Secured Multi Owner Data Sharing in Cloud Using AES Algorithm

[1]N. Praveen, [2]P. Satya Sai Manohar, [3]M. V. Praveen Kumar

Abstract--*Cloud Computing enables us to easily store data and simply share data with others. Due to the safety threats in any cloud, users take measures to secure their data, such as signatures, on their data to protect the integrity. With the advent of cloud computing, it becomes increasingly popular for the data owners while allowing the data users to retrieve these data. For privacy concerns, over encrypted cloud data, several researches under the single owner model have been done. However, most cloud servers which are in practice do not just serve one owner, instead, they support multiple owners to share the benefits brought by the servers. In our project we proposed a multiple owner file sharing system in cloud computing, here the user can use their particular owner file and also he can access other owner files. For accessing, the way of request and response is used. If another owner responds the user, it means that he can get the private key from the owner and then he can access the files.*

Key words--*Cloud Computing, Data Sharing, Advances Encryption Standard(AES), Key Distribution, Encryption, Group Creation*

I. INTRODUCTION

Cloud computing in these days is the most essential service and the cloud services are being available all over the globe irrespective of the location. Cloud computing gives us many services where, allocation of storage, encryption of data are some of the examples. These cloud services are provided by many different cloud service providers and all are not trust-worthy. These cloud services may be free or either some paid services. The cloud space being provided will decide the cost of the particular person's cloud space. In these days cloud space is the most used service for the purpose of data storage and data transfer.

As we can see the high usage of these cloud services there arises some security issues where some of the possible and frequently happening issues are that the data might be lost or the data might be stolen, that is the third party enters without the permission of the data owner. There are high chances for the data to be lost with the use of any untrusted cloud spaces or the cloud space having less security.

Cloud space providers should make sure that the space provided to any particular person should be possessing the features of providing the security for both data storage and data transfer. There are many possibilities for the data to be stolen in case of the cloud space being used by the providers which are not trust-worthy, those are like the third party entrance into the personal data is easy if there exists no security, and the data might be stolen.

[1]Department of Computer Science, SRM Institute of Science and Technology, Chennai, India, npraveencs29@gmail.com
[2]Department of Computer Science, SRM Institute of Science and Technology, Chennai, India, manoharparise@gmail.com
[3]Department of Computer Science, SRM Institute of Science and Technology, Chennai, India, praveenchowdarymalineni@gmail.com

DOI: 10.37200/IJPR/V24I8/PR280117
Received: 21 Jan 2020 | Revised: 08 Feb 2020 | Accepted: 14 Mar 2020

Secure Computing is known as the security which is applied to the information in all fields. This security provides protection from any sort of unplanned situations. It mainly concentrates on the providence of data encryption and security. For many reasons passwords are being formed in such a way that they are tough to crack out. It is known as the bridge between the user and any sort of system.

In order to make sure that the data is secured some basic formulation for the data encryption is done, where the data protection is not so easy. There are many cloud space providers and some security systems attached to it such as Data Encryption Standard(DES), 3DES, and Advanced Encryption Standard(AES) where they provide a particular key on the request of the user to the owner.

The main aim of the proposed system is the data security and it is done using

Advanced Encryption Standard: It is the most widely used and adopted algorithm for the encryption of the data which are in charge these days. It is mainly said to be the replacement for the DES algorithm as it is being attacked by the third party users. There are many salient features for the algorithm such as--

- Generation of symmetric key using the symmetric block cipher,
- Stronger and a little faster than the 3DES,
- Software implementation made easy using the daily usable programming languages,
- Mainly provides the full sort of specifications and all the data flow.

The development of this AES algorithm was started in the National Institute of Standards and Technology(NIST) in 1997. It is mainly developed in criteria that the existing algorithm named DES is getting attacked by brute force and by various other factors. Its major asset is to provide the high security for the data to be attacked from malwares and the stating about the cost factor, it is very effective in the matter of cost and bearable by everyone. And even the implementation is quite easier in programming languages like C, JAVA. There are also other security algorithms such as MARS, RC6, Rinjdael, Serpent, Twofish which mainly focuses on the data to be stored and transferred without being lost and ruined by others.

II. LITERATURE SURVEY

D.Song, Wagner, Perrig [1] discussed about the partial techniques for searching of the encrypted data which mainly deals about the data encryption format for the security of the uploaded data into the cloud or any other database. All the techniques are a real time useful encryption techniques which has its own specific manner of usage. This infers a sample requirement of info in the proposed system.

D. Goh, [2] proposed a technique for the encryption of data using different algorithms and out of which the cryptographical technique is the one which is helpful for the proposed system, the discussion went on using various encryption algorithms such as DES,3DES, blowfish, RC6. Out of which the 3DES has the least performance and so the AES techniques is used. This infers the data to be stored in packet format while the transfer of data occurs.

DOI: 10.37200/IJPR/V24I8/PR280117
Received: 21 Jan 2020 | Revised: 08 Feb 2020 | Accepted: 14 Mar 2020

Y.Chang and M. Mitzenmacher[3] made some discussions on the preservance on the data which is private and the encryption of data remotely. This technique gives a brief description for the data to be encrypted in the particular format where that will be accepted by the database and there occurs no problem for the transfer of data that is no loss of data or no entry for the maskers.

R.Curtmola, J. Garay, S. Kamara and R. Ostrovsky [4]improved some definitions for the symmetric approach of the data encryption which uses cipher block text in the encryption standards. They constructed a Computer Security System for the maintenance of the database in a standard that there occurs no breach and no data loss. This system and enhanced definitions make sure that the encryption technique should be strong so that no security breach occurs and get out the data and also no entry without proper authentication is allowed. E. Thambiraja [10] also discussed the usage of proper encryption techniques which are to be used in these days after the serious threat for the data to be lost without a proper security . He discussed the feature of image encryption and information encryption. As a result all the techniques are different in their own way and are useful in different applications.

K.Kurosawa and Y.Ohtaki [5] made a deep search in the data security field which makes sure that the data can be secured in different ways and all the ways are different in their own way and used in different situations. They also made a study on the Cryptography techniques by which the image can be processed and stored in the database for the secured storage of any format of data. This makes the proposed system enhanced towards the file uploading and the storage of different forms of data and securing the data.

Sudhansu Ranjan Lenka[8] proposed an algorithm using two different algorithms known as RSA and MD5 hashing. The combination of data always gives a high securable format for the data being uploaded or transferred . From the above two algorithms the RSA algorithm makes the data confidential and the MD5 algorithm makes the authentication secure. In the table from the database the public and private keys information which are being used makes sure that the user details given at the time of registration are updated in the database table only after hashing the data using MD5 algorithm’s hashing technique . Once the hashing process is completed ten the user is given the files which are encrypted to be decrypted using the private key which is generated using the algorithm. To the conclusion, this makes the technique which is being used in proposed system easier as the user data is to be authorised and then the files are uploaded and private key is to be generated using the AES algorithm.

P.Kalpana[13] discussed on the cloud security and implemented a separate method to make sure that the usage of RSA algorithm is to ensure that the data is to be secure. The issues for the cloud include privacy preservation, data integrity and confidentiality also other issues are like backup, recovery, and locating. In order to show this off, the RSA algorithm is used for the data to be secure in this case. The major advantage of using this is that only the registered user can be able to access the files only with private key and then the data gets decrypted and be shown to the user who placed a request. This makes a conclusion that the proposed system should make sure that the private key to be sent only to the authorised user who places a request. This enhances the data security.

DOI: 10.37200/IJPR/V24I8/PR280117
Received: 21 Jan 2020 | Revised: 08 Feb 2020 | Accepted: 14 Mar 2020

C.Bosch, Q.tang and Jonker [9]made a research about the retrieval of the document or any data from a encrypted database. This mainly deals about the data which is uploaded and encrypted in the database in some other form from which is not so easy to be stolen, that data can be decrypted and taken back into the normal form. This infers that the proposed system of ours mainly deals about the encryption process of the data being uploaded in the database and how that will be decrypted on the request of the user only having the private key.

D.Cash , Jutla, and Steiner [7] made a study on the symmetric encryption search for the key words with the boolean algorithm support. This mainly deals about the search flexibility of the words which are being required from the uploaded file of data which is of any type that is audio, video or any file format. The file format also can be of photo, any pdf file or any of the business operational file. This can be cost efficient and the search process will be highly scalable with the high rate accuracy and the time factor .This makes sure the data is safe with high security.

S. Aljawameh [11] made a study about the proposed algorithms before the threat to the stored data is less. Then the study makes sure that the features of the existing and recently proposed are completely different and the proposed system is a bit secure in the way of encryption of the data to another level where the data can not be accessed by the private key and that is also provided by the admin only if the user is an authorized user. This infers the proposed system about the security of the data being uploaded to be encrypted in a way that the data is not to be stolen and only with the specific permission and the access key , the data is to be decrypted.

III. PROPOSED WORK

The proposed system is according to the securing of data uploaded or transferred by the user, to the cloud space. The data sent in this way is encrypted using the AES encryption technique. The authentication of the user is done by the admin and the role of admin ends there with the registration process approval. The verified user is able to upload delete or view the files of his own and also the files in the encrypted format of others. The maskers are not aware of the encryption and the decryption of the data.

The working of the proposed approach for the data security is as follows:

- The user registration process takes on by the admin of the security approach.
- The request for the required files is sent to the particular data owner and then he takes the request and sends the acceptance as the key to access the particular file.
- This key is secret key for the data to be kept encrypted using the AES approach .
- The encrypted data is stored in the database.
- The key which is used is changed after one attempt to access the file and hence, the file is encrypted again, in order to prevent the loss of data.

DOI: 10.37200/IJPR/V24I8/PR280117
Received: 21 Jan 2020 | Revised: 08 Feb 2020 | Accepted: 14 Mar 2020

Working of AES approach:

It is the symmetric encryption standard which is effectively workable in software and hardware. Even the implementation is easier and it supports the block length of about 128 bits and the size of the key is 128,192,256 bits. This is majorly dependent on the length of the key. This uses 10,12,14 series for 128,192,256 bit keys respectively and where all the series are from the original AES key.

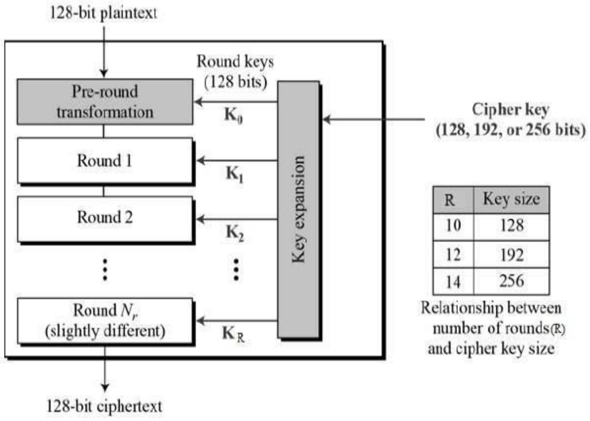


Figure 1: Structure of AES

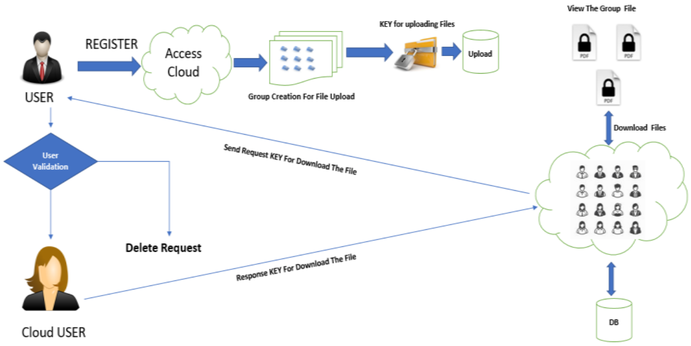


Figure 2: Architecture diagram of the system

IV. IMPLEMENTATION

A. System Implementation

The system is implemented in Netbeans using Java programming language. The data is sent to the cloud only when the authentication of the user is successful. The details provided by any user at the time of registration are asked to be entered for the purpose of authentication and the particular user can be logged in to the provided space to view, upload or delete their own files. They can also view the files belonging to other data owners and if the files of other owners are needed then the user places a request to the owner and if the owner is interested to share the files then he will be sending a particular key , which changes on one click using the technique of AES.

B. Encryption of Data

The data being uploaded can be of any type that is image, audio or video or any file format. The data file is specified by the system and then the data is stored in the cloud space and retrieved in the same format when the request is placed to the particular data owner. The key is automatically changed on one click of the original key. This key generation schema is of greater strength than the other existing other algorithms such as DES and RSA. Like, the key length in this AES algorithm is 128,192,256 bits while the key length is only 56 bis in the case of DES.

The encryption and decryption strategy in the case of AES algorithm is faster than the DES and RSA algorithms. The accuracy is also high in the case of this approach. The symmetric block cipher technique is used in the case of this algorithm since it is more efficient than the asymmetric block cipher. Even though the DES algorithm is having the symmetric block cipher technique it is taken out of practice in these days because of having many security threats and the algorithm is being cracked easily with out the knowledge of the data owners. If any of the test is to be conducted for knowing the accuracy of the algorithm then the precision is found for different algorithms towards the cipher technique and the one having the highest accuracy can be confirmed to be the algorithm being used in the approach.

C. Delay Calculation

As the cipher type used in this algorithm is the symmetric block cipher, The data which is being encrypted is not so easy to be understandable. As earlier, the time taken for a data file to be uploaded into the cloud differs from size of the file, that is if the file is larger it takes more time and if the file is small it takes other time . And this time is calculated using the delay concept. This majorly occurs because of the users using the cloud at a time, if the number of users are more then the time taken for a file to be uploaded is also more. And the cloud needs to answer all the users at a time and hence the traffic, when it is more the time required will also be more. The delay occurred for the process can be calculated[8] using the formula DELAY = T_S - T_B where T_S denotes the time after the successful upload and T_B denotes the time before upload of the data.

The encryption time is noted for the calculation of the delay. And , the difference is stated using the files of different size such as 8MB, 24MB, 50MB, 83MB. And the time is calculated in seconds where the below depicted graph shows the difference between the time taken by different size files to be uploaded into the cloud space. The cloud server database can be of any trusted database and the application of AES algorithm should be possible.

DOI: 10.37200/IJPR/V24I8/PR280117
Received: 21 Jan 2020 | Revised: 08 Feb 2020 | Accepted: 14 Mar 2020

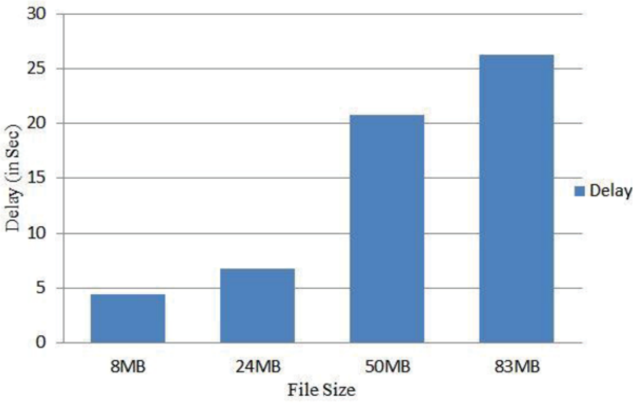
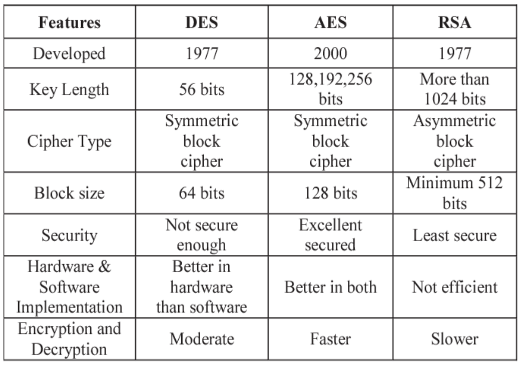


Figure 3: Delay Calculation

There are different features which can explain the uniqueness and the strength of the approach. The comparison of the stated algorithms can be depicted using the following:



Features	DES	AES	RSA
Developed	1977	2000	1977
Key Length	56 bits	128,192,256 bits	More than 1024 bits
Cipher Type	Symmetric block cipher	Symmetric block cipher	Asymmetric block cipher
Block size	64 bits	128 bits	Minimum 512 bits
Security	Not secure enough	Excellent secured	Least secure
Hardware & Software Implementation	Better in hardware than software	Better in both	Not efficient
Encryption and Decryption	Moderate	Faster	Slower

Figure 4: Comparison of the algorithms

V. RESULTS DISCUSSION

The data is encrypted by the AES technique in order to be attacked from third party uses. As there is no scope for third party users, once the user is authenticated, then the entrance of any malwares is avoided. If the authentication is not proved by the user then the particular user cannot move further. Now, after the successful authentication of any user all the groups from all users can be seen and thus any user who is having any requirement of a particular file, can place a request at the file and which itself leads to the owner of the particular file.

And then the owner gets a request and if the owner is interested to share is/her files then the response from owner is sent to the particular requested person. And then he can be accessing the files and once the file is accessed by a particular key the key is automatically changed and a new key is generated. And with the same key any file cannot be opened twice. This mainly reduces the false sharing of important data. This is achieved using AES faster than compared to the other data security algorithms.

DOI: 10.37200/IJPR/V24I8/PR280117

VI. CONCLUSION

From the system built, based upon the AES algorithm it can be concluded that the security method for the data to be secure, provides an increased security for data when the data transfer or data storage is required. Since there is no access for the third party owners, there is no possibility of any of the ones who wanted to enter without the permission or the key is not possible to the core. This makes sure that the system proposed gives us a confidence of having no threat for the stored data and thus an efficient AES encryption technique for the cloud data is built. From the above mentioned algorithm technique we can relate the data upload size with the delay in increase of time required for the file to get uploaded. This makes the existing system weak and the proposed system can make sure that the files being uploaded can be truly confidential and safe to be attacked by malwares. In this system, encryption and decryption is possible on all types of data such as, images audio and video.

REFERENCES

1. D. X. Song, D. A. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in 2000 IEEE Symposium on Security and Privacy, Berkeley, California, USA, May 14-17, 2000, 2000, pp. 44–55.
2. E. Goh, “Securing indexes,” IACR Cryptology ePrint Archive, vol. 2003, p. 216, 2003.
3. Y. Chang and M. Mitzenmacher, “Privacy preservation of the keywords searching on remotely encrypted data,” in Applied Cryptography and Network Security, Third International Conference, ACNS 2005, New York, NY, USA, June 7-10, 2005, Proceedings, 2005, pp. 442–455.
4. R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: Improved definitions and efficient constructions,” Journal of Computer Security, vol. 19, no. 5, pp. 895–934, 2011.
5. K. Kurosawa and Y. Ohtaki, “Uc-secure searchable symmetric encryption,” in Financial Cryptography and Data Security - 16th International Conference, FC 2012, Kralendijk, Bonaire, Februray 27-March 2, 2012, Revised Selected Papers, 2012, pp. 285–298.
6. ——, “How to update documents verifiably in a searchable symmetric encryption format,” in Cryptology and Network Security - 12th International Conference, CANS 2013, Paraty, Brazil, November 20-22. 2013. Proceedings, 2013, pp. 309–328.
7. D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Ros¸u, and M. Steiner, “Highly-scalable searchable symmetric encryption with support for boolean queries,” in Advances in Cryptology–CRYPTO 2013, 2013, pp. 353–373.
8. S. R Lenka and B. Nayak, “Enhancement of the Data Security in Cloud Computing using RSA Encryption and MDS algorithm, “ vol. 2, no. 3, pp. 60-64, 2014.
9. C. Bosch, Q. Tang, P. H. Hartel, and W. Jonker, “Selective document ¨ retrieval from encrypted database.” in ISC, 2012, pp. 224–241
10. E. Thambiraja, “A Survey on most common encryption Techniques,” vol. 2 no. 7, pp. 226-233,2012.
11. S. R Masadeh, S. Aljawameh, and N. Turab, “ A comparision of Data Encryption Algorithms with the proposed algorithm: Wireless Security,” pp. 2-6.
12. R. Kaur , “Effective Symmetric key Block Ciphers Technique for Data Security :RUNDAEL,” vol. 3, no. 7, pp. 2005-2008, 2014.
13. P. Kalpana , “ Data Security in cloud computing using RSA algorithm ,” vol. 1, no. 4, pp.143-146, 2012.
14. Yasar, Mustafa, and . 2019. The remember regeneration therapy method: An overview of new therapy protocol to approach diseases. Journal of Complementary Medicine Research, 10 (1), 68-80. doi:10.5455/jcmr.20181229122909
15. Yang, G., Hamacher, J., Gorshkov, B., White, R., Sridhar, S., Verin, A., Chakraborty, T., Lucas, R.The dual role of TNF in pulmonary edema(2010) Journal of Cardiovascular Disease Research, 1 (1), pp. 29-36. DOI: 10.4103/0975-3583.59983

DOI: 10.37200/IJPR/V24I8/PR280117
Received: 21 Jan 2020 | Revised: 08 Feb 2020 | Accepted: 14 Mar 2020