International Journal of Computer Engineering & Applications
Save Tree! Save World!

UGC Approved Journal
ज्ञान-विज्ञान विमुक्तये
UGC
Sr.No. 44835

IMPLEMENTATION OF SECURE ENCRYPTION FRAMEWORK USING AES

Akshay Bhagwan Bahadure , Rahul Dilpak , Darshan Satpute , Prof. Rama Barwal

***Dept of Computer Engineering, Savitribai Phule Pune University, Pune , Maharashytra, India*.**

ABSTRACT:

In this project we propose the data on cloud computing is encrypted due to security concern or the factor of third party digging into it. As the consequent to this, the search over encrypted data becomes a complex task. The traditional approaches like searching in plain ext cannot be apply over encrypted data. So the searchable encryption techniques are being used. In searchable encryption techniques the order of relevance must be consider as the concern because when it is large amount of data it becomes complex as relevant documents are more in number. We have discussed the Re-encryption technique. The expected result is to be that cloud server cannot penetrate in actual user data and provide the search on encrypted data will be performed and results will appear in order of relevance score. Even though with good security of Re-encryption the cloud can get the information of the plain text if differential attack occurred on the cipher text by calculating the differences between the cipher text.

Keywords: Security, framework AES, java, jsp, cloud, etc.

[1] INTRODUCTION

In this project we propose the data on cloud computing is encrypted due to security concern or the factor of third party digging into it. As the consequent to this, the search over encrypted data becomes a complex task. The traditional approaches like searching in plain text cannot be apply over encrypted data. So the searchable encryption techniques are being used. In searchable encryption techniques the order of relevance must be consider as the concern because when it is large amount of data it becomes complex as relevant documents are more in number. We have discussed the Re-encryption technique. The expected result is to be that cloud server cannot penetrate in actual user data and provide the search on encrypted data will be performed and results will appear in order of relevance score. Even though with good security of Re-encryption the cloud can get the information of the plain text if differential attack occurred on the cipher text by calculating the differences between the cipher text.

Literature Survey:

[1] S. Subashini and V. Kavitha, “A survey on security issues in service delivery

models of cloud computing,” Journal of Network and Computer Applications, 34(1): 1-11, 2011.
Conclusion: In this paper, a survey of the different security risks that pose a threat to the cloud is presented. This paper is a survey more specific to the different security issues that has emanated due to the nature of the service delivery models of a cloud computing system.

[2] A. Boldyreva, N. Chenette and A. ONeill, “Order-preserving encryp-tion revisited: improved security analysis and alternative solutions,” Advances in CryptologyCCRYPTO, 2011. Springer Berlin Heidelberg, pp. 578-595, 2011.

Conclusion: Finally we propose a simple and efficient transformation that can be applied to any OPE scheme. Our analysis shows that the transformation yields a scheme with improved security in that the scheme resists the one-wayness and window one-wayness attacks.

[3] L. Xiao, I.-L Yen, “Security analysis for order preserving encryption schemes,” Proc. of 46th Annual Conference on Information Sciences and System, pp. 1-6, 2012.

Conclusion: In this paper we analyze the security of the OP E encryption scheme SEm,n and give the upper bound on the probability for the adversary to recover the plain text encrypted by SEm,n under chosen plain text attacks

[4] C. Wang, N. Cao and K. Ren, “Enabling secure and efficient ranked keyword search over outsourced cloud data,” Parallel and Distributed Systems, IEEE Transactions 23(8), pp. 1467-1479, 2012.

Conclusion: In this paper, he define and solve the problem of secure ranked keyword search over encrypted cloud data. Ranked search greatly enhances system usability by enabling search result relevance ranking instead of sending undifferentiated results, and further ensures the file retrieval accuracy.

[5] S. Yu, C. Wang and K. Ren, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” INFOCOM, 2010 Proceedings IEEE. IEEE, pp. 1-9, 2010.

Description: This paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine grained data access control to untrusted cloud servers without disclosing the underlying data contents. he achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption.

PROPOSED SYSTEM:

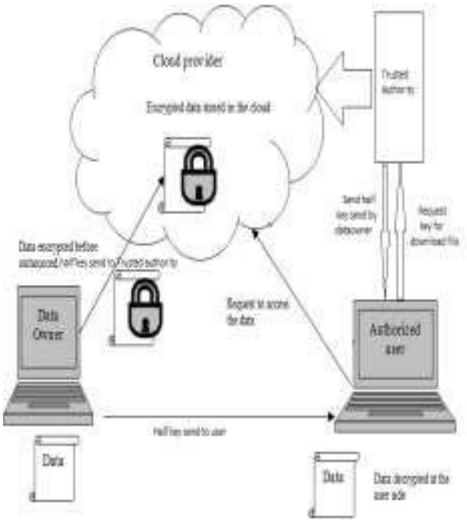

Cloud provider
Encrypted data stored in the cloud
Trusted Authority
Send half key send by dataowner
Request key for download file
Data encrypted before outsourced half files send to Trusted authority
Data Owner
Request to access the data
Authorized user
Half files send to user
Data
Data
Data decrypted at the user side

FIG: PROPOSED SYSTEM

Cloud users store their data in encrypted form to maintain data privacy. Two approaches that are used to securely share data in cloud storage. Firstly, encrypt data using a symmetric key and share that key among the authorized users. Secondly, encrypt data using the individual public key of the authorized users. Authorized users can access plaintexts data by decrypting the corresponding ciphertexts using their respective private key. However, the former approach incurs heavy overheads on the data owner, while storage overheads is more in the late Further, fine-grained access control in data sharing cannot be achieved from these two approaches. To these issues, ABE has emerged as a good alter-native to achieve scalable fine-grained access control while sharing encrypted data among a set of authorized users in cloud environment. It allows data owners to encrypt data using an access policy of different attributes. The users who have sufficient attributes can decrypt the ciphertexts. Although ABE schemes provide fine-grained access control in sharing data among a set of authorized users, revocation is remained challenging task. In ABE, more than one user may have same attributes. Therefore, user revocation should be done so that revoked users must not be able to access plaintexts data, while non-revoked authorized users should be able access plaintexts data without any difficulty.

Advantages:

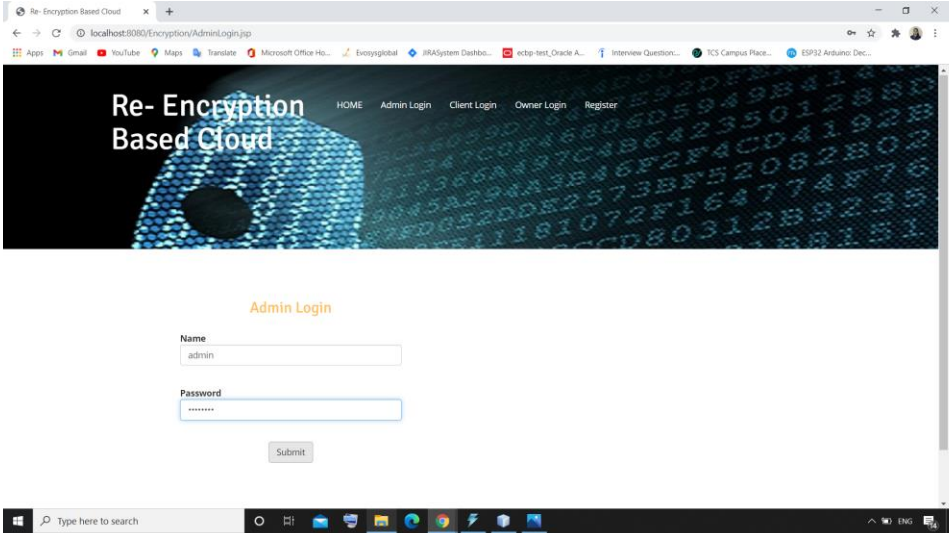
- More security is provided Encryption is provided to the data
- Enhances the authentication and verification

- Data is encrypted with AES algorithm so that it is more secure
- Provide better and secure way for the data security

Applications:

- This proposed system can be used for various applications
- Enterprises applications Business applications
- Real time data security application

Results:

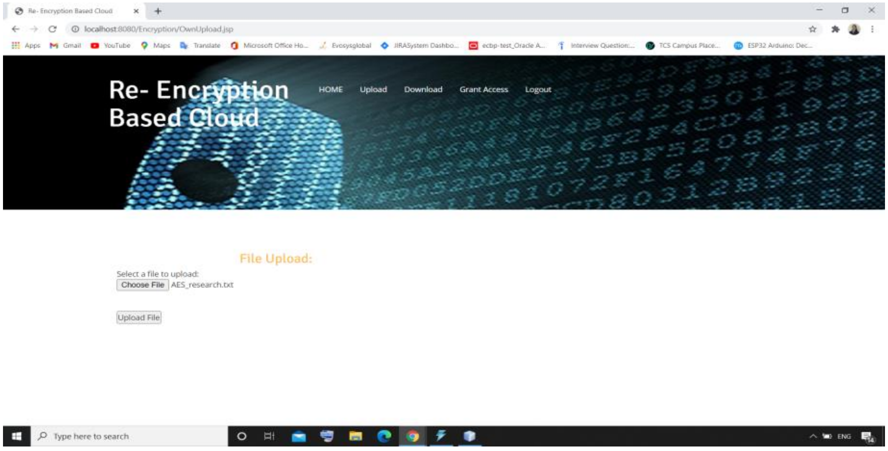


Admin Login

Name
admin

Password
••••••••

Fig: Login Page



File Upload:

Select a file to upload:
AES_research.txt

Fig: File Upload

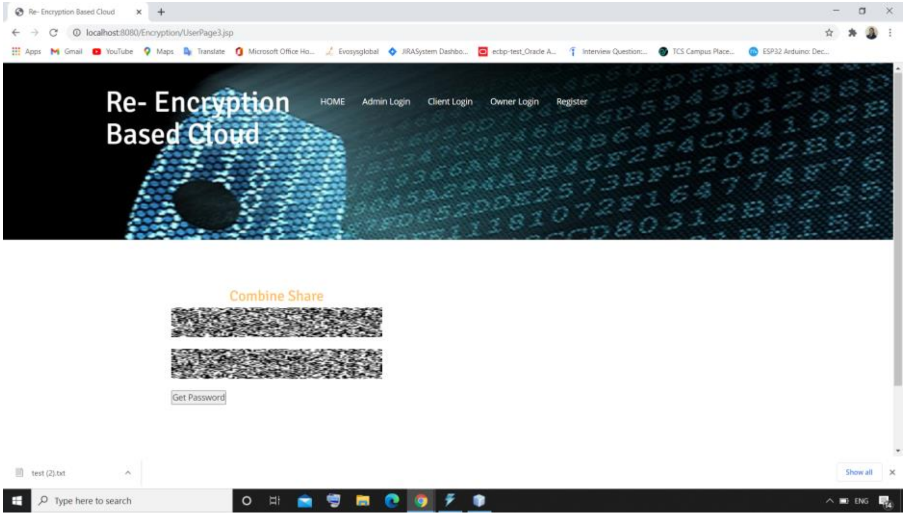


Fig: Visual Cryptography

Conclusion:

Nowadays, everything is being done with computer systems and applications so the security of the data in database system is an important issue. Many researchers are working on information security and proposing various techniques and algorithms. Each architecture has its own advantages and disadvantages, but none of them is fully secure and contains certain loopholes, however there is huge scope of improvement in information security area to and a perfect solution and scheme that is fully secure from all possible threat. In this method adding an extra security enhancement module between client and the database server works for the improvement of the security of the database server. Hence the security from the internal threats is achieved and even because of the addition of extra module the overhead is also reduced to improve the system performance.

REFERENCES

[1] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” Journal of Network and Computer Applications, 34(1): 1-11, 2011.

[2] A. Boldyreva, N. Chenette and A. ONeill, “Order-preserving encryp-tion revisited: improved security analysis and alternative solutions,” Advances in CryptologyCCRYPTO, 2011. Springer Berlin Heidelberg, pp. 578-595, 2011.

[3] L. Xiao, I.-L Yen, “Security analysis for order preserving encryption schemes,” Proc. of 46th Annual Conference on Information Sciences and System, pp. 1-6, 2012.

[4] C. Wang, N. Cao and K. Ren, “Enabling secure and efficient ranked keyword search over outsourced cloud data,” Parallel and Distributed Systems, IEEE Transactions 23(8), pp. 1467-1479, 2012.

[5] S. Yu, C. Wang and K. Ren, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” INFOCOM, 2010 Proceedings IEEE. IEEE, pp. 1-9, 2010.