A research on security problems with data storage in cloud computing

1Komuravelly Sudheer Kumar,2Kanegonda Ravi Chythanya,3Bhavana Jamalpur and 4Dandugudum Mahesh, 5Bonthala Prabhanjan Yadav

1 Department of Computer Science and Engineering, S R University, Warangal, Telangana.
2, 3, 4 Department of Computer Science and Engineering, S R Engineering College, Warangal, Telangana.
5Sumathi Reddy Institute of Technology for Women, Warangal, Telangana.

Email:sudheerkomuravelly@gmail.com

Abstract. Cloud computing is a transformative mechanism that changes the way hardware and software design and procurement are built for businesses. Everybody pushes data and application applications to cloud data centers due to cloud simplicity. The Cloud Service Provider (CSP) can maintain integrity, accessibility, privacy, and confidentiality, but CSP does not provide client and stored customer data with secure data services. This research discusses problems related to the storage of cloud data, such as data breaches, data theft, and cloud data unavailability. Finally, we are offering potential solutions to related cloud problems.

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

1. Introduction
Cloud Infrastructure is the transformative mechanism for the development and acquisition of enterprise applications and hardware. Cloud computing offers rich advantages for cloud users such as expensive resources, resource elasticity, fast internet access, etc. From small to large cloud-based enterprises, their businesses can develop and connect with other companies [1]. Although cloud storage has great advantages, cloud users do not want to provide personal and confidential data [33], it contains patient information, electronic-mails and files that are government sensitive [32]. Suppose the cloud customer lost control of the data sources until the data was placed in a cloud data centre. The cloud service provider (CSPs) promises to ensure data protection by using methods such as firewalls and virtualization through stored data from cloud clients. These systems are not highly secured due to their network instability, and cloud applications, software and client data managed by CSPs is totally out of the question. Sensible data encryption prior to hosting may warrant CSP privacy and confidentiality. One typical issue with encryption is the fact that vast quantities of communication overhead over the cloud access patterns make it difficult to use it. The cloud also requires protected storage and maintenance approaches to ensure security and confidentiality of the data [2] [5]. This paper is specifically dealing with protection and privacy concerns relating to consumer records.
2. Challenges & problems for cloud data management
Cloud computing does not track data stored in cloud computing environments. The data is managed by
the cloud service providers and can accomplish all malicious tasks like copying, destruction and
alteration, etc. Cloud computing guarantees a degree of automated machinery power. This lack of data
protection created greater security problems that were seen in Figure 1 in the conventional cloud model.
The only encryption offers a bit more than just basic data rather than absolute control of the stored data.
Virtualization and numerous attacks options and in the cloud model are part of the cloud computing
functionality. Figure 2 has different questions that are explicitly addressed below.
2.1 Issues with cloud storage

2.1.1 Data protection and credibility
While cloud computing offers minimal costs and least management of resources, may does present security threats. In the context of earlier discussion on cloud computing, integrity and secrecy must be ensured, as well. Databases should be kept safe in the generic cloud computing model. Due to the simplicity of cloud users, applications are being hosted in the cloud. This leads to increased security threats for cloud customers. If a data entity attack is successful, data breakage is carried out and data access for all cloud users is unauthorized. Cloud data lost a multi-tenant nature due to this integrity violation. SaaS providers in particular may also lose their technological data and have a significant risk of storing data. Apart from these threats, the transformation of data between multiple locators also poses a great risk. Due to virtualization, some physical resources are shared between users. This allows the CSP and/or the malicious insiders of the firm to invade. These situations can allow malicious users to invade the information which is deposited from other customers while cleansing their information. Another critical hazard is the outsourcing of information to CSP storage by third parties [5]. Cloud computing key generation and key control in cryptography is not standardized. However, the standard encryption algorithms do not function properly in the generic cloud computing model without standard and stable key management for the cloud. This can also ensure that cloud computing is subject to potential risks.

2.1.2 Recoverability of data and vulnerability
The flexible and then on-demand cloud ensures supply of resources to users due to resource pooling and flexibility characteristics. At some later time the resource allocated to a specific user may be allocated to the other user. When it comes to storage memory and money, a malicious user may use techniques to retrieve data from previous users [13]. The authors of Amazon machine images could recover 98 percent of the time in [13]. The weakness in information retrieval can pose serious hazards to confidential user information.

2.1.3 Inadequate media refinement
Data files are disinfect because (i) the disc will have to be replaced by another disc (ii) the disc massacre can no longer be retained or retained (iii). Improper refining places stored data at great risk. In the multi-tenant cloud, it is not practical to refine since it is a former tenant.

2.1.4 Backup the data
In unexpected and/or intentional disasters the data backup is a significant thing. In order to maintain data availability the CSP must periodically back up its stored data. In fact, security directives for preventing malicious acts like exploitation and unauthorized access should follow the backup data.

2.2 Management of identity and access
Data and services are related to the integrity and confidentiality of access control and identity management. It is necessary to maintain a user identity track record in order to prevent unauthorized access to the data files. Due to this data owners and stored data on various executive networks, identity and access controls in cloud computers are complex [36]. Various organizations use a varied authentication permission agenda in the cloud world. A membrane approach has been taken during a certain span by using various identity and access management approaches [35]. When pay-per-use service is restarted or started, cloud resources for cloud users and IP addresses are changed continuously. This allows cloud users to add cloud services and leave them on demand, i.e. access policies. All of these
functions include a secure, efficient ID and control of access. The cloud needs to easily upgrade and manage identity management to allow users to join and leave cloud services. There are various problems in access management and identity protection, such as the simple reselection of weak identities, denial of services, weak logging and tracking capabilities as well as the XML wrapping of attacks from web pages.

2.2.1 Insiders malicious
Employees, contractors and/or business associates of an organization can pose an insider threat. Side attacks on Cloud Service Provider (CSP) causing the loss of user integrity, confidentiality and protection in the cloud world. In all environments, this leads to knowledge loss and breaches. This attack is useful and is well known to much of the organization [7]. Multiple attack patterns by insiders are carried out due to complexity in the internal layout of the data storage structure of the organization. Most companies disregard this attack because the full solution for this attack is very hard to protect and difficult to find. The attack guarantees great risk in terms of both company and cloud data violations and damage confidentiality [8].

2.2.2 External intruders
Out-of-the-box attacks are known as foreign attacks [30]. The protection of data is one of the key issues of cloud computing. Service providers do not have permission to access the data centers’ physical security system. They must however rely on the provider for maximum data security. The service provider can only specify the security setting remotely in a virtual private cloud environment, and we do not know exactly how to execute it. In the sense of this process, the Provider of Infrastructures can achieve: (1) privacy, protection and access and (2) audit capacity [31]. This way confidential data stored in the cloud cannot be accessed by outside intruders.

2.3 The issues of contractual and legal matters
There are a number of problems after switching to a cloud computing system in regional jurisdictions, legislation, performance assurance, contract compliance. The problems mentioned above are protected by regulations, service level agreements and location of data in data centers [9].

2.3.1 Accords at service level
A protocol may be described as a Service Level Agreement (SLA), specifying the conditions and terms between the user and Cloud service provider. The SLA should specify: action taken by the CSP when data violation has occurred, corrective action and minimum level performance [5]. The users should have a good understanding of their resources’ security and the SLA should agree on all other specifications. The implementation of the contract becomes a problem as the CSP provides totally unproven statistics. Finally, contracts between CSP and consumer are non-negotiable and must be pre-defined. Sarbanes-Oxley and HIPAA, too, become an open question in regulatory legislation [10].

2.3.2 Legal concerns
Legal problems arise because CSP tools exist in separate jurisdictions that are geographically contradictory [11]. When the consumer is relocated to one geographical area, a problem will arise due to various rules. For the distribution of movement data through different data centers, which are CSP owned and have numerous laws and protection guidelines. In cloud computing this scenario could address the major problem.

3. Literature Solutions
We addressed the solutions for research in this section and addressed them at the same time. Results displayed in tables that make it easy to understand. There are a variety of sub-chapters for discussion.

3.1 Solutions of Problems with data management
The SecCloud is introduced by Wei et al.[12], provides a security storage protocol for the data for cloud users, not only secure the stored data, but also offers computer data security. For safe storage of data, the SecCloud protocol uses encryption. For cloud clients, CSP, and other business partners or trusted third parties, multiple grouping and cyclic addition combinations are used. The encrypted data and the checkable signature are sent with the session key to the cloud data centre. For session-key generation for both bilinear groups, the Diffie-Hellman algorithm is used. The cloud decrypts data, tracks the digital signature, and stores original data when encrypted data is received in cloud place. The SecCloud checks whether the data is being processed at the specified site. The Merkle hash tree is used for computer protection in the SecCloud protocol. The research agency verifies computer results with the aid of Merkle hash tree. The File Assured Deletion Protocol (FADE) provides the key management with data integrity and privacy[15].

File Assured Deletion Protocol (FADE) proposed in [18] guarantees the core management and data integrity and privacy. The protocol is simple to use and uses asymmetrical and symmetrical data coding. The Schamir device covers symmetric and asymmetrical keys in order to generously trust key control. A network of key managers is used by the FADE protocol as trustworthy third parties. The key k is used for file F of the client and another key for data key encryption (k.). The regulation file includes extensive files. The user can upload details by uploading a policy file p to the third party key pair. The key manager sends private and public keys to the user by using the policy file. To encrypt upload files with the random k and k generated, you use a symmetrical key. The created key pair and MAC for integrity control is decrypted with the public key. This file is created for encryption. The reverse procedure is performed by the recipients to recover original data.

Liu et al. [15] proposed a re-encryption scheme using the ABE algorithm in time to facilitate secure data sharing between the access control groups[34]. This scheme ensures that the transmitted data is safely reached by the community and that user revocation is preserved. The duration for each user and the revocation by the Cloud Service Provider (CSP) is automatically connected to this scheme. This time-based cryptographic system enables users to share keys before the generation of CSP and CSP, by requiring the user. The ABE protocol guarantees access control by checking the collection of attributes instead of identity[37-39]. This scheme guarantees privacy and data availability in the community, but does not depend on the integrity of data.

The probabilistic sample is used instead of restoring the entire tree to reduce the computer redundancy. The following list contains key data protection and productive key management guidelines from the Computer Security Alliances (CSA). Group or individual should retain the scope of the key. It is necessary to use the standard encryption algorithms and discard weak algorithms.

It is easier to use legal software technologies to ensure protection in storage, to apply the best guidelines for key management and encryption software products. Efficient key management can continue for customer or organizations and/or trusted third parties. When the incorrect protocol for auditing is designed, encryption can control external auditing data flows. However, encoding itself does not prevent flow of data to outside parties, but rather can minimize it. However, it requires a wide variety of key management processes and overheads for data storage. However, a cription key exposure contributes to data leakage and in the cloud world, it is still a concern. The homogeneous authenticator is combined with the random masking process[19] to resolve the problem. This is shown in Table 1 below.

Table 1. The potential solutions of data stocking challenges

| Authors          | Scheme Proposed | Services | Confidentiality | Integratedness | Offerings | Tiality of trust |
|------------------|-----------------|----------|----------------|----------------|-----------|-----------------|

5
3.2 Management of identities and solutions for access control

The authors suggested easy privacy protection to preserve identity management in cloud environments in [20] for identity management systems. SPICE guarantees community signature, access control and obligations, and unlink capabilities as well as user centric authorization for unspecified authentication. The SPICE only offers one registry of the properties mentioned above. All services offered by CSP receive unique credentials upon registration with a reputable third party. User uses the credentials to build authentication certificates. Different CSPs with various authentication attributes and users have to produce their required authentication form with the same credentials.

In [21], the Role Based Multi-Tenancy Access Control was proposed (RB MTAC). The RB MTAC fuses the role-based access control and ID management system. This requires CSP user registration and obtains unique credentials. You have to select the password during your CSP portal registration. These credentials enables users to access a cloud environment by transferring a user-identified ID module and then forwarding the user to the RB MTAC database role assignment module to allocate the user roles based on registered information.

As a system for identity management, Dhungana et al. [22] suggested a cloud network infrastructure scheme and the protocol User Managed Access (UMA) has been maintained. The CSP acts
here as a host, while the approved host is the owner of a service. The authorization manager also oversees users handled by authorization manager in the management of services and service. With the aid of authorization management, this system ensures identity management and the access check across many cloud providers. It was illustrated in Table 2 below.

### Table 2. Identity management and access management solutions

| Authors                              | Scheme Proposed                                      | Services                                      | Regulation of access | Authentizing | Management of identity |
|--------------------------------------|------------------------------------------------------|-----------------------------------------------|----------------------|--------------|------------------------|
| S.M.S. Chow, et al.[23]              | SPICE, framework for identity management             | Delegated and anonymous Access Control for Authentication Responsibility | ☐                    | ☐            | ☐                      |
| Z.Yan, P. Zhang[24]                  | Access control system focused on functions           | Regulation of access                          | ☐                    | ☐            | ☐                      |
| R.D. Dhungana, A. Mohammad[22]       | System for Identity Management                       | Management of Identity Authentizing           | ☐                    | ☐            | ☐                      |
| S. Ruj, M. Stojmenovic[25]           | Cloud storage decentralized access control           | Encryption based on attribute Signature attribute based | ☐                    | ☐            | ☐                      |
| Z. Wan, J. Liu[26]                   | HASBE                                                | Cloud Access Management Privacy re-encoding   | ☐                    | ☐            | ☐                      |

### 3.3 Contractual and legal issue solutions

Users benefit immensely from the flexibility of Cloud computing and face considerable risk in the event that service level agreements are broken. The authors in [27] suggested that a scheme to reduce safety risks in a cancellation / violation environment react to Service Level Agreements (SLA). This scheme focuses on the renegotiation of risk awareness algorithm. The scheme of the algorithm is used [28] Determination of a low risk service between service levels to meet user requirements. The algorithm conducts scrutinizing and renegotiation of services to substitute or cancel services in runtime environments. It eventually updates the SLA risk factors.
Table 3. Contractual and legal approaches feasible

| Authors                  | Scheme Proposed | Services                          | Negotiation | Implementation | Surveillance |
|--------------------------|-----------------|-----------------------------------|-------------|----------------|--------------|
| M.L. Hale, R. Gamble[28] | SecAgreement    | SLA integration of safety parameters According to WS | ☐           | ☐              | ☐            |
| M. Rak, N. Suri[29]      | SPECS, SLA-based | Matchmaking protection integration | ☐           | ☐              | ☐            |

Rak et al. [29] have proposed a method of SPECS to ensure that a service called SLA-based security is delivered as a service by architecture. Three aspects were mainly focused on negotiation, implementation and monitoring. By tracking and reporting or device start up, SPEC recommends compliance triggering variables.

4. Conclusion

Data and application applications are processed with minimum management effort in the cloud computing architecture and offer customers on-demand service online. However, the clients of Cloud Management have no worthwhile promises or policies. This leads to many safety concerns such as anonymity, confidentiality, completeness and accessibility. We concentrated in this study on cloud computing data storage security issues. We also initially provided cloud service models, implementation models and various security concerns for cloud-based data storage. We discussed possible solutions in the final section to data storage issues which provide cloud privacy and confidentiality.

5. References

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

[8] Khorshed, Md Tanzim, ABM Shawkat Ali, and Saleh A. Wasimi and 2012, "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing," Future Generation computer systems 28.6: 833-851.

[9] A. Andrieux, K. Czajkowski, A. Dan, K. Keahey, H. Ludwig, T. Nakata, J. Pruyne, J. Rofrano, S. Tucek and M. Xu ,2007 ,Web services agreement specification.

[10] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang and A. Ghalsasi, 2011, Cloud computing the business perspective, Decis. Support Syst. 51 (1) 176–189.

[11] B. Hay, K. Nance and M. Bishop, 2011, Storm clouds rising: security challenges for IaaS cloud computing, 44th Hawaii International Conference on System Sciences (HICSS), IEEE, pp. 1–7.

[12] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen and A.V. Vasilakos 2014, Security and privacy for storage and computation in cloud computing, Inform. Sci. 258 371–386.

[13] O.D. Alowolodu, B.K. Alese, A.O. Adetunmbi, O.S. Adewale and O.S. Ogundele,2013, Elliptic curve cryptography for securing cloud computing applications, Int. J. Comput. Appl. 66.

[14] M. Aslam, C. Gehrmann and M. Bjorkman, 2012, Security and trust preserving VM migrations in public clouds, IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 869–876.

[15] Y. Tang, P.P. Lee, J.C.S. Lui and R. Perlman,2012, Secure overlay cloud storage with access control and assured deletion, IEEE Trans. Dependable Secure Comput.9 (6) 903–916.

[16] Q. Liu, G. Wang and J. Wu, 2014, Time-based proxy re-encryption scheme for secure data sharing in a cloud environment, Inform. Sci. 258 355–370.

[17] Z. Tari, 2014, Security and privacy in cloud computing, IEEE Cloud Comput. 1 (1) 54–57.

[18] Cloud security alliance 2011, security guidelines for critical areas of focus in cloud computing v3.0.

[19] Y. Fu and Z. Lin, 2013, Exterior: using a dual-vm based external shell for guest-os introspection, configuration, and recovery, in: Proceedings of the 9thACMSIGPLAN/SIGOPS International Conference on Virtual Execution Environments, pp. 97–110.

[20] S.M.S. Chow, Y. He, L.C.K. Hui and S.M. Yiu, 2012, Spice simple privacy-preserving identity-management for cloud environment, in: Applied Cryptography and Network Security, Springer, Berlin, Heidelberg, pp. 526–543.

[21] S. Yang, P. Lai and J. Lin, 2013, Design role-based multi-tenancy access control scheme for cloud services, in: IEEE International Symposium on Biometrics and Security Technologies (ISBAST), pp. 273–279.

[22] R.D. Dhungana, A. Mohammad, A. Sharma and I. Schoen, 2013, Identity management framework for cloud networking infrastructure, in: IEEE International Conference on Innovations in Information Technology (IIT), pp. 13–17.

[23] Boneh, Dan, and Matthew Franklin, 2003, "Identity-based encryption from the Weil pairing." SIAM Journal on Computing 32.3: 586-615.

[24] Z. Yan, P. Zhang and A.V. Vasilakos,2014, A survey on trust management for Internet of things, J. Netw. Comput. Appl. 42 120–134.

[25] S. Ruj, M. Stojmenovic and A. Nayak, 2014, Decentralized access control with anonymous authentication of data stored in clouds, IEEE Trans. Parallel Distrib. Syst. 25 (2) 384–394

[26] Z. Wan, J. Liu and R.H. Deng,2012, HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing, IEEE Trans. Inform. Forensics Sec. 7 (2) 743–754.

[27] M.L. Hale and R. Gamble,2012, Risk propagation of security SLAs in the cloud, IEEE Globecom Workshops (GC Wkshps), pp. 730–735.

[28] M.L. Hale and R. Gamble,2012, Secagreement: advancing security risk calculations in cloud services, IEEE Eighth World Congress on Services (SERVICES), 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, IEEE 5th International Conference on Cloud Computing
[30] Patel, Ahmed, et al., 2013, "An intrusion detection and prevention system in cloud computing: A systematic review." Journal of Network and Computer Applications 36.1: 25-41.

[31] Reddy, V. Krishna, B. Thirumala Rao, and L. S. S. Reddy, 2011, "Research issues in cloud computing." Global Journal of Computer Science and Technology 11.11

[32] Sai Keerthana K, Harshavardhan A and Ramesh D, 2019, A privacy-preserving protocol for verifiable file search on the cloud. Int J Innov Technol Explor Eng; 8(6 Special Issue 4):476-479.

[33] Sunil G, Aluvala S, Yamsani N, Chythanya KR and Yalabaka S, 2019, Security enhancement of genome sequence data in health care cloud. Int J Adv Trends Comput Sci Eng; 8(2):328-332.

[34] Sampath Kumar T, Manjula B and Srinivas D, 2017, A new technique to secure data over cloud, J Adv Res Dyn Control Syst (Special Issue 11):391-396

[35] Ravi Chythanya K, Sunil G, Sudheer Kumar K, Korra SN and Harshavardhan A, 2019, Security and safety in amazon EC2 service – A research on EC2 service AMIs. Int J Innov Technol Explor Eng; 8(6 Special Issue 4):736-738

[36] Mahender K, Kumar TA and Ramesh KS, 2019 Simple transmit diversity techniques for wireless communications Advances in Intelligent Systems and Computing 669 329-342 10.1007/978-981-10-8968-8_28

[37] Rajasri I, Guptha AVSSKS and Rao YVD, 2016 Generation of Egts: Hamming Number Approach Procedia Engineering 144 537-542 10.1016/j.proeng.2016.05.039

[38] Seena Naik K and Sudarshan E, 2019 Smart healthcare monitoring system using raspberry Pi on IoT platform ARPN Journal of Engineering and Applied Sciences 14(4) 872-876.

[39] Chythanya KR, Kumar KS, Rajesh M and Tharun Reddy S, Sensor Cloud, 2020: A Breakdown information on the Utilization of Wireless Sensor Network by Means of Cloud Computing. Test Eng Manage; 82:13945-13954.