http://dx.doi.org/10.21172/ijiet.92.06

Data Storage and Security Issues in Cloud Computing -An Analysis

Mohammed Ahmed
Reseach Scholor, Rayalaseema Univ., Kurnool

Dr. Syed Abdul Sattar
Prof. & PRINCIPAL, Nawab Shah Alam Khan College of Engg and Tech., Hyd.

Md Riyazuddin
Research Scholor, JNTUH, Hyd.

Abstract - Cloud computing is a revolutionary mechanism that changing way to enterprise hardware and software design and procurements. Because of cloud simplicity everyone is moving data and application software to cloud data centers. The Cloud service provider (CSP) should ensure integrity, availability, privacy and confidentiality but CSP is not providing reliable data services to customer and to stored customer data. This study identifies the issues related to the cloud data storage such as data breaches, data theft, and unavailability of cloud data. Finally, we are providing possible solutions to few of the issues in cloud.

Keywords: Cloud Service Provider (CSP), cloud data storage, security issues, policies & protocols;

I. INTRODUCTION

Cloud computing is a revolutionary mechanism that changing way to enterprise hardware and software design and procurements. The cloud computing provides rich benefits to the cloud clients such as costless services, easy access through internet, etc. Even though cloud computing has enormous benefits, cloud user are unwilling to place their confidential or sensitive data, it includes personal health records, emails and government sensitive files. Suppose once data are placed in cloud datacenter; the cloud client lost their direct control over their data sources. The Cloud Service Provider (CSPs) has promise to ensures the data security over stored data of cloud clients by using methods like firewalls and virtualization. These mechanisms would not provide the complete data protection because of its vulnerabilities' over the network and CSPs have full command on cloud applications, hardware and client's data. Encrypting sensitive data before hosting can deserve data privacy and confidentiality against CSP. A typical problem with encryption scheme is that it is impractical because of huge amount communication overheads over the cloud access patterns. Therefore, cloud needs secure methods to storage and management to preserve the data confidentiality and privacy [2][5]. This paper mainly focuses on security vulnerabilities and issues in confidentiality and privacy over client data.

In this paper, we try to focus on how data is stored in cloud , various security threats to cloud and what are the various security measures. we propose an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users' data in the cloud.

II. ARCHITECTURE OF CLOUD COMPUTING

In this section, we present a top-level architecture of cloud computing that depicts various cloud service delivery models. Cloud computing enhances collaboration, agility, scale, availability and provides the potential for cost reduction through optimized and efficient computing. More specifically, cloud describes the use of a collection of distributed services, applications, information and infrastructure comprised of pools of compute, network, information and storage resources (CSA Security Guidance, 2009). These components can be rapidly orchestrated, provisioned, implemented and decommissioned using an on-demand utility-like model of allocation and consumption. Cloud services are most often, but not always, utilized in conjunction with an enabled by virtualization technologies to provide dynamic integration, provisioning, orchestration, mobility and scale.

While the very definition of cloud suggests the decoupling of resources from the physical affinity to and location of the infrastructure that delivers them, many descriptions of cloud go to one extreme or another by either exaggerating or artificially limiting the many attributes of cloud. This is often purposely done in an attempt to inflate or marginalize its scope. Some examples include the suggestions that for a service to be cloud-based, that the Internet must be used as a transport, a web browser must be used as an access modality or that the resources are always shared in a multi-tenant environment outside of the "perimeter." What is missing in these definitions is context.

From an architectural perspective, given this abstracted evolution of technology, there is much confusion surrounding how cloud is both similar and different from existing models and how these similarities and differences might impact the organizational, operational and technological approaches to cloud adoption as it relates to traditional network and information security practices. There are those who say cloud is a novel sea-change and technical revolution while other suggests it is a natural evolution and coalescence of technology, economy and culture. The real truth is somewhere in between.

There are many models available today which attempt to address cloud from the perspective of academicians, architects, engineers, developers, managers and even consumers. The architecture that we will focus on this paper is specifically tailored to the unique perspectives of IT network deployment and service delivery.

Cloud services are based upon five principal characteristics that demonstrate their relation to, and differences from, traditional computing approaches (CSA Security Guidance, 2009). These characteristics are:

(i) Abstraction of infrastructure,
(ii) Resource democratization,
(iii) Service oriented architecture,
(iv) Elasticity / Dynamism,
(v) Utility model of consumption and allocation.

Abstraction of infrastructure: The computation, network and storage infrastructure resources are abstracted from the application and information resources as a function of service delivery. Where and by what physical resource that data is processed, transmitted and stored on becomes largely opaque from the perspective of an application or services' ability to deliver it. Infrastructure resources are generally pooled in order to deliver service regardless of the tenancy model employed – shared or dedicated. This abstraction is generally provided by means of high levels of virtualization at the chipset and operating system levels or enabled at the higher levels by heavily customized file systems, operating systems or communication protocols.

Resource democratization: The abstraction of infrastructure yields the notion of resource democratization- whether infrastructure, applications, or information – and provides the capability for pooled resources to be made available and accessible to anyone or anything authorized to utilize them using standardized methods for doing so.

Service-oriented architecture: As the abstraction of infrastructure from application and information yields well-defined and loosely-coupled resource democratization, the notion of utilizing these components in whole or part, alone or with integration, provides a services oriented architecture where resources may be accessed and utilized in a standard way. In this model, the focus is on the delivery of service and not the management of infrastructure.

Elasticity/dynamism: The on-demand model of cloud provisioning coupled with high levels of automation, virtualization, and ubiquitous, reliable and high-speed connectivity provides for the capability to rapidly expand or contract resource allocation to service definition and requirements using a self-service model that scales to as-needed capacity. Since resources are pooled, better utilization and service levels can be achieved.

Utility model of consumption and allocation: The abstracted, democratized, service-oriented and elastic nature of cloud combined with tight automation, orchestration, provisioning and self-service then allows for dynamic allocation of resources based on any number of governing input parameters. Given the visibility at an atomic level, the consumption of resources can then be used to provide a metered utility-cost and usage model. This facilitates greater cost efficacies and scale as well as manageable and predictive costs.

Cloud Service Delivery Models :

Three archetypal models and the derivative combinations thereof generally describe cloud service delivery. The three individual models are often referred to as the "SPI MODEL", where "SPI" refers to Software, Platform and Infrastructure (as a service) respectively (CSA Security Guidance, 2009).

Software as a Service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure and accessible from various client devices through a thin client interface such as web browser. In other words, in this model, a complete application is offered to the customer as a service on demand. A single instance of the service runs on the cloud and multiple end users are services. On the customers' side, there is no need for upfront investment in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted and maintained. In summary, in this model, the customers do not manage or control the underlying cloud infrastructure, network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. Currently, SaaS is offered by companies such as Google, Salesforce, Microsoft, Zoho etc.

Platform as a Service (PaaS): In this model, a layer of software or development environment is encapsulated and offered as a service, upon which other higher levels of service are built. The customer has the freedom to build his own applications, which run on the provider's infrastructure. Hence, a capability is provided to the customer to deploy onto the cloud infrastructure customer-created applications using programming languages and tools supported by the provider (e.g., Java, Python, .Net etc.).

Infrastructure as a Service (IaaS): This model provides basic storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, data center space etc. are pooled and made available to handle workloads. The capability provided to the customer is to rent processing, storage, networks, and other fundamental computing resources where the customer is able to deploy and run arbitrary software, which can include operating systems and applications. The customer does not manage or control the underlying cloud infrastructure but has the control over operating systems, storage, deployed applications, and possibly select networking components (e.g., firewalls, load balancers etc.). Some examples of IaaS are: Amazon, GoGrid, 3 Tera etc.

Understanding the relationship and dependencies between these models is critical. IaaS is the foundation of all cloud services with PaaS building upon IaaS, and SaaS-in turn – building upon PaaS. An architecture of cloud layer model is depicted in Figure 1.

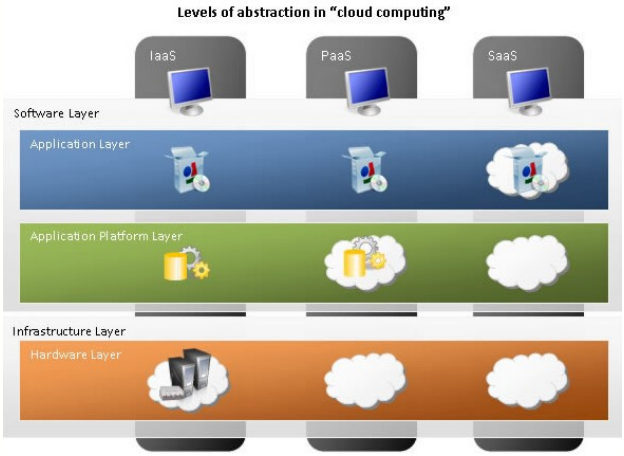

Figure 1: An architecture of the layer model of cloud computing

Cloud Service Deployment and Consumption Models :

Regardless of the delivery model utilized (SaaS, PaaS, IaaS) there are four primary ways in which cloud services are deployed (CSA Security Guidance, 2009). Cloud integrators can play a vital role in determining the right cloud path for a specific organization.

Public cloud: Public clouds are provided by a designated service provider and may offer either a single-tenant (dedicated) or multi-tenant (shared) operating environment with all the benefits and functionality of elasticity and the accountability/utility model of cloud. The physical infrastructure is generally owned by and managed by the designated service provider and located within the provider's data centers (off-premises). All customers share the same infrastructure pool with limited configuration, security protections, and availability variances. One of the advantages of a public cloud is that they may be larger than an enterprise cloud, and hence they provide the ability to scale seamlessly on demand.

Private cloud: Private clouds are provided by an organization or their designated services and offer a single-tenant (dedicated) operating environment with all the benefits and functionality of elasticity and accountability/utility model of cloud. The private clouds aim to address concerns on data security and offer greater control, which is typically lacking in a public cloud. There are two variants of private clouds: (i) on-premise private clouds and (ii) externally hosted private clouds. The on-premise private clouds, also known as internal clouds are hosted within one's own data center. This model provides a more standardized process and protection, but is limited in aspects of size and scalability. IT departments would also need to incur the capital and operational costs for the physical resources. This is best suited for applications which require complete control and configurability of the infrastructure and security. As the name implies, the externally hosted private clouds are hosted externally by a cloud service provider.

Hybrid cloud: Hybrid clouds are a combination of public and private cloud offerings that allow for transitive information exchange and possibly application compatibility and portability across disparate cloud service offerings and providers utilizing standard or proprietary methodologies regardless of

ownership or location. With a hybrid cloud, service providers can utilize third party cloud providers in a full or partial manner, thereby increasing the flexibility of computing. The hybrid cloud model is capable of providing on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to manage any unexpected surges in workload.

Table 1: Summary of the various features of cloud deployment models

Deployment Model	Managed By	Infrastructure Owned By	Infrastructure Located At	Accessible and Consumed By
Public	Third party provider	Third party provider	Off-premise	Untrusted
Private	Organization	Organization	On-premise Off-premise	Trusted
	Third party provider	Third party provider	On-premise Off-premise	
Managed	Third party provider	Third party provider	On-premise	Trusted or Untrusted
Hybrid	Both organization and third party provider	Both organization and third party provider	Both on-premise and off-premise	Trusted or Untrusted

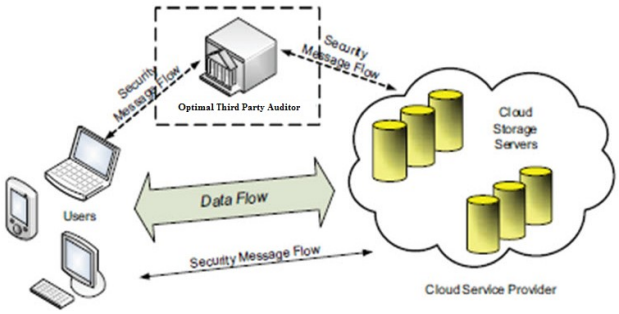

Figure 2: Cloud data storage model.

III. CLOUD DATA STORAGE CHALLENGES & ISSUES

The cloud computing does not provide control over the stored data in cloud data centers. The cloud service providers have full of control over the data, they can perform any malicious tasks such as copy, destroying, modifying, etc. The cloud computing ensures certain level of control over the virtual machines. Due to this lack of control over the data leads in greater security issues than the generic cloud computing model as shown in figure 1. The only encryption doesn't give full control over the stored data but it gives somewhat better than plain data. The characteristics of cloud computing are virtualization and multi tenancy also has various possibilities of attacks than in the generic cloud model.

The figure 2 has various issues those are discussed below in clearly.

According to Michael Gregg (2010) from Global Knowledge, an online IT training organization, provides several cloud-computing concerns regarding security in a white paper. These concerns can be visualized in Figure 3.

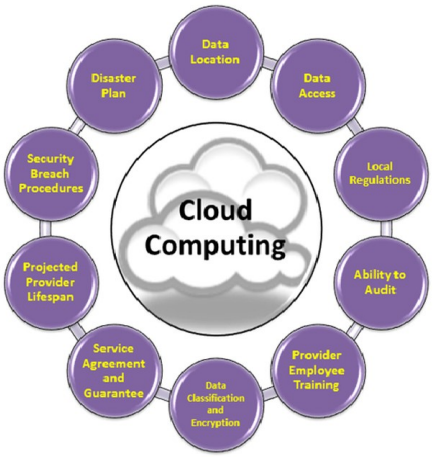

Figure 3. Ten concerns regarding cloud-computing security.

The Cloud Security Alliance (2010) has published a similar list but focuses on them more in the negative sense as threats. These are illustrated in Figure 4.

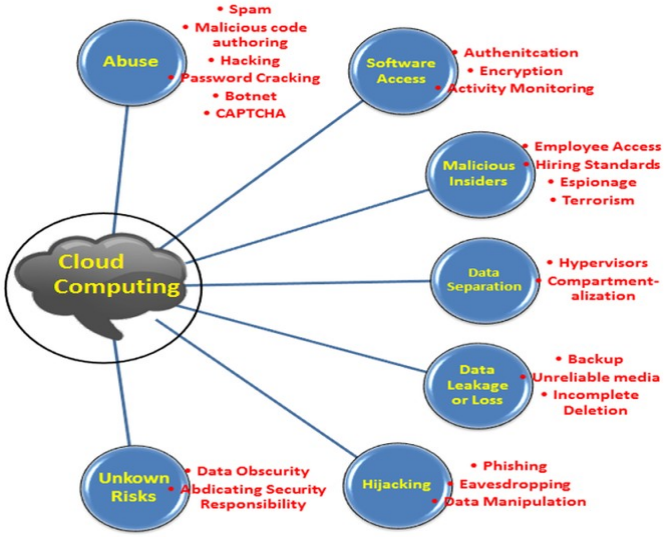

Figure 4. Seven Threats to security in cloud computing.

IV. LITERATURE SOLUTIONS

In this section, we explained the research work solutions and at the same time it also given the comprehensive discussion. The discussion can be made in several sub-chapters / sub sections.

4.1 Data storage issues solutions

The SecCloud is presented by Wei et al. [12], it provides a storage security protocol for cloud customer's data and it not only secures the stored data but also provides security on computational data. The SecCloud protocol uses encryption for storing data in secure mode. The multiplicative groups and cyclic additive pairing is used for key generation for cloud customers,

CSP, and other business partners or trusted third party. The encrypted data along with the verifiable signature is sent to cloud data center along with session key. The Diffie-Hellman algorithm is used for generation of session key for both bilinear groups. By receiving encrypted data the cloud decrypts the data, verifies the digital signature and stores the original data in specified location in cloud. The SecCloud verifies whether data is stored at specified location or not. The Merkle hash tree is used for computation security in SecCloud protocol. The verifying agency will verify the computational results that are building by using Merkle hash tree. The File Assured Deletion (FADE) protocol provides a key management with data integrity and privacy in [15].

The key management along with the data integrity and privacy are assured by File Assured Deletion protocol (FADE) proposed in [18].Because of FADE simplicity; it is a light weight protocol and uses both asymmetric and symmetric key encryption of data. The Shamir scheme protects symmetric and asymmetric keys to generous the trust in the key management. A group of key managers are used by FADE protocol, those acts as a trusted third party. The key *k* is used as encryption key for file *F* of the client and another key used for encryption of data key (*k.).* The policy file maintains the details that which files are accessible. So that, to upload data the user requests the key pair from the third party by sending policy file *p*. The key manager sends public and private keys to the user by using the policy file. The upload file encrypts with randomly generated *k* and *k* is encrypted with symmetric key. That encrypted file is decrypted with the public key of generated key pair and MAC is also generated for integrity check. The reverse process will be taken by the receiver to get back original data. Liu et al.[15] proposed a scheme that has a time based re-encryption with ABE algorithm to support secure data sharing among the group with access control. This scheme ensures that forwarded data safely reached to the group users and it maintains the user revocation. In this scheme, the time period is associated with every user and by expiration the revocation automatically by Cloud Service Provider (CSP). This time based encryption scheme allows users to share keys in prior with CSP and CSP generate re-encryption keys by taking request from user. The ABE protocol ensures an access control by examining the set of attributes rather than identity. This scheme ensures the privacy and availability of data among the group peoples but doesn't concentrate on data integrity.

4.2 Identity management and Access control solutions

The authors proposed Simple Privacy preserving Identity Management for Cloud Environments (SPICE) in [20] for identity management systems. The SPICE ensures group signature for providing the unidentified authentication, access control, accountability, unlink ability, and user centric authorization. The SPICE provides above mentioned properties with only a single registration. After user registration with trusted third party they obtain unique credentials for all the services provided by CSP. By using the credentials, user generates authentication certificate. Different CSPs expecting variety attributes for authentication and user has to generate their required form of authentication certificate with same credentials.

The Role Based Multi-Tenancy Access Control (RB_MTAC) been proposed in [21]. The RB_MTAC merges the role based access control scheme along with identity management. This requires user registration with CSP and obtains single credential that should be unique. The user has to choose the password while registration with CSP portal. By using these credentials the user can enter into the cloud environment by passing through identity module that uniquely identifies the user and after that it will be redirected to role assignment module that establish a connection to the RB_MTAC database and assigns the roles to registered user based on enrolled information.

4.3 Contractual and legal Issue solutions

In cloud computing environment, the users have great benefits because of simplicity and poses great risk in case of violation of service level agreements. The authors in [27] proposed a scheme

that reacts on Service Level Agreements (SLA) violations in order to reduce the security risks in cancellation / violation environment. This scheme concentrates on algorithm that performs renegotiation of risk awareness. The algorithm uses the scheme of to determine a minimum risk service among levels of service to fulfill the users need. The algorithm performs the scrutinizes and renegotiation of services at runtime environment for the replacement or cancellation of services. Finally it updates the risk factors according to the SLA.
Rak et al. [29] proposed a SPECS method that ensures architecture to provide a services termed as SLA-based security as a service. The proposed architecture mainly focused three aspects namely negotiation, enforcement, and monitoring. The SPEC recommends the enforcement activating factors by monitoring and reporting or system startup.

V. KEY SECURITY ISSUES IN CLOUD COMPUTING

Cloud computing consists of applications, platforms and infrastructure segments. Each segment performs different operations and offers different products for businesses and individuals around the world. The business application includes Software as a Service (SaaS), Utility Computing, Web Services, Platform as a Service (PaaS), Managed Service Providers (MSP), Service Commerce and Internet Integration. There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure and mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. The given below are the various security concerns in a cloud computing environment.

- Data Transmission
- Data Security
- Data Privacy
- Data Integrity
- Data Location
- Data Availability
- Data Segregation
- Securing Data-Storage

Data Transmission: Encryption techniques are used for data in transmission. To provide the protection for data only goes where the customer wants it to go by using authentication and integrity and is not modified in transmission. SSL/TLS protocols are used here. In Cloud environment most of the data is not encrypted in the processing time. But to process data, for any application that data must be unencrypted. In a fully homomorphism encryption scheme advance in cryptography, which allows data to be processed without being decrypted. To provide the confidentiality and integrity of data-in-transmission to and from cloud provider by using access controls like authorization, authentication, auditing for using resources, and ensure the availability of the Internet-facing resources at cloud provider. Man-in-the-middle attacks is cryptographic attack is carried out when an attacker can place themselves in the communication's path between the users. Here, there is the possibility that they can interrupt and change communications.

Data security: For general user, it is quite easy to find the possible storage on the side that offers the service of cloud computing. To achieve the service of cloud computing, the most common utilized communication protocol is Hypertext Transfer Protocol (HTTP). In order to assure the information security and data integrity, Hypertext Transfer Protocol Secure (HTTPS) and Secure Shell (SSH) are

the most common adoption. In a traditional on-premise application deployment model, the sensitive data of each enterprise continues to reside within the enterprise boundary and is subject to its physical, logical and personnel security and access control policies. However, in cloud computing, the enterprise data is stored outside the enterprise boundary, at the Service provider end. Consequently, the service provider must adopt additional security checks to ensure data security and prevent breaches due to security vulnerabilities in the application or through malicious employees. This involves the use of strong encryption techniques for data security and fine-grained authorization to control access to data. Cloud service providers such as Amazon, the Elastic Compute Cloud (EC2) administrators do not have access to customer instances and cannot log into the Guest OS. EC2 Administrators with a business need are required to use their individual cryptographically strong Secure Shell (SSH) keys to gain access to a host. All such accesses are logged and routinely audited. While the data at rest in Simple Storage Service (S3) is not encrypted by default, users can encrypt their data before it is uploaded to Amazon S3, so that it is not accessed or tampered with by any unauthorized party [13].

Data Privacy: The data privacy is also one of the key concerns for Cloud computing. A privacy steering committee should also be created to help make decisions related to data privacy. Requirement: This will ensure that your organization is prepared to meet the data privacy demands of its customers and regulators. Data in the cloud is usually globally distributed which raises concerns about jurisdiction, data exposure and privacy. Organizations stand a risk of not complying with government policies as would be explained further while the cloud vendors who expose sensitive information risk legal liability. Virtual co-tenancy of sensitive and non-sensitive data on the same host also carries its own potential risks [14].

Data Integrity: Data corruption can happen at any level of storage and with any type of media, So Integrity monitoring is essential in cloud storage which is critical for any data center. Data integrity is easily achieved in a standalone system with a single database. Data integrity in such a system is maintained via database constraints and transactions. Transactions should follow ACID (atomicity, consistency, isolation and durability) properties to ensure data integrity. Most databases support ACID transactions and can preserve data integrity. Data generated by cloud computing services are kept in the clouds. Keeping data in the clouds means users may lose control of their data and rely on cloud operators to enforce access control.

Data Location: In general, cloud users are not aware of the exact location of the datacenter and also they do not have any control over the physical access mechanisms to that data. Most well-known cloud service providers have datacenters around the globe. In many a cases, this can be an issue. Due to compliance and data privacy laws in various countries, locality of data is of utmost importance in many enterprise architecture. For example, in many EU and South America countries, certain types of data cannot leave the country because of potentially sensitive information. In addition to the issue of local laws, there's also the question of whose jurisdiction the data falls under, when an investigation occurs. Next in the complexity chain are distributed systems. In a distributed system, there are multiple databases and multiple applications [15].
In order to maintain data integrity in a distributed system, transactions across multiple data sources need to be handled correctly in a fail safe manner. This can be done using a central global transaction manger. Each application in the distributed system should be able to participate in the global transaction via a resource manager.

Data Availability: Data Availability is one of the prime concerns of mission and safety critical organizations. When keeping data at remote systems owned by others, data owners may suffer from system failures of the service provider. If the Cloud goes out of operation, data will become unavailable as the data depends on a single service provider. The Cloud application needs to ensure that enterprises are provided with service around the clock. This involves making architectural

changes at the application and infrastructural levels to add scalability and high availability. A multi-tier architecture needs to be adopted, supported by a load-balanced farm of application instances, running on a variable number of servers. Resiliency to hardware/software failures, as well as to denial of service attacks, needs to be built from the ground up within the application. At the same time, an appropriate action plan for business continuity (BC) and disaster recovery (DR) needs to be considered for any unplanned emergencies.

Data Segregation: Data in the cloud is typically in a shared environment together with data from other customers. Encryption cannot be assumed as the single solution for data segregation problems. In some situations, customers may not want to encrypt data because there may be a case when encryption accident can destroy the data. Make sure that encryption is available at all stages, and that these encryption schemes were designed and tested by experienced professionals [16].

Securing Data-Storage: Data protection is the most important security issue in Cloud computing. In the service provider's data center, protecting data privacy and managing compliance are critical by using encrypting and managing encryption keys of data in transfer to the cloud. Encryption keys share securely between Consumer and the cloud service provider and encryption of mobile media is an important and often overlooked need. PaaS based applications, Data-at-rest is the economics of cloud computing and a multitenancy architecture used in SaaS. In other words, data, when stored for use by a cloud-based application or, processed by a cloud-based application, is commingled with other users' data. In cloud computing, data co-location has some significant restrictions. In public and financial services areas involving users and data with different risks. The cloud-wide data classification will govern how that data is encrypted, who has access and archived, and how technologies are used to prevent data loss. At the cloud provider, the best practice for securing data at rest is cryptographic encryption and shipping self encrypting is used by hard drive manufacturers. Self-encrypting provides automated encryption with performance or minimal cost impact [17].

VI. CONCLUSION

The cloud computing architecture stores data and application software with minimal management effort and provides on demand services to customers through internet. But with cloud management customer don't have trust worthy commitments or policies. This will lead to many security issues with data storage such as privacy, confidentiality, integrity and availability. In this study we focused on data storage security issues in cloud computing and we first provided service models of cloud, deployment models and variety of security issues in data storage in cloud environment. In the final section, we addressed possible solutions for the data storage issues that provide privacy and confidentiality in cloud environment.

REFERENCES

[1] A. Abbas, K. Bilal, L. Zhang, S.U. Khan, A cloud based health insurance plan recommendation system: a user centered approach, Future Gener. Comput. Syst. (2014)
[2] P. Mell, T. Grance, The NIST definition of cloud computing (draft), NIST Special Publ. 800 (145) (2011) 7.
[3] J. Che, Y. Duan, T. Zhang, J. Fan, Study on the security models and strategies of cloud computing, Proc. Eng. 23 (2011) 586–593.
[4] R. Chandramouli, M. Iorga, S. Chokhani, Cryptographic key management issues and challenges in cloud services, in: Secure Cloud Computing, Springer, New York, 2014, pp. 1–30.
[5] C. Wang, Q. Wang, K. Ren, N. Cao, W. Lou, Toward secure and dependable storage services in cloud computing, IEEE Trans. Services Comput. 5 (2)(2012) 220–232.
[6] M. Balduzzi, J. Zaddach, D. Balzarotti, E. Kirda, S. Loureiro, A security analysis of amazon's elastic compute cloud service, in: Proceedings of the 27th Annual ACM Symposium on Applied Computing, 2012, pp. 1427–1434.
[7] Duncan, Adrian, Sadie Creese, and Michael Goldsmith. "Insider attacks in cloud computing." Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE, 2012.

[8] Khorshed, Md Tanzim, ABM Shawkat Ali, and Saleh A. Wasimi. "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing." Future Generation computer systems 28.6 (2012): 833-851.
[9] A. Andrieux, K. Czajkowski, A. Dan, K. Keahey, H. Ludwig, T. Nakata, J. Pruyne, J. Rofrano, S. Tuecke, M. Xu, Web services agreement specification.
[10] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, A. Ghalsasi, Cloud computing the business perspective, Decis. Support Syst. 51 (1) (2011) 176–189.
[11] B. Hay, K. Nance, M. Bishop, Storm clouds rising: security challenges for IaaS cloud computing, in: 44th Hawaii International Conference on System Sciences (HICSS), IEEE, 2011, pp. 1–7.
[12] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, A.V. Vasilakos, Security and privacy for storage and computation in cloud computing, Inform. Sci. 258 (2014) 371–386.
[13] O.D. Alowolodu, B.K. Alese, A.O. Adetunmbi, O.S. Adewale, O.S. Ogundele, Elliptic curve cryptography for securing cloud computing applications, Int. J.Comput. Appl. 66 (2013).
[14] M. Aslam, C. Gehrmann, M. Bjorkman, Security and trust preserving VM migrations in public clouds, in: IEEE 11th International Conference on Trust,Security and Privacy in Computing and Communications (TrustCom), 2012, pp. 869–876.
[15] Y. Tang, P.P. Lee, J.C.S. Lui, R. Perlman, Secure overlay cloud storage with access control and assured deletion, IEEE Trans. Dependable Secure Comput.9 (6) (2012) 903–916.
[16] Q. Liu, G. Wang, J. Wu, Time-based proxy re-encryption scheme for secure data sharing in a cloud environment, Inform. Sci. 258 (2014) 355–370.
[17] Z. Tari, Security and privacy in cloud computing, IEEE Cloud Comput. 1 (1) (2014) 54–57.
[18] Cloud security alliance, security guidelines for critical areas of focus in cloud computing v3.0, 2011.
[19] Y. Fu, Z. Lin, Exterior: using a dual-vm based external shell for guest-os introspection, configuration, and recovery, in: Proceedings of the 9th ACMSIGPLAN/SIGOPS International Conference on Virtual Execution Environments, 2013, pp. 97–110.
[20] S.M.S. Chow, Y. He, L.C.K. Hui, S.M. Yiu, Spicesimple privacy-preserving identity-management for cloud environment, in: Applied Cryptography and Network Security, Springer, Berlin, Heidelberg, 2012, pp. 526–543.
[21] S. Yang, P. Lai, J. Lin, Design role-based multi-tenancy access control scheme for cloud services, in: IEEE International Symposium on Biometrics and Security Technologies (ISBAST), 2013, pp. 273–279.
[22] R.D. Dhungana, A. Mohammad, A. Sharma, I. Schoen, Identity management framework for cloud networking infrastructure, in: IEEE International Conference on Innovations in Information Technology (IIT), 2013, pp. 13–17.
[23] Boneh, Dan, and Matthew Franklin. "Identity-based encryption from the Weil pairing." SIAM Journal on Computing 32.3 (2003): 586-615.
[24] Z. Yan, P. Zhang, A.V. Vasilakos, A survey on trust management for Internet of things, J. Netw. Comput. Appl. 42 (2014) 120–134.
[25] S. Ruj, M. Stojmenovic, A. Nayak, Decentralized access control with anonymous authentication of data stored in clouds, IEEE Trans. Parallel Distrib. Syst. 25 (2) (2014) 384–394
[26] Z. Wan, J. Liu, R.H. Deng, HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing, IEEE Trans. Inform. Forensics Sec. 7 (2) (2012) 743–754.
[27] M.L. Hale, R. Gamble, Risk propagation of security SLAs in the cloud, in: IEEE Globecom Workshops (GC Wkshps), 2012, pp. 730–735.
[28] M.L. Hale, R. Gamble, Secagreement: advancing security risk calculations in cloud services, in: IEEE Eighth World Congress on Services (SERVICES), 2012, pp. 133–140.
[29] M. Rak, N. Suri, J. Luna, D. Petcu, V. Casola, U. Villano, Security as a service using an SLA-based approach via SPECS, in: IEEE 5th International Conference on Cloud Computing Technology and Science (CloudCom), vol. 2, 2013, pp. 1–6.
[30] Patel, Ahmed, et al. "An intrusion detection and prevention system in cloud computing: A systematic review." *Journal of Network and Computer Applications* 36.1 (2013): 25-41.
[31] Reddy, V. Krishna, B. Thirumala Rao, and L. S. S. Reddy. "Research issues in cloud computing." *Global Journal of Computer Science and Technology* 11.11 (2011).
[32] V. Krishna Reddy, B. Thirumal Rao, Dr. L.S.S. Reddy, P.Sai Kiran "Research Issues in Cloud Computing " Global Journal of Computer Science and Technology, Volume 11, Issue 11, July 2011.
[33] Cloud Computing: Security Issues and Research Challenges Rabi Prasad Padhy1 Manas Ranjan Patra2 Suresh Chandra Satapathy3 Senior Software Engineer Associate Professor HOD & Professor Oracle India Pvt. ltd. Dept. of Computer Science Dept. of Computer Sc. & Engg. Bangalore, India Berhampur University, India ANITS, Sanivasala, India