Computer and Information Science; Vol. 10, No. 3; 2017
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

AES Encryption Algorithm Parallelization in Order to Use Big Data Cloud Naser Attar, Hossein Deldari, Marzie Kalantari

Naser Attar[1], Hossein Deldari[2] & Marzie Kalantari[3]

[1] Masters student, software, salman Institute of Higher Education, mashhad, iran and chief of Company Engineering Parta System, Iran

[2] Head of Department of computer, software, salman Institute of Higher Education, mashhad, Iran

[3] Masters student, software, Azad university of nyshabor, Iran

Correspondence: Naser Attar, Masters student, software, salman Institute of Higher Education, mashhad, iran and chief of Company Engineering Parta System, Iran. E-mail: Naser.Attar@Yahoo.com; hd@um.ac.ir; marzie.kalantari69@gmail.com

Received: January 18, 2017 Accepted: January 28, 2017 Online Published: July 30, 2017

doi:10.5539/cis.v10n3p23 URL: http://doi.org/10.5539/cis.v10n3p23

Abstract

Currently, standard encryption algorithms, such as AES, are used for encryption of data in cloud. As AES algorithm is a low-speed for serial, in addition to solving its low-speed, a Parallel Algorithms is introduced. Regarding the extent of cloud network, the most important feature of the proposed algorithm is its High speed and resistivity against the attacks. The algorithm is designed and implemented in java script in cloudsim environment. The results obtained from implementation of this algorithm in cloud simulating environment, are compared and evaluated relative to the other algorithms. Similar input was fed to the proposed and other algorithms. The proposed algorithm processed the data in 82 ms which is faster than the other algorithm.

Keywords: data, cloud computing, Parallel Algorithms, Parallel AES encryption algorithm, cloudsim

1. Introduction

Cloud computing in a network based environment focuses on sharing the computations and resources. The users pay according to their use of service and they don't have to pay considerable amount of money for management and maintenance.

Cloud computing provides many advantages for the users such as: developed efficiency, less software costs, fast and permanent software update, more compatibility, document format, global access to document and so on. Along with these advantages, there are some concerns.

One of the most important concerns is the extent of safety in the information and protection against unauthorized access (Gowrigolla, 2010; (Cloud Securuty and Privacy TimMather, SubraKumaraswamy, ShahedLatif). Security risks and the risk of privacy rarely occur, however, Cloud computing faces with them. This paper attempts to present a method for security establishment in cloud environment through algorithm. The proposed approach is based on Parallelism of AES Encryption Algorithm, which is different from conventional security schemes and High speed in cloud computing.

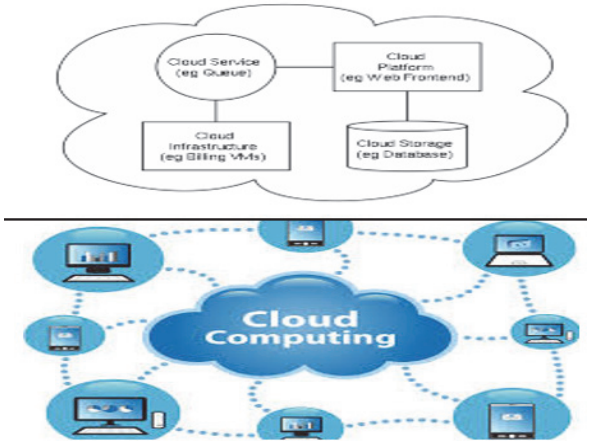

Figure 2. Concept of cloud processing (Narjeet & Gaurav, 2012)

2. Related Works

The studies conducted for improvement of AES encryption algorithm are listed here:

1. In a study with the approach of optimizing the speed of AES algorithm, it was shown that it is possible to enhance the speed by combining subbytes and ShftRows with MixColumns stage and converting them to a sequence of table searching. This requires four 32-bit tables with 256 entries which uses 4 KB memory (Efficient software implementation of AES on 32-bit platforms. Lecture Notes in Computer Science: 2523. 2003). By application of a byte-oriented approach combination of the stages and changing them to a single cycle is possible (http://code.google.com/p/byte-oriented-aes). The problem of this method is its high mempry consumption.
2. In another approach, application of cell machine programing was proposed. In this method, during encryption steps of AES, the mapping operations would be performed via cell automata laws. This leads to production of a complicated encrypted text. The main advantage of this method is its resistivity towards the attacks. Also due to parallelization of the commands, the speed of AES will not reduce. The problem is the attacks made to it (Debasis & Rajiv, 2011).
3. In another study, S-box implementation for decreasing the consumed volume in hardware was addressed. The main goal of this approach is to combine the constant matrices which were used in subByte operation (Canright, 2005).
4. Dynamic parameters were also proposed for improving the security of AES encryption algorithm. In this method the size of the data block and the key would be selected dynamically. This means that the data block and key sizes are not constant and these parameters will be assigned value dynamically during the run process (Fatma, Medien & Adel, 2013). Dynamic parameters will be added to the encrypted text in the form of codes, in this way they could be used in the decoding stage. The main advantage of this approach is that in this way the hacker would always be one step behind as he does not know the algorithm commands would be repeated how many times.
5. In another approach, CBC (Cipher Bock Chaining)was proposed for high security of AES encryption algorithm. The objective of this approach is to chain the encrypted blocks. In this method, each block is encrypted by the main text, key and a third value depending on the previous block. Repeating the encryption which is called chaining, would lead to hiding the repetitive patterns (Mazumdar, 2012). The advantage of this method is its resistivity toward the attacks but it is slow.
6. 256-bit key with 14 round, was proposed for improving the security condition of AES, in another study (Ashima & Simar, 2015). Some attacks were reported to this method.
7. In another research, it was proposed to encrypt the files by a password, prior to their storing in the cloud, and password produces key by AES and the file be encrypted by AES (Debajyoti, Gitesh, Parth, Sagar & Vibha, 2014). The advantage of this method is optimization of speed but due to storing the password in the cloud, there is always the possibility of theft.
8. AES encryption algorithm was proposed for data storing in cloud (Fang, Sun, Sun & Yang, 2013).

9. In another research, AES algorithm with key size of 512 byte and 10 rounds was proposed (Maheswari, Kanagaraj & Vasudevan, 2014). The advantage of this method is its high speed and security. But this method is not suitable for high volume data.

3. Importance of Security in Cloud

Along with the advantages of cloud computing, there are serious challenges about its security. Security and protection of privacy require policies and approaches to lead to trust of user to cloud computing methods. This is the main obstacle in approval of this scheme. Storing and processing of the data in a place other than their own organization, is not acceptable for many organizations and users as they can't insure that the unauthorized people do not have the access to their data. This concern is investigated from to aspect. One, prevention from reading of private data by others (like other customers), which is an obvious concern indicated by theft or other direct destructive operations, the other one is reading of the private data by the service provider, in fact the fundamental challenge is security and protection of privacy (Narjeet & Gaurav, 2012).

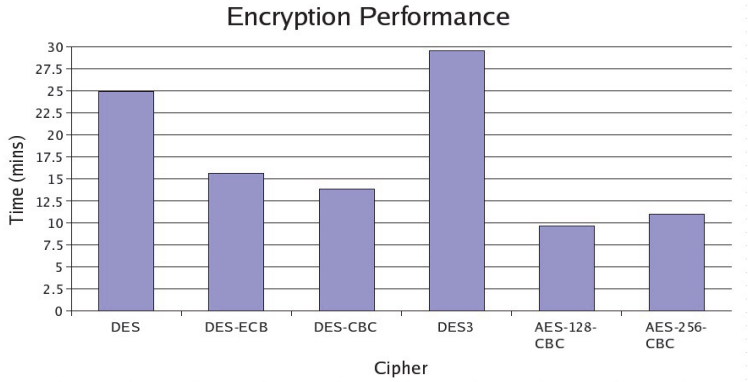

Figure 3. Comparison of the speed of encryption algorithms (Eman, Abdelkader & Sherif, 2013)

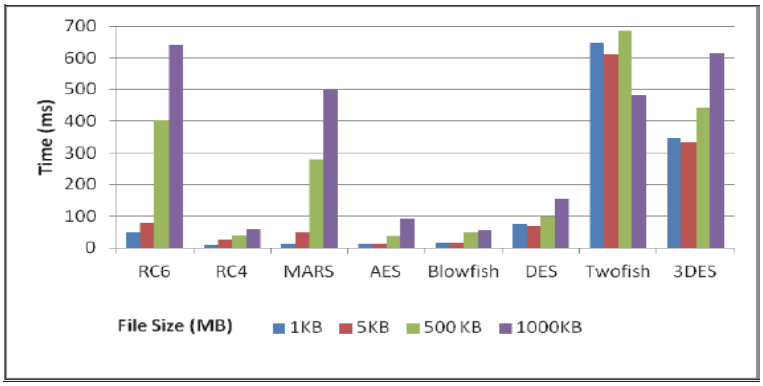

Figure 4. Comparison of the speed of encryption algorithms (Eman, Abdelkader & Sherif, 2013)

4. Proposed Approach

The proposed approach is addressed here. As it was mentioned before, due to parallelization technique and use of piece encryption, AES algorithm is so fast. This means that each piece could be assigned to one processor and the calculation could be done in parallel. In the proposed method, 128-bit AES is used which divides the data into 4 equal pieces and 4 processor perform the calculation in parallel. As the environment is inherently distributed with high data volume, AES is an appropriate algorithm for cloud data. As it can be seen, AES algorithm is faster and more efficient than the other algorithms, so it is an appropriate choice. One of the major concerns of symmetrical algorithms such as AES is sharing of the key. The solution of this paper for key transfer is as follows: they must be transferred physically or the key is divided into several parts and sent by different communicational channels to protect the security of the key.

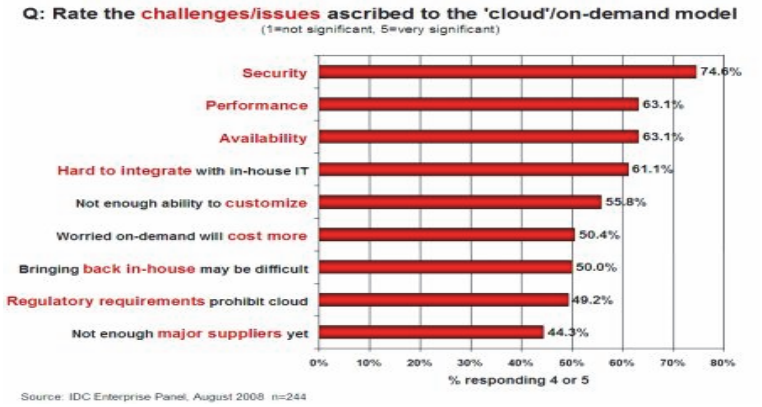

Figure 5. importance of security in cloud (Cloud Securuty and Privacy TimMather, SubraKumaraswamy, ShahedLatif)

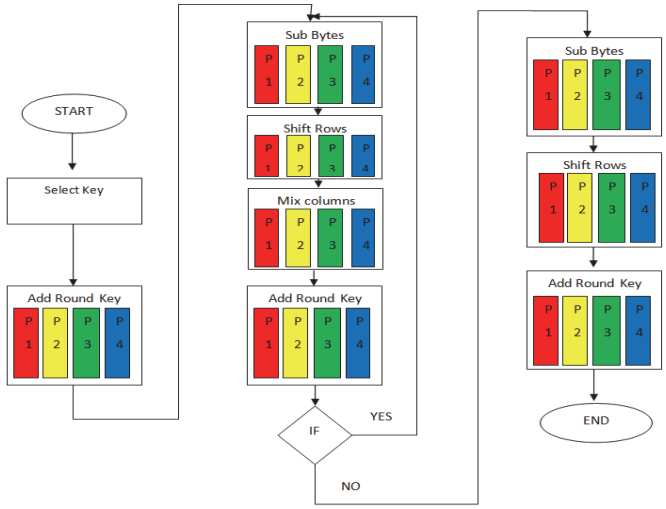

Figure 6. Parallel AES algorithm.

Table 1. Comparison of the speed of Parallel AES algorithm with other algorithms in cloudsim

algorithm	Speed (ms)
Parallel AES	82
Serial AES	146
DES	150
RSA	370

5. Comparing Parallel AES with Previous Algorithms

Proposed algorithm was investigated in previous section. In this section, we want to compare the proposed algorithm with previous encryption algorithm in terms of efficiency and speed. The results are presented in following table.

Table 2. Comparing the efficiency of Parallel AES algorithm with other algorithms

algorithm	efficiency	speed
Parallel AES	High	High
Serial AES	High	Low
DES	High	Low
RSA	Average	Low

It is observed that the proposed algorithm has very good results in all tested criteria.

6. Conclusion

Today, one of the important recommended methods for storing the data is application of cloud computing. But many people still have problem with that and prefer to store their data hard disks, rather than saving them in virtual environments. The main reason is their security concerns. In this regard, cloud computing has not yet convince the users completely. If they succeed in enforcement of their security condition, this method would be the best method for storing the data. One the advantages of cloud computing is the feasibility of access to IT resources. Due to high flexibility and versatile application of this capability, this field has been introduced as a platform for new generation of communication. But due to the security concerns, its application is with errors. Therefore, maybe security issue is the reason for its limited spread. Although data storing in virtual level has provided good capabilities and provided the space costs for users for data storing, but it has not yet succeeded in completely satisfying the users. Many companies and organizations either don't know this technology or even if they relatively know it, the first thing hits there is the vulnerability of the information against attacks. In this paper, cloud environment, the works done in relation with security condition in cloud, encryption algorithm types are investigated.

7. Future Works

As cloud network, is an extensive network of resources and security is also an important challenge, it is proposed to add a layer, called security, to cloud layers to protect the security of cloud services. Also the following recommendations can be presented:

1. Identification of new attacks and presenting solutions in AES encryption algorithm.
2. Identification of threats and damages due to successful attacks.
3. Discovery of security weaknesses in AES encryption algorithm.
4. Investigation of security errors in AES encryption algorithm.
5. Increasing the speed of AES encryption algorithm for its optimized use in cloud.
6. Hardware implementation of AES encryption algorithm for optimal application of cloud sources.

References

Ashima, P., & Simar, P. S. (2015). Cloud Security Algorithms. *International Journal of Security and Its Applications, 9*(10), 353-360.

Ayanzadeh, R., Mousavi, & Azamshahamatnia, E. (2012). Fuzzy cellular Automata Based Random Numbers Generation. Academic Journals inc. ISSN 1819-3579.

Canright, D. (2005). A Very Compact Rijndael S-box," In: Naval Postgraduate School Tech- nical Report: NPS-MA-04-001.

Chen, D. Y., & Zhao, H. (2012). *Data Security and Privacy Protection Issues in Cloud Computing.* 2012 IEEE International Conference on Computer Science and Electronics Engineering.

Cloud Securuty and Privacy TimMather, SubraKumaraswamy, ShahedLatif.

Daemen, J., & Rijmen, V. (1999). Resistance against Implementation Attacks: A Comparitive Study of the AES Proposals" In Second AES Candidates Conf., Mar. 1999, Availableonlineat.

Debajyoti, M., Gitesh, S., Parth, S. G., Sagar, B., Vibha, M., (2014). Enhanced Security for Cloud Storage using File Encryption.

Debasis, D., & Rajiv, M. (2011). Programmable Cellular Automata Based Efficient Parallel AES Encryption Algorithm. *International Journal of Network Security & Its Applications (IJNSA), 3*(6).

Efficient software implementation of AES on 32-bit platforms. Lecture Notes in Computer Science: 2523. 2003

Eman, M., Abdelkader, S., & Sherif, E. (2013). *Data Security Model for Cloud Computing.* The Twelfth International Conference on Networks.

Fang, Z. Y., Sun, Y., Sun, Y. J., & Yang, J. M. (2013). The Reseach of AES algorithm and application in cloud storage system, 2nd International Conference on Science and Social Research.

Fatma, S., Medien, Z., & Adel, B. (2013). An efficient Encryption scheme based on Block Cipher Algorithms, Recent Advances in Telecommunications, Informatics and Educational Technologies. ISBN: 978-1-61804-262-0

Gowrigolla, S. (2010). Masillamani Design and Auditing of Cloud Security 2010, LEEE.

Hardware Implementation of AES Algorithm, Marko Mali, Franc Novak, Anton Biasizzo.

Maheswari, T. S., Kanagaraj, S., & Vasudevan, S. K. (2014). Enhancement of Cloud Security Using AES 512 Bits. *Research Journal of Applied Sciences, Engineering and Technology, 8*(20), 2116-2120.

Manavski, S. A. (2007). *CUDA Compatible GPU As an Efficient Hardware Accelerator for AES ryptography.* In Proceedings of IEEE International Conference on Signal Processing and Communication (ICSPC 2007), Dubai, United Arab Emirates, 65–68.

Mangard, S. (2004). Securing Implementations of Block Ciphers against Side-Channel Attacks, Ph.D. Thesis, Institute for Applied Information Processing and Communications (IAIK), Graz University of Technology, Austria.

Mangard, S., Oswald, E., & Popp, T. (2007). Power Analysis Attacks: Revealing the Secrets of Smart Cards, Springer – Verlag.

Mazumdar, B. (2012). Design for Security of Block Cipher S-Boxes to Resist Differential Power Attacks, International Conference on VLSI Design (VLSID), 7-11.

Narjeet, S., & Gaurav, R. (2012). Security on BCCP through AES Encryption Technique. International Journal of Engineering Science & Advanced Technology.

Narjeet, S., & Gaurav, R. (2012). Security on BCCP through AES Encryption Technique. *2012 International Journal of Engineering Science & Advanced Technology.*

National Institute of Science and Technology. (2011). The NIST Definition of Cloud Computing, p7. Retrieved July 24 2011.