An Approach for Distributed Data Possession in Multi-Cloud using SelCSP

Shaikh Rahil Ahemad[1], **Lalit Dole**[2]

[1]Department of CSE, G.H. Raisoni COE, Nagpur

[2]Assistant Professor, Department of CSE, G.H. Raisoni COE, Nagpur

Abstract: ***The important concept in the cloud storage is checking integrity in the remote data. It can provide the user with verification of the outsourced user files without downloading the complete data. There are some situations in which user needs their files to be kept on multiple cloud servers, so as to provide security and better prediction of cloud servers. The ID-DPDP (identity-based distributed provable data possession) enhance model for checking remote data integrity in multiple clouds. The proposed model can provide various levels of verifications. The ECC (Elliptic Curve Cryptography) algorithm is used for generating keys and symmetric encryption algorithm for encryption of data and the corrupted files concept is introduced in our system also for enhancing the security of the system use the SelCSP (Select Cloud Service Provider) is done. Which will check the authenticity of cloud service provider will also collect the user feedbacks on various cloud service providers weather the cloud service provider is malicious or trustworthy.***

Keywords: Cloud computing, ID-DPDP, Select Cloud Service Provider, symmetric encryption algorithm, Elliptic Curve Cryptography

1. Introduction

The important element in today‟s computing environment is cloud. As it has larger availability in spite of any geographical barriers. User can access their data any time anywhere just user need an internet connection and a computer system. As the user demands are increasing to use the cloud storage there are many 3rd party cloud service providers emerging out into this system. The owner‟s store their data into the cloud system there need to be some mechanism so as to provide security to owner‟s data to maintain its confidentiality, integrity and availability at the right time when they need it.

The users are using the cloud storage as the number of copies of data stored on the cloud increases in the same way the price also increases [1], the organizations are currently storing their data onto the cloud servers. The data stored into the cloud server may be misused if the cloud server is malicious so as to avoid this the agreement between the user and the provider is signed so that the user data will be kept safe and untouched by any third party. [3], The proposed PDP model was having a major drawback of certificate management so as to overcome this current system of ID-DPDP provides various level of verifications to the clients also gives a verification of data through the verifier the security of the system increases. [8]

The current system the upload of owner‟s data into the cloud system so as to protect the owner‟s data to be misused by any un authorized access we are using elliptic curve cryptography for key generation and symmetric algorithm to encrypt the data. The Elliptic Curve Cryptography (ECC) was found in 1985 by Victor Miller (IBM) and Neil Koblitz (University of Washington) as an option component for executing open key cryptography. ECC depends on discrete logarithms that is substantially more hard to challenge at proportionate key lengths. [17], The major challenge arrive before user is of trust. In today‟s environment, the level of trust is at a peak level [7], Presently there is no product structure which can naturally record cloud suppliers in view of their needs. The need to propose a structure and a component, which measure the quality and organize Cloud administrations. Such structure can have huge effect and will make sound rivalry among Cloud suppliers to fulfil their Service Level Agreement (SLA) and enhance their Quality of Services (QOS). [12], we can use a system to provide a greater level of data security as follows.

In the ID-DPDP protocol we use the concept of blog tag pairing. through this model the owner of data are able to provide different verification stages. In this model the PKG Private Key Generator is used to develop the encryption key by using the ECC algorithm There may be various levels of keys generated i.e. user and owner key through which different access rights of both are determined. The verifier is used to monitor the data from one end to another the total track of data is kept by verifier it also monitors when a particular user accessed those files into multiple cloud servers. The system is encrypted by using Symmetric encryption algorithm through the cloud server encryption is done the encrypted data is stored on the multiple cloud server. Data duplication is the concept which the storage space of the cloud servers get utilized and data is being duplicated in a very high level the user are not able to verify their data and corrupted data upload checking is used so that corrupted files cannot be uploaded.

2. Related Work

The earlier system the PDP has a drawback of i.e. insert operation was not supported and the ID DPDP protocol the selection of cloud service provider weather malicious or trustworthy. If the cloud service provider is malicious the user will come to know about it by SelCSP which will give the users a detail view about the service provider

A.F Barsoum, et al. [1] The number of copies of data stored

Licensed Under Creative Commons Attribution CC BY

on the cloud increases in the same way the price also increases. The access right is developed so that the particular user can have their own access Rights. There may be access rights through which the data will be viewed to user and as well as administrator. The corrupted copies of data will be checked before uploading to the cloud server and also duplication of data will be checked.

Ateviese, et al. [2] The PDP model i.e. provable data possession generally allows a client to store the data on the 3rd party cloud vendors. They provide user to verify their data without downloading the data form the cloud storage also the whole activity is being tracked by a verification system i.e. the verifier which allows the different types of user‟s different levels of data access.

M.A Hasan, et al. [3] The users store large amount of data into the cloud server and charges for the stored data into the server. But the data stored into the cloud server may be misused if the cloud server is malicious so as to avoid this the agreement between the user and the provider is signed so that the user data will be kept safe and untouched by any third party. The security of the user is increased in a manner such that the user will get access right from the verifier i.e. the owner of the file and then only he can make changes into the files.

S.K Habib, et al. [4] The Service layer agreement is not enough to provide the detailed security from the data to be corrupted and been fallen into the wrong hands so as to increase the security of the system the trust management is used to detect the trustworthy service providers and have a secured access to the important data stored into the system this mechanism deals with the cloud service provider for providing the user a freedom to keep the data on the cloud service provider.

Nirnay Ghosh, et al. [5] The transparency in the data storage is an important concept in multicloud storage. Service level agreement are used between the user and the cloud service provider to maintain the user data transparency the user trust is gained by direct interaction and selection of the best suited provider for the user. Quality of service is very important concept into the cloud service provider they provide high quality services.

Cong Wang, et al. [6] The users now a day‟s store data into the cloud storage huge amount of data which was stored into local system gets stored so that users can access their data anytime anywhere. To increase the user security and privacy TPA (Third Party Auditor) is used to audit and verify the data is stored into the cloud storage in this system multiple cloud storages can be audited using the TPA. It is also more secure and effective in nature.

Khaled M Khan, et al. [7] The cloud technology gives a good range of features offering a great work into enterprises the best thing is the scalable Technology which is very useful in any enterprises but as we know all good things comes with some challenges. The major challenge arrive before user is of trust. In today‟s environment, the level of trust is at a peak level. The enterprises trust the cloud server‟s potential they generally question its ability.

Huaqun Wang [8] The given ID-DPDP provides various level of verifications to the clients also gives a verification of data through the verifier the security of the system increases as it is based on CDH (Computational Deffie Helmen) the previous concept of certificate management has been removed from the current system due to which the durability of this system increases as compared to other systems.

H. Takabi, et al. [9] The distributed computing worldview is as yet advancing, however has as of late increased colossal force. In any case, security and protection issues act like the key detour to its quick selection. In this article, the writers introduce security and protection challenges that are exacerbated by the one of a kind parts of mists and show how they're identified with different conveyance and sending models. They talk about different ways to deal with address these difficulties, existing arrangements, and future work expected to give a reliable distributed computing environment.

G. Schryen, et al. [10] This system introduces a novel trust estimation strategy for conveyed frameworks, and makes utilization of propositional rationale and likelihood hypothesis. The aftereffects of the subjective part incorporate the detail of a formal trust dialect and the representation of its terms by method for propositional rationale recipes. In light of these recipes, the quantitative part returns trust measurements for the assurance of dependability with which given appropriated frameworks are expected to satisfy a specific security necessity.

T. Noor, et al. [11] The propose the "Trust as a Service" (TaaS) structure to enhance courses on trust administration in cloud situations. Specifically, represent a versatile believability demonstrate that recognizes sound trust criticisms also, noxious criticisms by considering cloud administration buyers' capacity also, dominant part accord of their criticisms. The methodologies have been approved by the model framework and exploratory outcomes.

S. K. Garg, et al. [12] With the development of Cloud Computing, increasingly and more organizations are putting forth unique cloud administrations. From the client's perspective, it is constantly hard to choose whose administrations they ought to utilize, in light of clients' necessities. Presently there is no product structure which can naturally record cloud suppliers in view of their needs. The need to propose a structure and a component, which measure the quality and organize Cloud administrations. Such structure can have huge effect and will make sound rivalry among Cloud suppliers to fulfill their Service Level Agreement (SLA) and enhance their Quality of Services (QoS).

I. Brandic, et al. [13] To begin with, in this system we use mapping low-level asset measurements to SLA parameters essential for the distinguishing proof of disappointment sources. Second, we devise a layered Cloud engineering for the base up proliferation of disappointments to the layer, which can respond to detected SLA infringement dangers.

Licensed Under Creative Commons Attribution CC BY

Besides, we introduce a correspondence display for the proliferation of SLA infringement dangers to the fitting layer of the Cloud framework, which incorporates arbitrators, intermediaries, and programmed benefit deployer.

F. Sebe, et al. [14] Checking information ownership in organized data frameworks, for example, those identified with basic foundations involves vital significance. Remote information ownership checking conventions allow watching that a remote server can get to an uncorrupted document in a manner that the verifier does not have to know heretofore the whole record that is being checked. Tragically, current conventions just permit a predetermined number of progressive confirmations on the other hand are illogical from the computational perspective. we display another remote information ownership checking convention such that 1) it permits a boundless number of document trustworthiness checks and 2) its most extreme running time can be picked at set-up time.

Y. Zhu, et al. [15] The system deals with the migration of data and service stability in the PDP and how to increase the efficiency of the corporate clients and maintaining them. The performance of the cloud system by using the corporative PDP is increased into a significant manner. The system also has lowered the overheads generated by communications into the systems

D. Boneh, et al. [16] We propose a completely practical character based encryption plot (IBE). The plan has picked cipher text security in the arbitrary prophet display accepting a variation of the computational Diffie Hellman issue. Our framework depends on bilinear maps between gatherings. The Weil blending on elliptic bends is a case of such a guide. We give exact definitions for secure personality based encryption plans and give a few applications for such frameworks

C.Research [17] Elliptic Curve Cryptography (ECC) was found in 1985 by Victor Miller (IBM) and Neil Koblitz (University of Washington) as an option component for executing open key cryptography. Open key calculations make an instrument for sharing keys among vast quantities of members or substances in an intricate data framework. Not at all like other mainstream calculations, for example, RSA, ECC depends on discrete logarithms that is substantially more hard to challenge at proportionate key lengths.

3. Proposed Work

In the ID-DPDP protocol we are using the concept of blog tag pairing. through this model the owners are able to provide different verification stages. In this model the symmetric key algorithm is used to encrypt and decrypt the data by using the keys provided by ECC. ECC (Elliptic Curve Cryptography) ECC is a deviated cryptography calculation which includes some abnormal state estimation utilizing numerical bends to scramble and unscramble information. It is like RSA as it's unbalanced yet it utilizes a little length key when contrasted with RSA.

The verifier is used to monitor the data from one end to another the total track of data is kept by verifier it also monitors when a particular user/owner accessed those files into multiple cloud servers. the encrypted data is stored on the multiple cloud server. Data duplication is the concept which the storage space of the cloud servers get utilized and data is being duplicated in a very high level the user are not able to verify whether their data is duplicated or corrupted data. The checking of file is done so that corrupted files cannot be uploaded.

The owner stores their data on 3rd party cloud server so user is not able to determine whether the cloud server is trustworthy. The owner data may be unsecured so to increase the security of users the owner"s data the concept of select cloud service provider is used the registered users will be able to give their feedback on the 3rd party cloud service provider on the basis of feedback and reviews the owner can decide the trustworthiness of the service provider and can save their confidential data on the multiple cloud server. As the important owner"s data is stored on the 3rd party cloud server if the cloud server is trustworthy the data will be secure but if the cloud server is malicious it may miss use the owner"s data so the use of SelCSP for detecting malicious cloud server.

The steps are as follows

- The owner uploads the data to a multiple cloud server.
- After which the data is encrypted through symmetric encryption algorithm and keys will be generated by ECC Elliptic curve cryptography.

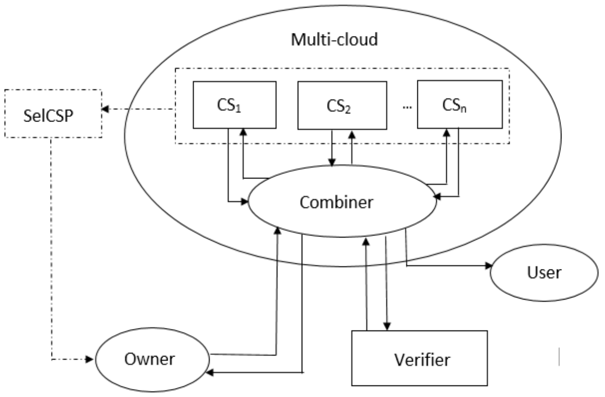

Figure 1: Architecture of system

- The Blocks of data are uploaded into multi-cloud through combiner before uploading the data it is checked for duplication and corruption of data.
- The various activities will be monitored by verifier and also various permissions can be provided to owner and user.
- Now SelCSP service provider will provide API for user and owner to register themselves and give their review on cloud the services provider.

4. Conclusion and Future Work

The use of ECC for the key generation and the symmetric algorithm for encryption of data we are using the ID-DPDP

Licensed Under Creative Commons Attribution CC BY

model into the system and also use of select cloud service provider had added an extra level of security to the system. The use of corrupted data detection and redundancy removal has made system more efficient for the use into the organizations for data security. Which will be able to remove corrupted data also and redundant files which are of no use by the system owners. The system will also be able to detect the trustworthy cloud service provider on the basis of reviews given by the other registered users and owners. The future work may consist of increasing more security in system by improving SelCSP.

References

[1] A.F. Barsoum and M.A. Hasan, „„Provable possession and replication of data over cloud servers,‟‟ Centre Appl. Cryptogr. Res., Univ. Waterloo, Waterloo, ON, Canada, Rep. 2010/32. [Online]. Available: http://www.cacr.math.uwaterloo.ca/ techreports/2010/cacr2010-32.pdf

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, „„Provable Data Possession at Untrusted Stores,‟‟ in Proc. CCS, 2007, pp. 598-609. K. Elissa, "Title of paper if known," unpublished.

[3] A.F. Barsoum and M.A. Hasan, „„On verifying dynamic multiple data copies over cloud servers,‟‟ Int. Assoc. Cryptol. Res., New York, NY, USA, IACR eprint Rep. 447, 2011. [Online]. Available: http://eprint.iacr.org/2011/447.pdf.

[4] S. K. Habib, S. Ries, and M. Muhlhauser, "Towards a trust management system for cloud computing," in Proc. IEEE 10th Int. Conf. Trust, Secur. Privacy Comput. Commun., 2011, pp. 933–939

[5] Nirnay Ghosh, Soumya K. Ghosh, and Sajal K. Das, "SelCSP: A Framework to Facilitate Selection of Cloud Service Providers" IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 3, NO. 1, JANUARY-MARCH 2015

[6] C. Wang, Q. Wang, K. Ren, and W. Lou, „„Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,‟‟ in Proc. IEEE INFOCOM, Mar. 2010.

[7] K. M. Khan and Q. Malluhi, "Establishing trust in cloud computing," IT Prof., vol. 12, no. 5, pp. 20–27, Oct. 2010.

[8] Huaqun Wang "Identity-Based Distributed Provable Data" IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 8, NO. 2, MARCH-APRIL 2015.

[9] H. Takabi, J. B. D. Joshi, and G. J. Ahn, "Security and privacy challenges in cloud computing environments," IEEE Secur. Privacy, vol. 8, no. 6, pp. 24–31, Nov./Dec. 2010.

[10] G. Schryen, M. Volkamer, S. Ries, and S. M. Habib, "A formal approach towards measuring trust in distributed systems," in Proc. ACM Symp. Appl. Comput., 2011, pp. 1739–1745.

[11] T. Noor and Q. Sheng, "Trust as a service: A framework for trust management in cloud environments," in Proc. 12th Int. Conf. Web Inf. Syst. Eng., 2011, pp. 314–321.

[12] S. K. Garg, S. Versteeg, and R. Buyya, "A framework for ranking of cloud computing services," Future Gener. Comput. Syst., vol. 29, no. 4, pp. 1012–1023, 2013.

[13] I. Brandic, V. C. Emeakaroha, M. Maurer, S. Dustdar, S. Acs, A. Kertesz, and G. Kecskemeti, "LAYSI-A layered approach for SLAviolation propagation in self-manageable cloud infrastructures," in Proc. 34th IEEE Annu. Comput. Softw. Appl. Conf. Workshops, Jul. 2010, pp. 365–370

[14] F. Sebe ´, J. Domingo-Ferrer, A. Martı ´nez-Balleste ´, Y. Deswarte, and J. Quisquater, „„Efficient Remote Data Integrity Checking in Critical Information Infrastructures,‟‟ IEEE Trans. Knowl. Data Eng., vol. 20, no. 8, pp. 1034-1038, Aug. 2008

[15] Y. Zhu, H. Hu, G.J. Ahn, and M. Yu, „„Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage,‟‟ IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 12, pp. 2231-2244, Dec. 2012

[16] D. Boneh and M. Franklin, „„Identity-Based Encryption from the Weil Pairing,‟‟ in Proc. CRYPTO, vol. 2139, LNCS, 2001, pp. 213-229.

[17] C.Research „„Elliptic Curve cryptography.‟‟[Online]. Available: https://www.certicom.com/content/certicom/en/ecc.html

Author Profile

Shaikh Rahil Ahemad is a M. Tech student from G.H Raisoni College of Engineering, Nagpur (An Autonomous Institute Affiliated to RTM Nagpur) he has completed his Bachelor of Engineering from Dr. Baba Saheb Ambedkar Marathwada University in the year 2014. His area of interest includes cloud computing, data mining, and has greater interest in programing languages

Lalit Dole is an Assistant Professor at the G.H Raisoni College of Engineering, Nagpur (An Autonomous Institute Affiliated to RTM Nagpur) he has completed a Post graduate degree in Information Technology at the Devi Ahilya University, Indore in the year 2011. His area of interest includes Communication, Database management system, Operating systems, Mobile operating system, Data mining and Data warehouse

Licensed Under Creative Commons Attribution CC BY