Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 6, July, 2021: 4630 - 4637

Research Article

Security Issue & Challenges In Cloud Computing

Shabina. G. Sayyed[1*,]
Computer Science And Engineering Department
Karmaveer Bhaurao Patil College Of Engineering Engineering
Satara, Maharashtra, India.
Shabina.Sayyad@Kbpcoes.Edu.In

Tarannum. J. Sayyed[2*,]
Computer Science And Engineering
Department Karmaveer Bhaurao Patil College Of
Satara, Maharashtra, India.
Tarannum.Sayyed@Kbpcoes.Edu.In

Sunita V. Mane[3*,]
Electronics & Telecommunication Department
DepartmentKarmaveer Bhaurao Patil College Of Engineering
EngineeringSatara, Maharashtra, India.
Sunita.Mane@Kbpcoes.Edu.In

Archana N. Ulmek[4*,]
Electronics & Telecommunication Department
Karmaveer Bhaurao Patil College Of Engineering
Satara, Maharashtra, India.
Archana.Ulmek@Kbpcoes.Edu.In

Abstract:

Cloud Computing Is A New Computing Method That Is Gaining Traction In The Field Of Computer Science. Cloud Computing Is A Kind Of Computing Based On The Internet And Represents The Next Stage Of The Internet's Development. Although It Has Garnered Much Attention In Recent Years, Security Concerns Are A Key Impediment To Cloud Computing Development. It Moves User Data And Application Software To Distant Data Centres, I.E., The Cloud, Over Which The User Has No Control And Where Data Management May Be Less Secure. However, This Unique Characteristic Of Cloud Computing Presents A Slew Of Security Concerns That Must Be Addressed And Properly Understood. This Expansion Of The Cloud Computing Ecosystem Imposes Additional Security Problems On Cloud Developers. Additionally, The Article Covers Current Cloud Security Methods And

Approaches. This Article Will Educate Academics And Professionals On Various Security Risks And The Models And Methods To Address Them.

Keywords: Cloud Security, Security Threats, Security Techniques, Cloud Security Standards.

I. Introduction

Cloud Computing Is A Relatively New Technology That Has Lately Garnered Considerable Interest From Businesses And Academics. Cloud Computing Delivers Services Via The Internet; Users May Access Various Software Applications Online Rather Than Buying Or Installing Them On Their Machines. As Well-Defined By The National Institute Of Standards And Technology (Nist), Cloud Computing Is A Paradigm For Providing Appropriate, On-Demand Network Entree To A Collective Pool Of Reconfigurable Computing Possessions [1]. As Gartner [2] Described, Cloud Computing Is A Method Of Delivering It Capabilities To End-Users Through The Internet. According To A Recent Study Conducted By International Data Group (Idg), The Top Three Obstacles To Successfully Adopting A Cloud Strategy In An Organization Differ Considerably Across It And Line-Of-Business Departments (Lob). Security Concerns Are A (66%) Issue For It, And 42% Of Cloud-Based Initiatives Are Ultimately Moved Back In-House Due To Security Concerns (65%) [3]. According To A 2011 Idc Study, 47% Of It Executives Were Worried About Cloud Computing Security Risks [4]..

1.1 Classification Of Cloud Computing

Multi-Tenancy, Enormous Scalability, Elasticity, Pay-As-You-Go, And Resource Self-Provisioning Are The Primary Characteristics Of Cloud Computing [18]. Cloud Computing Services Are Classified Into Three Types. (1) Infrastructure As A Service (Iaas) Enables The Usage Of A Computer-Generated Computer Set-Up, Online Storage, Computer Hardware, Servers, And Networking Apparatuses; (2) Paas (Platform As A Service) Is A Software Stage That Enables The Development Of Applications In A Variety Of Program Design Languages (3) Saas (Software As A Service) Allows Users To Entree Cloud-Hosted Apps And Services. Cloud Computing Has Many Deployment Models: (1) Public Clouds Are Those That Are Possessed By Facility Providers And Whose Possessions Are Leased Or Traded To The General Community (2) An Organization's Private Cloud, Which Is Either Possessed Or Leased (3) Public Cloud Computing Is Comparable To Remote Cloud Computing, Except That Cloud Possessions Are Joint Across Several Closed Communities (4) The Term "Hybrid Cloud" Refers To A Cloud Computing Environment That Combines Two Or More Deployment Methods [19]. The Framework For Cloud Computing Defined By Nist Is Shown In Figure 1.

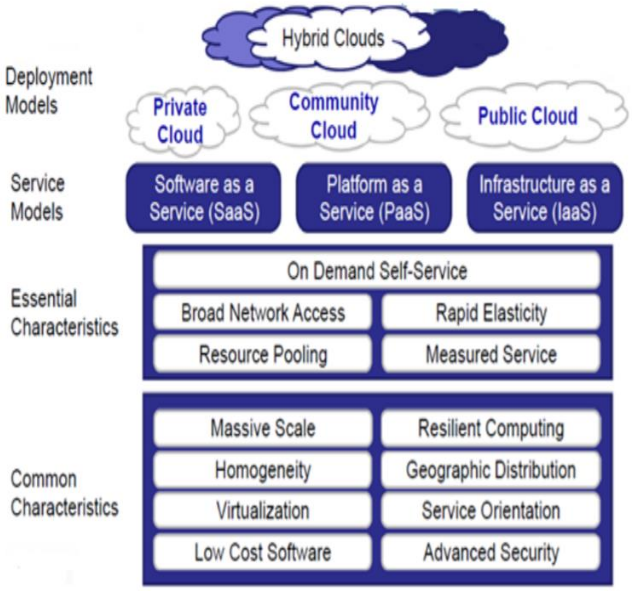

Figure 01: Nist Cloud Definition Frame Work [20]

We Concentrated On The Problem Of Data Security In A Cloud Computing Environment In Our Study Effort.

II. Review Of Literature

Following Section Gives The Details Overview Of Existing Work,

In 2016, It Was Determined That The Internet Of Things (Iot) Encompasses Any Devices Linked To The Internet And Capable Of Exchanging Data Over The Network; However, Poor Design And Set-Up Of Technology May Result In Security Risks. [19] Outlined The Internet Of Things (Iot) Security Risks And Then Offered A Security Architecture For Mitigating Such Vulnerabilities. Cloud Computing Is Self-Motivated Know-How That Enables Data Revolution And Alleviates Cloud Users' Burdens Associated With Local Storage. [20] Suggested A Way For Enhancing Security Employing Stenography And Cryptographic Methods. Security-As-A-Service (Saas) Model Offers Security In A Cloud Atmosphere, And Users May Access These Services Simply Through A Web Browser. The Method Is Clever In That It Divides Encryption Into Numerous Encryptions [21]. The Author Of This Article Used An Intelligent And Transparent Approach To Encryption And Decryption In Cloud Services.

In 2017, Writers Discussed How Cloud Computing Platforms Are Executed And Planned To Run Web Requests And Share Data Via Cyberspace. This Type Of Expertise Is Made Using The Openstack Outline And Is Exposed To Multimodal Developments. Utilizing Fingerprints As A Unique Biometric Validation Method Ensures Safe Access For Many Users And Provides Comprehensive Security. Multi-Cloud Storage Is A Necessary Service In The Cloud Because It Enables Remote Storage And Access To Cloud Data, And Storage Is Capable Of Encrypting And Storing Information Across Multiple Cloud Drives [26]. The Proposed Model Protects Against Various Insider Attacks, Privacy For Various Records Uploaded By Various Users, And Decentralized Information Storage Via Index-Based Cryptography.

In 2018, Cloud Security Became A Top Priority For Cloud Researchers Due To Increased Unauthorized Activities Reported By Cloud Users [27]. New Security Planning For Cloud Frameworks

Was Proposed To Secure Information Transformation And Shield Information From Leakage. Information Possessors And Cloud Servers Have Distinct Characteristics; This Architecture Provides Information Storage And Addresses Distinct Security Concerns; A Separate Process Is Needed To Ensure That Cloud Information Is Properly Stored On The Cloud Server [28]. Cloud Computing Uses "Utility Computing" And "Software-As-A-Service" To Deliver The Services Needed By The Cloud User. Cloud Security Is A Key Aspect Of Cloud Computing With Many Difficulties And Problems [29]. Described The Factors That Influence Security And Examined Security Concerns And Difficulties That Cloud Service Providers And Customers Confront, Such As Data Privacy, Security, And Infected Applications.

III.

IV. Cloud Security Issues

Organizations Use Various Cloud Computing Services, Including Iaas, Paas, Saas, And Different Cloud Computing Models, Including Public, Private, And Hybrid. These Architectures And Services Provide Several Cloud Securities Challenges. Each Service Model Has Several Problems Connected With It. Security Problems Are Seen From Two Outlooks: First, From The Service Provider's Perspective, Who Guarantees That Their Services Are Protected And Control The Customer's Identification. The Other Perspective Is That Of The Client, Who Guarantees That The Facility They Are Using Is Sufficiently Protected.

Multi-Tenancy

A Cloud Paradigm Is Developed To Facilitate Resource Sharing, Memory Sharing, Storage Sharing, And Collaborative Computation [2]. Multi-Tenancy Enables Supplementary Effective Resource Use, Which Reduces Costs. It Entails Sharing Computing Resources, Storage Space For Services, And Applications With Other Tenants Who Share The Same Physical/Logical Platform On The Provider's Facilities. Consequently, It Cooperates With Information Confidentiality, Ensuing In Data Leakage And Encoding And Increasing The Likelihood Of An Outbreak.

Elasticity

Elasticity Is Designated As A System's Capability To Regulate Changing Workloads Via Autonomous Resource Supply And Depletion, Ensuring That Available Resources Meet Current Demand As Precisely As Feasible At Any Point In Time. Scalability Is A Necessary Condition For Elasticity. Consumers May Scale Up Or Down As Required, It States. This Scalability Allows Residents To Use Resources Previously Owed To Another Resident. This May, However, Create Problems Of Secrecy.

Insider Attacks

Cloud Computing Is A Multitenant Architecture That Is Managed Centrally By The Provider. This Is An Internal Danger. For Cloud Workers, There Are No Recruiting Criteria Or Suppliers [1]. As A Result, A Third-Party Vendor May Breach An Establishment's Information And Corrupt Or Trade It To Another.

Outsider Attacks

This Is A Serious Problem For An Organization Since It Exposes Its Private Information To The Public. Clouds Are Not Comparable To Private Networks In That They Contain Much More Interfaces. Thus, Hackers And Attackers Benefit From Exploiting The Api's Flaws And May Attempt To Break A Connection [1]. These Assaults Are Less Damaging Than Insider Attacks Since The Latter Are Often Undetectable.

V. Security Techniques For Securing Cloud

Cloud Data Encoding Is Not A Viable Option For Information That Can Maintain Trust In The Cloud's Security. It May Be Accomplished By Using Established Security Methods Such As Validation And Individuality Management, Encoding, Truthfulness Checking, Admittance Control, Secure Exposure, And Information Masking. All Of These Security Approaches Are Relevant To Cloud Information. Security Methods Are Explained In Figure 2.

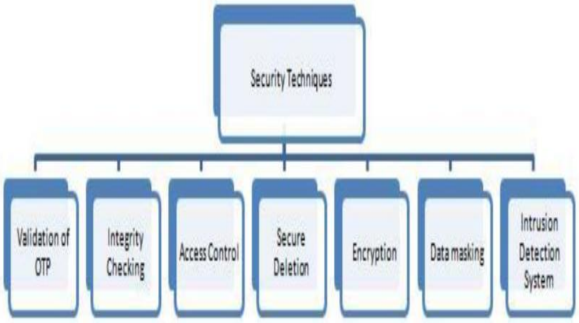

Figure 2 Security Techniques For Securing Cloud

A. Validation Of Otp

In The Current Environment, Many Banks Provide Authentication Via The One Time Password (Otp) Technique, Which Is Produced Randomly And Used To Authenticate The Cloud User's Identity. Occasionally, This Method Is Used For One-Time Validation, Referred To As System Factor Validation, As Illustrated In Figure 3. While It Is Sometimes Used For Two-Factor Validation, The Term "Multiple Authentication Factor" Refers To This.

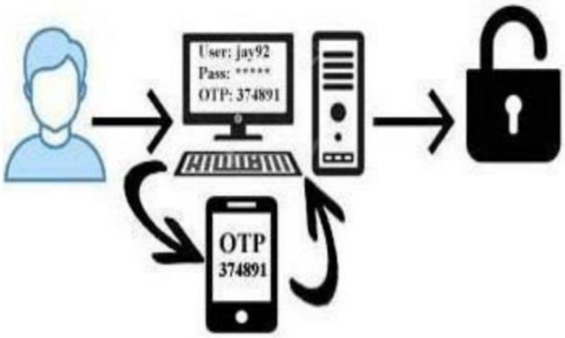

Figure 3 Otp Authentication

B. Integrity Checking

The Integrity Of Cloud Data Ensures That It May Be Altered Or Retrieved Only By An Approved User. In Simple Words, It Is A Cloud-Based Information Authentication Procedure That Guarantees The Information Is Unaltered, Accurate And That Fundamental Data Integrity Methods Are Followed. Provable Pdp Is A Method For Ensuring The Truthfulness Of Cloud Information Saved On A Distant Server, While Por Is A Technique For Obtaining And Verifying Proof That Cloud Data Placed On The Server By The User Has Not Been Altered [24].

C. Access Control

Access Control Implies That The Cloud Data Possessor May Provide Restricted Access To Their Data Outsourced To The Cloud, And Authorized Users Can Access Cloud Data While Unauthorized Users Cannot. As A Result Of Access Control, Cloud Data Is Secured Against Alteration Or Unauthorized Disclosure.

D. Secure Deletion

Understanding How Data Is Removed From The Server Is Critical. Deletion Employs Various Methods, Including Clearing; Using This Technique, We Erase Media Before Reusing Them While Still Protecting Accepting The Previously Included Data In The Media. Sanitization, In This Case, No Security Is Provided For Longsuffering Preliminary Information, And This Kind Of Information Is Routinely Disseminated At A Lower Classification Level [32].

E. Encryption

Cloud Security Offers Information Encoding Services To Encode Cloud Information Before Transfer From Local Storage To Cloud Storage. It Is Intolerable To Decrypt Data Without A Decryption Key From Any System, Database, Or File, And Encrypted Data Can Be Accessed Only By An Authorized User Who Has The Decryption Key. Separating Encoded Information And The Encoding Key Is Required For Information Security. The Encryption And Decryption Processes Described Below Are Shown In Figure 4.

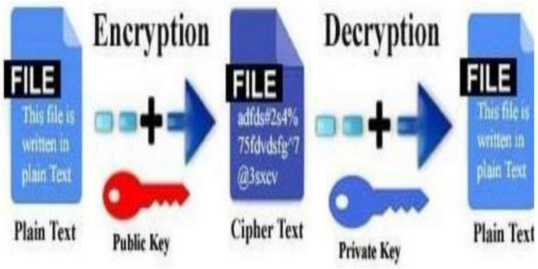
Encryption
Decryption
FILE
This file is written in plain Text
Plain Text
Public Key
FILE
adfds#2s4% 75fdvdsfg^7 @3sxcv
Cipher Text
Private Key
FILE
This file is written in plain Text
Plain Text

Figure 4 Data Encryption And Decryption

VI. Conclusions

Cloud Computing Has Many Advantages, Including Cost Savings, Rapid Implementation, And Increased Accessibility. However, Many Practical Issues Remain. One Of Them Is The Protection Of Personal Data. Numerous Researchers Have Contributed To Addressing The Data Security Problem In This Area Via Various Methods Outlined In This Work. A Study Of The Literature In Cloud Computing Data Security Is Performed, And The Significance Of Each Technique Is Briefly Discussed, Although They May All Be Used For Cloud Data Security.

References

1. R. Choubey, R. Dubey, And J. Bhattacharjee, “A Survey On Cloud Computing Security, Challenges And Threats,” Int. J. Computer. Sci. Eng., Vol. 3, No. 3, Pp. 1227–1231, 2011.
2. R. P. Padhy, M. R. Patra, And S. C. Satapathy, “X-As-Service: Cloud Computing With Google App Engine, Amazon Web Services, Microsoft Azure And Force.Com,” Int. J. Computer. Sci. Telecomm., Vol. 2, No. 9, Pp. 8–16, 2011.

3. G.K. Ravikumar “Design Of Data Masking Architecture And Analysis Of Data Masking Techniques For Testing”, International Journal Of Engineering Science And Technology, Vol. 3, No. 6, Pp. 5150-5159, 2011. 4. A. Behl , K. Behl, “An Analysis Of Cloud Computing Security Issues,” 2012 World Congr. Inf. Commun. Technol., Pp. 109– 114, 2012.

5. D Chopra, D Khurana, K Govinda, “Cloud Computing Security Challenges And Solution,” International Journal Of Advances In Engineering Research, Vol. 3, No. 2, 2012.

6. G. R. Vijay, “An Efficient Security Model In Cloud Computing Based On Soft Computing Techniques,” Vol. 60, No. 14, Pp. 18–23, 2012.

7. H. Tsai, N. Chiao, R. Steinmetz, And T. U. Darmstadt, “Threat As A Service?: Virtualization's Impact On Cloud Security,” No. February, Pp. 32–37, 2012.

8. K. Kumar, V. Rao, S. Rao, And G.S. Rao, “Cloud Computing : An Analysis Of Its Challenges & Security Issues,” Ijcsn,Vol. 1, No. 5, 2012.

9. K. D. Kadam, S. K. Gajre, And R. L. Paikrao, “Security Issues In Cloud Computing,” Proceedings Published By International Journal Of Computer Applications,Pp. 22–26, 2012.

10. M. Shrawankar, A. Kr. Shrivastava “Comparative Study Of Security Mechanisms In Multi- Cloud Environment,” Vol. 77, No. 6, Pp. 9–13, 2013.

11. N. Aggarwal, P. Tyagi, B. P. Dubey, And E. S. Pilli, “Cloud Computing : Data Storage Security Analysis And Its Challenges,” Vol. 70, No. 24, Pp. 33–37, 2013.

12. P. Aggarwal, M. M. Chaturvedi, “Application Of Data Mining Techniques For Information Security In A Cloud: A Survey,” Int. J. Comput. Appl., Vol. 80, No. 13, Pp. 11–17, 2013.

13. A. Botta, W. De Donato, V. Persico, And A. Pescape, “On The Integration Of Cloud Computing And Internet Of Things,” Proc. - 2014 Int. Conf. Futur. Internet Things Cloud, Ficloud 2014, Pp. 23–30, 2014.

14. D. Panth, D. Mehta, R. Shelgaonkar “A Survey On Security Mechanisms Of Leading Cloud Service Providers,” Int. J. Comput. Appl. , Vol. 98, No. 1, Pp. 24–34, 2014.

15. D. Porwal, P. Mohmood Khan And D. Shankar Ray, “Cloud Computing Security Threats And Countermeasures”, International Journal For Innovations In Engineering Science And Management, Vol. 2, No. 4, Pp. 1-4, 2014.

16. D. Parwani, A. Dutta, P. Kumar Shulka, And M. Tahilyani, “Various Techniques Of Ddos Attacks Detection And Prevention At Cloud: A Survey,” Orient. J. Comput. Sci. Technol., Vol. 8, No. 2, Pp. 110–120, 2015.

17. G. Al, “Cloud Computing Architecture And Forensic Investigation Challenges,” Int. J. Comput. Appl., Vol. 124, No. 7, Pp. 20–25, 2015.

18. M. U. Shankarwar And A. V. Pawar, “Security And Privacy In Cloud Computing: A Survey,” Adv. Intell. Syst. Comput., Vol. 328, Pp. 1–11, 2015.

19. A. F. A. Rahman, M. Daud, And M. Z. Mohamad, “Securing Sensor To Cloud Ecosystem Using Internet Of Things (Iot) Security Framework,” Proc. Int. Conf. Internet Things Cloud Comput. - Icc ’16, Pp. 1–5, 2016.

20. B. Pathankot, “Review Paper On Enhancing Data Security For Cloud Environment Cryptography And Steganography,” International Journal Of Engineering Applied Sciences And Technology, Vol. 2, No. 1, Pp. 44–48, 2016.

21. D. H. Sharma, C. A. Dhote, And M. M. Potey, “Intelligent Transparent Encryption-Decryption As Security-As-A-Service From Clouds,” 2016 Int. Conf. Comput. Syst. Inf. Technol. Sustain. Solut. Csitss 2016, Pp. 359–362, 2016.

22. B. Mahesh, “Data Security And Security Controls In Cloud Computing”, International Journal Of Advances In Electronics And Computer Sciecne, Pp. 11-13, 2016.

23. T. Singh, S. Verma, V. Kulshrestha And S. Katiyar, “Intrusion Detection System Using Genetic Algorithm For Cloud”, International Journal Of Advances In Electronics And Computer Science, Pp. 1-6, 2016

24. S. Sharma, “Data Integrity Challenges In Cloud Computing”, 4 Th International Conference On Recent Innovations In Science Engineering And Management, Pp. 736-7436, 2016.

25. G. L. Masala, P Ruiu, E Grosso, “Biometric Authentication And Data Security In Cloud Computing,” Comput. Netw. Secur. Essentials, Pp. 337–353, 2017.

26. K. Subramanian And F. L. John, “Secure And Reliable Unstructured Data Sharing In Multi-Cloud Storage Using The Hybrid Crypto System,” Ijcsns, Vol. 17, No. 6, Pp. 196–206, 2017.

27. A. Hussain, C. Xu, And M. Ali, “Security Of Cloud Storage System Using Various Cryptographic Techniques,” International Journal Of Mathematics Trends And Technology (Ijmtt), Vol. 60, No. 1, Pp. 45–51, 2018.

28. A. Venkatesh And M. S. Eastaff, “A Study Of Data Storage Security Issues In Cloud Computing,” Ijsrcseit, Vol. 3, No. 1, Pp. 1741–1745, 2018.

29. G. Jain And A. Jaiswal, “Security Issues And Their Solution In Cloud Computing”, Concepts Journal Of Applied Research(Cjar), Vol. 02,No. 03, Pp. 1-6, 2018.

30. Y. Guo And B.Wang Et.Al., “Feature Selection Based On Rough Set And Modified Genetic Algorithm For Intrusion Detection” , The 5th International Conference On Computer Science & Education Hefei, China, Pp. 1441-1446, 2018.

31. Data Clustering Algorithms[Online] Https://Sites.Google.Com/Site/Dataclusteringalgorithms/Kmeans-Clustering-Algorithm (Accessed 08 March 2019).

32. Cloudcodes [Online] Https://Www.Cloudcodes.Com/Blog/ Dataprotection-Controls-Techniques.Html (Accessed 20 December 2019).

33. Digital Guardian [Online] Https://Digitalguardian.Com/Blog/What-Cloud-Encryption (Accessed 25 December 2019).