International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET

An Empirical Study of Security Challenges in Cloud Data Storages

Farhadeeba Shaikh[1], Tazaeen Shaikh[2]

[1]Sr Lecturer, Computer Science & Engineering, MIT Polytechnic, Pune, Maharashtra, India
[2]Research Scholar, Computer Science & Engineering, MIT WPU, Pune, Maharashtra, India

Article Info
Volume 9, Issue 4

Page Number : 120-129

Publication Issue :
July-August-2022

Article History
Accepted : 01 July 2022
Published: 04 July 2022

ABSTRACT

A revolutionary process, cloud computing is transforming the way in which company hardware and software design and purchase are carried out. Because of the ease with which cloud data centers can be accessed, users are opting to transfer their data and application to cloud storages. However, the services and support expected from the cloud service providers to the users or towards the data stored by the users is not sufficient. Ease of access and round the clock availability of the data is not the only thing expected by the CSP. The integrity of the data, privacy of the data, and security of the data should be utmost responsibility of the CSP. According to this report, security rift, information theft, and unreliability of cloud-based data storage are all problems associated with the use of cloud storage. Finally, we are presenting potential cloud-based solutions to the difficulties that have been identified.

Keywords: Cloud Computing, Cloud Data Storage, Policies & Protocols, Security Issues.

I. INTRODUCTION

A revolutionary process, cloud computing is transforming the way in which company hardware and software design and purchase are carried out. Cloud service providers offer numerous improvement to public clients, including costless services, resource elasticity, and ease of entree over the internet, among others. Cloud computing is becoming increasingly popular. Cloud computing is already becoming incredibly popular among organisations of all sizes, from small to large, as a means of growing their operations and forging strategic connections with other businesses [1]. In regardless of the reality that cloud computing provides a plethora of benefits, many users are hesitant to store their confidential or sensitive information in the cloud. This comprises personal health information, emails, and government sensitive papers. Take for example the scenario in which data is housed in a cloud datacenter and the cloud client loses complete control around their data sources.

Edge computing is a novel technology that puts processing and storage resources closer to the data source, reducing reaction times and saving bandwidth. Due to a variety of difficulties, cloud storage technology cannot meet the demands of IoT and mobile applications. These include lack of real-time services, bandwidth limits, expensive operational expenses, and worries about data privacy. These limitations of cloud computing open the door for edge computing, a technology envisioned globally to meet the increasing runtime and real-time requirements of

IoT and smart devices linked to the network, among other gadgets.

Cloud Service Providers (CSPs) have pledged to securing customer data hosted in the cloud using methods like firewalls and virtualization. These solutions would not guarantee full data security due to network flaws and CSPs' total control over cloud applications, hardware, and client data. Prior to hosting, sensitive data may be encrypted to protect data security and privacy. Encryption techniques are sometimes impractical owing to the enormous amount of communication overheads that arise during cloud access patterns. To preserve data confidentiality and anonymity, secure cloud data storage and management are necessary [2]. This research focuses on security flaws, as well as difficulties relating to consumer data confidentiality and anonymity.

The current access control methods, such as identification and cryptographic hash functions, can only cope with a limited number of internal risks. Academics are increasingly focusing on the implementation of information security in benefit smart cities. To summarise, edge of the network networks use a hierarchical system of border infrastructure server farms to manage smart phones and different machine learning duties formerly handled by restricted edge devices. Edge computing networks are gaining popularity.

Edge computing can help construct smart city applications by delivering location-aware, bandwidth-sufficient, real-time, private data, and reduced services. Edge computing has grown rapidly in recent years due to its benefits over cloud technology. Edge computing offers several benefits besides being a viable system software for significant infrastructure networking and other applications. However, by expanding real-world attack surfaces from several angles, its incorporation may increase security and privacy concerns.

While current research focuses on modelling security engineering, it ignores frequent node re-evaluation. Malicious nodes change their behaviour periodically, losing fewer data packets and increasing the network's dispersed processing share. To successfully fight against internal assaults, smart city networks need a more comprehensive approach to dealing with rogue devices that compromise security and privacy. The authors of this study investigated the current CC mechanisms working across smart city networks. We specified durability, scalability, computing, non-repudiation, compatibility, information derivation, networking life, and quality of service criteria.

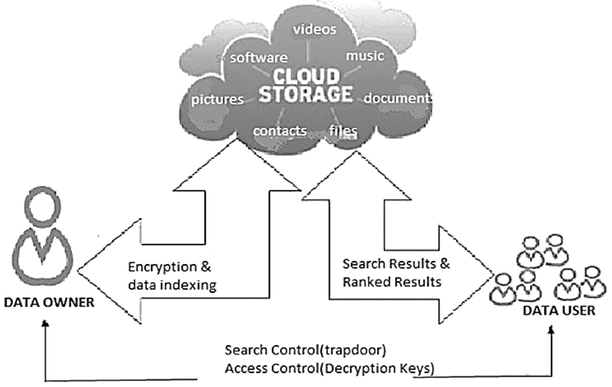

Fig. 1. Environmental factors

1 Challenges & Issues in Cloud Data Storage Infrastructure

There is no control over the data that is stored in cloud data centers since cloud computing does not provide that control. With complete control to the data, cloud service providers can execute any nefarious operations such as copying, erasing, or manipulating the data without being detected. Cloud computing provides a certain measure of influence over through the virtual machines because of its distributed nature. There are many more security issues associated with this absence of confidentiality and privacy than it does with the typical cloud infrastructure, as illustrated in figure 1. The sole encryption method does not provide complete control over the data stored, but it does provide a level of protection that is superior to plain data. Aspects of cloud computing that distinguish it from the generic cloud model include virtualization and multi-tenancy, as well as more attack opportunities than the generic cloud model. The figure 2 contains a number of difficulties, which are described in greater detail below.

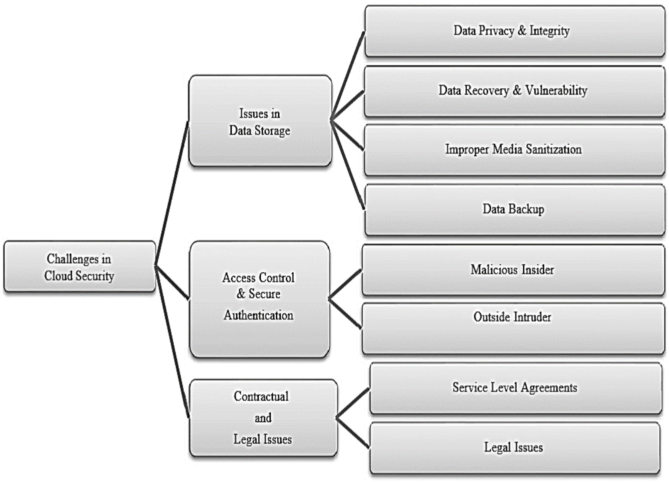
Challenges in Cloud Security
Issues in Data Storage
Access Control & Secure Authentication
Contractual and Legal Issues
Data Privacy & Integrity
Data Recovery & Vulnerability
Improper Media Sanitization
Data Backup
Malicious Insider
Outside Intruder
Service Level Agreements
Legal Issues

Fig. 2. Challenges in Cloud Storage Security

1.1 Issues in Cloud Storage

There is no control over the data that is stored in cloud data centers since cloud computing does not provide that control. With complete control to the data, cloud service providers can execute any nefarious operations such as copying, erasing, or

1.1.1 Data Integrity and privacy preservation

Regardless of the fact that cloud computing is less costly and uses less resources, it poses significant security risks. Because of the above criteria, cloud computing must secure the confidentiality, integrity, data availability and user privacy in the generic cloud computing model. However, because of the above conditions, the cloud computing model is more exposed to security attacks than other computing models. Because of its ease, cloud users are growing at an exponential rate, and the number of applications hosted in the cloud is increasing rapidly. As a result of these circumstances, cloud clients are exposed to additional security risks. If an attack on a provided by individuals is successful, it will result in a data breach, which will allow unauthorized access to the data of any and all cloud customers. The multi-tenant nature of cloud data was lost as a result of this integrity violation. Particularly vulnerable are SaaS companies, who may also lose their scientific information and face significant risks in terms of data storage. Additionally, data processing is fraught with danger when data is being converted among various tenants, in addition to these hazards. Because of virtualization, users can share a large number of physical resources among themselves. As a result, cybercriminals of such CSP and/or organisations initiate attacks against the CSP and/or organisations. These circumstances may provide an opportunity for a rogue user to launch attacks against encrypted information of other customers while analyzing this data. Another significant risk occurs when data is transferred from the CSP to a third-party storage facility [5]. The authentication process and key distribution processes in security for cloud computing are not yet fully standardized to meet industry standards. Although typical cryptography methods perform well in a general cloud computing architecture, they do not perform well in the absence of a standard and safe key management system for the cloud. As a consequence, cryptography is useful in mitigating the risks connected with cloud computing.

1.1.2 Data recoverability and vulnerability

As a result of the capacity pooling and elasticity properties of the cloud, customers can take advantage of variable and on-demand resource supply. The resource that has been assigned to a certain user may be transferred to another user at a later time. Malicious users can utilised data recovery techniques to get the data of prior users if they have access to computing and storage resources [13]. Amazon machine picture data were recovered 98 % of the time, according to the authors of [13]'s research. The computer forensics vulnerability has the potential to cause significant risks to confidential user information.

1.1.3 Improper media refinement.

The storage media are sanitized for the following reasons: (i) the disc may need to be replaced with another disc; and (ii) the disc may be corrupted. In addition, there is no longer the need to even maintain the disc, and there is no longer the same need to manage the services. Improper refining creates a significant risk to stored information. It's not really permitted to improve in a multi-tenant cloud because the tenant is the previous tenant.

1.1.4 Data backup

When there is an inadvertent and/or planned calamity, having a data backup is critical. In order to maintain data availability, the CSP must undertake routine copies of the data stored. The backup data, in reality, should adhere to strict security requirements in order to avoid hostile behaviors including such modification and unauthorized access from occurring.

1.2 Access Control and Identity Management

Multifactor authentication and information security are crucial components of securing data and services. It is vital to maintain track of who has used the system to avoid unauthorised access. Identity and access control issues arise in cloud computing since the data owner and the data being stored are on different executive platforms. Businesses use a variety of authentication and authorisation strategies in the cloud. Using many authentication and authorisation methods over time creates a difficult scenario. When stated before, cloud users' IP addresses change often as services, such as backups, are performed or resumed. Cloud users may engage and leave cloud resources as required, taking advantage of on-demand access policies. All of these issues demand efficiency and efficacy in identity and authenticity management. The cloud's identity management system must be kept current and manageable promptly so users may join and depart cloud resources. On the other hand, XML wrapping attacks on web sites, for example, are a worry with weak credentials that can be easily reset.

1.2.1 Malicious Insiders

An organization's workers, contractors, and/or third-party business partners can all represent a threat to the organization's security. Cyberattack against the cloud environment, namely on the Cloud Service Provider (CSP) side, result in the loss of the validity, authenticity, and protection of the user's information. As a result, network failure or intrusions occur in both of these situations. This attack is quite valuable, and it is generally known to the majority of the organisation [7]. Because of the sophistication of insiders' understanding of the inner architecture of an organization's data storage structure, there is a wide range of attack tactics that they can employ. The majority of organisations are ignoring this attack since it is extremely difficult to defend against and impossible to discover a comprehensive answer to this attack. This attack poses a significant danger in associated with data thefts and unauthorized disclosure, both within the enterprise and in the cloud [8].

1.2.2 Outside Intruder

Outsider attacks [3] are defined as attacks that originate from outside the organisation. Information security is amongst the most essential concerns when it comes to cloud computing. Because service providers do not have access to a particular protection system of data centers, they cannot deliver services to customers. However, if they want complete data protection, they must rely on the infrastructure provider. A private networks cloud environment is one in which the network operator can only define the security settings remotely, and we have no way of knowing whether or not such settings have been effectively implemented. In this Procedure, the resulting in a stronger must achieve the following goals: (1) confidentiality, which allows for safe data transfer and access; and (2) auditability, which allows for data auditing. In order to prevent outside intruders from accessing sensitive data that is kept in the cloud.

1.3 Legal Contractual Issues

Following the transition to a cloud computing systems, there are numerous concerns to consider, including regional authorities, subordinate legislation, deserved promotion, contract enforcement, and so on. The above-mentioned difficulties fall under the categories of legality, Service Level Agreements, and network infrastructure location [9].

1.3.1 Service level agreements

When it comes to cloud computing, the Contract Agreement can be considered a protocol because it establishes a number of requirements and agreements between such a subscriber and the cloud computing service provider, which can be considered a protocol in its own right. The SLA should also include the following clauses to protect the parties: If there is a data breach, CSP will take steps to rectify the situation and maintain a minimum level of service [5]. Users ought to have a clear awareness of the privacy of their capabilities, and any specific provisions should be discussed and agreed upon prior to the execution of the service agreement. It is getting increasingly difficult to enforce contracts attributed to the reason that the data provided by CSP are absolutely unverifiable. The agreements must always be discussed in a collaborative manner between the CSP and the end user due to the fact that they are non-negotiable and pre-define. Whether to comply with regulatory standards like as Sarbanes-Oxley and HIPAA [10] becomes an issue of whether to comply or not.

1.3.2 Legal Issue

The regulatory issues occur as a result of the availability of CSP resources in a number of legal authorities that are physically in conflict with one another [11]. If a user is transferred from one geographical location to another, a problem may arise as a result of the different legal jurisdictions. For a movement, data is split over a number of data centers, each of which is owned by a different CSP and each of which has its own set of rules and security guidelines. This process has the potential to create a severe problem in cloud computing.

II. Literature Review

In this part, we discussed the research effort approaches while also providing a thorough explanation of the subject matter. Tables are used to present the findings so that the reader may readily comprehend them. There are various sub-chapters that might be used to explain the topic.

1.4 Solution for Data Storage Issues

The computer combines this block into a circuit specification [9] that is not exposed in any other blocks since it has no transmitted characteristics. Fair-play promotes two competing entities to make best use of resources and achieve favorable results. Unlike Beaver's underlying FairplayMP protocol, which has a fixed number of touches. New features and major improvements have been introduced to the present methodologies as part of an ongoing collaboration effort to modernize the BMR. Given that the number of rounds used in the procedure is important to the protocol's final efficacy, we should use this method.

It is typical practice for small groups inside larger organisations to distribute documents among themselves to successfully complete tasks while remaining concealed from others. User groups and documentation develop throughout time, therefore users need a document indexing system that enables them to find documents quickly without (1) divulging additional document information, (2) burdening administrators, and (3) requiring users to trust just one authority. [10] captures the notion of privacy, which is defined as the degree to which information escapes from the index in conjunction with anything like the constraints specified in the restricted item. These techniques also leverage secret divisions and term mergers to set adjustable constraints on information leakage, even in reaction to statistical assaults. These tools are supplied.

This document [11] eliminates the need for a confidential authority. The study offers a solution based on centralised PPI with distributed search compliance access control mechanism. Even after the index is produced, this PPI keeps all information private. This gadget has been tested in the field. Second, system implementers maintain total control over the balancing of privacy and efficiency in their individual domains or document searches when employing PPI applications on their systems. Situations and words invest them with significance. The author presents the first e-PPI attempt for statistically differentiated distributed record search and privacy protection.

Subashini and Kavitha [12] performed a survey on healthcare service delivery model security vulnerabilities. Insecure storage, cookie manipulation, and insecure configuration are some of the data security vulnerabilities that may arise in the SaaS model. Network security problems, session management weaknesses, and dangerous SSL trust setting are validated in the SaaS paradigm.

Varsha et al. [13] reviewed cloud computing security challenges and recognised the Cloud Security Alliance's top seven security weaknesses (CSA). The analysis identifies multi-tenancy as the biggest security risk.

Wei et al. [14] identified two primary cloud computing security classifications: Cloud Storage Security (CSS) and Cloud Computation Security (CCS) (CCS). CSS refers to the security of data stored on unrecoverable cloud services. The CCS value shows the computation accuracy of unreliable cloud servers. This paper proposed a novel core Sec-Cloud structure and thoroughly discussed its functioning. The study detailed three kinds of attacks: Storage cheating attack models, computation cheating attack models, and privacy cheating attack models are all types of storage cheating attacks. A scalability and reliability study has also been performed to show the recommended protocol's efficacy. The SecCloud protocol solves issues with cloud storage and computing.

Taxonomies of security issues, DDoS assaults in the cloud, and DDoS defence solutions in the cloud were presented by Gupta and colleagues [15]. The article detailed the technique of a DDoS attack as well as countermeasures. The essay also addresses Cloud security risks. Cloud service delivery methods allow for DoS attacks, DNS server assaults, Mac address attacks, impersonation, cross-VM attacks, security breaches, privacy invasions, cross-site request forgery, authorization violations, infrastructure damage, and other security flaws. The essay also compares and contrasts numerous DDoS defence methods.

Multi-tenancy, elasticity, insider and foreigner attacks, inability to manage, data leakage, etc. were all mentioned. Data encryption, data auditing, safe information management information integrity and privacy, SQL-injection attack solution, and flooding attack are examples of security techniques given by Khan et al. To keep your cloud environment secure, employ SAML, Universal Identification, OpenID, and SSL/TLS.

The Cloud Service Provider commences the revocation procedure automatically when the time period associated with each user expires (CSP). This time-based encryption solution allows users to exchange credentials with the CSP in the past and request re-encryption keys in the present. The ABE protocol ensures access control by examining attributes rather than individuals. This strategy ensures data confidentiality and accessibility for certain members of the group, but not for all.

Rather of rebuilding the tree from scratch each time, random selection was employed to reduce computational repetition. A number of significant recommendations for data security and adequate key management have been released by the Computer Security Alliances (CSA) [18]. The credential's scope should be handled by a group or a person. Poor cryptography approaches should have been avoided at all costs. The finest rules for multifactor authentication and cryptographic algorithms solutions should be followed, and it is preferable to use heuristic detection technology to optimize data security while being stored on a computer system. The customer or businesses, as well as any trusted third parties, should practise sound key management practises. If the auditing protocol is constructed incorrectly, the encryption process may be used to restrict the transmission of data to third party companies even during auditing process. However, encryption in and of itself cannot prevent data from being transmitted to third parties, but it can restrict it to a bare minimum. However, it necessitates a large number of key management processes as well as significant overhead for key generation when storing data. However, the disclosure of an encryption key results in data leakage, which continues to be an issue in cloud environments. This issue has been addressed by integrating the elliptic curve authentication mechanism with both the randomized disguising procedure [19], which is described in detail below. Table 1 shows an illustration of this concept.

Table 1. Cloud data storage issues comparison

Ref	Methodology	Integrity	Confidentiality	Availability	Privacy
[12]	Cloud data security using Bilinear Pairing Encryption Data Integrity checking by Third Party Auditor	✓	✓	×	✓
[15]	Data Integrity and Privacy Preserving through FADE Threshold secret sharing	✓	✓	×	✓
[16]	Secure data sharing in cloud through Attribute based encryption	×	✓	×	✓
[17]	Resident Data Security and Data Redundancy through Erasure correcting Code	✓	✓	✓	×

1.5 Access Control Solutions and Identity Management

Simple Privacy-Preserving Identity Management for Cloud Environments (SPICE) was proposed by the authors in [20] for use in identification and authentication systems. The SPICE ensures group signature in order to provide unidentifiable identification, access control, accountability, unlink ability, and participatory design authorization, among other functions and features. The SPICE gives the above-mentioned capabilities with nothing more than a single registration, making it extremely convenient. After registering with a reputable third-party, users are issued a unique set of credentials that can be used for all of the benefits rendered by CSP. The authentication certificate is generated by the user when the credentials are used. Different CSPs require a range of authentication qualities, and the user must generate the appropriate form of identification certificates using the same credentials for each CSP's requirements.

In [21] the author proposes the Role Based Multi-Tenancy Access Control (RB MTAC), which is a type of multi-tenancy access control. The RB MTAC is a combination of a role-based access control scheme and an identity management system. The user must first register with the CSP in order to receive a single certificate that should have been distinct from other credentials. During the registration process with the CSP portal, the user must select a password. In order to gain entry into the cloud environment, users must first pass through into the identity module, which uniquely identifies the user, and then they are directed to the role assignment module, which determines the relationship to the RB MTAC database and assign appropriate roles to registered users based on the information that has been enrolled.

Several researchers, including Dhungana et al. [22], have proposed a method for public telecommunication protocols as an authentication and authorization architecture, which is maintained using the Users maintained Accessing (UMA) protocols, which would be discussed in greater depth below. In this situation, CSP acts as a host, while the authorized user acts as the operator (or service provider). Users who seek services are likewise managed by the authorization manager, who is in charge of the service administration and service requesting users. With the support of authorization management, this scheme is able to provide multifactor authentication and network management across a wide range of Cloud service providers. As seen in the accompanying Table 2, there are several options.

Table 2. Access Control in Cloud Environment System Comparison

Ref	Methodology	Services	Access Control	Authentication	Identity Management
[23]	Identity Management Framework (IMF), SPICE	Anonymous and Delegable Access Control	✓	✓	×
[24]	Role Based Access Control	Role Based Access Control	✓	✓	×
[22]	IMF	Identity Based Access Control	✓	×	✓
[25]	Decentralized Access Control	Attribute Based Encryption	×	✓	✓
[26]	HASBE	Cloud Access Control	✓	✓	×

III. CONCLUSION

Dynamic data software is stored in the cloud with the least amount of administration labour, and on-demand services are supplied to clients via the internet as a result of the cloud services infrastructure. The opposite is true for customers who, when it re-lates to cloud management, do not have dependable pledges or procedures in place. Because of this, there will be several security concerns associated with data storage, including those relating to privacy, privacy, reliability, and accessibility. We focused on data storage security concerns in cloud computing in this study, and we began by outlining cloud platform models, deployment methods, and a variety of security issues related with data processing in a cloud computing systems. Finally, in the con-cluding section, we examined different solutions for information storage challenges inside the cloud infrastructure that guarantee privacy and secrecy.

IV. REFERENCES

[1]. A. Abbas, K. Bilal, L. Zhang, S.U. Khan, A cloud based health insurance plan recommen-dation 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).

[3]. 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.

[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 ser-vices in cloud computing, IEEE Trans. Services Comput. 5(2012) 220–232.

[6]. M. Balduzzi, J. Zaddach, D. Balzarotti, E. Kirda, S. Loureiro, a security analysis of ama-zon'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 com-puting." 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 busi-ness 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]. S. Subashini and V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, 34 (2011) 1-11.

[13]. Varsha, Amit Wadhwa and Swati Gupta, Study of security issues in cloud computing, International Journal of Computer Science and Mobile Computing, 4 (6) (2015) 230 - 234.

[14]. Lifei Wei, Haojin Zhu, Zhenfu Cao, Xiaolei Dong, Weiwei Jia, Yunlu Chen and Athanasios V. Vasilakos, Security and privacy for storage and computation in cloud computing, Information Sciences, 258 (2014) 371–386.

[15]. K.Bhushan and B.B.Gupta, Security challenges in cloud computing: state-of-art, Int. J. Big Data Intelligence, 4 (2) (2017) 81-107.

[16]. Shaireen Khan, Shadab Hasan, Shashank Singh, Sumera Zafar and Shobhit Joshi, Cloud computing: security issues and security standards, International Journal of Engineering and Management Research, Special Issue (ACEIT - 2018) 31-36.

[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 Interna-tional 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 authen-tication 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.

Cite this article as :

Farhadeeba Shaikh, Tazaeen Shaikh, "An Empirical Study of Security Challenges in Cloud Data Storages", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 9 Issue 4, pp. 120-129, July-August 2022.
Journal URL : https://ijsrset.com/IJSRSET229430