International Journal of Engineering & Technology, 7 (2.4) (2018) 161-164

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Hybrid algorithm designed for handling remote integrity check mechanism over dynamic cloud environment

Shakti Arora [1] *, Surjeet Dalal [1]

[1] Department of Computer Science and Engineering, SRM University, Sonepat, Haryana, Indi
**Corresponding author E-mail: shakti.nagpal@gmail.com*

Abstract

Cloud computing is the becoming the architecture information technology of next generation. Cloud computing provides dynamic set of resources for different category of users. Remote access of resources is available on the pay per basis. Cloud is using the storage, computing, infrastructure services according to the requirements. Cloud manages all the user data at distributed level and provides reliability, flexibility and on demand services to user with very low cost. In Now days scenario cloud applications and data over the cloud machines are increasing day by day which indirectly invites different threats for the crucial and sensitive data on cloud. In this paper, we proposed a security model that will give the computational enhancements in different modules data. The different proposed modules: 1) key generation 2) access control strong encryption 4) remote integrity checks. The proposed model enhances t confidentiality, authentication and integrity of data. From the result analysis, it has been concluded that computation and communication overhead are minimized as compared to previous model with higher efficiency achieved.

Keywords: *Cloud Data; Security Issue; Integrity; Secure Cloud Architecture*

1. Introduction

Cloud computing is application running on distributed network using virtualized resources and accessed by common internet-working protocols and standard. Cloud hides the system details from user. Physical Location of data is unknown to user. Cloud is combination of abstraction and virtualization. Resources on cloud can be extended unlimitedly, got any time and used on demand; the degree of acceptance of any computing environment is based on the strength and weaknesses of the technology. Aim of the paper is security aspects of cloud computing every cloud user want to avoid un-trusted cloud provider for personal and important information such as your credit/ debit and online bank credentials. We are focusing on the secure cloud database service that will stop the unwanted activities. In dynamic environment of cloud computing we adopted the approach based on secret key sharing for increasing the trust of users. It has following objectives as given below:

To create the trust mechanism so that user will rely on cloud

To eliminate the issues like Privacy preservations, computation integrity etc.

For achievement of the above objective an adaptive architecture is designed that will work on the keypoints of confidentiality, integrity and authentication.

2. Related work

Pritchard et al. (2009) tended to "Do the security challenges acted by virtualisation make it a non-starter for your delicate business appli-cations?" There was much practical discourse about circulated processing, which ensured to pass on utility-based virtual enlisting to the front door of every association. Some are ousting it as advancing development – however if it passes on the points of interest it claims, it can change undertaking handling. So what are the troubles – and what are the open entryways posed by this improvement?

Naruchitparames et al. (2011) proposed stun planning organization using trusted in enrolling segments to give improved professional tection and trustworthiness to potential customers. Utilizing blind correspondence and execution benefits, a customer exchanged his/her sensitive information with a cloud system by methods for disengaged methodology whose execution condition and data was shielded from whatever is left of the structure in the wake of ensuring the system had cure gear, place stock in preparing base, change accreditations, and de-pendable state. Zissis et al. (2012) surveyed cloud security by recognizing amazing security necessities and furthermore to try to demonstrate an appropriate arrangement that discards these potential risks. This paper proposed displaying a Trusted Third Party, endowed with ensuring standard ticular security characteristics inside a cloud circumstance. The proposed plan called upon cryptography, especially Public Key Infrastructure cooperating with SSO and LDAP, to ensure the affirmation, trustworthiness and mystery of included data and trades.

Modi et al. (2013) checked on the factors impacting Cloud handling assignment, vulnerabilities and attacks, and perceived appropriate plan requests to strengthen security and assurance in the Cloud condition. Conveyed registering offered versatile on-ask for administra-tions to buyers with more noticeable flexibility and lesser establishment theory. Since Cloud organizations were passed on utiliz-ing set up framework traditions and sorted out finished the Internet, comprehended vulnerabilities existing in these traditions and furthermore dan-gers exhibited by additional a la mode plans raised various security and insurance concerns.

Zou et al. (2014) stretched out trusted affix to memory by making watching devices in favored space utilizing highlights gave by virtual machine screen to screen and record runtime conditions of security basic application in focused virtual machine occasion. Moving by standard security advancement, for example, sandbox, we made and finished an "out-of-box" fine-grained security key application viewing uti-lizing framework call intervention and virtual machine examination. Estimations of framework courses of action set away in sort out design regis-ters of TPM close by runtime conditions of utilization in cloud client's virtual machine were spoken to relating cloud client through remote attestation which was a key section of place stock in dealing with too with a specific extreme target to offer good 'ol fashioned confirmations to cloud client.

Luna et al. (2015) introduced another view on this issue by exploring and isolating, from the association and danger assessment perspec-tive, the affirmation of security in cloud advantage level assentions (secSLA) as a promising way to deal with oversee interface with clients in investigating and understanding cloud security. Other than isolating the proposed chance based approach and focus the fundamental scene, this article demonstrated a honest to goodness situation to help the creation and portion of secSLAs as connecting with administrators for sorting out, evaluating, and viewing the master security levels in cloud associations.

Marquez et al. (2016) showed a relevant investigation on the layout of the migration of the security segments of a legacy application to Cloud providers by using the methodology called SMiLe2Cloud. The Cloud Computing offered a broad assortment of focal points, yet furthermore an important test from the viewpoint of security, in truth security remained the rule hindrance to advance. Development of legacy systems to the cloud allowed them to take control over security in legacy structures. The strategy called SMiLe2Cloud proposed to deal with the issue of secure movement legacy information systems to cloud.

Sahi et al. (2017) investigated the related work on security and assurance sparing and furthermore catastrophe recovery in the eHealth cloud space. By then it proposed two strategies, the Security-Preserving approach and the Privacy-Preserving approach, and a disaster recu-peration outline. The Security-Preserving approach was an incredible strategies for ensuring the security and genuineness of Electronic Health Records, and the Privacy-Preserving approach was a capable check approach which guaranteed the insurance of Personal Health Rec-ords. Finally, they discussed how the fused strategies and the failure recovery configuration can ensure the dependabil-ity and security of cloud wanders.

Katsikas et al. (2017) communicated that IT cost reducing was expert by offloading data and figurings to conveyed compu-ting. Regardless of the way that dispersed processing as a money related model has found versatile ground and is pulling in a lot of venture, numerous are up 'til now reluctant to use cloud organizations because of a couple of security, assurance, and trust issues that have risen. The underly-ing reaction of the security gathering to the security issues of dispersed registering was that these could be settled using existing systems procured from standard IT structures or even passed on systems that are the begetters of appropriated processing conditions. Stun ingly, this approach does not work, because of the scale and the building of the dispersed processing model. In this way, a need to re-think about security, insurance and trust stresses with respect to the disseminated figuring perspective develops

3. Proposed architecture

There are following steps of the proposed architecture as given below:

Step 1

Cloud client will get register with cloud server and one cloud id will be generated by the cloud server to the cloud client.

Step 2

Cloud id will be submitted to the certified channel for registration by the cloud server

Step 3

Encryption algorithm will be applied at the client side only by certified channel and cipher text plus parity bits will be passed to cloud server for storage with particular cloud id of client

Step 4

Cloud server will only save the cipher text on its disk so that if any comporomisation will be held with the cloud then intruder is not able to find the exact information.

Step 5

Certified channel is having the decryption key only and it can be applied at the certified channel only on the client side with a proper time based id. Every time a decryption key will be different for cloud client.

Step 6

During transmission attack can be verified by parity bits applied on the cipher text at the server side

Limitation of this algorithm is communication overhead, little bit increased due to the transmission of key every time but security is increased up to greater extent. Encryption can be applied with asymmetric algorithms

4. Algorithm working

Key generation:- after the registration of valid user a key will be generated for the communication between client and server. A 128 bit key is distributed to n number of users and for communicating with server threshold value of key shares are required.

Authentication Tag generation; authentication tag is calculated with each data block stored on the server with respect to client. Authentication tag is generated with public key of user and private key of server.

Proof: - challenge algorithm will work between auditor and third party channel and cloud server. Verifier will send a challenge or will ask for the proof of information which is saved on the server. Server will run the proof algorithm at its end and reply with computed authentication tag of data.

Integration of different modules in architecture

Step 1& 2:- covers the registration module on the virtual machine as we deployed cloud security application on the virtual server. VM will ask for the user registration and two step verification processes is applied for user registration approval.

Algorithms

i) Generate a key K, which is an arbitrary byte string and share it securely with client
ii) Settle a time T0 an d start counting time steps from, an interval , T1 which will be used to calculate the value of counter C
iii) Calculate the hash value with a cryptographic functions
iv) Finalize the token length

Key management (encryption algorithm)

Data encryption before outsourcing the data to cloud is a common privacy activity. Although a number of encryption algorithms are public, but provides highly security to data because the key used to encrypt the data remains secure. And overall burden goes with the key management in encryption and decryption process

Encryption is offline activity that means computation overhead is not added with server computation only the key exchange and retrieval activity is handled by server. Proposed algorithm generates 128 bit block sized encryption and to break the 2128 combination key is difficult for super computer as well. Encryption key is generated with user attributes or we can say to decrypt the data we should reach a threshold value of key collection to retrieve the key. Threshold value is decided by the algorithm at staring time.

Shamir's Secret Sharing

A *(K, n)*- Decided scheme [23] partition (based on polynomials) a secret S into n shares. Key can collected for decryption using any k-1 shares nearby threshold value. reaching to threshold can form a key, Using k pints , algorithm can uniquely define a degree of polynomial k-1, by choosing k-1 random positive integers $c1$, $c2$, $\cdot \cdot \cdot$, $ck-1$ from a finite filed of size q and set $C_0 = S$, we can construct the polynomial :$f(x) = c_1 + c1x + c2x\ 2 + \cdot \cdot \cdot + ck-1x\ k-1$, where c_i< *q*and *q* is a prime number. There are n number of users participating with in key sharing .we can construct n points out of *f(x)*as *(j, f (j))*1≤ *j*≤*n* and give each participant a point. At any Kpoint out of these n points, coefficient of f(x) can be computed using interpolation

1) Divide secret key into n parts. By collecting any of k shares up to threshold point can recover the secret. With less than k or k-1 attempt of shares, secret cannot be retrieved.
2) These k points can be defined with polynomial number of k-1 degree, by selecting any positive k-1.
3) a_1,a_2,a_3…a_{k-1} from a finite filled of size q
4) A polynomial: $f(x) = c_0+c_{1x+c2x2+\ldots\ldots\ldots ck-1x.}$ where ci<q and c is prime number
5) Among n participants, the shared secret key can be constructed out of f(x).

4.1. Access control

Trusted domain are used for storing data of clients and server so accessing protocol for different user should be efficient to remove the unauthorized and unwanted access . Cloud servers are not seen trustworthy to outside users and organization. So most efficient method to access control is to make privilege list of different users and provide different keys for encryption and decryption to each user. The possible solution for making the data secure is to encrypt the data with certain cryptographic algorithm and disclose the key only to authorized user. Complexity of this scheme is increasing-lpropotionally to the scale of users. Or we can say this solution lacks scalability.

Proposed access control mechanism is based on key derivation methods. Access control will be based on the attribute of user, users attribute will be added with the cloud server key to generate an encryption key and will be stored with third party so server overhead for storing the key and user overhead of keeping and exchanging the key will be reduced

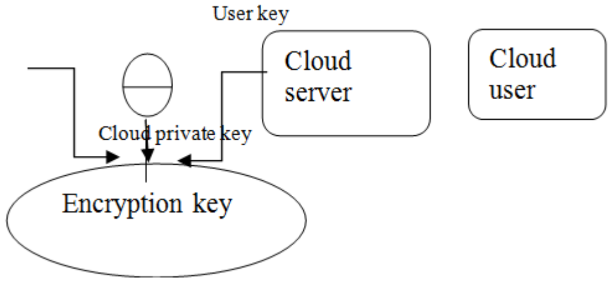

Fig. 1: Access Control

4.2. Remote integrity control

Storing data on cloud is becoming a common practice, user store his data on the cloud without maintaining a local copy of data, so maintaining the integrity of remote data is becoming challenging factor. Every time when user want to check the integrity of data, downloading of complete data on local machine is consuming a lot of communication bandwidth. Earlier proposed approach was checking the integrity of memory data but not having the explicit knowledge of full data functional data was meaningless approach. Blum explored the mechanism of checking memory management properly. Later on find out the concept of third party which keeps some information about data for auditing and verification. but all the above schemes are not applicable to remote data integrity. The limitations of the algorithm lies in the complexity of server computations .computation cost is increasing linearly as the number of users.

Problems specified in the earlier phase can be removed by privacy preserving RIC protocol. Main focus of the protocol is public verifiability of user without disclosing any information. Verifier can have the public key of the data owner. Exceptionally good when the size of data is very much large and number of user are increasing proportionally

5. Comparison of running algorithm with the proposed scheme

The figure 1 and 2 shows the comparison between the existing algorithm and proposed algorithm as given below:

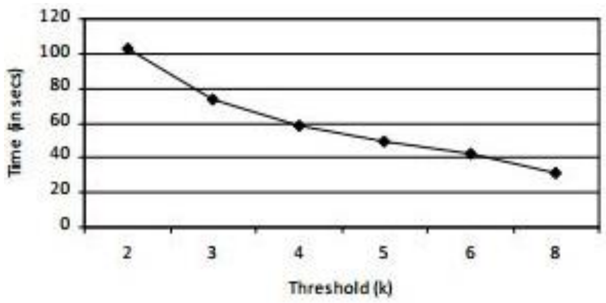

Fig. 2: Computation Time.

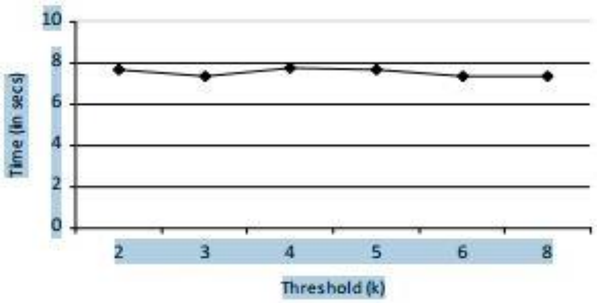

Fig. 3: Computation Time Gain.

It has been compared with following factors as given below:

Public verifiability: - data integrity auditing is a frequent task; during the auditing/ integrity checking information about the content of data file of the client should not be known to verifier.

Protocol execution: during data transmission, different protocols are used for the execution of data transmission successfully. It should not give the information about type of data travelling on the path

Sampling:-It's very difficult to check the integrity of larger files at once as well as its atime consuming process. To avoid this, block or samples of complete data is generated and no leakage of information will be produced during sampling.

Storage cost:- RIC algorithms generates a tag value after applying the computation . That tag value is stored for future auditing so with number of updated and user the size of log file will be increased and cost of the storage will also be increased.

Communication cost: - After performing the auditing, if data is found altered then notification message will flow from server to client via third party. So every time, communication cost is added with changes done.

6. Conclusion

Proposed RIC algorithm will achieve the public verifiability without disclosing of any client data. Reduce the leakage of information in time of sampling. When the size of data is increasing with number of users, that proposed scheme performance degrades.

5.1. Threat identified

Third party is sending a challenge to the cloud server for verification of data. If the cloud is unable to run challenge signifies that there is a data loss. Cloud server want to convince the verifier that there is no loss of data partially a file is missing. Sometimes server reclaims the storage occupied by rarely used data & files. Proposed technique can verify the client data & having the privilege to retrieve the data at any time.

5.2. Complexity analysis

From three different perspectives; storage, communication cost, overall transmission cost. With the proposed technique storage cost is efficient, each user maintains his long lived secret key for communication. Computational cost is also acceptable for a regular party extra overhead cost goes with key confirmation. Secret m sharing schemes permits the party to efficiently recover the key themselves.

References

[1] G. Cheng, H. Jin, "Building Dynamic Integrity Protection for Multiple Independent Authorities in virtualization-based Infrastructure ", in proceeding of IEEE 10th ACM International Conference on Grid Computing" pp 113-119, 2009.

[2] Z. lianhong "Secuirty Storage in the Cloud Computing: A RSA-based Assumption DataIntegrity Check without Original Data" in proceeding of IEEE International Conference on Educational and Information Technology" pp 143-148, 2010.

[3] R. Neisse, D. Holling, "Implementing Trust in Cloud Infrastructures", in proceeding of 11th International Symposium on Cluster, Cloud and Grid Computing, pp 524-533, june 2011.

[4] S. Ni-Na, Z. Hai-Yan "On providing integrity for dynamic data based on the third-party verifier in cloud computing", in proceeding of IEEE international Conference on Instrumentation, Measurement, Computer, Communication and Control, pp 145-150, 2011.

[5] F. Barsoum, M. Hasan, "Integrity Verification of Multiple Data Copies over Untrusted Cloud Servers" in proceeding of 12th International Symposium on Cluster, Cloud and Grid Computing, pp 829-840, dec, 2012 .

[6] T. Thao Phuong, K. Omote "Improvement of Multi-user Searchable Encrypted Data Scheme" in proceeding of 7th International Conference for Internet Technology and Secured Transactions, pp 263-266, 2014.

[7] S. Shen, "An Effective Integrity Check Scheme for Secure Erasure Code-Based Storage Systems",inIeee Transactions On Reliability, 64(3), pp 840-851, 2015.

[8] Z. Zhu, R. Jiang, " Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud", IEEE Transactions On Parallel And Distributed Systems, 27(1), pp 40-51, 2016

[9] C. Wang, K. Ren, "Secure Optimization Computation Outsourcing in Cloud Computing: A Case Studyof Linear Programming" IEEE Transactions on Computers, 65(1), Pp 216-227, 2016.

[10] P. Hu, C. Sung, "Optimal Coding and Allocation for Perfect Secrecy" in IEEE Transactions On Information Forensics & Security, 11(2), pp 388-399, 2016.

[11] Shan, D., Cao, G.H., Dong, H.: LGMS-FOA: An Improved Fruit Fly Optimization Algorithm for Solving Optimization Problems. Journal of Mathematical Problems in Engineering. pp 1-9 (2013)

[12] Zhang, P., Wang, L.: Grouped Fruit Fly Optimization Algorithm for the No-Wait Lot Streaming Flow Shop Scheduling. In: International Conference on intelligent Computing. pp 664-674, Springer (2014)

[13] Abdullahi, M., Ngadi, M.A.: Hybrid Symbiotic Organisms Search Optimization Algorithm for Scheduling of Tasks on Cloud Computing Environment. PloS One. 11, pp 1-29 (2016)

[14] Wu, L., Zuo, C., Zhang, H.: A Cloud Model Based Fruit Fly Optimization Algorithm. Knowledge-based Systems. 89, pp 603-617 (2015)

[15] Dai, H., Zhao, G., Lu, and J.: Comment and Improvement on New Fruit Fly Optimization Algorithm: Taking the Financial Distress Model as an Example. Knowledge-based Systems. 59, pp 159-160 (2014)

[16] Pan, Q.K., Sang, H.Y., Duan, J.H., Gao, L.: An Improved Fruit.