ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

Enhanced Cloud Data Security Using AES Algorithm

Pooja Vilas Barawakar, Bhagyashri Kailas Pasalkar, Pooja Dilip Kshirsagar, Prajakta Rajendra Gaikwad,

Suryavanshi P.M.

BE Students, Department of Computer Engineering, H.S.B.P.V.T's GOI Faculty of Engineering, India

Professor, Department of Computer Engineering, H.S.B.P.V.T's GOI Faculty of Engineering, India

ABSTRACT: Outsourcing data to a third-party administrative control, as is done in cloud computing, it gives rise to security concerns. The data compromise may occur due to attacks by other users and nodes within the cloud. Therefore, high security measures are required to protect data within the cloud. Cloud storage can make data users store and access their files any time, from any where and with any device. To ensure the security of the outsourced data,data owner needs to periodically check data is present and store data in secure format. On the basis of the novel system model and data structure, thescheme helps the users review the integrity of their uploaded or downloaded data at any time by checking uploaded data is present or not.

KEYWORDS: Cloud storage, lightweight cryptography, Symmetric key, Security,

I.INTRODUCTION

I.II.MOTIVATION:-

On web large number of documents are stored in a cloud server, searching against a keyword will result into large number of documents, not related to topic. The formation of scholarly big data is actually the result of the great development of scientific theory research . Scholarly big data include research scholars' personal information, papers, experimental data sets, and results. These data may include information regarding the authors' privacy and social relationships, copyright and right of authorship, and experimental data related to personal privacy, such as medical data . These data are complex and extremely important. If the coauthor of an academic achievement is likely to be tampered with, the author's academic reputation may be affected. If malicious users are using legitimate users' identities to upload data to the system, the researchers' results may be tampered with or replaced.

II. REVIEW OF LITERATURE

1. Algorithms play an important part in solving research problems. Scientific publications host a tremendous amount of such high-quality algorithms developed by professional researchers. In digital libraries, being able to extract and catalog these algorithms would introduce a number of exciting applications including algorithm searching, discovering, and analyzing. We discussed the prototype of AlgorithmSee,a search system for algorithms in large scale scholarly documents, along with providing an illustration of the actual demo system[11].

2.With the rapid growth of digital publishing, harvesting, managing, and analyzing scholarly information have become increasingly challenging. The term Big Scholarly Data is coined for the rapidly growing scholarly data, which contains information including millions of authors, papers, citations, figures, tables, as well as scholarly networks and digital libraries. Nowadays, various scholarly data can be easily accessed and powerful data analysis technologies are being developed, which enable us to look into science itself with a new perspective. In this paper, we examine the background and state of the art of big scholarly data. We first introduce the background of scholarly data management

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

and relevant technologies. Second, we review data analysis methods, such as statistical analysis, social network analysis, and content analysis for dealing with big scholarly data. Finally, we look into representative research issues in this area, including scientific impact evaluation, academic recommendation, and expert finding. For each issue, the background, main challenges, and latest research are covered. These discussions aim to provide a comprehensive review of this emerging area. This survey paper concludes with a discussion of open issues and promising future directions[12].
3. propose a new secure outsourcing algorithm for (variable-exponent, variable-base) exponentiation modulo a prime in the two untrusted program model. Compared with the state-of-the-art algorithm, the proposed algorithm is superior in both efficiency and checkability. Based on this algorithm, we show how to achieve outsource-secure Cramer-Shoup encryptions and Schnorr signatures[13].

4. proposed algorithm is more efficient than the state-of-the-art algorithms. On the other hand, we point out in this paper that the first outsource-secure algorithm for simultaneous modular exponentiations proposed recently is insecure, where the sensitive information can be leaked to the malicious servers. As a result, we propose a new and more efficient algorithm for simultaneous modular exponentiations. We also propose the constructions for outsource-secure Cramer-Shoup encryptions and Schnorr signatures which are also more efficient than the state-of-the-art algorithms[14].

5.Present the system that Formalize the notion of verifiable database with incremental updates (Inc-VDB). Besides, we propose a general Inc-VDB framework by incorporating the
primitive of vector commitment and the encrypt-then-incremental MAC mode of encryption. We also present a concrete Inc-VDB scheme based on the computational Diffie-Hellman (CDH) assumption. Furthermore, we prove that our construction can achieve the
desired security properties[15].

6. Transform of an anonymous identity-based encryption (IBE) scheme to a secure PEKS scheme that, unlike the previous one, guarantees consistency. Finally, we suggest three extensions of the basic notions considered here, namely anonymous hi-erarchical identity-based encryption, public-key encryption with temporary keyword search, and identity-based encryption with keyword search[1].

7. One of our constructs, called RSA-DOAEP, has the added featureof being length preserving, so that it is the first example of a public-key cipher. We generalize this to obtain a notion of efficiently-searchable encryption schemes which permit more flexible privacy to search-time trade-offs via a technique called bucketization[2].
8. Solve the challenging problem of privacy-preserving multi-keyword ranked search over encrypted data in cloud computing .It ranks the document according to matching result[4].

9. single-keyword searches and offers asymptotically optimal server index size, fully parallel searching, and minimal leakage. Our implementation effort brought to the for a several factors ignored by earlier coarse-grained theoretical performance analyses, including low-level space utilization, I/O parallelism and good put[5].

10. Proposed SSE scheme to satisfy all the properties outlined above. Our construction extends the inverted index approach in several non-trivial ways and introduces new techniques for the design of SSE[8].

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

III. PEOPOSED WORK

III.I PROPOSED SYSTEM ARCHITECTURE

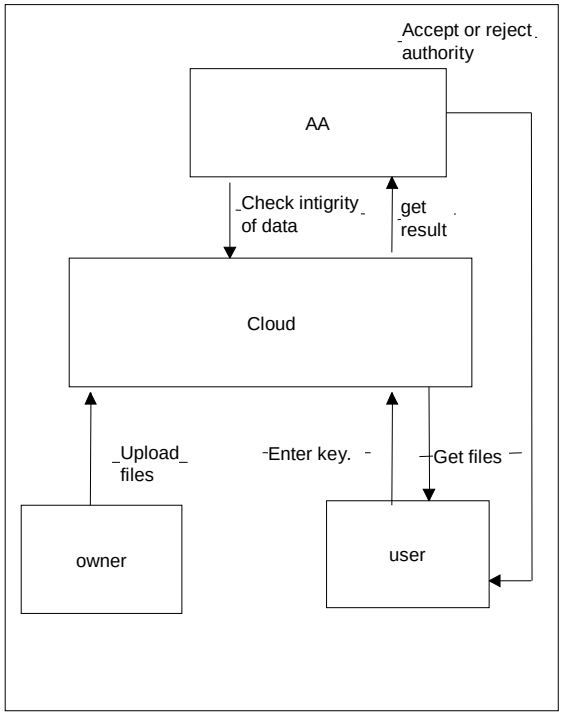

Fig.1: System architecture

SYSTEM OVERVIEW-

Proposed system will provide security to data. Secure search protocol that can an efficient and easy-to-implement searchable and verifiable encryption scheme for search, In proposed system computing model, three entities are involved such as data owners, data users, and TPA .Data owners have collection of files. Data owners upload the file .Data owners encrypt files and outsource encrypted files to cloud server. Data user view file and send request for key to get file. System will give matched files. Then TPA send request for decryption key , user will get that on mail. If key matches then only file will download to client. then data client download files and decrypts these files. Third party auditor check file uploaded file data is presentor not and inform to owner.

III.II.ALGORITHM:

AES(advanced encryption standard).It is symmetric algorithm.It used to convert plain text into cipher text .The need for coming with this algo is weakness in DES. The 56 bit key of des is no longer safe against attacks based on exhaustive key searches and 64-bit block also consider asweak.AES was to be used128-bit block with128-bit keys. Rijendeal was founder. In this drop we are using it to encrypt the data owner file.

Input:

128_bit /192 bit/256 bit input(0,1)

secret key(128_bit)+plain text(128_bit).

Process:

10/12/14-rounds for-128_bit /192 bit/256 bit input

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

Xor state block (i/p)
Final round:10,12,14
Each round consists:sub byte, shift byte, mix columns, add round key.
Output:
cipher text(128 bit)

RESULT:

1) Execution time for entered query:

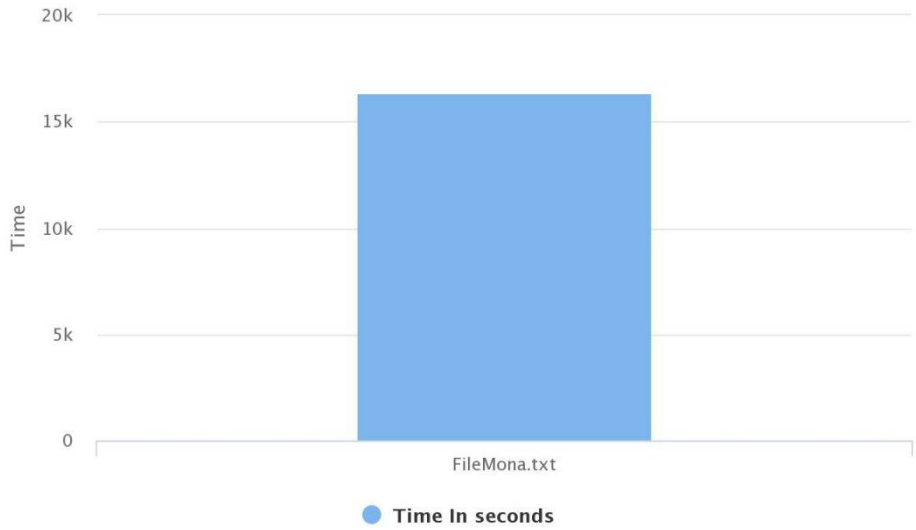

Fig.3Shows time to upload the file

Explanation: Graph shows time to upload the file after encryption by AES Algorithm which is Symmetrik algorithm.

IV. CONCLUSION

construct a system model that can distinguishthe users according to their roles and special requirementsof scholarly big data. Moreover, an innovativeAES Algorithm used and key is used for encryption is system current date considers and the encrypt data. On the basis of thenovel system and data structure, we present a novel secure data and verifiable data protection scheme for scholarly bigdata. The security and performance analyses show that ourscheme is efficient for scholarly big data.

REFERENCES

1.Michel Abdalla, Mihir Bellare, Dario Catalano, Eike Kiltz, Tadayoshi Kohno, Tanja Lange, John Malone-Lee, Gregory Neven, Pascal Paillier, and Haixia Shi. Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions. volume 21, pages 350–391. Springer, 2008.
2.Mihir Bellare, Alexandra Boldyreva, and Adam ONeill. Deterministic and Efficiently Searchable Encryption. In Annual International Cryptology Conference, pages 535–552. Springer, 2007.
3. Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano. Public Key Encryption With Keyword Search. In International Conference on the Theory and Applications of Cryptographic Techniques, pages 506–522. Springer, 2004.
4. Ning Cao, Cong Wang, Ming Li, Kui Ren, and Wenjing Lou. Privacy- Preserving Multi-Keyword Ranked Search Over Encrypted Cloud Data. volume 25, pages 222–233. IEEE, 2014.
5.David Cash, Joseph Jaeger, Stanislaw Jarecki, Charanjit S Jutla, Hugo Krawczyk, Marcel-Catalin Rosu, and Michael Steiner. Dynamic Searchable Encryption in Very-Large Databases: Data Structures and Implementation. volume 2014, page 853. Citeseer, 2014.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

6.Yoshinao Uchide and Noboru Kunihiro. Searchable symmetric encryption capable of searching for an arbitrary string. Wiley Online Library, 2016.
7.Reza Curtmola, Juan Garay, Seny Kamara, and Rafail Ostrovsky. Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions. volume 19, pages 895–934. IOS Press, 2011.
8.Seny Kamara, Charalampos Papamanthou, and Tom Roeder. Dynamic Searchable Symmetric Encryption. In Proceedings of the 2012 ACM conference on Computer and communications security, pages 965–976. ACM, 2012.
9.Jonathan Katz and Yehuda Lindell. Introduction to Modern Cryptography. CRC press, 2014.
10.Muhammad Naveed, Seny Kamara, and Charles V Wright. Inference Attacks on Property-Preserving Encrypted Databases. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pages 644–655. ACM, 2015.
11] S. Tuarob, S. Bhatia, P. Mitra, and C. L. Giles, "Algorithmseer: A system for extracting and searching for algorithms in scholarly big data," IEEE Transactions on Big Data, vol. 2, no. 1, pp. 3–17, 2016.
[12] F. Xia, W. Wang, T. M. Bekele, and H. Liu, "Big scholarly data: A survey," IEEE Transactions on Big Data, vol. 3, no. 1, pp. 18–35, 2017.
[13] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New algorithms for secure outsourcing of modular exponentiations," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 9, pp. 2386–2396, 2014.
[14] J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, "An efficient public auditing protocol with novel dynamic structure for cloud data," IEEE Transactions on Information Forensics and Security, vol. 12, no. 10, pp. 2402–2415, 2017.
[15] X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, "Verifiable computation over large database with incremental updates," IEEE transactions on Computers, vol. 65, no. 10, pp. 3184–3195, 2016.