International Journal for Rapid Research in Engineering Technology & Applied Science
ISSN (Online): 2455-4723
Vol 2 Issue 5 June 2016

Comparison between Different key sizes of AES on cloud computing

[1]Nitin Rajput ,
[1]M.Tech Scholar,
[1]Department of Computer Science & Engineering, Oriental University Indore, India
[1]*nitin17rajput@gmail.com*

Abstract

Cloud security term refers to a broad field that has to do with the protection of data and cloud systems. Cloud security has historical roots that include ciphers, subterfuge, and other practices whose goals were to protect the confidentiality of written messages. In our era, cloud security is generally understood to involve domains that are involved in the security of IT systems as well as with the non-IT processes that are in interaction with IT systems. The objective of cloud security is to protect data as well as cloud systems from unauthorized access, use, disclosure, disruption, modification, or destruction. We will create public cloud using openshift cloud then apply Advanced Encryption Standard algorithm on file, which will store on cloud storage and also calculate encryption and decryption time.

Keywords: Public Cloud, Cloud Security, AES, Open Shift.

1. INTRODUCTION

We define the concept of cloud computing and cloud services, and we introduce layers and types of cloud computing. We discuss the difference between cloud computing and cloud services. New technologies that enabled cloud computing are presented next. We also discuss cloud computing features, standards, and security issues. We introduce the key cloud computing platforms, their vendors, and their offerings. We discuss cloud computing Challenges and the future of cloud computing.

1.1 Properties of Cloud Computing

1.1.1 Elasticity

Cloud elasticity entails continual reconfiguration in network and related controls from the cloud internet ingress through core switches and down to individual virtual machine (VMs) and storage. This amounts to infrastructure shape shifting.

1.1.2 Security

There are profound security implications to performing such dynamic changes to security controls; each one must be orchestrated correctly and performed to successful completion.

1.1.3 Shape-Shifting

This elastic and shape-shifting quality demands a sophisticated management infrastructure that continually reflects both the desired state and the actual state of infrastructure configuration controls along with all resource allocation.

1.2 Foundation for Cloud

In this section, we take a high level look at the underlying technology pieces from which cloud computing infrastructure is built. These can be broadly categorized as follows:

- **Virtualization** allows for server consolidation with great utilization flexibility. For cloud computing, virtualization has great value in rapid commissioning and decommissioning of servers.
- **Software** Enables all aspects of cloud infrastructure management, provisioning, service development, accounting, and security. It critical that cloud infrastructure is able to dynamically enforce policies for separation, isolation, monitoring, and service composition.
- **Service Interfaces** The service interface between the provider and the consumer is a key differentiator for cloud. It represented a contract that enforces the value proposition with SLAs and price items.

2. RELATED WORK

K. Valli Madhvi et. al. [17] investigated the problem of data security in cloud data storage, which is essentially a distributed storage system. To ensure the correctness of users' data in cloud data storage, we proposed an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append. We rely on erasure-correcting code in the file distribution preparation to provide redundancy parity vectors and guarantee the data dependability.

Dhaval Patel et. al. [8] In our system we use trusted computing platform for performing the operation like user authentication, data verification. In our system we use three way protection scheme in which first we use Diffie Hell-man algorithms for key exchange algorithms for the AES encryption algorithms. Digital signature is responsible for the authentication and we use SHA as hashing algorithms for the computing the signature and AES as encryption algorithms. Cloud computing is the apt technology for the last decade

Amandeep Kaur et. al. [13] gives a brief introduction about cloud computing by giving its definition, characteristics of cloud computing, components, types, categorization of cloud services which described Platform as a Service, Infrastructure as a Service and Software as a Service.

3. EXISTING WORK:

3.1 Advanced Encryption Standard (AES) Algorithm

The Advanced Encryption Standard (AES) to replace DES and Triple DES. Its basic features are as follows:

- AES is a block cipher with a block length of 128 bits.
- AES provides three levels of security using three cipher key sizes—128, 192, or 256 bits.
- Number of encryption rounds is related to the size of the cipher key.
  128-bit key 10 rounds
  192-bit key 12 rounds
  256-bit key 14 rounds
- The round key is always 128 bits long irrespective of the cipher key size. AES is a 11on-Feistel cipher.

3.2 Overall Structure of AES

Figure 4.2 shows the structure of AES cipher for 128-bit cipher key. Only the encryption rounds have been shown in the Figure. We will look at the decryption rounds later.

(a) There are ten rounds of encryption for 128-bit cipher key. The structure remains same for other key sizes, except that additional encryption rounds get added.

(b) Key expansion schedule generates eleven 128-bit round keys from the cipher key K. Each round key consists of four words. For example, the first round key is [W0 W1 W2 W3].

(c) Key expansion schedule embeds the scrambling function g which diffuses each bit of the cipher key K into some bits of several round keys. When round keys are added to the state arrays, each bit of the cipher key gets diffused into several bits of the ciphertext block.

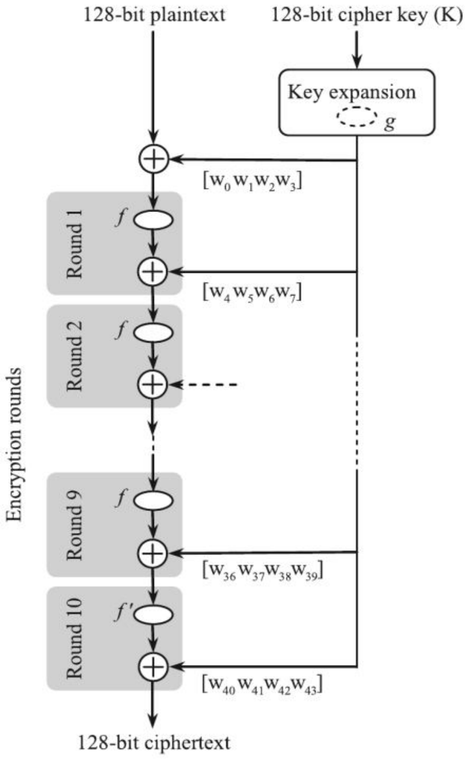

Figure: 4.1 Structure of AES encryption rounds.

Each encryption round consists of transformation of input state using function followed by round key addition. Function f is so designed that each bit of the input state is diffused into several bits at the output. Note that transformation by function f does not require the round key and as such provides no security till round key is added after this transformation.

4. PROPOSED WORK:

AES uses notion of state array and word. A 128-bit data block of 128 bits is depicted as a 4 X 4 square matrix of 16 bytes. The bytes of the block are arranged sequentially co1urrmwise, i.e., the first four bytes occupy the first column. The 4 X 4 matrix of input plaintext undergoes several rounds of encryption to get finally 4 X 4 matrix of output ciphertext. After each round of encryption, the 4 X 4 matrix is called state array or simply state [Figure (a)].

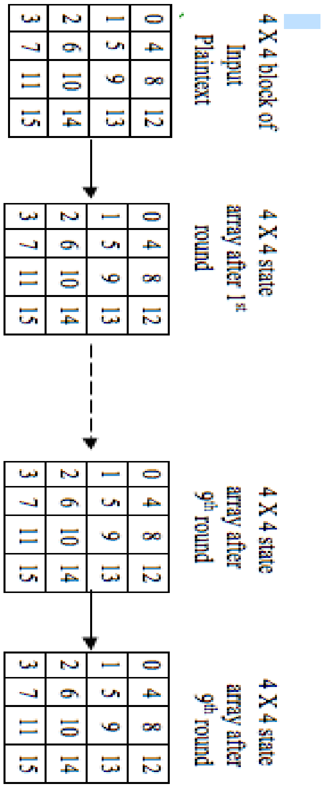
4 X 4 block of Input Plaintext
4 X 4 state array after 1st round
4 X 4 state array after 9th round
4 X 4 state array after 9th round
0 4 8 12
1 5 9 13
2 6 10 14
3 7 11 15

Figure:4.2 128-bit plaintext block, state arrays, ciphertext block

Similarly the 128-bit cipher key is depicted as 4 X 4 square matrix of 16 bytes. This key is expanded into a 44 column matrix [Figure 6.2(b)]. Each column of matrix is referred to as a word. Schedule of 44 columns provides 11 round keys, each consisting of four words, i.e., 16 bytes or 128 bits.

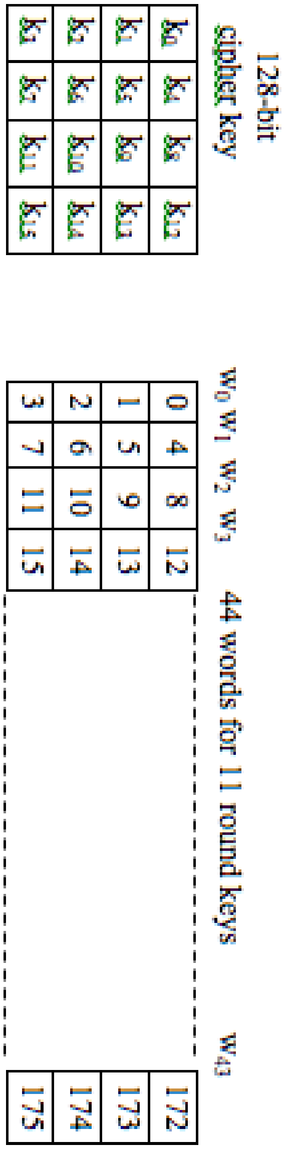

Figure: 4.3 Key expansion in AES

4.1 Encryption Round

Each round of encryption has the following four stages of transformation. The last round is an exception. It does not have Mix Columns transformation stage.

(a) Substitute bytes (Sub Bytes)
(b) Shift rows (Shift Rows)
(c) Mix columns (Mix Columns)
(d) Add round key (Add Round Key)

All these transformations are invertible. The first three stages carry out substitution and permutation at byte and bit levels. The round key as secret parameter is added in the last stage of a round.

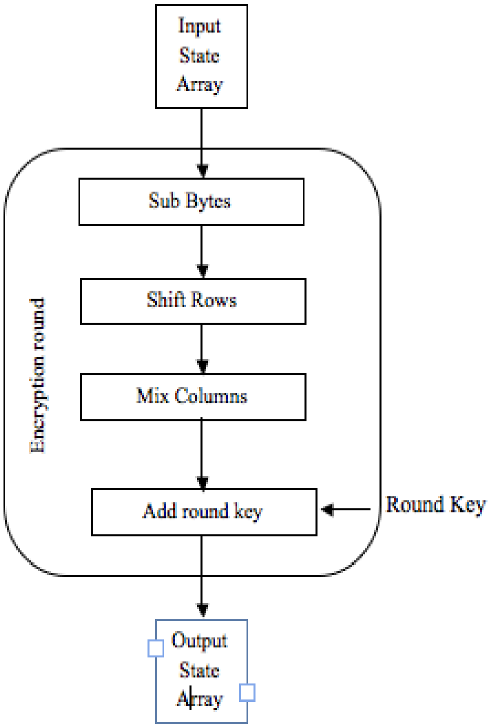

Figure4.3 Composition of an encryption round.

(a) Substitute Bytes (Sub Bytes) Transformation
Each byte b of the input state is transformed into byte b' by a substitution process defined by the following equation:

$$b'=Mb-1 \ + N$$

(b) Mix Columns Transformation (Mix Columns)
After Sub Bytes and Shift Rows transformations, a byte retains its identity as a substituted byte iii a different locatio11 in the state array. Mix columns transformation scrambles the bits of a column of the state array. This transformation involves multiplication of a column 11 by a constant 4 X 4 matrix C. The multiplication is modulo (100011011), i.e., using irreducible polynomial X8 + X4 + X3 + X + 1.

$$v = C \times u \bmod (100011011)$$

$$C=\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$$

4.2 Decryption Round

Each decryption round consists of the following inverse transformations:
(a) Inverse shift rows transformation (Inv Shift Rows)
(b) Inverse substitute bytes transformation (Inv Sub Bytes)
(c) Add round key transformation (Add Round Key)
(d) Inverse Mix columns transformation (Inv Mix Columns)

5. RESULT ANALYSIS:

Results are measured and analyzed on above factors and compared between AES with different key size 128, 192 and 256. Several tables and graphs are shown which can make effective comparison on different views, which strongly confirms the applicability of suggested approach. Graphs and tables are also summarized to clearly understand the results. Totally three tables and three graphs are used for these results evaluations and many more still waiting to be presented with some futuristic research modifications.

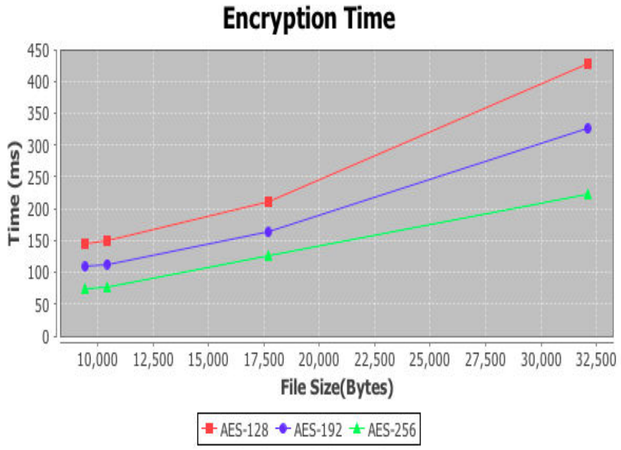

Figure 5.1: Encryption time in AES using 128,192,256 key size

We encrypted the different file with different size using Advance Encryption Algorithm with different key size like 128,192 and 256 and calculate encryption time of each file. We observed that calculated encryption time of AES with key size 128,192 and 256 is increased and gap between times is also increase. AES with 128 is taking More time from 192 and 256 key size.

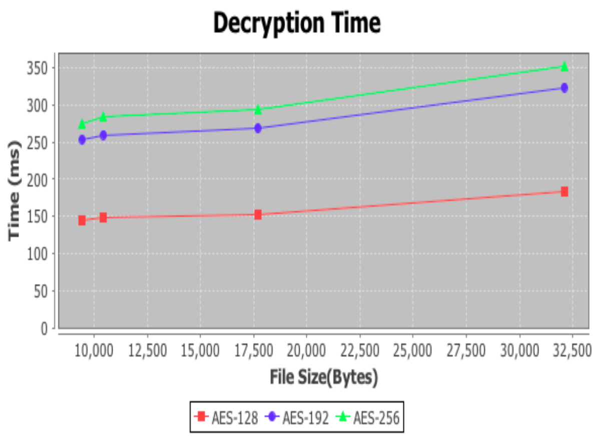

Figure 5.2: Decryption time in AES using 128,192,256 key size

We decrypted the different file with different size using Advance Encryption Algorithm with different key size like 128,192 and 256 and calculate decryption time of each file. We observed that calculated encryption time of AES with key size 128,192 and 256 is decreased. AES with 128 is taking less time from 192 and 256 key size.

6. CONCLUSION:

This paper presenting an algorithm for generating hybrid dimensional association rules mining as a generalization of inter-dimension and Intradimensional rule. The algorithm is based on the concept that the larger number of values/categories in a dimension/attribute means the lower degree of association among the items in the transaction. Moreover, to generalize inter-dimension association and intra-dimensional rules. we measured the following factors for creating our new idea, which are the time and the no of iteration, these factors, are affected by the approach for finding the frequent itemsets. Work has been done to develop an algorithm, which is an improvement over Apriori with using an approach of improved Apriori algorithm for a transactional database.

REFERENCES

[1] Joshi, J.B.D., Gail-Joon Ahn. Security and Privacy Challenges in Cloud Computing Environments. IEEE Security Privacy Magazine, Vol 8, IEEE Computer Society, 2010, p.24-31.

[2] Farzad Sabahi. Cloud Computing Security Threats and Responses. Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference.

[3] Ashish Agarwal, Aparna Agarwal. The Security Risks Associated with Cloud Computing. International Journal of Computer Applications in Engineering Sciences [VOL I, SPECIAL ISSUE ON CNS, JULY 2011] [ISSN: 2231-4946].

[4] Ashutosh Kumar Dubey, Animesh Kumar Dubey, Mayank Namdev, Shiv Shakti Shrivastava. Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment. Software Engineering (CONSEG), CSI Sixth International Conference, Sept. 2012

[5] M.Venkatesh, M.R.Sumalatha, Mr.C.SelvaKumar. Improving Public Auditability, Data Possession in Data Storage Security for Cloud Computing. Recent Trends In Information Technology (ICRTIT), 2012 International Conference, April 2012.

[6] Prashant Rewagad, Yogita Pawar in. Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing. 2013 International Conference on Communication Systems and Network Technologies.

[7] Hai Yan, Zhijie Jerry Shi. Software Implementations of Elliptic Curve Cryptography. Information Technology: New Generations, Third International Conference, April 2006.

[8] W. Diffie and M.E. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, 1976.

[9] Ravi Gharshi, Suresha. Enhancing Security in Cloud Storage using ECC Algorithm. International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064 Volume 2 Issue 7, July 2013.

[10] H. Modares, M. T. Shahgoli, H. Keshavarz, A. Moravejosharieh, R. Salleh. Make a Secure Connection

Using Elliptic Curve Digital Signature. International Journal of Scientific & Engineering Research Volume 3, Issue 9, September-2012 ISSN 2229-5518 IJSER © 2012.

[11] Aqeel Khalique Kuldip Singh Sandeep Sood. Implementation of Elliptic Curve Digital Signature Algorithm. International Journal of Computer Applications (0975 – 8887) Volume 2 – No.2, May 2010

[12] Alfred Menezes, Minghua Qu, Doug Stinson, Yongge Wang. Evaluation of Security Level of Cryptography: ECDSA Signature Scheme. Certicom Research. January 15, 2001.

[13] W. Stallings. Cryptography and Network Security: Principles and Practice. (3rd ed.). Prentice Hall, Upper Saddle River, New Jersey, 2003. [14] Koblitz, N., 1987. Elliptic curve cryptosystems. Mathematics of

[14] Jaishree Singh, Hari Ram, Dr. J. S. Sodhi: Improving Efficiency of Apriori Algorithm Using Transaction Reduction, In proceeding of International Journal of Scientific And Research Publication (IJSRP), ISSN 2250-3153, Volume 3, Issue 1, January 2013,p.p1-4.

[15] Partibha Parikh ,Dinesh Waghela: Comparative Study of Association Rule Mining Algorithms. In: Proceeding of UNIASCIT, ISSN 2250-0987, Vol. 2, Issue 1, 2012, p.p170-172.

[16] Niklas Olofsson :Implementation of the Apriori algorithm for effective item set mining, In Vigi Base TM august 2010,p.p 1-29.

[17] K. Geetha, Sk. Mohiddin: An Efficient Data Mining Technique for Generating Frequent Item Sets, In: Proceeding of IJARCSSE, ISSN 2277-128X, Vol. 3, Issue 4, April 2013,p.p 571-575.

[18] Mamta Dhanda, Sonali Guglani, Gaurav Gupta: Mining Efficient Association rules Through Apriori Algorithm Using Attributes, In: Proceeding of IJCST, ISSN 0876- 8491, Vol. 2, Issue 3, September 2011,p.p342-344.

[19] Suhani Nagpal :Improved Apriori Algorithm Using Logrithmic Decoding and Pruning, In: Proceding of International Journal of Engineering Research and Applications, ISSN 2248-9622, Vol. 2, Issue 3, May-June 2012, pp. 2569-2572.

[20]Djoni Haryadi Setiabudi, Gregorius Satia Budhi, I Wayan Jatu Purnama, Agustinus Noertjahyana, “Data Mining Market Basket Analysis’ Using Hybrid-Dimension Association Rules, Case Study in Minimarket X”, International Conference on Uncertainty Reasoning and Knowledge Engineering, IEEE, 2011.