A LITERATURE SURVEY ON CLOUD COMPUTING FOR DATA SECURITY

Palvadi Srinivas Kumar [1][0000-0002-1359-6152], Dr. Ranjana Rajdhan[2][0000-0002-5403-5749]

*Research Scholar, Department of Computer Science Engineering, University of Madras, Chennai, Tamilnadu, India.

**Professor, Department of Computer Science Engineering, University of Madras, Chennai, Tamilnadu, India.

Abstract

Now a day's cloud computing has became an interesting topic in research using various components and architectures for proposing cloud communication through user interface. Data reliability and security is provided by the cloud computing for various users and also it is a demanded computing service by using various algorithms for cloud server data storage for user. Cloud computing technique utilizes a third party auditor (TPA), Cloud severs which contains data centre and server for computations, data accessible unit and users input for components maintenance and communication for processing data. Different encryption techniques are used for maintaining data security and privacy to users which are proposed by various authors. The present paper tells about the contribution survey about various available encryption and data security techniques for enhancing data authentication. Here it monitors various algorithms like KP and CP -ABE (Attribute Based Encryption), AES (Advanced Encryption Standard), ECC (Elliptical curve cryptography) and Homo- orphic methods including new algorithms which are available in cloud but our contribution is extended to monitor pros and cons which present in same field of cloud are computing. Here further investigation must be done by researchers for consideration of available methods that work for leading the maximum cloud security which has high efficiency and also other computational parameters.

Keywords

TPA (third party auditor), Cloud server, Data authentication, Data encryption, Cloud computing

1. Introduction

Cloud computing technology of data storage and keeping up security of the information Hosting its own advantage Also accordingly it gatherings give client a surety capacity Also right over starting with At whatever and only the universe. [1] Cloud computing additionally the table looking into request calculation with user's information should backing different gadget and similarity. Similarly as contrasted with the customary server computing there may be constraint for storage and benefits to the client which client use for its optimized requirement, such prerequisite needing offices succeeds by that cloud computing dynamicity. Cloud gives a versatile and proficient result for administration use. A

progressive storage, pay by for every utilization particular idea settle on cloud that's only the tip of the iceberg usable as for every prerequisite. By client uses a totally mixture about accessible services, client required on pay just for the individuals benefits. [2] Cloud computing furnish An specific level of security through its secure structure which hold numerous parts Likewise : CSP (cloud service provider) An get-together in the situation which employments Similarly as An manager from claiming cloud benefits Also keep up An information enter, information storage fittings and different related prerequisite administration go about as An supplier. These would the merchant for example, such that IBM, AMAZON, INTEL and different fittings productive supplier they would look after those benefits and go about as cloud administration suppliers. TPA (third party authenticator) [3] will be an alternate essential a piece from claiming cloud computing situation which bargains alternately convey amidst the client end and CSP(Cloud Service Provider), [4] it validate the computation, looking into request information integument checksum utilizing diverse hashing plan And different obliged calculation carried out In this wind. CU (cloud user) may be a client or a customer framework client which really use those administration of the CSP (Cloud Service Provider) Also TPA, (Third Party Audit Authentication) [5] client might store Also control its printed And media information done secure manifestation Toward those consent from claiming TPA (Third Party Audit Authentication) Also get verification enter starting with it, Subsequently ready should handle its information from those CSP (Cloud Service Provider) alternately information enter. [6] So as will get integument confirmation for the at that point saved data, client can place a test will TPA (Third Party Audit Authentication) et cetera TPA (Third Party Audit Authentication) methodology those same with CSP (Cloud Service Provider) [7] and gives those innovation reaction evidence starting with the server information storage [8].

Here are some steps involved in cloud computing:

1. In order to connect with cloud computing user gets key from TPA. (Third Party Audit Authentication) [9]
2. File storage and file manipulations are performed only when the user connects with authenticated key. [10]
3. Assigning a file identity and hash value is done only when the user requests from file data proof.[11]
4. Based on the response given by the cloud server user gets original file proof. [12]
5. Then finally TPA (Third Party Audit Authentication) and CSP (Cloud Service Provider) keep a track in cloud data for monitoring and sorting of all data storage performers so that the execution scenario is performed in same manner. [13]

II. Literature review

In this paper [14] creator recommended An mixture encryption framework the place An mixture algorithm to those information encryption may be recommended clinched alongside which thought is done with three encryption methodologies. In the paper creator viewed as three diverse rounds to the encryption Also information methodology, additionally those various levels give the large amount from claiming information security done cloud information. To start with stage a mono alphabetic substitution is utilized which When make enter as plaintext Also apply those calculation with those plaintext Also give an yield from claiming substituted information. Those second round holds those plan the place the odd

amount alphabet is annex for once more those following alphabet following those odd position alphabet et cetera the information transforming is performed matching premise. Once more the yield from claiming second encryption plan may be made to third et cetera three co-efficient utilized for those fourth round of encryption. The yield algorithm which may be furnished toward those framework may be powerful by it gives a consolidation of compacted information and yield information size may be decreased up to half.

In this paper [15] creator introduce another system which use BLS (Bohen Lynn Shacham) strategy to encryption which utilization to enter matching framework Also store those information for encrypted text, further transfer of the cloud server information focus. This paper additionally utilization hashing procedure SHA-1 (Secure Hash Algorithm-1) which may be integument confirmation system to the information outperformed to the integument and change. Those security from claiming this signature plan relies with respect to another problem, in particular k-CAA alternately k + 1EP. It will be demonstrated that k + 1EP is no harder over those CDHP (Computational Diffle Hellman Problem). In light of this essential signature scheme, An ring signature plan And another system to assignment are suggested in this paper research, bilinear algorithm is a matching built algorithm which is protection preserving And ready should perform those information security without interference And concealing those unique information without interference in the auditing procedure and the hashing might have been performed for those assistance about sha-1 which prepare 128 spot magic period in place on look after the information to checksum methodology clinched alongside verification, they need utilized JPBC (Java Pairing Based Cryptography) java library in place on perform the execution And perform the re-enactment to the exhibit algorithm , those Boneh-Lynn-Shacham employments signature based plan to the information verification, they employments elliptic bend plan to those encryption built plan. This plan permits a shorter mark plan over the FDH (Full Domain Hash) signature plan. Additionally creator employments BLS (Basic Life Support) based plan for the information security Also capacity design.

In this paper[16] they have acted on Different quality confidentiality, integrity, availability, accountability, And privacy-perceivability Also performed those Different security worry issues Previously, aspects, creators need efficiently concentrated on the security And protection issues over cloud registering In light of an attribute-driven methodology, we bring identifier the greater part illustrative security/privacy qualities (e. G. , confidentiality, integrity, availability, responsibility and privacy- perceivability), and also examining the vulnerabilities, which might a chance to be misused By adversaries in place should perform Different strike. Resistance methodologies and suggestions were examined Likewise well, In this way this will be the paper incorporated those security Also consider viewpoints in cloud computing, the information integument confirmation made managing encryption algorithm and the review might have been performed for the help for hashing calculation accessible in place on confirm the worth created once more same time checking those information integument accessible with those connected file, here they need acted once diverse parts [17] for example, such that client account entry approach, accessibility from claiming data, information evolving alternately integument confirmation and the techno babble ought further bolstering make protection preserving so that those information ought not a chance to be spill Throughout the cloud execution.

Done their paper [18] proposes presenting a trusted third Party, tasked with guaranteeing particular security aspects inside cloud surroundings. Those recommended result calls upon cryptography, particularly open magic foundation working in show for SSO(Single Sign On) and LDAP,(Light weight Directory Access Protocol) to guarantee those authentication, integument and secrecy for included information And interchanges. The solution, displays an level for service, accessible to everyone embroiled entities that understands a security mesh, inside which crucial trust will be supported. In this examination they bring suggested recognized nonexclusive plan standards of a cloud earth which stem from the need to control important vulnerabilities and dangers. A blending for PKI(Public Key Infrastructure), LDAP,(Light weight Directory Access Protocol) And SSO(Single Sign On) might address The greater part of the distinguished dangers over cloud registering managing those integrity, confidentiality, genuineness Also accessibility from claiming information Also correspondences. The solution, displays An level about service, accessible to at embroiled entities, that understands a security network through federations, inside which vital trust is maintained, with those system given By them An profound substance examination might have the capacity should perform and consolidate techno babble might have been equipped location Different strings and issues related issue with the information And its integument identified with the information storage.

In this paper [19] content based two round encryption plan may be utilized which uses symmetric enter encryption method for the information capacity , this calculation execute double expansion operation calculation , hardware touch moving operation will be also performed for symmetric magic encryption techno babble may be used Toward the creator. For those deviated way encryption they need determined the idea for ECC(Elliptical Curve Cryptography), RSA (Rivert,Sheldon and Adalson) algorithm and DES (Data Encryption Standard) algorithm Also for those symmetric enter encryption techno babble 3DES(3Data Encryption Standard), blowfish and AES (Advanced Encryption Standard) technique may be used Toward the writer for encryption reason. Further a bitwise hardware technique which may be substance built and used to the picture information security will be utilized the place magic era will be carried utilizing MSB (most significant bit) of the data information document and further unscrambling may be performed utilizing its opposite transform. In this paper creator taken a straightforward plaintext Alice@202 as information string also performed two rounds encryption to furnish information security. At last as stated by creator the encryption methodology may be straightforward Also utilization viable method for magic era and information encryption , also further upgrade could make carried out ahead taking different information formats for the encryption for example, such that doc, content which could make consolidate with picture steganography.

In this paper[20] the cloud must give acceptable the verification that its giving or looking after complete information capacity And in that they need stated with give those evidence that is information will be keeping up Toward those cloud, there they need expressed the record majority of the data identified with workstation macintosh deliver identified with which information might have been created Also they need utilized macintosh Similarly as a information integument proof, their framework consider conservative evidences with just you quit offering on that one authenticator quality this can prompt evidences for Similarly as little Likewise 40 bytes of correspondence. They bring Gave two results to it two results with comparative structure. Those person will be privately variable

and manufactures elegantly ahead pseudorandom capacities (PRFs); those second considers publicly variable evidences And is constructed starting with the mark plan for Boneh, Lynn, and Shacham over bilinear gatherings. Both results depend around homomorphism properties with aggravator verification under one little authenticator worth. They bring functioned with those parameters for example, such that efficiency, government funded verifiable, government funded retrievable – the place effectiveness they have stated that those framework ought further bolstering be as productive By workable As far as both computational unpredictability And correspondence complexity, that might have been provided for a stress should fill in for And an arrangement will be publicly certain if At whatever (untrusted) substance might perform the confirmation review. This will be alluring on settings the place numerous clients could shareable storage alternately at a outsider is utilized should review those storage servers. In the paper they need specified two schemes redundantly encode equipped for an eradication code and apply a review that probabilistically ensures sufficient obstructs would retrievable on recreate the record.

In this paper [21] creator describe another approach to those cloud information security which may be the blending for two accessible algorithms, those To begin with may be des which is information encryption framework system and different is cast block cipher procedure is utilized. As stated by creator des may be suggested Toward IBM Also it is dependent upon those cipher which may be fiestel based cipher plan. It holds those touch shuffle, substitution and selective XOR operations were performed utilizing that algorithm. Those algorithm holds a enter length for 64 bit which is solid in the event of encryption. Creator combines this calculation with case block cipher encryption which In light of those symmetric magic encryption framework. That calculation architecture holds the S boxed substitute system for encryption of data. That algorithm holds two sub steps for example, perplexity and dispersion. The usage of the algorithm may be performed utilizing Python 3. 4 and example enter made as exceed expectations sheet information which is encrypted and saved over those cloud registering. As stated by creator calculation gatherings give an secondary security and could a chance to be apply with 3G and 4G LTE nature's domain. And further change can make done to move forward execution such-and-such might a chance to be utilized for 5G nature's domain.

In this paper[22] they study how on settle on a unscrambling magic a greater amount capable in the feeling that it permits unscrambling for different cipher texts, without expanding its extent. Specifically, the issue articulation may be “To configuration an proficient public-key encryption plan which backs adaptable assignment in the feeling that any subset of the cipher writings (produced by those encryption scheme) will be unscramble unable Toward a constant-size unscrambling way (generated By the holder of the master-secret key). ” they take care of those issue of open magic encryption which might stake people in general way idea should intruder, Therefore they provided for another plan which may be Key aggravate Cryptography (KAC) to the information security And Dependability. Those enter holder And information manager holds a ace in broad daylight undertakings system which will be approached Likewise expert information key for those information commitment Also further information may be encrypted and store utilizing this secure techno babble.

In this paper [23] creator describe that calculation which employments trusted outsider built encryption plan. In the paper they consolidate both symmetric And deviated

built encryption plan which use those point purpose for both those calculation. The paper suggested three substances based plan for example, such that CSP (Cloud Service Provider) module made information and scramble utilizing the symmetric key encryption system for those information transmission. Second HTTP (Hyper Text Transfer Protocol) module which administers a mystery enter And magic return framework utilizing those cloud clients privileges to information return. Third those administration supplier store client information and administration way a mystery fact that created. The calculation employments AES(Advanced Encryption Standard) symmetric magic based algorithm to the encryption and At long last three period plan construction modelling set information soundness And security to client cloud information. As stated by creator further worth of effort could make annex with respect to minimizing information transmission overhead Also execution, reaction time for information trade with those cloud ought to a chance to be lessen with match with constant prerequisite. [24]

Table 1: Survey of Different Algorithms with its usage, Advantages and Disadvantages

S. no	Author	Algorithm	Description	Advantage	Disadvantage
1	Henry C.H. Chen and Patrick P.C. Lee	FMSR-DIP codes	Here FMSR (Functional minimum storage regenerating) code implementation is presented in this paper for giving less fault tolerance and high accuracy algorithm with limited time.	1. Low bandwidth 2. High fault tolerance value. 3. Implementing high security version.	Encryption investigating technique is not present.
2	Cheng-Kang Chu, Sherman S.M.Chow	Key Aggregate crypto system (KAC)	Here we introduce an open key distribution technique. KAC produces stable cipher text size so that effective allocation of decrypted set of cipher text is possible.	Steady state encrypted and decrypted key size. Here key size is self-governing for max number of cipher text class.	Key leakage causes data modification and deletion.
3	Nandita Sengupta and Ramya Chinnasamy	Hybrid DESCAST algorithm	In order to propose DESCAST technique, we combine DES and Cast block cipher algorithms.	Here security is provided by using hybrid technique and encrypted multiple key technique.	While dealing with large dataset this algorithm is very slow.

4	Dimitrios Zissis, Dimitrios Lekkas	SSo and LDAP techniques	Here we introduce a new multiple functional algorithm using SSO and LDAP for conforming and classification of information interchange.	Data storage provides a complex algorithm for high security.	It requires multiple steps and long execution time for large dataset.
6	Fangguo Zhang, Reihaneh Sfavi Naini	BLS, SHA-1 algorithm	Encryption technique uses bilinear mapping and data integrity for storing large data set in cloud model.	Bilinear mapping provides a symmetric key technique that compares both symmetric and asymmetric algorithm.	SHA-1 has less key size and requires more security

Table 2: Various Encryption Algorithms with comparisons

Factors	DES	AES	RSA	ECC
Contributor	IBM 75	Ryman, Joan	Rivest,Shamir 78	Neal Koblitz,Victor S.Miller
Key Length	56-Bits	128,192 and 256	Based on No.of bit in N = p*q	135 Bits
Block Size	64-Bits	128 Bits	Variant	Variant
Security Rate	Not Enough	Excellent	Good	Less
Execution Time	Slow	More Fast	Slowest	Fastest

III. CONCLUSION

Cloud computing technology for information storage Also gaining entrance to framework is needed today, the place the advanced universe oblige at sort information over safe Also organized organization. Different schemes whichever autonomous alternately mixture approach performed by diverse writer. In this paper we Audit every last one of distinctive systems Gave by the writer contributed done cloud registering security. The FMSR-DIP codes algorithm that is secondary tolerance, low transfer speed and high security rendition will be actualized. Disservice may be the no encryption strategy may be investigated. The magic of Key Aggregate cryptosystems (KAC), in this techno babble steady encryption furthermore unscrambling enter measure utilized and the key extent will be free of the most extreme amount about cipher content classes. Those framework also Hosting disservice that is those key spill might result in a few information erasure alternately

adjustment. The mixture DESCAST Algorithm, in this technique security Gave utilizing mixture methodology also various fact that Gave to the encryption. The fundamental hindrance of the algorithm will be generally moderate when managing huge information. The SSO Also LDAP (Light weight Directory Access Protocol) techno babble is utilized. The creator gives structural engineering to secondary security model for information capacity. Those disservice will be the secondary execution occasion when for substantial dataset, by it needs should transform numerous steps. This Audit paper likewise depicts cloud structure, component, diverse Look into performed Also advantage, disservice of the techniques. Different security imperatives were provided for in AES (Advanced Encryption Standard), KP-ABE(Knowledge Based Attribute Based Encryption), CP-ABE(Cipher Based Attribute Based Encryption), Homo-orphic technique, ecc built cloud capacity procedure which cases to secure information upkeep. Our further worth of effort will be on finding a suitableness calculation which dispenses with those detriment for existing situation calculations.

IV. References

1.M. Jelassi, C. Ghazel and L. A. Saïdane, "A survey on quality of service in cloud computing," 2017 3rd International Conference on Frontiers of Signal Processing (ICFSP), Paris, 2017, pp. 63-67.

2. Sourabh Chandraa,BidishaMandalb , Sk. safikulAlamc , Siddhartha Bhattacharyya," Content based double encryption algorithm using symmetric key cryptography", Procedia Computer Science 57 (2015) 1228 – 1234,Elsevier.

3. Zhifeng Xiao and Yang Xiao,– "Security and Privacy in Cloud Computing" IEEE June 2013 conference.

4. Chandu P.M.S.S and D. Kata, "Integrating and enhancing the quality of services in cloud computing with software testing," 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, 2016, pp. 2008-2010.

5. Nandita Sengupta* and Ramya Chinnasamy," Contriving Hybrid DESCAST Algorithm for Cloud Security", Procedia Computer Science 54 (2015) 47 – 56,Elsevier.

6. J. Upadhyaya and N. J. Ahuja, "Quality of service in cloud computing in higher education: A critical survey and innovative model," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, 2017, pp. 137-140.

7. Vishwanath S Mahalle, Aniket K Shahade," Enhancing the Data Security in Cloud by Implementing Hybrid (Rsa&Aes) Encryption Algorithm", 2014 IEEE.

8. Syed rizvi, Katie cover, Christopher gates, "A trusted third party (TTP) based encryption scheme for ensuring data confidentiality in cloud environment", Procedia Computer Science 36 (2014) 381 – 386, Elsevier.

9. M. Jelassi, C. Ghazel and L. A. Saïdane, "A survey on quality of service in cloud computing," 2017 3rd International Conference on Frontiers of Signal Processing (ICFSP), Paris, 2017, pp. 63-67.

10. A. Maarouf, A. Marzouk and A. Haqiq, "Towards a Trusted third party based on Multi-agent systems for automatic control of the quality of service contract in the Cloud Computing," 2015 International Conference on Electrical and Information Technologies (ICEIT), Marrakech, 2015, pp. 311-315.

11. Fangguo Zhang, ReihanehSafavi-Naini and Willy Susilo "An Efficient Signature Scheme from Bilinear Pairings and Its Applications". IEEE 2013

12. C. Jeong, T. Ha, J. Kim and H. Lim, "Quality-of-service aware resource allocation for virtual machines," 2017 International Conference on Information Networking (ICOIN), Da Nang, 2017, pp. 191-193.

13. N. K. Sharma, P. Sharma and R. M. R. Guddeti, "Energy efficient quality of service aware virtual machine migration in cloud computing," 2018 4th International Conference on Recent Advances in Information Technology (RAIT), Dhanbad, 2018, pp. 1-6.

14. Y. Awano and S. Kuribayashi, "Reducing Power Consumption and Improving Quality of Service in Cloud Computing Environments," 2012 15th International Conference on Network-Based Information Systems, Melbourne, VIC, 2012, pp. 1-6.

15. Henry c.h. Chen and patrick p.c. Lee."Enabling data integrity protection in regenerating-coding-based cloud storage: theory and implementation".ieee transactions on parallel and distributed systems, vol. 25, no. 2, february 2014.

16. D. Boneh, b. Lynn, and h. Shacham, "short signatures from theweil pairing," proc. Seventh int'l conf. Theory and application of cryptology and information security: Advances in Cryptology (ASIACRYPT '01), pp. 514532.

17. C. Wang, Q. Wang, K. Ren, and W. Lou, "PrivacyPreserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM '10, Mar. 2010.

18. H. S. Mondal, M. T. Hasan, T. K. Karmokar and S. Sarker, "Improving quality of service in cloud computing architecture using fuzzy logic," 2017 4th International Conference on Advances in Electrical Engineering (ICAEE), Dhaka, 2017, pp. 149-152.

19. Z. Liu, J. Dai, B. Wu and H. Lin, "Communication-aware motion planning for multi-agent systems from signal temporal logic specifications," 2017 American Control Conference (ACC), Seattle, WA, 2017, pp. 2516-2521.

20. A. Bono, G. Fedele and G. Franzè, "A distributed model predictive control strategy for vehicle teams in uncertain narrowed environments," 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Zaragoza, Spain, 2019, pp. 927-932.

21. Cloud Security Alliance, "Top Threats to Cloud Computing", 2010.

22. A. Maarouf, A. Marzouk and A. Haqiq, "Automatic control of the quality of service contract by a third party in the Cloud Computing," 2014 Second World Conference on Complex Systems (WCCS), Agadir, 2014, pp. 599-603.

23. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “Above the Clouds: A Berkeley View of Cloud Computing,” Technical Report UCB-EECS-2009-28, Univ. of California, Berkeley, Feb. 2009.

24. N. V. S. N. Kalluri and D. V. Yarlagadda, "Cognizance and Ameliorate of Quality of Service Using Aggregated Intutionistic Fuzzy C-Means Algorithm, Abettor-Based Model, Corroboration Method, and Pandect Method in Cloud Computing," 2016 IEEE 6th International Conference on Advanced Computing (IACC), Bhimavaram, 2016, pp. 84-95.