A Study of Security Issues in Cloud Computing on Data Storage

Mrs.S.Sivakamasundari, Assistant Professor, Dept of Computer Science ,New Prince Shri Bhavani Arts and Science College

Dr.V.Umadevi, Associate Professor, Dept of Computer Science ,New Prince Shri Bhavani Arts and Science College

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 respective issues in cloud.

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

1. Introduction:

Cloud computing is a revolutionary technology that changing way to enterprise hardware and software design and procurements. Cloud Computing is a network of remote servers hosted on the internet for storing and retrieving data. The cloud provides a number of IT services such as servers, databases, software, virtual storage, and networking, among others. Companies that offer all the services are called cloud providers. The cloud computing gives wealthy benefits to the cloud clients such as costless services, flexibility of resources, simple access through web, etc.

From little to expansive enterprises strong towards cloud computing to extend their trade and tie-ups with other undertakings [1]. Even though cloud computing has enormous benefits, cloud user are unwilling to put their private or touchy information, it includes individual health records, emails and government touchy records. 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 instruments would not give the total data security since of its vulnerabilities' over the arrange and CSPs have full command on cloud applications, hardware and client's data. Encrypting touchy data some time recently hosting can merit data security and privacy
against CSP. A ordinary issue with encryption
plot is that it is unreasonable since of huge sum communication overheads over the cloud get to designs.
Therefore, cloud needs secure methods to storage and management to preserve the data confidentiality and privacy [2][5]. This paper mainly centers on security vulnerabilities and issues in privacy and protection over client data.

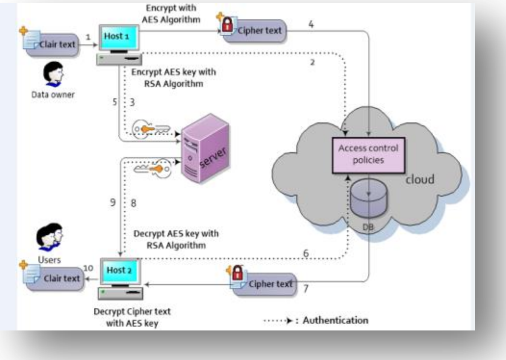


Figure 1: Cloud data storage model.

2. Cloud Data Storage Challenges & Issues:

The cloud computing does not provide control over the stored data in cloud data centers. The cloud service suppliers have full of control over the information, they can perform any malicious tasks such as duplicate, destroying, altering, etc. The cloud computing ensures certain level of control over the virtual machines. Due to this need of control over the information leads in more prominent security issues than the bland 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 different possibilities of attacks than in the generic cloud model. The figure 2 has various issues those are discussed below in clearly.

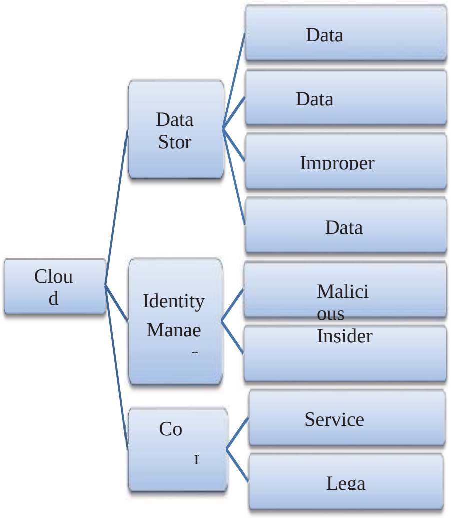


Figure 2. Cloud security Challenges

2.1 Cloud Storage issues:

2.1.1 Data privacy and Integrity:

Even though cloud computing give less cost and less asset administration, it has a few security dangers. As we examined prior cloud computing needs to guarantee integrity, privacy, security and accessibility of information in nonexclusive cloud computing demonstrate but the cloud computing demonstrate is more defenseless to security threats in terms of over conditions. .Since of simplicity cloud users are increasing exponentially and applications are facilitated in cloud is exceptionally tall. These situations lead to more prominent security threats to cloud clients. In case any assault is effective on data substance will leads to information breach and takes an unauthorized get to information of all cloud clients. Because of this integrity violation cloud data lost multi-tenant nature. Especially SaaS providers may also lost their technical data and they have great risk over data storage. Apart from these risks, data processing also has great risk while data being transformed among multiple tenants. Because of virtualization multiple physical resources are shared among the users. This leads to launch attacks by malicious insiders of the CSP and/or organization. These situations may allow the malicious user to perform attacks on stored data of other customer while processing their data. Other major risk is when data is outsourced to third party storage by the CSP [5]. The key generation and key management in cryptography for cloud computing is not standardized up to the mark. But without standard and secure key management for the cloud doesn’t allow the standard cryptography algorithms to perform well in generic cloud computing model. Such that cryptography may also ensures the potential risks to cloud computing.

2.1.2 Data recoverability and vulnerability

Due to resource pooling and elasticity characteristics, the cloud ensures dynamic and on-demand Resource provisioning to the users. The resource allocated to a particular user may be assigned to the other user at some later point of time. In case of memory and storage resources, a malicious user can employ data recovery techniques to obtain the data of previous users [13]. The authors in [13] were able to recover Amazon machine images files 98 % of the times. The data recovery vulnerability can pose major threats to the sensitive user data .

2.1.2 Improper media refinement.

The storage medias are sanitize because of following reasons
(i) the disk may needs to replace with other disk
(ii) No need to maintain the disk or no longer to maintain
(iii) massacre of services. Improper refinement ensures great risk to stored data. In multi-tenant cloud it is not possible to refine as it is earlier tenant.

2.1.3 Data backup:

The data backup is an important when accidental and/or intentional disasters. The CSP has to perform regular backups of stored to ensure the data availability. In fact, the backup data should be keeping with security guidelines to prevent malicious activities such as tampering and unauthorized access.

2.2. Identity Management and Access Control:

The judgment and privacy of information and administrations are related with get to control and character administration. It is vital to preserve track record for client personality for dodging unauthorized get to to the put away information .The personality and get to controls are complex in cloud computing since of that information proprietor and put away information are at diverse official stages. In cloud environment, diverse organizations utilize assortment of verification authorization plan. By utilizing distinctive approaches for confirmation and authorization gives a compound circumstance over a period of time. The cloud assets are energetic and are versatile for cloud client and IP addresses are ceaselessly changed when administrations are begun or restarted in pay per utilization demonstrate .That permits the cloud clients to connect and take off include to cloud assets when they required i.e., on-demand get to approach. All these highlights require proficient and successful get to control and personality administration. The cloud has got to keep up rapidly upgrading and overseeing character administration for joining and taking off clients over cloud assets. There are numerous issues in get to control and personality administration, for case frail qualifications may reset effectively, refusal of benefit assault to bolt the account for a period of time, Frail logging and observing capacities, and XML wrapping assaults on web pages.

Malicious Insiders:

An insider risk can be postured by representatives, temporary workers and /or third party trade accomplices of an organization. In cloud environment i.e., at Cloud Benefit Supplier (CSP) side assaults leads to misfortune of user's data keenness, privacy, and security. This leads to information incident or breaches at both situations..This assault is valuable and it is well known to most of the organization [7].There is assortment of assault designs performed by insiders since of modernity almost inside structure of an organization information capacity structure. Most organizations disregarding this assault since it is exceptionally difficult to guard and inconceivable to discover the total arrangement for this assault. This assault guarantees awesome chance in terms of information breaches and misfortune secrecy at both organization and cloud level [8].

2.1.2 outside Intruder:

Assaults that come from outside roots are called pariah assaults [30]. Information security is one of the critical issue in cloud computing. Since benefit suppliers does not have authorization for get to to the physical security framework of information centers. But they must depend on the foundation supplier to induce full information security. In a virtual private cloud environment, the benefit supplier can as it were indicate the security setting remotely, and we don't know precisely those are completely executed. In this Handle, the framework supplier must reach the taking after targets: (1) privacy, for secure information exchange and get to, and (2) review capacity [31]. So that exterior gatecrashers can't access delicate information which is put away in cloud.

2.3 Contractual and Legal issues:

After moving to cloud computing environment, there are numerous issues in geographic locales, administrative law, execution confirmation, contract authorizations, etc. The over said issues are comes beneath the legalities, Benefit Level Understandings and information area in information centers [9].

2.3.1. Service level agreements:

The Benefit Level Understanding (SLA) can be portrayed as a convention, it indicates set of conditions and terms among client and Cloud benefit supplier. The SLA ought to indicate the taking after: Activities that CSP will taken when information breach happened, medicinal activities and execution level at least level [5]. The clients ought to have clear see on security for their assets and all other necessities ought to be concurred upon the SLA. The contract authorization getting to be issues since insights given by CSP are completely problematic. At last, the contracts are non-negotiable and pre-defined that has got to be in inviting way between CSP and client. The administrative laws such as Sarbanes- Oxley and HIPAA gotten to be an open issue [10].

2.3.2. *Legal issues:*

The legitimate issues emerge since that the nearness CSP assets in topographically clashing different lawful purviews [11]. In the event that the client is moved to one geological to other, an issue will happen since of diverse lawful locales. For a development information is conveyed over a different information centers, those are possessed by CSP those have diverse laws and security rules. This situation may takes into the genuine issue in cloud computing.

3. Literature Solutions:

In this area, we clarified the investigate work arrangements and at the same time it too given the comprehensive dialog. Comes about displayed in tables that make the peruser get it effortlessly The talk can be made in a few sub-chapters.

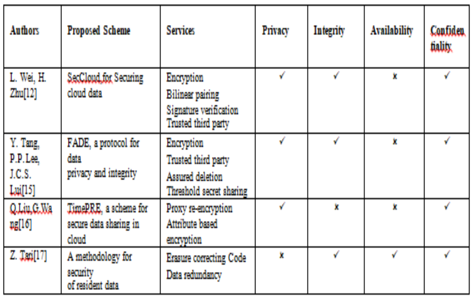
3.1 *Data storage issues solutions:*

The SecCloud is displayed by Wei et al. [12], it gives a capacity security convention for cloud customer's information and it not as it were secures the put away information but moreover gives security on computational information. The SecCloud convention employments encryption for putting away information in secure mode. The multiplicative bunches and cyclic added substance blending is utilized for key era for cloud clients, CSP, and other commerce accomplices or trusted third party. The scrambled information beside the verifiable signature is sent to cloud information center at the side session key. The Diffie-Hellman calculation is utilized for era of session key for both bilinear bunches. By accepting scrambled information the cloud unscrambles the information, confirms the advanced signature and stores the first information in indicated area in cloud. The SecCloud confirms whether information is put away at indicated area or not. The Merkle hash tree is utilized for computation security in SecCloud convention. The confirming office will confirm the computational comes about that are building by utilizing Merkle hash tree. The Record Guaranteed Cancellation (Blur) convention gives a key administration with information keenness and security in[15].

The key administration at the side the information astuteness and protection are guaranteed by Record Guaranteed Deletion protocol (FADE) proposed in [18].Because of Blur effortlessness; it could be a light weight convention and employments both hilter kilter and symmetric key encryption of information. The Shamir plot ensures symmetric and deviated keys to liberal the believe within the key administration. A gather of key directors are utilized by Blur convention, those acts as a trusted third party. The key k is utilized as encryption key for record F of the client and another key utilized for encryption of information key (k.). The approach record keeps up the subtle elements that which records are open. So that, to transfer information the client demands the key combine from the third party by sending approach record p. The key supervisor sends open and private keys to the client by utilizing the arrangement record. The transfer record scrambles with haphazardly produced k and k is scrambled with symmetric key. That scrambled record is unscrambled with the open key of produced key combine and MAC is additionally produced for judgment check. The invert handle will be taken by the collector to induce back original data. Liu et al.[15] proposed a plot that contains a time based re-encryption with ABE calculation to back secure data sharing among the bunch with get to control. This plot guarantees that sent information securely come to to the gather clients and it keeps up the client denial. In this conspire, the time period is related with each client and by close the disavowal consequently by Cloud Benefit Supplier (CSP). This time based encryption plot permits clients to share keys in earlier with CSP and CSP produce re-encryption keys by taking ask from client. The ABE convention guarantees an get to control by looking at the set of traits instead of character. This plot guarantees the security and accessibility of information among the bunch people groups but doesn't concentrate on information keenness.

The probabilistic examining is utilized to diminish the computational excess rather than revamping the total tree once more. The underneath list are key suggestions by the Computer Security Collusions (CSA) [18] for the information security and successful key administration. The scope of key ought to be kept up by gather or person. The standard encryption calculations ought to be utilized and frail calculations ought to discard. The best rules for key administration and encryption program items ought to be utilized, it is superior to utilize authentic program innovation to guarantee security on capacity. The client or organizations and/or trusted third party ought to keep up successful key administration. In the event that the disgraceful reviewing convention is planned, encryption handle may control the information stream to outside parties amid the examining. But encryption itself does not avoid information stream to outside parties but instep it can diminish it a few negligible level. But it requires incredible extend of key administration handle and overheads for key era whereas putting away information. But introduction of encryption key leads to information spillage and it still a issue in cloud environment. This issue is tended to by combining the homomorphic authenticator in conjunction with the arbitrary veiling handle [19]. Outlined within the taking after Table 1.

Table 1. The Possible Solutions of Data storage issues

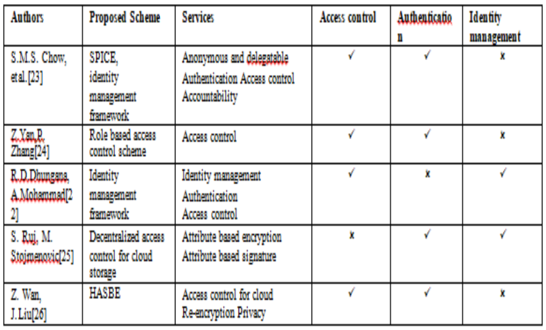


Authors	Proposed Scheme	Services	Privacy	Integrity	Availability	Confiden tiality
L. Wei, H. Zhu[12]	SecCloud for Securing cloud data	Encryption Bilinear pairing Signature verification Trusted third party	✓	✓	✗	✓
Y. Tang, P.P.Lee, J.C.S. Lui[15]	FADE, a protocol for data privacy and integrity	Encryption Trusted third party Assured deletion Threshold secret sharing	✓	✓	✗	✓
Q.Liu,G.Wang[16]	TimePRE, a scheme for secure data sharing in cloud	Proxy re-encryption Attribute based encryption	✓	✗	✗	✓
Z. Tari[17]	A methodology for security of resident data	Erasure correcting Code Data redundancy	✗	✓	✓	✓

3.2 Identity management and Access control solutions:

The creators proposed Basic Protection protecting Personality Administration for Cloud Situations (Flavor) in [20] for personality administration frameworks. The Flavor guarantees gather signature for giving the unidentified verification, get to control, responsibility, unlink capacity, and client centric authorization. The Flavor gives over said properties with as it were a single enrollment. After client enlistment with trusted third party they get interesting qualifications for all the administrations given by CSP. By utilizing the accreditations, client creates verification certificate. Diverse CSPs anticipating assortment properties for verification and client must create their required frame of confirmation certificate with same accreditations. The Part Based Multi-Tenancy Get to Control (RB_MTAC) been proposed in [21]. The RB_MTAC combines the part based get to control conspire together with personality administration. This requires client enlistment with CSP and gets single credential that ought to be interesting. The client has got to select the secret word whereas enrollment with CSP entrance. By utilizing these qualifications the client can enter into the cloud environment by passing through personality module that interestingly identifies the client and after that it'll be diverted to part task module that build up a association to the RB_MTAC database and allocates the parts to enlisted client based on enlisted data. Dhungana et al. [22] proposed a conspire for the cloud organizing framework as character administration system and it is kept up by Client overseen Get to (UMA) convention. Here CSP acts as a have, whereas the authorized utilized acts as benefit proprietor. The authorization director handles the benefit administration and benefit asking clients moreover overseen by authorization supervisor. This plot guarantees the personality administration and get to control over different Cloud suppliers with the assistance of authorization administration. Illustrated in the following Table 2.

Table 2. The Solutions of Identity management and Access control



Authors	Proposed Scheme	Services	Access control	Authenticatio n	Identity management
S.M.S. Chow, et.al.[23]	SPICE, identity management framework	Anonymous and delegatable Authentication Access control Accountability	✓	✓	✗
Z.Yan,P. Zhang[24]	Role based access control scheme	Access control	✓	✓	✗
R.D.Dhungana, A.Mohammad[22]	Identity management framework	Identity management Authentication Access control	✓	✗	✓
S. Rui, M. Stojmenovic[25]	Decentralized access control for cloud storage	Attribute based encryption Attribute based signature	✗	✓	✓
Z. Wan, J.Liu[26]	HASBE	Access control for cloud Re-encryption Privacy	✓	✓	✗

Conclusion:

The cloud computing engineering stores information and application computer program with negligible administration exertion and gives on request administrations to clients through web. But with cloud administration client don't have believe commendable commitments or approaches. This will lead to numerous security issues with information capacity such as protection, secrecy, judgment and accessibility. In this ponder we centered on information capacity security issues in cloud computing and we to begin with given benefit models of cloud, arrangement models and assortment of security issues in information capacity 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. ServicesComput. 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. DependableSecure 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, IEEETrans. 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).