use services is known as SaaS. A Model of SaaS is the Salesforce.com CRM application this model represents the second layer in the cloud environment architecture.

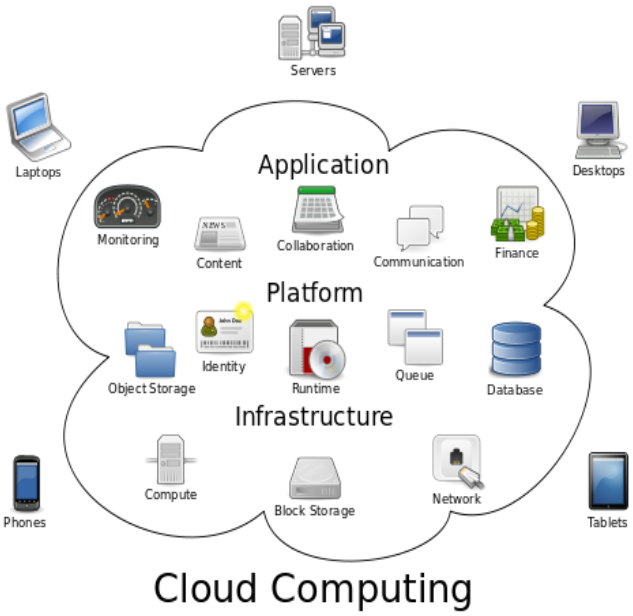

Fig.2: Cloud Applications structure

Cloud deployment models contain public, community, private and hybrid clouds. A cloud environment that is available for multi-tenants and is accessible to the public is called a public cloud. A private cloud is accessible for a particular group, even as a community cloud is modified for a specific group of customers. Hybrid cloud communications is a composition of two or more clouds. This model represents the third layer in the cloud environment architecture.

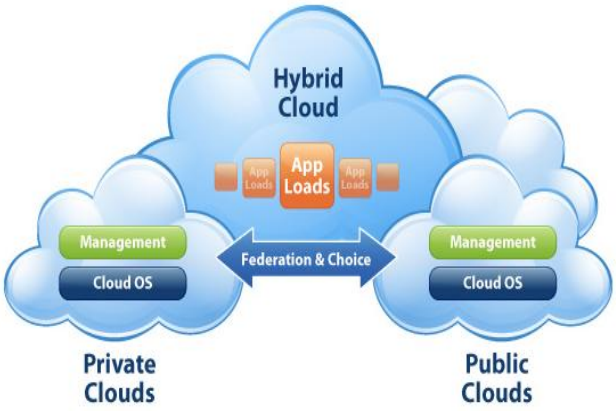

Fig.3: Cloud types

2.2 Cloud Service Providers Examples

In the commercial world, various computing needs are provided as a service. The service providers take care of the customer's requirements by, for illustration, maintaining software or purchasing luxurious hardware. For example, the service EC2, created by Amazon, offers customers with scalable servers. There are many features of cloud computing. First, cloud storages, such as AmazonS3, MicrosoftSkyDrive, or NirvanixCLoudNAS, authorize consumers to access online data. Second, it offers computation resources for users such as Amazon EC2. Third, Google Apps or versioning repositories for source code are examples of online collaboration tools

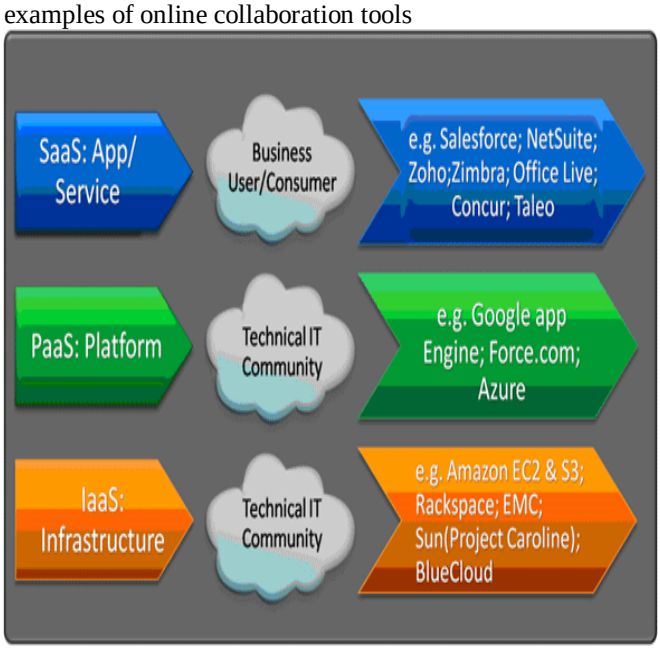

Fig 4: Cloud Computing Providers

III. SECURITY RISKS IN CLOUD COMPUTING

In different cloud service models, the security responsibility among users and providers is different. According to Amazon network, their EC2 addresses security control in relation to physical, and virtualization security, environmental, whereas, the

users remain responsible for addressing security control of the IT system including the operating systems, applications and data.

3.1. Data Integrity

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.

3.2. 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. Detecting and responding to those attacks has become the norm and is considered due diligence when it comes to security.

3.3. 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. 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.

IV. MULTI-CLOUDSCOMPUTING SECURITY

4.1. DepSky System: Multi-Clouds Model

The term "multi-clouds" is similar to the terms "interclouds" or "cloud-of-clouds" that were introduced by Vukolic. These terms suggest that cloud computing should not end with a single cloud. Using their design, a cloudy sky incorporates unlike colors and shapes of clouds which lead to different implementations and administrative domains. In the proposed system Bessani 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.

4.2. DepSky Architecture and Data Model

The DepSky architecture consists of four clouds and every cloud uses its own particular interface. The DepSky algorithm exists in the client's machines as a software library to communicate with each cloud. These four clouds are storage clouds, so here no codes to be executed. The DepSky library authorizes reading and writing operations with the storage clouds. The use of diverse clouds requires the DEPSKY library to deal with the heterogeneity of the interfaces of each cloud provider. An aspect that is especially important is the format of the data accepted by each cloud. The data model allows us to ignore these details when presenting the algorithms.

DepSky Data model:

As the DepSky system contract with various cloud providers, the DepSky library deals with various cloud interface providers and as a result, the data format is acknowledged by each cloud. The DepSky data models consist of three abstraction levels: the conceptual data unit, a generic data unit, and the information unit implementation.

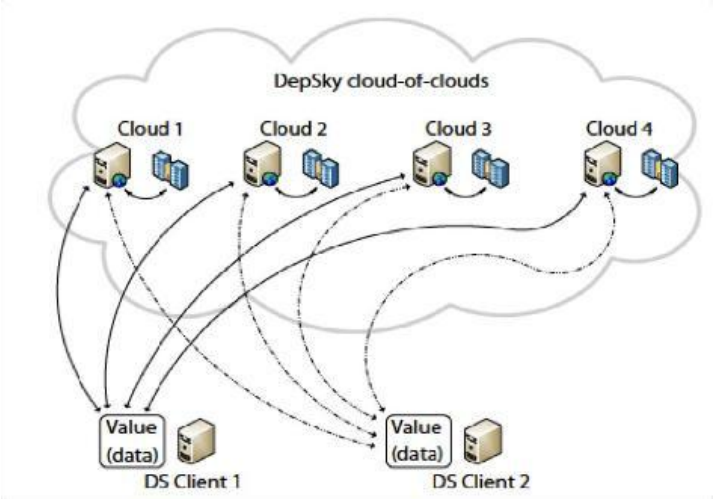

Fig.5: DepSky Architecture

The DEPSKY data model with its three abstraction levels. In the first (left), there is the conceptual data unit, which communicates to the basic storage object with which the algorithms work a register in distributed computing. A data unit has a exclusive name, a version number, verification data and the data stored on the data unit object. In the second level (middle), the theoretical data unit is implemented as a generic data unit in an abstract storage cloud. Each basic data unit, or container, holds two types of files: a signed metadata file and the files that store up the data. Metadata files hold the version number and the verification data, jointly with other information's that applications may

demand. Notice that a data unit can store more than a few versions of the data, i.e., the container can hold several data files. The name of the metadata file is simply metadata, while the data files are called value<Version>, where <Version> is the version number of the data (e.g., value1, value2, etc.). Finally, in the third level (right) there is the data unit implementation, i.e., the container translated into the specific constructions supported by each cloud provider.

V. ANALYSIS OF MULTI-CLOUD RESEARCH

Moving from single clouds or inner-clouds to multi- clouds is reasonable and important for many reasons showed that over 80% of company management "fear security threats and loss of control of data and schemes". Author Vukolic deduces that the main reason of moving to interclouds is to improve what was accessible in single clouds by distributing dependability, trust, and security among multiple cloud providers. The reliable distributed storage space which utilizes a subset of BFT techniques was recommended by Vukolic to be used in multi-clouds. A number of current studies in this area have built protocols for interclouds. RACS (Redundant Array of Cloud Storage) for example, utilizes RAID-like techniques that are normally used by disks and file systems, but for multiple cloud storage and assume that to avoid "vender lock-in", distributing a users data among multiple clouds is a cooperative solution. This replication also decreases the cost of switching providers and offers better fault tolerance. Therefore, the storage load will be extend among several providers as a result of the RACS proxy.

HAIL (High Availability and Integrity Layer) is an additional example of a protocol that pedals multiple clouds. HAIL is a disseminated cryptographic system that allows a set of servers to ensure that the client's stored data is retrievable and essential. HAIL offers a software layer to address accessibility and integrity of the stored data in an inter cloud. Cachin present a design for inter cloud storage (ICStore), which is a step nearer than RACS and HAIL as a dependable service in multiple clouds. Cachin develop theories and protocols to address the CIRC attributes of the data stored in clouds.

5.1 Current Solutions of Security Risks

In order to decrease the risk in cloud storage, customers can make use of cryptographic methods to protect the stored data in the cloud. Hash function is a good solution for data integrity by keeping a short hash in local memory. In this manner, authentication of the server replies is done by recalculating the hash of the received data which is compared with the local stored data. If the amount of data is large, then a hash tree is the answer. Many storage system prototypes have implemented hash tree functions; claim that this is an active area in research on cryptographic methods for stored data authentication

VI. CONCLUSION AND FUTURE WORK

Now a days the use of cloud computing has speedily increased and cloud computing security is still measured the major issue in the cloud computing atmosphere. Customers do not want to misplace their private data as a consequence of malicious insiders in the cloud. The loss of service availability has caused many problems for a large number of customers in recent times. Additionally, data intrusion leads to many troubles for the users of cloud computing. The principle of this work is to survey the recent research on single clouds and multi-clouds to address the security risks and solutions. The research has been done to ensure the security of the single cloud and cloud storage whereas multi- clouds have received less attention in the area of security. We maintain the immigration to multi-clouds due to its ability to decrease security risks that affect the cloud computing user. For future work, we intend to offer a framework to supply a secure cloud database that wills assurance to avoid security risks facing the cloud computing community. This structure will be relevant multi-clouds and the secret sharing algorithm to decrease the risk of data intrusion and the loss of service accessibility in the cloud and ensure data integrity.

REFERENCES

[1] I. Abraham, G. Chockler, I. Keidar and D. Malkhi, "Byzantine disk paxos: optimal resilience with Byzantine shared memory", Distributed Computing, 18(5), 2006, pp. 387-408.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, "Provable data possession at untrusted stores", Proc. 14th ACM Conf. on Computer and communications security, 2007, pp. 598-609.

[3] H. Abu-Libdeh L. Princehouse and H. Weatherspoon "RACS: a case for cloud storage diversity", SoCC'10:Proc. 1st ACM symposium on Cloud computing, 2010, pp. 229-240.

[4] Ittai Abraham, Gregory Chockler, Idit Keidar, and Dahlia Malkhi. Byzantine disk Paxos: optimal resilience with Byzantine shared memory. Distributed Computing, 18(5):387– 408, April 2006.

[5] Hussam Abu-Libdeh, Lonnie Princehouse, and Hakim Weatherspoon. RACS: A case for cloud storage diversity. Proc. of the 1st ACM Symposium on Cloud Computing, pages 229–240, June 2010.

[6] Hagit Attiya and Amir Bar-Or. Sharing memory with semi-Byzantine clients and faulty storage servers. In Proc. of the 22rd IEEE Symposium on Reliable Distributed Systems - SRDS 2003, pages 174–183, October 2003.

[7] Alysson N. Bessani, Eduardo P. Alchieri, Miguel Correia, and Joni S. Fraga. DepSpace: a Byzantine fault-tolerant coordination service. In Proc. of the 3rd ACM European Systems Conference – EuroSys'08, pages 163–176, April 2008.

[8] Kevin D. Bowers, Ari Juels, and Alina Oprea. HAIL: a high-availability and integrity layer for cloud storage. In Proc. of the 16th ACM Conference on Computer and Commu- nications Security - CCS'09, pages 187–198, 2009.

[9] Matthias Brantner, Daniela Florescu, David Graf, Donald Kossmann, and Tim Kraska. Building a database on S3. In Proc. of the 2008 ACM SIGMOD International Conference on Management of Data, pages 251–264, 2008.

[10] Christian Cachin and Stefano Tessaro. Optimal resilience for erasure-coded Byzantine distributed storage. In Proc. of the Int. Conference on Dependable Systems and Net- works - DSN 2006, pages 115–124, June 2006.

[11] Gregory Chockler, Rachid Guerraoui, Idit Keidar, and Marko Vukolic´. Reliable distributed storage. IEEE Com- puter, 42(4):60–67, 2009.

[12] Gregory Chockler and Dahlia Malkhi. Active disk Paxos with infinitely many processes. In Proc. of the 21st Sym- posium on Principles of Distributed Computing – PODC'02, pages 78–87, 2002.

[13] Ariel J. Feldman, William P. Zeller, Michael J. Freedman, and Edward W. Felten. SPORC: Group collaboration using untrusted cloud resources. In Proc. of the 9th USENIX Symposium on Operating Systems Design and Implementation – OSDI'10, pages 337–350, October 2010.

[14] Eli Gafni and Leslie Lamport. Disk Paxos. Distribu ted Computing, 16(1):1–20, 2003.

[15] Sanjay Ghemawat, Howard Gobioff, and Shun- Tak Leung. The Google file system. In Proc. of the 19th ACM Symposium