IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114178

Survey on Efficient storage management system in Cloud Computing using Encryption Algorithm

Prof. A. B. Bagwan[1], Karan Gupta[2], Sulekha Awale[3], Ankita Jagtap[4], Firdose Inamdar[5]

Professor, Computer Engineering, Siddhant College, Pune, India[1]

Student, Computer Engineering, Siddhant College, Pune, India[2,3,4,5]

Abstract: Now a day's cloud computing is used in many areas like industry, military colleges, healthcare etc. to storing huge amount of data. We can retrieve data from cloud on request of user. To store data on cloud we have to face many issues. To provide the solution to these issues there are n number of ways. In Cloud Users can remotely store their data to cloud & realize the data sharing with other. In Some Common cloud storage system such as the electronic health records system, the cloud file might contain some sensitive information. Encrypting the whole shared file can realize the sensitive information hiding, but will make this shared file unable to be used by others. In cloud computing more Sensitive information hiding in cloud. This is very big problem that remote data integrity auditing scheme that realizes data sharing with sensitive information hiding in this cloud. In our System, our scheme makes the file stored in the cloud able to be shared and used by others on the condition that the sensitive information is hidden, while the remote data integrity auditing is still able to be efficiently executed. Meanwhile, the proposed scheme is based on identity-based cryptography, which simplifies the complicated certificate management.

Keywords: Cloud service provider (CSP), cloud server (CS), Encryption, Decryption, Delay, Integrity.

INTRODUCTION

The process of cryptography encrypts data so that it cannot be decoded. Strictly speaking, there are two types of cryptography: symmetric key and public key. This method makes data unreadable by encoding it with special keys. So only those who have been granted access to the cloud server are able to access the data. All people can see the cipher text data.

Symmetric key cryptography algorithms are AES, DES, 3DES, IDEA, BRA and blowfish. The main issue is delivering the key to receiver into multi user application. These algorithm require low delay for data encode decode but provides low security. Public key cryptography algorithm is RSA and ECC algorithm. Public and private keys are manipulated into public key cryptography algorithms. These algorithms accomplished high level security but increase delay for data encode and decode. Steganography hide the secret data existence into envelope. In this technique existence of data is not visible to all people. Only valid receiver knows about the data existence. Text steganography technique is used to produce high security for data. Secret data of user hide into text cover file. After adding text into text cover file it looks like normal text file. If text file found by illegitimate user than also cannot get sensitive data. If illegitimate user try to recover original data than large amount of time is essential. DES algorithm is used for text encode and decode. Advantage of text steganography technique is providing security to text.

MOTIVATION

- Data sharing with sensitive information hiding.
- New concept generating called identity- based shared data integrity.
- Cloud Data Security.

PROBLEM STATEMENT

- To build and Implement Secure File storage in Cloud Computing using Hybrid Cryptography Algorithm

Proposed System

In Our System proposed an identity-based data integrity auditing scheme for secure cloud storage, which supports data sharing with sensitive information hiding. In our Application user upload the data into cloud with user and researcher when Doctor Share the data with User that file go to Admin and admin convert into Binary format and after that binary format file again convert into Homomorphic encryption and Stored into Block Level.

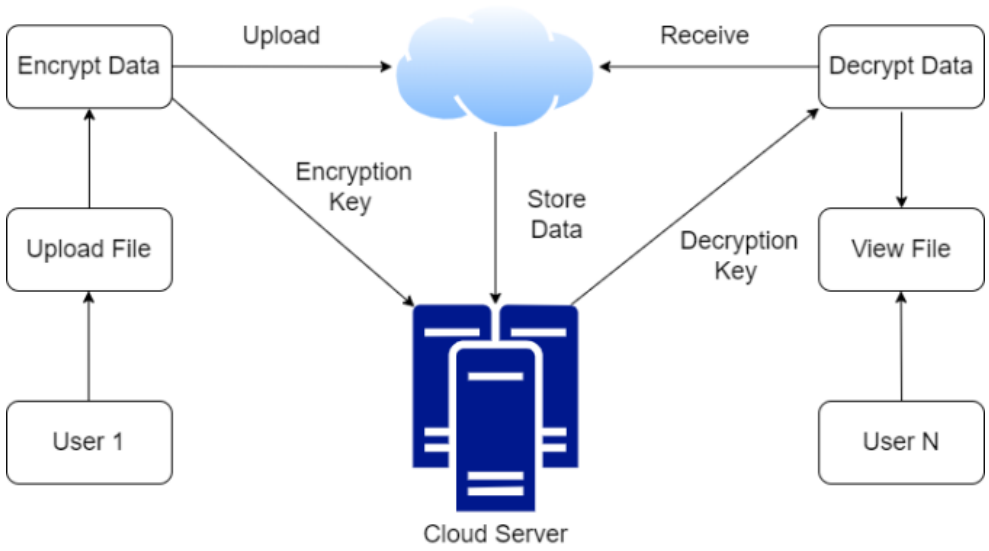
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114178

1. Figure 1. System Architecture



- In our system cloud then sensitive information is hidden with help of hidden data identity Auditing called as the identity based shared data.
- In Our System the file stored in the cloud able to be shared and used by others on the condition that the sensitive information is protected while the remote data integrity auditing is still able to be efficiently executed.
- In Cloud Stored using Block Level concepts.

DATA FLOW DIAGRAMS

1.The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.

2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information ows in the system.

3. Figure 4.1 shows level 0 DFD which shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information ow and the transformations that are applied as data moves from input to output.

ADVANTAGES

- In our system cloud then sensitive information is hidden with help of hidden data identity Auditing called as the identity based shared data.
- In Our System the file stored in the cloud able to be shared and used by others on the condition that the sensitive information is protected while the remote data integrity auditing is still able to be efficiently executed.
- In Cloud Stored using Block Level concepts.

CONCLUSION

In this paper, we proposed an identity-based data integrity auditing scheme for secure cloud storage, which supports data sharing with sensitive information hiding. In our scheme, the file stored in the cloud can be shared and used by others on the condition that the sensitive information of the file is protected. Besides, the remote data integrity auditing is still able to be efficiently executed. The security proof and the experimental analysis demonstrate that the proposed scheme achieves desirable security and efficiency.

DOI: 10.17148/IJARCCE.2022.114178

Applications

- Group sharing applications
- Security Applications
- Searching applications

FUTURE SCOPE

Furthermore, our work motivates interesting open problems as well including designing new scheme without random oracles or proposing a new scheme to support more expressive keyword search.

REFERENCE

1. J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, "An efficient public auditing protocol with novel dynamic structure for cloud data," IEEE Trans. Inf. Forensics Security, vol. 12, no. 10, pp. 2402–2415, Oct. 2017.
2. Y. Li, Y. Yu, G. Min, W. Susilo, J. Ni, and K.-K. R. Choo, "Fuzzy identity-based data integrity auditing for reliable cloud storage systems," IEEE Trans. Depend. Sec. Comput., to be published
3. J. Hur, D. Koo, Y. Shin, and K. Kang, "Secure data deduplication with dynamic ownership management in cloud storage," IEEE Trans. Knowl.Data Eng., vol. 28, no. 11, pp. 3113–3125, Nov. 2016.
4. J. Li, J. Li, D. Xie, and Z. Cai, "Secure auditing and deduplicating data in cloud," IEEE Trans. Comput., vol. 65, no. 8, pp. 2386–2396, Aug. 2016.
5. Y. Zhang, J. Yu, R. Hao, C. Wang, and K. Ren, "Enabling efficient user revocation in identity-based cloud storage auditing for shared big data," IEEE Trans. Depend. Sec. Comput., to be published.
6. H. Wang, D. He, J. Yu, and Z. Wang, "Incentive and unconditionally anonymous identity-based public provable data possession," IEEE Trans. Serv. Compute., to be published.
7. Y. Yu et al., "Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage," IEEE Trans. Inf. Forensics Security, vol. 12, no. 4, pp. 767–778, Apr. 2017.
8. Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki, Sugata Sanyal, "A Survey on Security Issues in Cloud Computing" in ACTA TEHNICA CORVINIENSIS – Bulletin of Engineering Tome VII [2014] Fascicule 4 ISSN: 2067 – 3809.
9. N.N Mosola, M.T Dlamini, J.M Blackledge, J.H.P Eloff, H.S Venter, "Chaos-based Encryption Keys and Neural Key-store for Cloudhosted Data Confidentiality", in Southern Africa Telecommunication Networks and Applications Conference (SATNAC) (2017)
10. Shakeeba S. Khan, Prof.R.R. Tuteja, "Security in Cloud Computing using Cryptographic Algorithms", in International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 1, (2015)
11. AL-Museelem Waleed, Li Chunlin, "User Privacy and Security in Cloud Computing", in International Journal of Security and Its Applications Vol. 10, No. 2 (2016), pp.341-352
12. Dr. Ramalingam Sugumar, K. Raja, "EDSMCCE: Enhanced Data Security Methodology for Cloud Computing Environment" in International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 3 | Issue 3 | ISSN: 2456-3307(2018).
13. Reshma Suryawanshi, Santosh Shelke, "Improving Data Storage Security in Cloud Environment Using Public Auditing and Threshold Cryptography Scheme", in International Conference on Computing Communication Control and Automation (ICCUBEA),(2016).
14. Timothy, Divya Prathana and Ajit Kumar Santra. "A hybrid cryptography algorithm for cloud computing security." 2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS) (2017): 1-5.
15. Khari, Manju, Manoj Kumar and Vaishali. "Secure data transference architecture for cloud computing using cryptography algorithms." 3rd International Conference on Computing for Sustainable Global Development (INDIACom) (2016): 2141-2146.

ACKNOWLEDGMENTS

It gives us great pleasure in presenting the preliminary project report on 'Survey on Efficient storage management system in Cloud Computing using Encryption Algorithm'. We would like to take this opportunity to thank our internal guide **Prof. A. B. Bagwan** and external guide for giving us all the help and guidance we needed. We are really grateful to them for their kind support. Their valuable suggestions were very helpful. We are also grateful to Prof. Sushma Shinde, Head of Computer Engineering Department, Principal **Dr. R. L. Khandagale** whose constant encouragement and motivation inspired us to do our best.SCOE for his indispensable support, suggestions. In the end our special thanks to the college

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022
DOI: 10.17148/IJARCCE.2022.114178

for providing various resources such as laboratory with all needed software platforms, continuous Internet connection, for our Project.

Karan Shriram Gupta
Sulekha Sambhaji Awale
Ankita Milind Jagtap
Firdose Aslam Inamdar