ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Security Risks and Impact of Data Protection Techniques in Cloud Computing

Shouket Ahmad Kouchay

Research Scholar, Department of Computer Science

ABSTRACT*:* Cloud computing is a generally promising commercial computing model based on the virtualization of resources. Large huge amounts of data can be calculated and managed. With the continuous development of society and economic progress, when a large amount of data enters the cloud computing system, people will pay more attention to data security. Cloud computing securityis a challenging task wherein the data transfer is going on each moment.Data protection techniques are very essential in cloud computing security irrespective of lot of challenges. This research explores to review, analyze the most important security techniques and their impact on data protection in cloud computing. This paper also discusses threats, vulnerabilities for existing security techniques and suggestions for securing data in the cloud.

I.INTRODUCTION

Cloud computing is found everywhere and has limitless computation. The definition of cloud computing provided by National Institute of Standards and Technology (NIST) says that: "Cloud computing is a model for enabling on-demand and convenient network access to a shared pool of configurable computing resources (e.g., networks, servers, storage applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1].

While studying the subject of cloud computing, the researchers describe that cloud has enormous potential to handle any IT related activity and deliver it to the right user within time as a service [2]. Cloud technology is often considered one of the most important discovery to handle technological tasks successfully by organizations [3].

The three service models in cloud computing are– Software-as-a-Service, Platform-as-a-Service, and Infrastructure-as-a-Service to offer cloud services by a Cloud Service Provider (CSP) to its clients. The 4 deployment models are Private cloud, Community cloud, Public cloud, and Hybrid cloud. [1]. The NIST definition of cloud computing can be summarized in figure- 1.

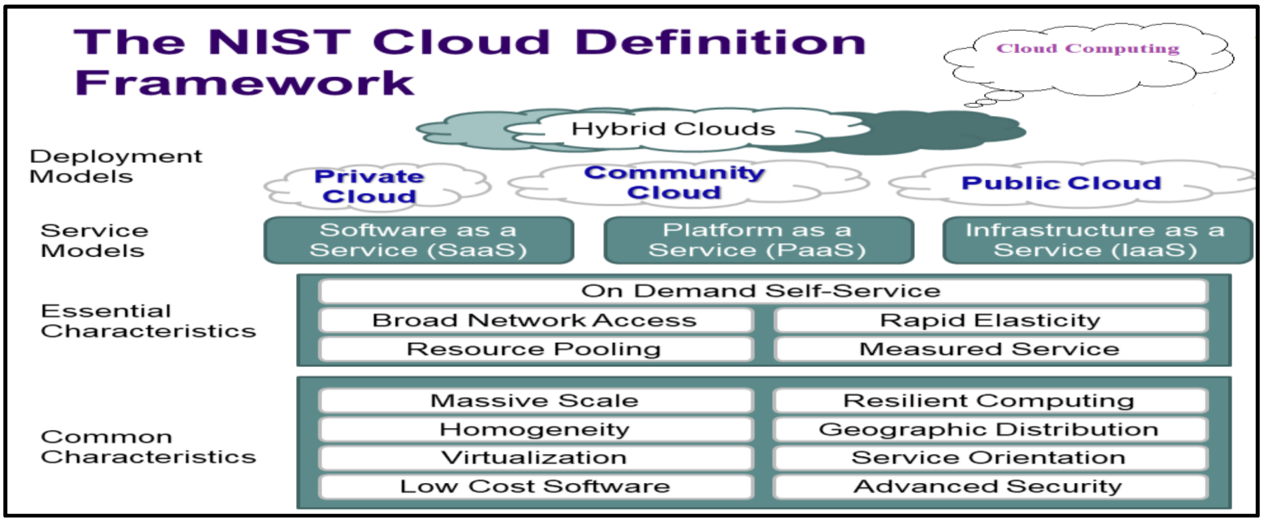
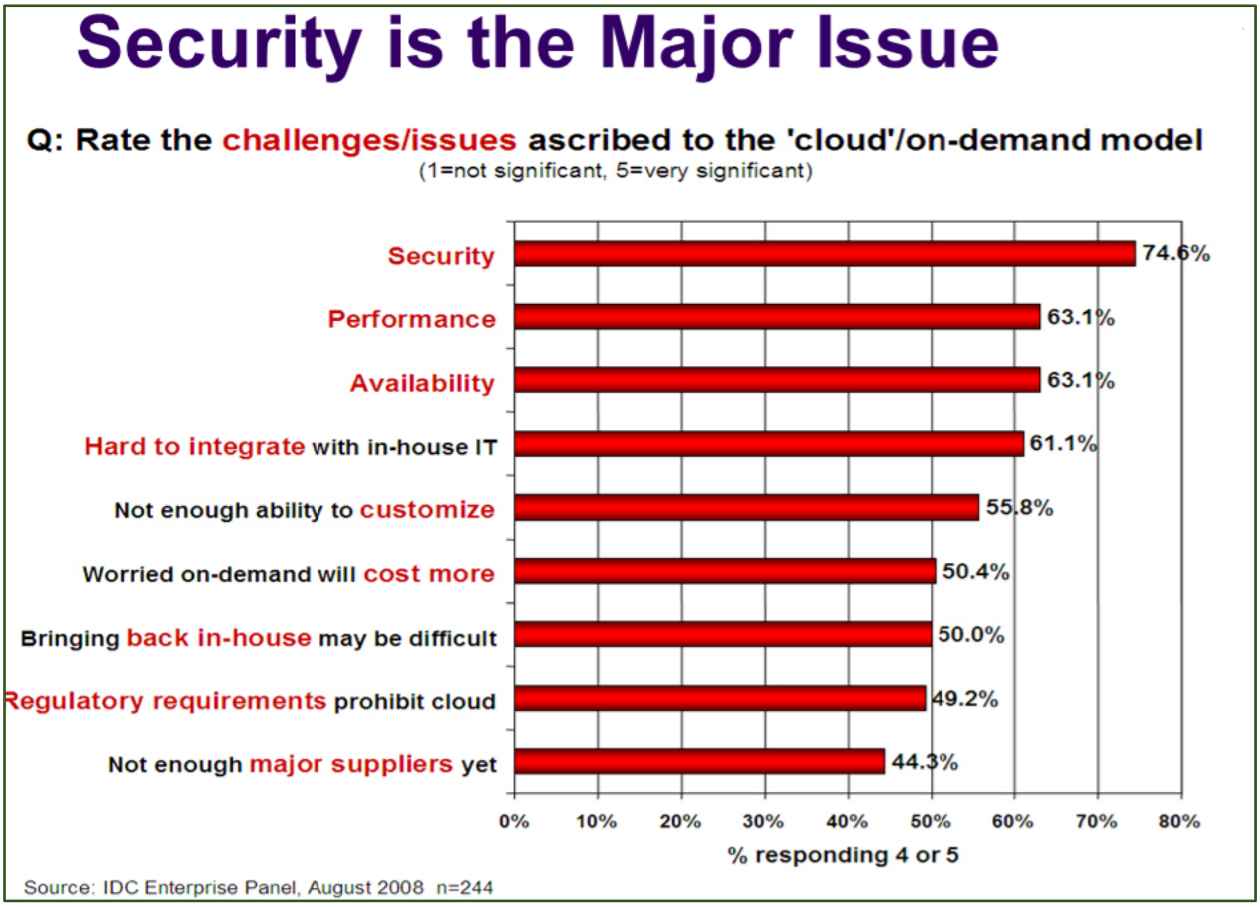


Figure-1- The Summarized NIST definition of cloud computing

Cloud Computing enables pervasive, suitable, on-demand network access to shared computing resources (e.g., networks, servers, storage, applications, and services). The importance of Cloud Computing is growing and is gaining hold in all spheres of life. Research by the author [4] considered Cloud Computing as the first among the top 10 most significant technologies and with a better prospect in upcoming years by businesses and organizations.

When we utilize cloud computing we run our software on hard disks and CPUs that are not in front of us. That is why users are having more worries about security concerns when they are using this. So, a lot of different kinds of attacks could occur in cloud computing. The most known attacks comprise message modification, phishing, IP spoofing, traffic analysis, IP ports, etc. As per the IDC enterprise survey, security is the main concern in Cloud Computing as shown in figure-2.



Source: IDC Enterprise Panel, August 2008 n=244

The security challenges in cloud computing must be properly resolved and reduced. The security techniques of cloud computing offer authentication, confidentiality, access control, and authorization.During our systematic literature review method various data security risks, challenges, techniques in cloud computing have been identified and discussed in this paper. The central aim of this research is to study various security techniques and their impact and also to discuss different of types of attacks, threats, vulnerabilitiesfor data security in cloud computing.

The survey conducted by international data corporation shows the strength of cloud computing to be implemented in the IT industry and gives the prospective motivation to CCSP. This is related to the growth of cloud, security part, the cloud is the priority to the vendors, revenue report, future and current usage, state of cloud to the IT users and popularity survey of cloud computing[4].,[5]

The paper is organized as follows: Section II provides the related work and literature review. In section III security risks in cloud computing have been identified and discussed. Section IV covers Security Techniques; Section V includes results and discussion of Systematic Literature Review. The brief description of recommendations and suggestions for Improving Data Security in Cloud Computing is discussed in section VI, and finally, section VII includes a conclusion.

II. LITERATURE REVIEW

The data security in cloud computing is a tough job, although a lot of research is going on to address the security challenges in Cloud Computing. The data that is transferred over the Cloud servers is susceptible to different attacks. So security techniques to counter such attacks are important for user authentication and data privacy.

In [6] the author discusses the service-level security view from the end-user perspective. They have enlightened on various threats, weaknesses, and potential solutions along with their inter-related mapping. In [7] recognized confidentiality, integrity, availability, accountability, and privacy-preservability as the five most determining traits for analyzing the vulnerabilities, attacks, and their solutions.

The author [8] identified cloud collaborative Trust model I which is well-matched with a firewall devoid of affecting its proficiency. A protocol to create trust and confidentiality when accessing data is projected by authors in [9]. User behavior trust evaluation based on time, abnormal degree of behavior and access times are debated by authors in [10]. Computing cloud security by assessing parameters and functions is the suggested result of the study. Various approaches for security and its quantification measure are proposed in the literature. CSA security guidance [11] provides a list of areas for analyzing and evaluating cloud services. It delivers the various aspects to be considered for determining risk beforegoing for the cloud.

In [12] authors presented various cloud data security and privacy techniques. Concerns such as lack in the integrity of data, lack of support for dynamic data operations, and lack of availability of high resource and computation cost were identified in different techniques. Further, the TPA was applied to provide a clear view of all the data security techniques and methods which previously existed. The security technique proposed by authors [13] wherein the file at the user's end can be encrypted and decrypted such that the security of data during transmission can be exchanged. A study associated with the various data security and privacy techniques applied in cloud applications is presented [14].The ability to challenge the cloud server to ensure the correctness of data storage is provided through public audit ability.

A secure cloud also guarantees of providing data protection. Some of the techniques to provide data security by various researchers are discussed as follows. Pearson in [15] discusses policies and assessment procedures for privacy enhancement methods and tools. Authors in [16] discussed the privacy issue by retaining data control forthe user to increase confidence. Cloud computing attacks are discussed and some provisions and means to overcome from the same are proposed. A novel patient-centric framework and a suite of mechanisms for data access control of Patient Health Record are presented by the authors in [17]. The data protection issue is partially discussed in [18].

CSA is an international body dealing with security and other fields of cloud computing. They publish broad analytic reports and procedures about various challenges and deficiencies in cloud computing [11]. A Survey is prepared from these security challenges. The question and how well the issue is addressed are tabularized in table2

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

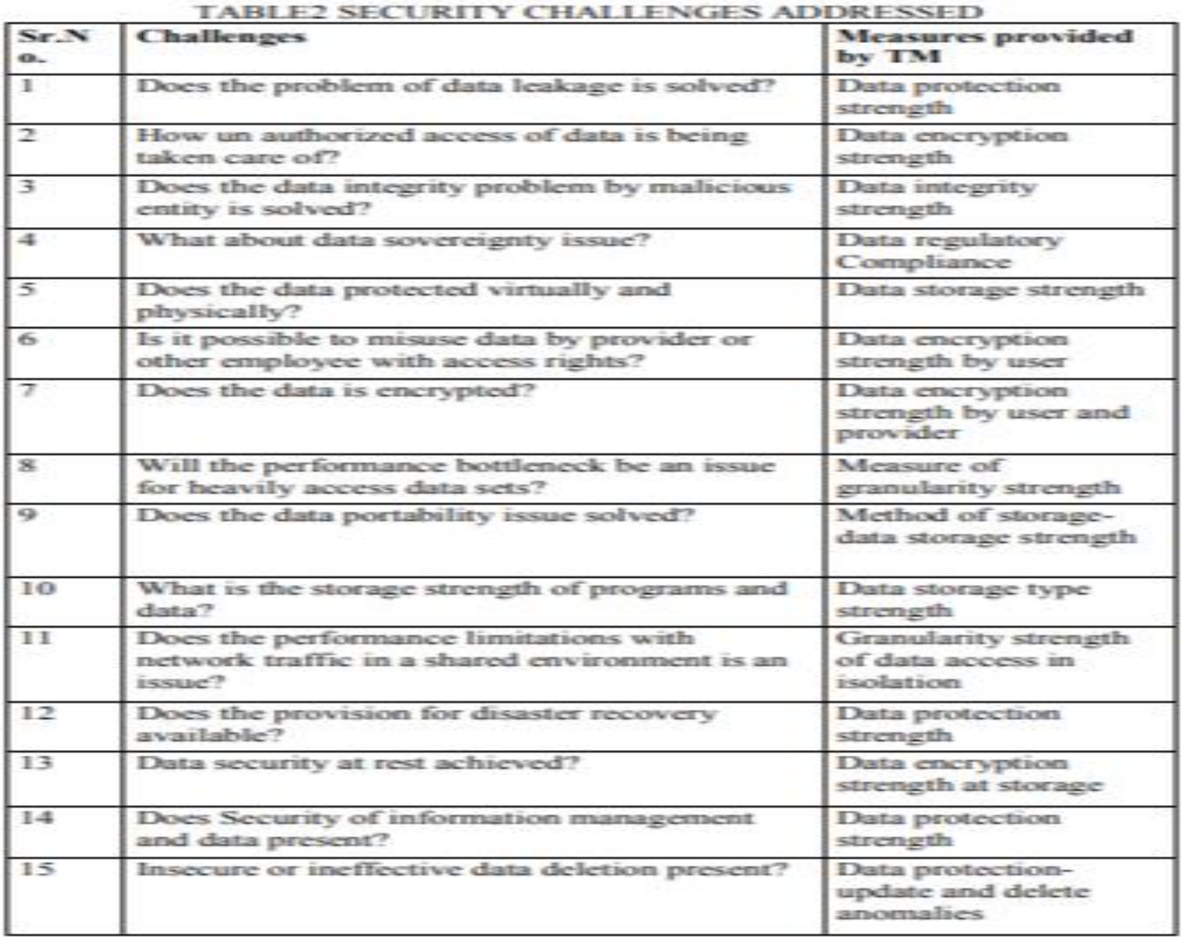


TABLE2 SECURITY CHALLENGES ADDRESSED

Sr.No.	Challenges	Measures provided by TM
1	Does the problem of data leakage is solved?	Data protection strength
2	How un authorized access of data is being taken care of?	Data encryption strength
3	Does the data integrity problem by malicious entity is solved?	Data integrity strength
4	What about data sovereignty issue?	Data regulatory Compliance
5	Does the data protected virtually and physically?	Data storage strength
6	Is it possible to misuse data by provider or other employee with access rights?	Data encryption strength by user
7	Does the data is encrypted?	Data encryption strength by user and provider
8	Will the performance bottleneck be an issue for heavily access data sets?	Measure of granularity strength
9	Does the data portability issue solved?	Method of storage-data storage strength
10	What is the storage strength of programs and data?	Data storage type strength
11	Does the performance limitations with network traffic in a shared environment is an issue?	Granularity strength of data access in isolation
12	Does the provision for disaster recovery available?	Data protection strength
13	Data security at rest achieved?	Data encryption strength at storage
14	Does Security of information management and data present?	Data protection strength
15	Insecure or ineffective data deletion present?	Data protection-update and delete anomalies

.

III. SECURITY RISKS AND VULNERABILITIES IN CLOUD COMPUTING

When there are loopholes in cloud security it leads to security risks and vulnerabilities in the cloud.Some security risks and vulnerabilities are discussed in this section which poses serious threats and could impact Cloud computing.

Virtualization and Multi-Tenancy

Although virtualization and Multi-tenancy techniques provide efficient utilization of resources, it poses also security concerns. This means sharing of computational resources with other users at Cloud Computing Service Provider's (CCSP) site. Therefore it infringes the confidentiality of data and consequences in data leakage and raises the chances of attacks.[19]

Data privacy and integrity

Data integrity in a cloud environment approves maintaining data integrity i.e. user's statistics need to no longer be modified using any unlawful person or using the CCSP. The data stored in the cloud may be corrupted by both administrative errors as well as malicious attacks. Software integrity becomes a problem since the CCSP provides the applications the user consumes. Thus the software providers must have a clear security procedure on how to guarantee that any software used will not do unexpected things to the users' data. [20]

Malicious Inside and Outside attacks

Multitenant based model in the cloud can pose threat incorporation and data can be hacked. This concern affects the confidential information. Clouds are not like a private network; they have more interfaces than a private network. So hackers and attackers have the benefit of manipulating the API, flaw and may do a connection breaking [21]. These attacks are less harmful than insider attacks because in the later we sometimes unable to identify the attack.

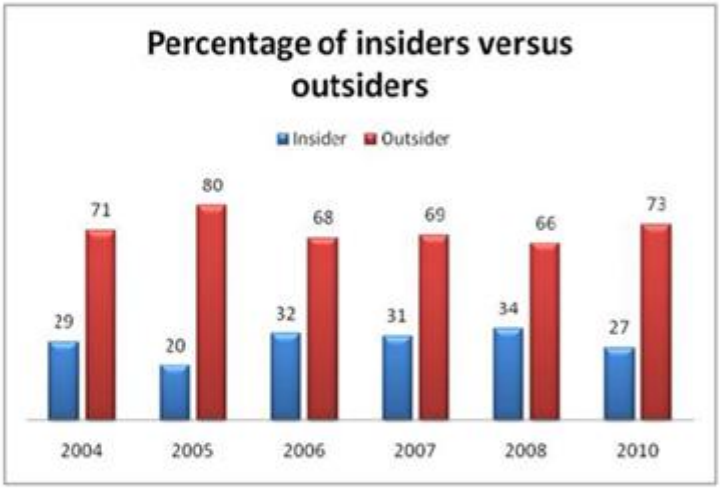


Figure -3 Percentage of Insiders versus Outsiders[19]

Data Loss and Leakage

When the CCSPstays its services due to some grounds; there may additionally be data loss. Users are no longer in a position to get access to data.
An important example of this can be updating and deletion of data without having any backup of that data. Once data is available to mischievous users Data leakage occurs.

Data Location and Segregation

The users are ambiguous about the data location. Users do not understand about original data storage place. It might be saved inside or outside the country. In cloud computing, improper isolation of data steadily increases the threat. This issue may be resolved by thorough segregation of storing the user’s data in the cloud server.[22]

Unwanted Access

Cloud computing has many risks for preserving the confidentiality of information or file. For example, if the user's data are saved outside their country, the concerned authorities can view the real data. [22]

Vendor Lock-in

Vendor lock-in is a technique, Vendor lock-in technique permits users to depend on the vendor's services. Vendor lock-in is accomplished by building IT solutions. It is considered as one of the key matter of cloud computing. When a vendor stops to deliver a service, the CSP tries to deliver the provider from any other vendor, which may additionally be belonging to another cloud server. [22]

Data Deletion and Data Investigation

One more key concern in the cloud server is about knowing full deletion and recovery of data or files from the cloud server. Currently, there are no methods to know whether the user's data is completely deleted. Searching data in Cloud distributed systems is very tough. When users make a data request, the CSP takes a lot of time to investigate the data. So, it increases the response time. [22]

Distributed denial of service attacks: -

The servers and networks are brought down by an enormous quantity of network traffic and users are denied to access service. [23].

Port scanning: -

The information exchange in Port scanning is taking place when the subscriber configures the group. Port scanning is done automatically when you configure the internet so this violates the security issues [23].

Deduplication

Deduplication is a technique where the server stores only a single copy of each file, irrespective of how many users demanded the storage of a similar file. This saves the cloud servers and network bandwidth. But, the deduplication cloud leaksthe sensitive side-channel information.So there isa different type of attacks in cloud services such as Cloud malware injection attack, DoSattack, Side-channel attack, wrapping attack, Insider attack, advanced persistent threats, and meltdown. Therefore, there is an urgent need to provide security measures to counter such attacks. Some security techniques are discussed in the next section. [24]

IV. SECURITY TECHNIQUES

Authentication and Encryption in Cloud Computing

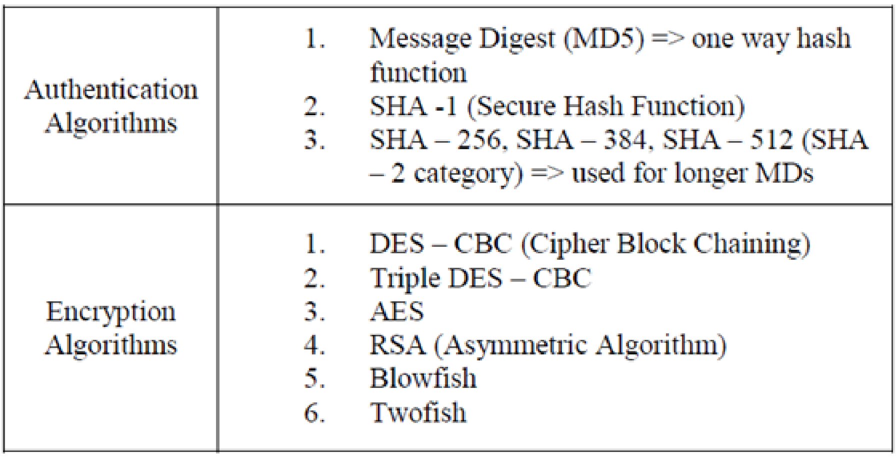
Authentication identifies the techniques and methods for verification in a cloud. The privacy can be breached in case of being used improper identity technique. Authentication of users and even communicating systems is performed by various methods, but the most common is cryptography [25]. Authentication of users takes place in various ways like in the form of passwords that are known individually, in the form of a security token, or in the form a measurable quantity like a fingerprint. One problem with using traditional identity approaches in a cloud environment is met when the company uses multiple CCSPs. In this situation synchronizing identity info with the company is not scalable. Other problems arise with traditional identity approaches when migrating infrastructure toward a cloud-based solution. [25]

Data Encryption

Encryption is a technique of translation of data into secret code and Encryption algorithms and keys are used for data confidentiality and integrity. The improper encryption algorithm and a weak key management procedure lead to encryption vulnerability that exploits the data confidentiality and integrity. The encrypted data cannot be read without an encryption key and is useless to the intruder. [26].

This is Trust management, a process of validating credentials. Ensuring Authentication and Encryption leads to a Trusted end to end communication. Data protection can be achieved by implementing cryptographic techniques Algorithms used in cloud authentication and encryption process are given in Table 1.

TABLE 1. TRADITIONAL AUTHENTICATION AND ENCRYPTION ALGORITHMS



Authentication Algorithms	1. Message Digest (MD5) => one way hash function 2. SHA -1 (Secure Hash Function) 3. SHA – 256, SHA – 384, SHA – 512 (SHA – 2 category) => used for longer MDs
Encryption Algorithms	1. DES – CBC (Cipher Block Chaining) 2. Triple DES – CBC 3. AES 4. RSA (Asymmetric Algorithm) 5. Blowfish 6. Twofish

Source [24]

Information integrity and Confidentiality

Information privacy and integrity are can be affected by sharing computing resources to multiple users which can let malicious users attack data used by another user in a cloud [26].

A suitable resolution to information integrity issues is to deliver mutual trust between CCSP and users. The proper authentication, authorization, and accounting control so the process of accessing information should go through various multi-levels of checking to ensure authorized use of resources is also the solution. Some secured access mechanisms should be provided like RSA certificates, SSH-based tunnels. [25[[27]28]]

The procedures for attaining data confidentiality in communications between provider and user can be measured for the privacy strength provided by the service.

Access Control in Cloud Computing

Access control for authorization is important as the end-user must be authenticated before allowed to use the allowable resource. Attribute-Based Access Control (ABAC) is preferred over Role-Based Access Control [29] proposed a model of access control for the cloud users that combines role-based and trust-based access control.

The user's role classes describe the role assessment weights. In [30] author proposed a flexible and Efficient Access Control Scheme that uses the Attribute-Based Encryption framework which facilitates dynamic membership, accurate and efficient access policy definition and evaluation.

The Rules that command how and when a user can access privileges and decide on what application levels their access should be possible are vital in keeping access control security. In the SaaS model, the cloud provider is the one responsible for all things network, server and application-related and the responsibility of user control falls to the customer. The customer must ensure only the intended users gain access rights by managing passwords and alike internally in the IaaS model the customer is the one responsible for managing all aspects of access control, including resources such as host platform, network and so on. They are also responsible for managing access to their virtual machines and storage. Access control problems can be not resolved with good policy management. There are still risks associated with access control that are more technical. [31], [32].

Authorization in Cloud Computing

The basic security procedure like authentication, authorization data protection is very important in the cloud.
Consequently, a cloud security tool is needed to assess security concerns concerning cloud services. The authorization

strength can be used to ensure that the user is given any unauthorized roles. An action including service access, performing any operations, and all input/output related activities requires authorizing users at these stages. A CCSP provides authorization by using various techniques. It is measured for the stored ACL (Access Control Strength) integrity, Presence of PMI (Privilege Management Information) and the process of performing validation checks of the user.[[33]

Availability of Information (SLA)

One of the major issues in cloud services is when data is not available. The availability of network resources to the user is provided by the Service Level Agreement. It is a trust contract between the user and CCSP [34]. The method to provide availability of resources is to have a backup plan for local resources and other important information. This enables the user to have the information about the resources even after their unavailability.

Secure Information Management

It is a technique of information security for a collection of data into the central repository. It is comprised of agents running on systems that are to be monitored and then sends information to a server that is called "Security Console". The security console is managed by an admin who is a human being who reviews the information and takes actions in response to any alerts. As the cloud user base, dependency stack increase, the cloud security mechanisms to solve security issues also increase; this makes cloud security management greatly extra complex. It is also called Log Management. CCSP also provides some security standards like PCI DSS, SAS 70. Information Security Management Maturity is another model of the Information Security Management System. [34]

Malware-injection attack solution

The malware injection attack can be prevented by using a File Allocation Table. This solution creates many client virtual machines and stores all of them in central storage. It utilizes the File Allocation Table consisting of virtual operating systems [35]. The application that is run by a client can be found in the FAT table. All the cases are accomplished and planned by Hypervisor. IDT (Interrupt Descriptor Table) is used for integrity checking.This type of attack can also be prevented by integrity check or by storing a hash value on the original service instance's image file. [36]

Flooding Attack Solution

When the flooding attack is applied to cloud services, two types of DoS could happen in cloud computing systems: direct DoS and indirect DoS. The flood attack could cause indirect DoS to other servers in the same cloud. [37]

One fleet of a server is considered for system type requests, one for memory management and the last one for core computation related jobs. These servers communicate with each other. When one of the servers is overloaded, a new server is brought and used in the place of that server and another server that is called name server has all the records of current states of servers and will be used to update destinations and states. The hypervisor can be used for managing jobs Hypervisor also do the authorization and authentication of jobs. An authorized customer's request can be identified by PID. Even the RSA algorithm can be used to encrypt the PID. [35].

V. RESULTS AND DISCUSSION

A massive expanse of research has been carried out in the area of Cloud Computing. Although a systematic literature review is a challenging task in cloud security. We have researched 150 research articles related to cloud computing security from the different databases and libraries such as IEEE Xplore, Springerlink, Science Direct, Scopus, and Web of knowledge during the process of systematic literature review. A lot of security issues and techniques were identified during this process. Some of the techniques are- Virtual Machine and Hypervisor Security ,Multi-tenancy based access control model, TLS- Handshake, Public key homomorphic, probabilistic-sampling technique, Diffle – Hellman key exchange, Private face recognition, 3rd party auditor, MACs, Data coloring and watermarking, A novel Cloud dependability model, KP-ABE, RBAC, ARVTM, Identity based authentication, Security assertion markup language, TPM, Virtual Image security, Proof of retrievability, RSA algorithm, Fair MPNR protocol, Sobol-sequence, Redundant array of independent Net-storages, Hadoop distributed file system, self-cleansing intrusion tolerance, searchable symmetric encryption, Provable data possession, Data Privacy manager, Trust framework, Data sanitization, Digital Signature, intrusion Detection, and Prevention System, Data integrity and availability, Accountability, Time bound ticket-based mutual authentication scheme, Security Access Control Service, IDS, The Service Level Agreement, These Security techniques have strong impact on the Security, Confidentiality, Efficiency, Performance, Access control, trust and Recovery. The security and Confidentiality are the main factors that are impacted and improved mostly by these security techniques whereas the impact of identified techniques is least on access control and recovery and backup of data.

These security techniques have displayed in some way improvement on the overall services in the Cloud Computing environment. The result is shown in figure 4.

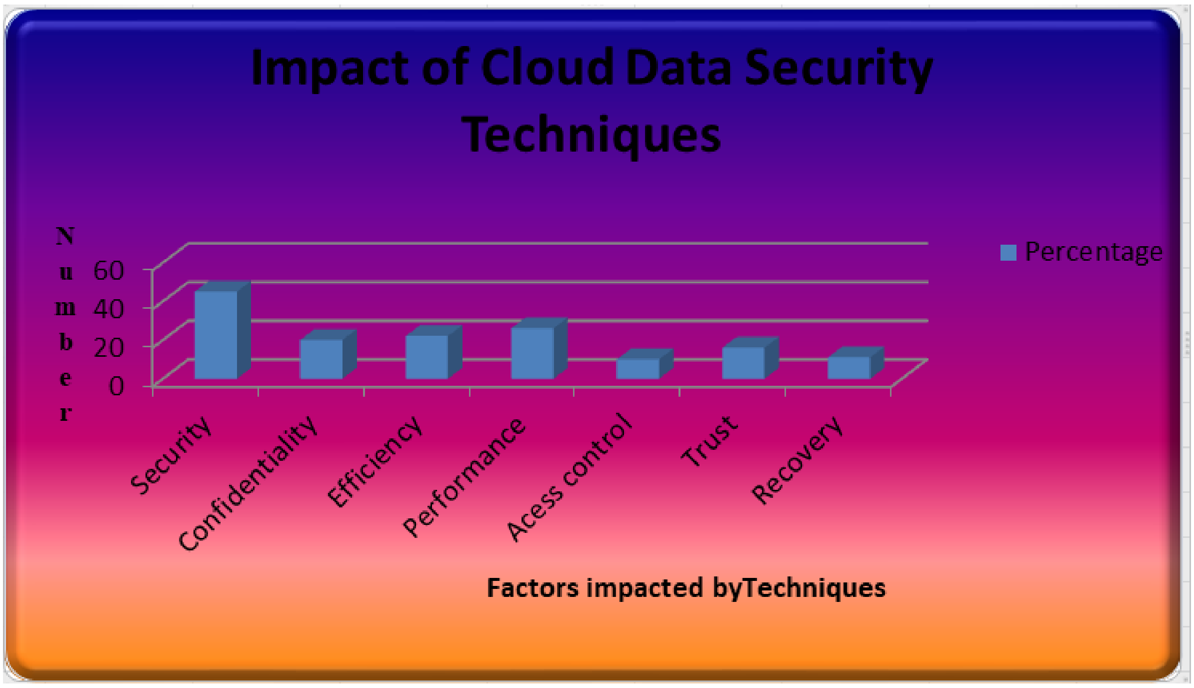


Figure-4 Impact of Security Techniques on Cloud

Cloud computing security has shown topmost significance in the above results. The results show comprehensively and comparatively how security, confidentially, performance and efficiency are important techniques in cloud computing. As in [38] important data is located in cloud infrastructures of untrusted third parties, ensuring data security and confidentiality are of top-most significance.

VI. RECOMMENDATIONS FOR IMPROVING DATA SECURITY IN CLOUD COMPUTING

Properly following the security guidelines and measures would ensure secure cloud services like strong authentication and access management, and Data protection and Intrusion Detection and prevention system. From thorough review and analysis of Cloud Security, following are some concise recommendations and suggestions from various researchers and industry experts, corporate professionals for improving data security in cloud computing: -

- Authors in [39]suggested shared responsibilities of both CSP and users to implement IaaS security procedures. They recommended metrics to analyze susceptibility marks of applications being developed and installed by the Passcloud users.
- Cloud security alliances mentioned that CSP does not maintain adequate control over systems to evade being hacked. The CSA recommends a few precaution measurements such as strict registration process, secure identity check procedure and enhanced monitoring skills to prevent such attacks, [40].
  - Risk management and risk awareness should be focused more to enhance cloud services.
  - Standardized security techniques and resolutions.
  - Rise efforts to mitigate harmful code; Legal responsibility, and increased security measurements at levels of objects and elements of objects.
  - Scrutinize the security model of cloud provider interfaces.
  - Certifying strong authentication and access controls are implemented in concert with the encrypted transmission.
  - Enforcing strict supply chain management and conduct a comprehensive supplier assessment.
  - Implement strong API access control.
  - Analyzes data protection at both design and run time.
  - Improved algorithms, define a security policy and decouple the security architecture with technical infrastructure
  - Use Data traceability technology as it uses the logs obtained on data traffic as well as the characteristics of the related textto make visible the data used in the cloud [41].
  - CSP should be aware of new changes and assure that customers' access privileges are limited.
  - Data transferring shouldbe protected and secured by standard security techniques and managed by experts.
  - CCSP will define and usually facilitate the IPSec device to install user network where it connects to the internet and to facilitate high-speed encryption and decryption without keeping workload on servers.
  - Decoy technology with user behavior profiling [42]
  - Awareness about new changes and updates

A lot of research is going on from different experts to mitigate or prevent Cloud Computing security problems. Various practices and techniques identified and recommended by researchers to improve data security and privacy in cloud computing are described in [43-50].

VII. CONCLUSION

Cloud Computing has created high expectations in individuals, industries, and organizations due to its flexibility and high-performance computing resources and power. However, security is a major concern.Different techniques and their impact on data security in cloud computing have been explored in our systematic literature review. Different types of attacks, threats, vulnerabilities for data security in cloud computing have also been identified in this research. We found that security and confidentiality are the core aspects that are impacted and enhanced mostly by these security techniques. Some security recommendation has also been suggested to maintain secure data communication in a cloud. This research can act as bases in the direction of a better understanding of cloud computing and its security techniques in future research efforts.

REFERENCES

[1] P.M. Mell, T.Grance, The NIST Definition of Cloud Computing,Tech. Rep.,National Institute of Standards &Technology,Gaithersburg, MD, United States(2011)
[2] 3.Fu, Z., Sun, X., Linge, N. and Zhou, L. (2014). Achieving effective cloud search services: multi-keyword ranked search over encrypted cloud data supporting synonym query. IEEE Transactions on Consumer Electronics, 60(1), pp.164-172.
[3]P. Sill, A. (2015). Emerging standards and organizational patterns in cloud computing. IEEE Cloud Computing, (4), 72-76.
[4]Gartner Inc Gartner identifies the Top 10 strategic technologies for 2011.
[5] Shuai Z; Shufen Z; Xuebin C; Xiuzhen H; (2010), “Cloud Computing Research and Development Trend”, 2nd International conference on Future Networks, 2010.ICFN ' 10. pp 23, 22-24 Jan 2010.
[6] K. Hashizume, D.G. Rosado, E. Fernández-Medina, E.B. Fernandez, An analysis of security issues for cloud computing, J. Internet Serv. Appl.(ISSN: 1869-0238) 4 (1) (2013) 1–13,
[7] Z. Xiao, Y. Xiao, Security and privacy in cloud computing, IEEE Commun. Surv. Tutor. (ISSN: 1553-877X) 15 (2) (2013) 843–859,
[8]Bouazza, N. B., Lemoudden, M., & El Ouahidi, B. (2014, May).Surveing the challenges and requirements for identity in the cloud. In Proceedings of the 4th Edition of National Security Days (JNS4) (pp. 1-5). IEEE.
[9]. Mahbub Ahmed, Yang Xiang, Ali S, “Above the Trust and Security in Cloud Computing: A Notion towards Innovation”, IEEE/IFIPInternational Conference on Embedded and Ubiquitous Computing, Australia, 2010.
[10]. Tian Li, Chuang Lin, Yang Ni, “Evaluation of User Behavior Trust in Cloud Computing”, International Conference on ComputerApplication and System Modeling -ICCASM, China, 2010.
[11] CSA, Security Guidance for Critical areas of focus in Cloud Computing V3.0, 2011.
[12] Fraunhoferverlag, “ thesecurity of clous storage servises" Fraunhoferinstiitute for secure info technolgy 2012
[13] SanjoliSingla, Jasmeet Singh “Cloud Data Security using Authentication and Encryption Technique” International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 7, July 2013
[14] BhavnaMakhija ,VinitKumar Gupta “Enhanced Data Security in Cloud Computing with Third Party Auditor”, International Journal of Advanced Research in Computer Science and Software Engineering, 2013
[15] Pearson S, “Taking account of privacy when designing cloud computing services”, Software Engineering Challenges of Cloud Computing, pages, 44 – 52, Vancouver, BC, 2009.
[16] Descher M, Masser P, Feilhauer T, A Min Tjoa and Huemer D, “Retaining data control to the Client in Infrastructure Cloud”, International Conference on Availability, Reliability and Security, pages 9-16, Dornbirn, 2009.
[17] RizwanaShaikh and Dr. M. Sasikumar, Trust Model for Measuring Security Strength of Cloud Computing Service, Procedia Computer Science Journal, Volume 45, Pages 380–389, ISSN : 1877-0509, 2015.
[18] RizwanaShaikh and Dr. M. Sasikumar, Data Classification for achieving Security in cloud computing, Procedia Computer Science Journal, Volume 45, Pages 493 – 498, ISSN: 1877-0509, 2015.
[19]Dillon, T., Wu, C., & Chang, E. (2010, April).Cloud computing: issues and challenges.In 2010 24th IEEE international conference on advanced information networking and applications (pp. 27-33).Ieee.
[20]Raghuwanshi, D. S., &Rajagopalan, M. R. (2014, January). MS2: Practical data privacy and security framework for data at rest in cloud. In 2014 World Congress on Computer Applications and Information Systems (WCCAIS) (pp. 1-8). IEEE.
[21] Gupta, S., & Kumar, P. (2015). An immediate system call sequence based approach for detecting malicious program executions in cloud environment. Wireless Personal Communications, 81(1), 405-425.
[22]Neela, K. L., &Kavitha, V. (2013). A survey on security Issues and vulnerabilities on cloud computing. Int. [24]Stanek, J., Sorniotti, A., Androulaki, E., &Kencl, L. (2014, March). A secure data deduplication scheme for cloud storage. In International conference on financial cryptography and data security (pp. 99-118).Springer, Berlin, Heidelberg.
[23] N. Phaphoom, X. Wang, P. Abrahamsson, Foundations and technological landscape of cloud computing, ISRN Softw. Eng. 2013 (2013)
[24] W. Diffie and M. Hellman, “New directions in cryptography,” IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, Nov 1976.
[25] Sharma, S., Gupta, G., &Laxmi, P. R. (2014). A survey on cloud security issues and techniques.
[26]Huang, Y. L., Dai, C. R., Leu, F. Y., & You, I. (2015).A secure data encryption method employing a sequential-logic style mechanism for a cloud system. International Journal of Web and Grid Services, 11(1), 102-124.
[27]Mathur, R., Agarwal, S., & Sharma, V. (2015, May). Solving security issues in mobile computing using cryptography techniques—A Survey. In International Conference on Computing, Communication & Automation (pp. 492-497).IEEE.
[28]Schuster, F., Costa, M., Fournet, C., Gkantsidis, C., Peinado, M., Mainar-Ruiz, G., &Russinovich, M. (2015, May). VC3: Trustworthy data analytics in the cloud using SGX. In 2015 IEEE Symposium on Security and Privacy (pp. 38-54).IEEE.
[29] L. Xie, C. Wang, Cloud multidomain access control model based on role and trust-degree, J. Electr. Comput. Eng. 2016 (2016)
[30] Y. Zhang, J. Chen, R. Du, L. Deng, Y. Xiang, Q. Zhou, FEACS: A flexible and efficient access control scheme for cloud computing, in: 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, 2014, pp. 310–319, http://dx.doi.org/10.1109/TrustCom. 2014.42, ISSN 2324-898X.
[31] Sabahi, F. (2011, May). Cloud computing security threats and responses. In 2011 IEEE 3rd International Conference on Communication Software and Networks (pp. 245-249). IEEE.
[32]Younis, Y. A., Kifayat, K., &Merabti, M. (2014). An access control model for cloud computing. Journal of Information Security and Applications, 19(1), 45-60.
[33]Aikas, E. V., &Erb, D. (2015). U.S. Patent No. 9,209,973. Washington, DC: U.S. Patent and Trademark Office.
[34] AkhilBehl&KanikaBehl (2012), An Analysis of Cloud Computing Security Issues.
[35] R. Balasubramanian, Dr.M.Aramuthan (2012) Security Problems and Possible Security Approaches In Cloud Computing
[36]D. Jamil and H. Zaki, “Security Issues in Cloud Computing and Countermeasures,” International Journal of Engineering Science and Technology, Vol. 3 No. 4, pp. 2672-2676, April 2011.

[37]Te-Shun-Chou,"SECURITY THREATS ON CLOUD COMPUTING VULNERABILITIES",Int-Journal of Computer Science-Information Technology Vol 5, No 3, June 2013

[38] Jansen, W. A., &Grance, T. (2011). Guidelines on security and privacy in public cloud computing.

[39] Subashini, et all, A survey on security issues in service delivery models of cloud computing, J. Netw. Comput. Appl. (ISSN: 1084-8045) 34(1) - (2011) 1–11

[40]Top Threats to Cloud Computing V1.0; Cloud Security Alliance: March 2010.

[41] Ko, R. K. (2014). Data accountability in cloud systems. In Security, Privacy and Trust in Cloud Systems (pp. 211-238). Springer, Berlin, Heidelberg.

[42] Jayapandian, M. N., &Karthikeyan, S. Enhanced Multi Owner Security System in Cloud Environment using Offensive Digital Forensics and Decoy Technology (DFD). International Journal of Applied Engineering Research, 10(38), 2015.

[43]Ateniese, G., Di Pietro, R., Mancini, L. V., &Tsudik, G. (2008, September).Scalable and efficient provable data possession.In Proceedings of the 4th international conference on Security and privacy in communication netowrks (pp. 1-10).

[44]Shouket Ahmad Kouchay(2015), Research Review on Cloud Computing: Security Threats and Challenges ,International Journal of Innovative Research in Computer and Communication Engineering,Vol. 3, Issue 12, p12828

[45]M. Hadavi, E. Damiani, R. Jalili, S. Cimato, Z. Ganjei, "AS5: A Secure Searchable Secret Sharing Scheme for Privacy Preserving Database Outsourcing", Proc. Fifth Int'l Workshop Autonomous and Spontaneous Security, 2013-Sept.

[46]W. Jansen, T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing", 2011.

[47]Wang, Q., Wang, C., Li, J., Ren, K., Lou, W.: Enabling public verifiability and data dynamics for storage security in cloud computing. In: Proceedings of the 14th European Symposium on Research in Computer Security, ESORICS'09, Charleston, pp. 355–370. Springer, Berlin/Heidelberg (2009)

[48]Vines, R. L. K. R. D., &Krutz, R. L. (2010). Cloud security: A comprehensive guide to secure cloud computing (pp. 35-41). Wiley Publishing, Inc.

[49]Darve, N. R., &Theng, D. P. (2015, February). Comparison of biometric and non-biometric security techniques in mobile cloud computing. In 2015 2nd International Conference on Electronics and Communication Systems (ICECS) (pp. 213-216).IEEE.

[50].Winkler, V. J. (2011). Securing the Cloud: Cloud computer Security techniques and tactics. Elsevier.