



## Turnitin Originality Report

AES CLOUD by Shobana Thanapal

From Paper (CSE Papers)

Processed on 11-Nov-2014 12:06 PM

SGT

ID: 476202270

Word Count: 1489

Similarity Index

4%

### Similarity by Source

Internet Sources:	3%
Publications:	2%
Student Papers:	1%

### sources:

1

1% match (Internet from 14-Dec-2010)

<http://www.maxwellsci.com/print/rjaset/v2-227-232.pdf>

2

1% match (Internet from 23-Jan-2014)

[http://www.ee.oulu.fi/~vassilis/courses/ubicomp10S/projects/11\\_dropbox.pdf](http://www.ee.oulu.fi/~vassilis/courses/ubicomp10S/projects/11_dropbox.pdf)

3

1% match (Internet from 17-Dec-2012)

[http://dsns.cs.nctu.edu.tw/blog/components/com\\_agora/img/members/9/2-Crypto-doc.pdf](http://dsns.cs.nctu.edu.tw/blog/components/com_agora/img/members/9/2-Crypto-doc.pdf)

4

1% match (publications)

[Ramesh, G., and R. Umarani. "UMARAM: A novel fast encryption algorithm for data security in local area network". 2010 INTERNATIONAL CONFERENCE ON COMMUNICATION CONTROL AND COMPUTING TECHNOLOGIES, 2010.](#)

5

1% match (publications)

[Wang, Y.. "A chaos-based image encryption algorithm with variable control parameters". Chaos, Solitons and Fractals, 20090830](#)

6

< 1% match (publications)

[Jararweh, Yaser, Lo'ai Tawalbeh, Hala Tawalbeh, and Abidalrahman Moh'd. "28 Nanometers FPGAs Support for High Throughput and Low Power Cryptographic Applications". Journal of Advances in Information Technology, 2013.](#)

### paper text:

**1 Research Journal of Applied Sciences, Engineering and Technology**

ISSN: © Maxwell Scientific Organization, 2014 Submitted: Accepted: Published: Enhancement of Cloud Security Using AES 512 Bits T. Shobana Maheswari, S. Kanagaraj and K. Shriram Vasudevan Department of Computer Science and Engineering, Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham University, India Abstract: This project aims at the increasing the security features of cloud environment using AES 512 bits. In cloud computing the valuable information of user is stored in the remote location. It has been accessed through different devices such as mobile, personal computer and

with different types of processor of the machine. Security of data stored in cloud is the major issues for both user and service provider. In existing AES 256 bits is used for security where it includes many rounds of processing and time consuming. In this study we improved the cloud security using AES 512 bits for encrypting and decrypting the data of user in secure manner. Keywords: AES 512 Bits, cloud access, cloud computing, cloud security, cloud storage, network security

**INTRODUCTION** Information on Network is being improved with large amount of data sets that are stored on the distributed cloud network. Security for user data on the cloud is being a great challenge for both service provider and user. In cloud the user share the same resource and access data in the wide network. Providing an important data to the user, security has to be mainly focused. In existing AES 256 bits algorithm is used for encrypting the data, which is less secure and more time for processing. AES 512 bit encryption technique consists of input block of 512 bits and its key size is also 512 bits. It provides high security to the data when compare to AES 256 bits encryption. Files uploaded to the cloud will be stored in encrypted format. When the file is accessed or downloaded by the user it will authenticate the user and provide original text after decrypting it with AES 512 bits algorithm. The process of encryption and decryption has been discussed in this study. The clear cut objective of this research is to increase/enhance the security of the cloud environment using AES 512 bits schema.

**MATERIALS AND METHODS** Information in the cloud is accessed by different kind of end user such as server, application software mobile etc. Cloud computing undergoes a problem in data security. Such problems can be overcome by providing security to the data present in the cloud. Hence there are many algorithms to secure data in cloud. Providing confidentiality and integrity is being a major challenge for cloud user and provider. Thus the cloud storage and usage is show in Fig. 1 (Jain et al., 2014). The cloud architecture is shown in Fig. 2. Integrity: It does with the assurance of the message have not been altered during the time of transmission. Firewall is used to ensure the integrity only by restricting the outside hacker to the cloud. Whereas encrypting the content in file will protect the data from hackers inside the cloud. Confidentiality: To prevent data access from the unauthorized user that can be done through the security protocol, authenticating service and encryption methods. where, AES : Advance Encryption Standard Units : One byte is equal to eight bits Block size is referred to as the collection of 128/256/512 bytes of data. Existing encryption technique: In existing AES 256 bits encryption mechanism is used for the security of data in cloud. The number of rounds determined by key size may be 128,192 or 256 bits. The processing time of number of rounds in AES is more and complex. The encrypted data can be attacked and original text can be retrieved easily because of the 32 bits key size. But whereas in AES 512 bits the key size in more AES 256 bits Hence AES 512 bits is more secure than AES 25 (Jain et al., 2014; Fang et al., 2013). Corresponding Author: T. Shobana Maheswari, Department of Computer Science and Engineering, Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham University, India 1 Fig. 1: Application access cloud storage Fig. 2: Cloud architecture Proposed System: To attain the higher level of security in encrypting data in cloud AES 512 bits can be used. The architecture of AES 512 bits is similar to 128 bits AES the difference between AES 128 and AES 512 is that the key size. AES 512 has a key of the size same as the plain text size. Thus the algorithm provides more security and increases the processing speed. It performs four operations such as s-box

**3substitution, row shifting, column mixing and adding round key**

is used at final step of AES. Hence AES 512 bits mechanism provides security for portable or virtual data storage service to the end user (Open Grid Forum, 2009). Architecture of AES 512: In AES 512 bits plain text and 512 bits key will used to encrypt. It process given plain text block into 10 rounds for obtaining the secured encrypted text (Sanyal and Iyer, 2013).

## 5 Encryption process (Fig. 3) and decryption process (Fig. 4)

has performed by the AES algorithm whenever the file is uploaded and downloaded from the cloud (Selen, 2010). Operations in AES 512 bits: AES includes the following process for encryption process such as (Sanyal and Iyer, 2013). Fig. 3: Fig. 4: Decryption process in AES 512 Fig. 5: AES 256 bit encryption Fig. 6: AES 512 bits encryption Table 1: Characteristics AES 256 Bits AES 512 Bits

Byte substitution:	The input size of 512 bits key which Block size 256 bits 512 bits is same as key size is organized in 64 array of 64 bytes
Key size Differ from key size Same as key size (8*8) as s-box. It is used as look up table for Security Less secure More secure substituting bytes.	Time taken encrypt 128 30-50 sec 20-40 sec bit block Shift row: Shifting of each bytes in the rows of the Processing time More Less No. of rounds 14 10 table obtain after substitution is done in shift row transformation. Mix column: Column of data matrix is multiplied with the predefined matrix. Every individual byte considered as polynomials. The polynomial is expressed in term of GF (2 <sup>n</sup> ) where n = 8. Each column is operated individually and each byte in column is mapped into a new value. Key expansion and rounds: Rounds in AES will generate input

### 4 512 bits key is used to generate the sub key

by ten rounds AES. Thus the sub keys are used to do logical bitwise OR operation with respective bytes after processing of GP (2<sup>n</sup>). The outcome of 10th round in AES will be the encrypted text of 512 bits. Decryption process involves the following operations: • Inverse byte substitution • Inverse row displacement • Inverse column mix • Add round key RESULTS AND DISCUSSION Thus the result shown below shows the encrypted text of AES 256 bits with the key size of 32 bits and AES 512 bits with the key size of 512 bits (Fig. 5 and 6). AES 256 Bits encrypted text: AES 512 encrypted text: The performance analysis of AES 256 bits and AES 512 bits are tabulated below (Table 1): CONCLUSION AES 512 is a modern cryptographic algorithm that can be used for more reliable and secures the data. When it is encrypted and decrypted with AES 512 bits the number of key size is increased it will minimize the rounds of processing. Key size will ensure the security of data. As the size of key in AES 512 is more and it is difficult for the hacker/attacker to retrieve the original text from the cloud. It provides

### 6 high level of security to the data

stored in cloud. ACKNOWLEDGEMENT We thank Amrita University and department of computer science engineering for providing us continuous support and infrastructure to get this project done. REFERENCES Fang, Z., Y. Sun, Y. Sun and J. Yang, 2013. The research of AES algorithm and application in cloud storage system. Proceeding of 2nd International Conferences on Science and Social Research (ICSSR 2013). Jain, R., R. Jejurkar, S. Chopade, S. Vaidya and M. Sanap, 2014. AES algorithm using 512 bit key implementation for secure communication. Int. J. Innovat. Res. Comput. Communi. Eng., 2(3). Open Grid Forum, 2009.

## 2 Cloud Storage for Cloud Computing, Storage Networking Industry Association and the Open Grid Forum.

(White Paper), Retrieved form: [http://ogf.org/Resources/ documents/Cloud Storage For Cloud Computing. pdf](http://ogf.org/Resources/documents/Cloud%20Storage%20For%20Cloud%20Computing.pdf)). Sanyal, S. and P.P. Iyer, 2013. Cloud computing-An approach with modern cryptography. Cornell University Library, arXiv: 1303.1048v1. Selen, D., 2010. Advance encryption standard. Rivier Acad. J., 6(2), Retrieved form: [https:// www.rivier. edu/journal/ROAJ-Fall-2010/J455-Selent-AES.pdf](https://www.rivier.edu/journal/ROAJ-Fall-2010/J455-Selent-AES.pdf). Note: Provide self explanatory caption of Figure 3 and Table 1. Res. J. Appl. Sci. Eng. Technol., Res. J. Appl. Sci. Eng. Technol., Res. J. Appl. Sci. Eng. Technol.,

**1 Res. J. Appl. Sci. Eng. Technol., 2 3**