An Enhanced Data Storage Technique on Cloud Computing

Kamlesh Sharma, Nidhi Garg

Abstract*: Exercising a collection of similar numerous easy to get sources and resources over the internet is termed as Cloud Computing A Cloud storage system is basically a storage system over a large scale that consist of many independent storage servers. During recent years a huge changes and adoption is seen in cloud computing so security has become one of the major concerns in it. As Cloud computing works on third party system so security concern is there not only for customers but also for service providers. In this paper we have discussed about Cryptography i.e., encrypting messages into certain forms, it's algorithms including symmetric and asymmetric algorithm and hashing, its architecture, and advantages of cryptography.

Keywords*: Cloud storage system, Cryptography, Robustness, Hashing.

I. INTRODUCTION

Cloud computing has shown a drastic change in the way information and data is stored and applications executed. Instead of reading programs and data on a single desktop PC, all portable equipment is stored in the "cloud," a deep collection of computers and servers entered over the Internet. Cloud computing allows us to capture all our applications and documents from any place in the world, regardless of desk restrictions and facilitating the contribution of group members in various areas. Modifications in network technology and an increase in the need for computing resources have led many organizations to put aside their storage and computing needs. Data robustness is a major requirement for storage systems. There have been many proposals of storing data over storage servers [4][7][17][19]

There is a large scope of improvement in this field of research.[5].We can use cryptography in numerous places in order security in cloud. For example, Cryptography can be used for maintaining cloud data access control, cloud data trust management, verifiable computing, cloud data authorization and authentication and secure data storage.[1][12]

This new computing model is generally known as cloud computing and includes several types of services such as: infrastructure as a service (IaaS), where a client uses the resources of a service provider, storage or network infrastructure; platform as a service (PaaS), where a client takes advantage of the provider's resources to execute customized applications; and finally software as a service (SaaS), where customers use software that runs on the provider's infrastructure. Infrastructures in the cloud can also be called private or public. In a private cloud, the architecture is managed and owned by the client and detected in the postulate. In a non-private cloud, the structure is taken and controlled by the cloud service provider and detected in the postulate (that is, in the control region of the service provider) This can also be referred as user data is beyond any control and can't be used by unfair parties.

The threshold proxy re-encryption scheme supports encoding, forwarding, and partial decryption operations in a distributed way [14][15].

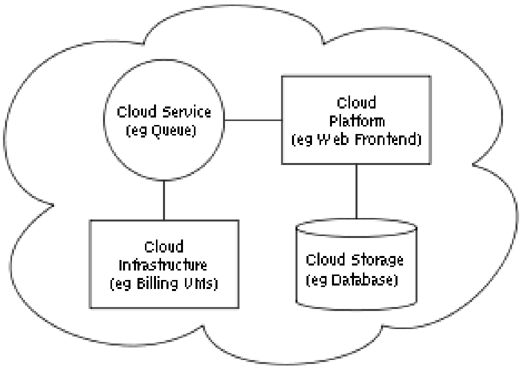

Fig 1: Cloud Computing Structure

II. SECURITY SERVICES

In order to handle the previous agreement and to enrich the beginning of cloud storage, we requested the preparation of a virtual nonpublic storage facility based on recently created cryptographic methods [13]. This service should try to get the best of both parties by giving the security of a nonpublic cloud and functionality and money excluding a non-private cloud.

A. Security: The cloud space provider should exclude any information of customer data.

B. *Honesty:* Any not authorized changes of customer data by the cloud space provider should be seen by the user as well as hold the main benefits of a non-private space service.

C. Availability: Customer data should be affordable from any device and at every time.

Manuscript received on 11 May 2021 | Revised Manuscript received on 29 May 2021 | Manuscript Accepted on 15 June 2021 | Manuscript published on 30 June 2021.

* Correspondence Author

Dr. Kamlesh Sharma*, Associate Professor, Department of Computer Science & Engineering, Manav Rachna International Institute of Research & Studies, Faridabad, India. Email: kamlesh.fet@mriu.edu.in

Nidhi Garg, Assistant Professor, Department of Computer Science & Engineering, Manav Rachna International Institute of Research & Studies, Faridabad, India. Email: nidhigarg.fet@mriu.edu.in

© The Authors. Published by Lattice Science Publication (LSP). This is an open access article under the CC-BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

Retrieval Number:100.1/ijdcn.B5007021221
DOI:10.54105/ijdcn.B5007.061321
Journal Website: www.ijdcn.latticescipub.com

Published By:
Lattice Science Publication (LSP)
© Copyright: All rights reserved.

D. Responsibility: Customer data is calculable hold back.
E. Productive Retrieval: Data get back times are similar to a non-private cloud storage service.
F. ***Data Transfer:*** Customers should be able to share the data with fair parties. An important fair side of a cryptographic storage service is security properties mentioned above are attained based on cryptographic guarantees as opposed to legal and access control mechanisms. Given section provides a general survey of cloud computing.

III. CRYPTOGRAPGY

Cryptography is just a simple technique in which data is converted into certain code and generates some key which is then used to convert that code into normal form again so this simple method is used to make our cloud data to be more secured. These algorithms are Symmetric-key algorithms and Hashing.

4.1 Symmetric Key Algorithms

In this only single key is comes into play for converting the data into one form and then converting back into normal form. By this way user gets assurance of its security in the storage system. Since only single key is used in this algorithm so it is very simple and mostly use algorithm. In this size of key doesn’t vary known as block cipher, in which it varies it is known as Stream cipher.

4.2 Asymmetric Key Algorithms

It is just opposite to the symmetric key system, In this not a single key is used for converting the data into one form and then back to the same, multiple keys are used for that processes, it is little bit complex but more secure than others due to different keys in the processes.

4.3 Hashing

In this hash code is used for converting the data into one form and then to another. Many hash codes can be generated using binary system or other system. You can also generate your own hash code but basically predefined codes are used by general public.

IV. ARCHITECTURE OF A CRYPTOGRAPHY TECHNIQUE

The architecture is basically a framework or structure which has three parts or layers [5]

- DATA PROCESSOR (DP): As its name suggest it is used for processing the data at a time when data is being sent to the cloud.
- DATA VERIFIER (DV): It is basically used by the user to check whether its data is secure or not.
- TOKEN GENERATOR (TG): It is used to produce the tokens which are further used for retrieving the data from the cloud.

4.1 A Consumer Structure: This architecture is very simple. To define this architecture [16], we will consider some examples. Suppose there are three persons you can take any name according to your preferences. Alice (any person), who uses cloud for storing the data. Bob (any other person) is a friend of Alice who wants some data from Alice for any use. For this both download all the three components of the Cryptography. In starting Alice generates a cryptographic key which is assumed as a master key and this key is very unique and which is kept hidden even from the cloud service provider. Whenever Alice wants to add some data on his cloud DP is called. DP does not directly upload the data; it adds some extra data such as time, especial keywords etc. and then data is encrypted by using various cryptographic applications. Alice will call DV whenever he has a doubt for the honesty of service provider to verify its data whether it is safe or not. When Alice wants to use his data that is when he wants to get back his data TG is called which will produce token. This token is then sent to the service provider which gives the required data to the user in encrypted form after that user will decrypt the data using decryption key[6][18].
The sharing of data between Alice and Bob will take place in similar way. Bob will use TG to produce tokens and credentials which will be then sent to the cloud, token is used for obtaining the data whereas credentials will be used for decrypting the data.

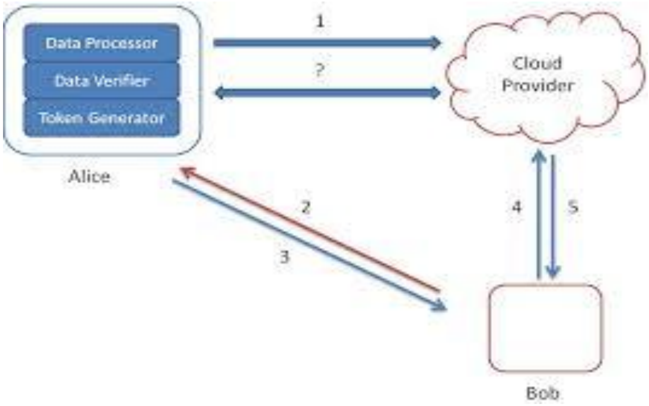

Fig 2: A Consumer Structure

[1]: DP comes into the action when the data is going to sent to the cloud basically it manages the data
[2]: Bob request for keyword from Alice.
[3]: Alice gives token as well as credentials for future references.
[4]: Token is then sent to the cloud provider.
[5]: Cloud than send the encrypted requested data which is then changes into normal form using credentials.
At last DV can be used to check the honesty of the system at any time.

4.2 An Enterprise Structure: We have studied about the consumer structure in which basically a normal people cloud usage is shown and data sharing. In this Enterprise Architecture we will study about how cloud Storage is use in the big enterprises and companies. To explain this we will use different companies names as an examples, let MegaCorp (MC) be the first company who stores it’s data in the cloud, let another company be PartnerCorp (PC) from which MC wants to share its data stored in the cloud. Firstly, MC will use some machine s for generating the master key.

Since Master key is critical for any company, therefore, depending upon situations different machines should be used for generating Master key.

Master key is kept hidden from all even from the service providers. For a normal enterprise DP, DV and TG is used. But for high budget companies many other components can also be used to make the data more secure. [8]

At starting both MC and PC receives a credential generator which will generate the credentials for both. Suppose there is an employee in MC which wants to upload some data in the cloud then it will send the data to the devoted computer with some decryption numbers.[9] These decryption numbers will help in selecting the data which is needed to select the particular type of credentials. Whenever the integrity of data is needed to be verified than DV is used Master key is the one which will decide whether the integrity is available or not.

Now if any PC employee wants to access the data from MC cloud than it will send the keyword to the devoted computer which in return the token which will be then sent to the cloud [10]. The service provider will verify the data and then send the encrypted file to the PC employee. In view of the fact that the file is still in the encrypted form, the credentials will be used for decrypting the file [11].

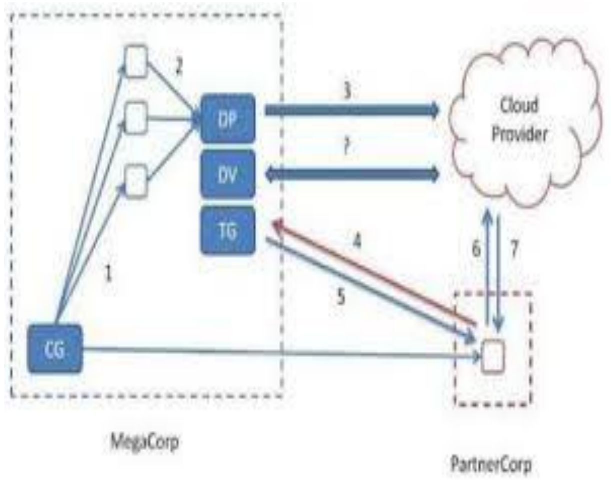

Fig 3 (1): An Enterprise Structure

Figure 3(1): [1] It shows some credentials is being produced to both MC as well as PC people and sent to them.

[2] MC will send the data to the devoted machine.

[3] Data is sent to the cloud after data is processed before sending it to the cloud using DV.

[4] PC worker will send some keyword to the MC devoted machine.

[5] The devoted machine will give back the token.

[6] Token is then sent to the cloud

[7] The cloud provider then utilize the token to return the encrypted message to the PC worker which will than decrypt it using credentials

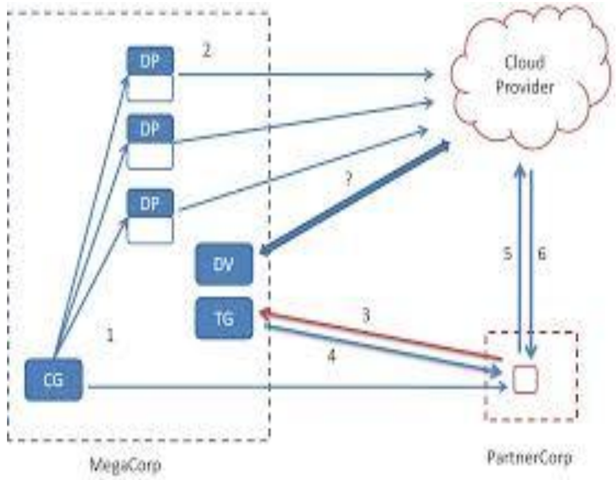

Fig 3 (2): An Enterprise Structure

Figure 3(2): It is just same as the above figure but some other components are added in DP to make the data more secure. This structure is used by the companies having high budgets.

V. BENEFITS OF A CRYPTOGRAPHY IN CLOUD COMPUTING SECURITY

1. **Security Satisfaction:** In Cryptography the data is processed in the front of user by DP. By using this way users have satisfaction that their security is maintained by the service providers using cryptography.
2. **Geographic constraints:** Since the data is put in the encrypted form. So, the rules which defines which type of data should be stored in the cloud has no constraints on the user and hence helping them.
3. **User is the head**: Since the data is stored in the encrypted form so everyone who wants to access the data has to produce key from the users which will help the user to sustain its preference in the system.

VI. PROPOSED SYSTEM BY S. POONKODI, V.KAVITHA, AND K.SURESH. [2]

document addresses many problems of passing data to other users from storage servers directly under the command of the real owner of the data. We look at the system model, which have a varied storage servers and key servers. Because the storage of cryptographic keys in a one device can be risky, a user distributes their cryptographic keys to the key servers that must perform cryptographic functions for the user. These key in networks are securely protected by security process. To adjust the distributed structure of the systems, the servers must perform all the operations independently. With this reflection, we state a new point assignee encryption scheme & summed it with a secure decentralized code to form a secure varied storage system. The encryption plan supports encryption over encrypted communication and forwarding over encrypted and encrypted communication. By tightly integrating encryption, encryption and routing, the storage system meets the minimum requirements for data robustness, data privacy and routing. Achieving summation in account of a varied structure is demanding.

Our method fulfill the requirement that storage servers uniquely perform encryption and decryption independently, and key servers manages little decryption.

VII. RESULT AND DISCUSSION CONSEQUENCE AND FUTURE OF CLOUD COMPUTING

Cloud computing is becoming larger as something new, and this is indeed the new incline. Many companies' that are generally large companies are walking towards the cloud, but they are falling behind due to various security issues. Cloud security is the last concept that will overcome the disadvantages of the adoption of the cloud by large multinationals, associates. There are many security algorithms that can be implemented in the cloud. Cloud computing, however, requires security algorithms that allow a linear search of deciphered data that guarantees the security of the data.

There are great improvements in particular area of examination. We have to usage cryptography in multiple locations to guarantee security on the cloud. For example, cryptography is used to manage the control of access to data on the cloud, administer trust in the cloud, checkable computing, authorize and authenticate data in the cloud and secure data storage. In addition to all this, lattice-based cryptography and ID-based cryptography are the two most important factors that guarantee the security of data in the cloud in today's world. There is still a lot of research in this area..

REFERENCES

1. Rishav Chatterjee, Sharmistha Roy, "Cryptography in Cloud Computing: A Basic Approach to Ensure Security in Cloud", IJESC, Vol 7, Issue No. 5, Pg. 11818-11821.
2. S.Poonkodi, V.Kavitha, K.Suresh, "Providing a Secure Data Forwarding In Cloud Storage System Using Threshold Proxy Re-Encryption Scheme", IJETAE, International Conference on Information Systems and Computing (ICISC-2013), INDIA. Pg-468-472, (ISSN 2250-2459 (Online).
3. SECURE CLOUD STORAGE Mahima Joshi, Yudhveer Singh Moudgil
4. P. Druschel and A. Rowstron, "PAST: A Large-Scale, Persistent Peer-to-Peer Storage Utility," Proc. Eighth Workshop Hot Topics in Operating System (HotOS VIII), pp. 75-80, 2001.
5. Sanjoli Singla, Jasmeet Singh ,"Cloud computing security using encryption technique", IJARCET, vol.2, ISSUE 7.
6. Towards Secure Cloud Storage SeongHan Shin and Kazukuni Kobara
7. Official Arbitration with Secure Cloud Storage Application, Alptekin Ku¨p¸cu¨ Ko¸c University, ˙Istanbul, Turkey
8. G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," ACM Trans. Information and System Security, vol. 9, no. 1, pp. 1-30, 2006. [CrossRef]
9. Bokefode Jayant.D, Ubale Swapnaja A, Pingale Subhash V., Karane Kailash J. , Apate Sulabha S. ,"Developing Secure Cloud Storage System by Applying AES and RSA Cryptography Algorithms with Role bases Access Control Model", International Journal of Computer Applications, Volume 118-No.12, May2015 [CrossRef]
10. THIRD PARTY AUDITING FOR SECURE DATA STORAGE IN CLOUD THROUGH DIGITAL SIGNATURE USING RSA, K.Govinda, V.Gurunathaprasad, H.Sathishkumar
11. A Survey of Various Techniques to Secure Cloud Storage, Satyendra Singh Rawat, Mr. Alpesh Soni
12. J. Shao and Z. Cao, "CCA-Secure Proxy Re-Encryption without Pairings," Proc. 12th Int'l Conf. Practice and Theory in Public Key Cryptography (PKC), pp. 357-376, 2009. [CrossRef]
13. Rashmi Nigoti, Manoj Jhuria, Dr. Shailendra Singh, "A survey of Cryptographic algorithms for cloud computing", International Journal of Emerging Technologies in Computational and Applied Sciences, March 2013, ISSN (online)-2279-0055.
14. R. Bala Chandar, M. S. Kavitha , K. Seenivasan," Aproficient model for high end security in cloud computing", International Journal of Emerging Research in Management &Technology, Vol.5, Issue 10.
15. Karun Handa, Uma Singh," Data Security in Cloud Computing using Encryption and Steganography", International Journal of Computer Science and Mobile Computing", Vol.4 Issue.5, May-2015, pg.786-791
16. Douglas R. Stinson," Cryptography: Theory& Practice",Chapman and Hall Publications.
17. J. Kubiatowicz, D. Bindel, Y. Chen, P. Eaton, D. Geels, R. Gummadi, S. Rhea, H. Weatherspoon, W. Weimer, C. Wells, and B. Zhao, "Oceanstore: An Architecture for Global-Scale Persistent Storage," Proc. Ninth Int'l Conf. Architectural Support for Programming Languages and Operating Systems (ASPLOS), pp. 190- 201, 2000. [CrossRef]
18. Aarti P Pimpalkar, Prof. H.A. Hingoliwala, "A Secure Cloud Storage System with Secure Data Forwarding", International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013 3002, ISSN 2229-5518.
19. Adya, W.J. Bolosky, M. Castro, G. Cermak, R. Chaiken, J.R. Douceur, J. Howell, J.R. Lorch, M. Theimer, and R. Wattenhofer, "Farsite: Federated, Available, and Reliable Storage for an Incompletely Trusted Environment," Proc. Fifth Symp. Operating System Design and Implementation (OSDI), pp. 1-14, 2002. [CrossRef]

AUTHORS PROFILE

Dr. Kamlesh Sharma is currently working as a Associate Professor, MRIIRS, Faridabad, India (more than 15 years teaching experience). MCA, M. Tech from MDU University and Ph. D. in Computer Science and Engineering from Lingaya`s Vidyapeeth, India. is currently Supervising five Ph. D. scholars. She has also supervised and guided research projects of M. Tech, B.Tech and application based projects for different competitions. She is also associated with four Govt. research projects in filed of health recommender system, IOT, Machine Learning, AI and NLP. She has published more than 55 research papers in field of NLP, IOT, Bigdata, Green Computing and Data Miningin reputed Journal (Web of Science, Scopus, UGC, Elsevier) and Conferences (ACM, IEEE). Her research area "Natural Language Processing" is based on innovative idea of reducing the mechanized efforts and adapting the software to Hindi dialect.

She is associated with various professional bodies and renowned journals in varied capacities viz. CSI (Computer Society of India), Member, International Journal of Computer Networks and Applications (IJCNA) as Editoral Board Member, BJIT - BVICAM's International Journal of Information Technology, ISSN 0973 – 5658, Springer Index as Reviewer, International Journal of Computer Science and Information Security (IJCSIS), Google Scholar Index as Reviewer & Editorial board member, International Journal of Science & Engineering Development Research - IJSDR, UGC Approved Journal, Google Scholar Index as Member of referral/ review Management System.

Nidhi Garg, is currently an Assistant Professor in the Faculty of Engineering and Technology, Manav Rachna International Institute of Research & Studies, Faridabad. She received her Master's in Technology - Computer Science and Engineering from Maharishi Dayanand University, Rohtak in year 2012 and has 10+ years of teaching experience. Her current research interest includes Artificial Intelligence, Machine Learning and Image Processing. To add to her credits she has authored and co-authored many journals and conference papers in various computer science domains including Networking, Artificial Intelligence, and Machine Learning. She has also active member of IAENG and reviewer of conferences and journals like ICIMMI, ICCS, CIAIS'21 etc.