International Journal of Engineering &Technology, 7 (3.12) (2018) 269-271

International Journal of Engineering & Technology

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

Research paper



Protection Preserving Over Encrypted Data Using Key with Similarity Check

G.Sabari prasanth[1], M.Rajasekaran[2]

[1,2]Department of Computer Science and Engineering, SRM University, Kattankulathur, Tamilnadu, India
[1]sabarigovindaraj@srmuniv.edu.in, [2]smrajamani1981@gmail.com

Abstract

Computing gives people to store enormous data efficiently and economically since it depends on third party management security is the million dollar question. In order to provide protection over the private data user can encrypt the data and can upload in cloud. Encryption process could be done by Advanced Encryption Standard (AES) algorithm which is highly secure and unbreakable. Encrypted data with key management play significant role in cloud computing in order to get decrypted data user should appropriate key for the file to get decrypted data which would be transferred very securely. Proposed system try to avoid update of unwanted data like inappropriate sentences will be avoided from malicious user to misuse the data .The concept of data mining plays a vital role. This concept of combination of cloud computing and data mining gives us the good result of security of personal detail and unwanted data would not accommodate on the internet .This process would help mostly on providing authenticated data by only legitimate user can access the data even legitimate user cannot find the decrypted content if unwanted data exist in the file. This approach have overcome security issues of own personal or organization data.

1. Introduction

In today world Information about anything would play a major role in their field information is referred and as wealth of any person or organization. Mostly information is shared and known in the internet via social media or some authorized website there is a chance that information would be spread in wrong way this is a detrimental for an individual or as an . so to ensure the authentication over the data and method to prevent the data loss from some malicious attacker is an important task to do. There might be a lot of method to avoid loss of data but exchange of key for data to get decrypt from legitimate user and sharing the information that way plays a major role and better method to avoid unauthorized to access the data and cannot modify the data without the permission of an individual who responsible for all these process for data of unwanted will be gathered and stored in the database. When the data is processed each and every data word would be matched against set of words stored in database in order to process these required queries in database and execute and finding unwanted list of words in the file required proper arrangement which is tedious to achieve. there are various method have been proposed for searching key words over the database. One among the existing system is privacy-preserving multi-keyword Top-k similarity search over Encrypted data which choose multi-keyword search which search all the path of tree like structured index which increase the efficiency of path search will increase the query time over encrypted data. So system based on existing system approach keywords which is an unwanted words would be matched against an each every word in the data of file in multipath.

2. Literature Survey

There are various research have been undergone in these field few among are [1]detecting duplication over the cloud data and try to avoid upload of duplicated data repeatedly. this approach help in avoid updating of duplicated data of even encrypted format in cloud avoiding duplication over encrypted data in cloud is quite challenging task to achieve. it just overcome the traditional de duplication method which would not work on the encrypted data. [2] prevention against attack of DDOS in cloud .In this paper they found that detection and protection of an individual cloud server from the DDOS attack though sole objective of DDOS attack by resource requirement the big organizational vendor does not have any issue about the resource insufficiency .but this approach have help to individual cloud servers.[3] introducing search functionalities over encrypted data in cloud this approach would help an individual to search a particular keyword with PPGQ scheme it is based on the technique of KNN. searching of data in normal form is not tedious but in encrypted format require lot work to do. This method have a great potential to be introduce search in our work.[4] image sharing also has to be secured over the internet sharing inappropriate image content is unfair thing
so securely transferring the mobile data of image content from various type of data base like geographical database and multimedia database

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

3. Proposed System

The proposed system highly focus on avoiding the security, scalability and authentication of data. The proposed system has processes of whenever user upload the file in the cloud they first encrypt the file and upload it. as user want the particular file then user has to get permission from the administrator. The administrator is only an authority can verify the user and can send appropriate key to particular requested user then user can access the file only key matches to the particular file otherwise file could be only in decrypted format. The key for any particular file will be generated when user upload it. For cryptography in our proposed system we use an Advanced Encryption Standard(AES) algorithm in our system. The key sizes of this Algorithm are 128,256 and 192 and each block size would be of approximately 128 bits which means total data will be split into each 128 bit and encryption will be applied on it for the process of decryption work in opposite manner . so this method is infeasible to break.so security issue where resolved by encrypting and decrypting using AES algorithm.next concern of our system is user authentication on accessing the data that will be analyzed and ganted by administrator.our next issue to be tackeled is presense of unwanted data in our file by accident by legitimate user itself or by malicious attacker.

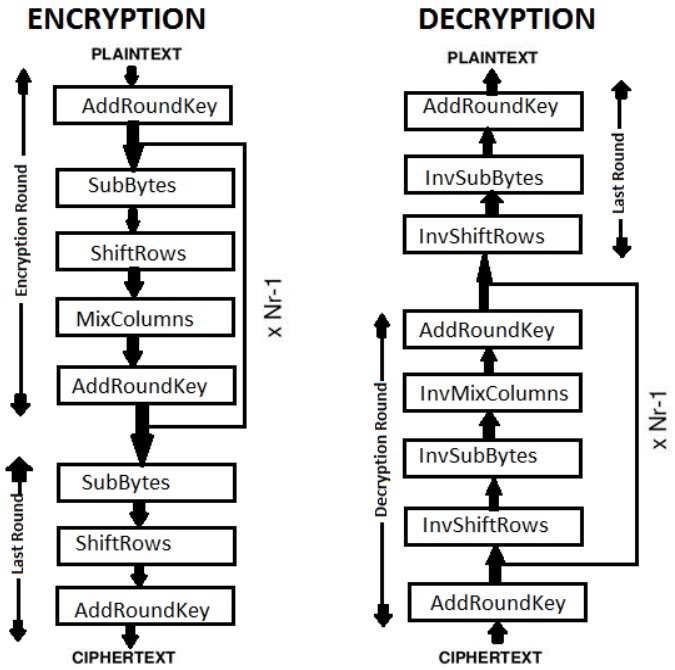

Fig. 1: Structure of AES algorithm

Through similarity check administrator have set of words to that should not present in any form of file. so every data will be matched individually against list of words present in administrator database any word matches then that file never turn to an decrypted format then it will show only in encrypted format through this authentication over private data will be achieved. An existing system only search multiple key word instantly on the encrypted set of data to increase search efficiency but in proposed system additionally providing hindering of unwanted data. This would increase the security, accuracy and clarity of data in cloud.

4. System Architecture

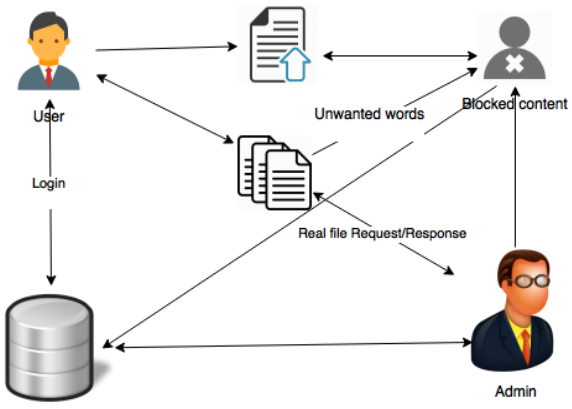

Fig. 2: System Architecture

The system of Architecture would explain about the data flow and existence of an entities etc. The order of data flow are user would upload in cloud database Administrator would analyze the data and dealt up to the content in database.

5. Algorithm

Algorithm for analyze unwanted data.

1: **function** SEARCH(*A*, *B*, *C*)
2: **for** query *ADi* in query group *AD* **do**
3unwanted(*ADi*, root of *IDi*, 0, *L*)
4: Merge top-*k* documents *listi* of *ADi* into *DList*
5: **end for**
6: **for** document *Ei* in *DList* **do**
7: **if** Score(*AS*, *ISi*) > *k*-th score in c*Se* **then**
8: Insert *i* into c*Se*
9: **end if**
10: **end for**
11: **return** to documents of c*Se*
12: **end function**
13:
14: **function** unwanted(*ADi*, *node*, *sdo*, *L*)
15: **if** sco < *k*-th score in *listi* **then**
16: return
17: **end if**
18: **if** *node* is leaf node **then**
19: Insert the *fid* of *node* into *listi*.
20: **else**

21: **end if**
22: **end if**
23:**if**(!unwanted)
24:send decrypted content
25:**else**
26send encrypted content
27: **end if**
28: **end function**

6. Conclusion

We focus on the task of increasing efficiency over data authentication user authentication avoiding data loss over the network. The method of searching an unwanted data over the encryption have achieved an avoidance of un appropriate content it help an individual or any organization to avoid wrong information and which turn detrimental them.
Future Enhancement of this project could be finding unwanted word would be added by individual that would miss some word . In future anybody can come with method to increase the number of unwanted content to be found and increase the efficiency of finding an unwanted word and more increasing search efficiency than this method.

References

[1] J. Tang, Y. Cui, Q. Li, K. Ren, J. Liu, and R. Buyya, "Ensuring security and privacy preservation for cloud data services," ACM Computing Surveys, 2016.
[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, 2010.
[3] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," in Proceedings of the 13th ACM Conference on Computer and Communications Security. ACM, 2006, pp. 79–88.
[4] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in Cryptology-Eurocrypt 2004. Springer, 2004, pp. 506–522.
[5] Z. Ying, H. Li, J. Ma, J. Zhang, and J. Cui, "Adaptively secure ciphertext-policy attribute-based encryption with dynamic policy updating," Sci China InfSci, vol. 59, no. 4, pp. 042 701:1–16, 2016.
[6] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Security and Privacy, 2000. SP 2000.Proceedings. 2000 IEEE Symposium on, 2000, pp. 44–55.
[7] E.-J. Goh et al., "Secure indexes." IACR Cryptology ePrint Archive, vol. 2003, p. 216, 2003.
[8] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Applied Cryptography and Network Security. Springer, 2005, pp. 442–455.