ACSIJ Advances in Computer Science: an International Journal, Vol. 5, Issue 2, No.20 , March 2016
ISSN : 2322-5157
www.ACSIJ.org

ACSIJ
WWW.ACSIJ.ORG

Enhancing Data Security in the Cloud Using the Proposed Algorithm

Naser Attar
Parta System Company, Mashhad, Iran
Naser.Attar@Yahoo.com

Abstract

The distinctive advantages of the clouds have attracted the attention of many organizations, but the aspect leading to hesitation of these organizations is the method used for securing the data in the clouds and insuring about the security of the environment. By entrance of computers to human life and its development, the security has always been an issue. In this content, various schemes have been applied for security maintenance one of which is application of proper algorithm for encryption of data. Currently, standard encryption algorithms, such as WER, are used for encryption of data in cloud. As WER algorithm has been the subject of some attacks, in addition to solving its problems, a new algorithm is introduced. Regarding the extent of cloud network, the most important feature of the proposed algorithm is its resistivity against the attacks. The algorithm is designed and implemented in java script in cloudsim environment.

Keywords: *data security; cloud computing security; encryption algorithm; 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 [1,2]. 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 proposed algorithm. The proposed approach is based on development of AES Encryption Algorithm, which is different from conventional security schemes in cloud computing. In continue, the second section expresses the works in relation with security in cloud and development of AES Encryption Algorithm. Third section explains the importance of security in cloud, while forth section provides the description of different types of attacks. The proposed approach is presented in section five and it is compared with previous methods in section six. Finally, the conclusion and future works is presented.

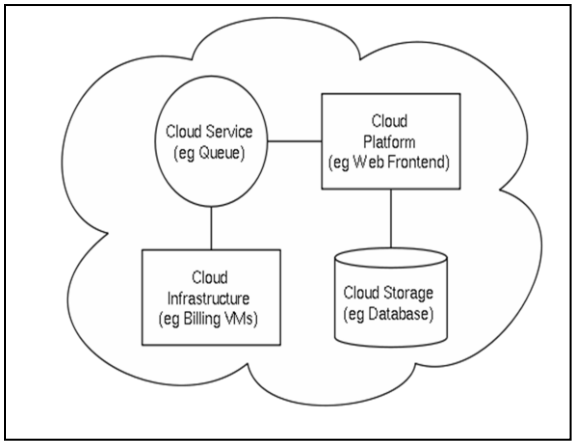

Figure 1. a diagram under cloud processing [3]

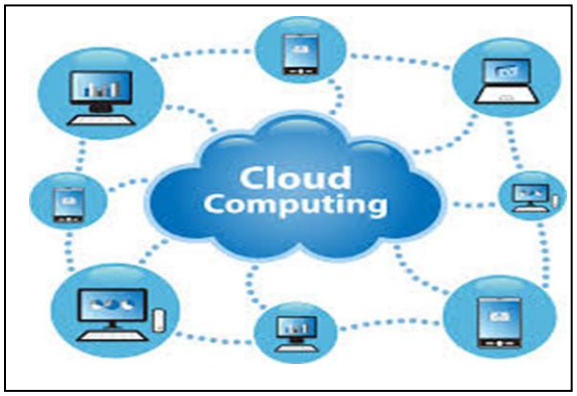

Figure 2. concept of cloud processing[4]

2. RELATED WORKS

As security is one of the most important challenges in clouds, methods and approaches have been presented which are addressed in following section.

2.1 intrusion detection system

Intrusion detection is a method preventing from unauthorized intrusion and prohibits unauthorized access to cloud resources. In fact, intrusion detection system completes firewall whose main goal is identification of destructors [5]. Below, a sample of intrusion detection system is presented.

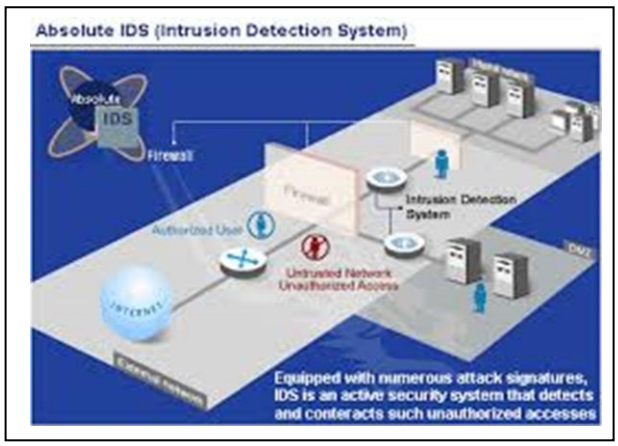

Figure 3. intrusion detection system [5]

2.2 security policies in clouds

Security policy is in fact management of security risks in cloud which could include employment of expert security team, management and recovering f vulnerabilities and updating the software packages and operating systems and use of safe connections [5].

2.3 application of encryption algorithm

Encryption algorithms vary a lot, but only a few numbers of them have been standardized. Encryption is the knowledge of investigation and recognition of principles and methods of transform or saving the data safely. DES algorithm was introduced in 70s in USA as a standard encryption method [5]. This algorithm gets strings of the main text with a fixed length as the input and after doing some complicated tasks, produces the output with the length equal with the input length. This algorithm also uses a key for creation of the code and those who know the key cloud decode the data. Although some analysis have been done on DES, but the most applicable attack against this algorithm is exhaustive key search attack. AES algorithm was recognized as a standard encryption method in 2001. This algorithm uses a new structure. This algorithm is secure against the exhaustive key search and is also faster than DES. This algorithm uses 128-bit blocks and 256/192/128 key size. AES algorithm comprises 4 main stages: the first step is the simple substitution of each bite, second, the lines would be shifted, the first line does not change, the second line undergoes a rotational shift equal to 1-bit shift toward left, the third line would face to a 2-bit shift toward left while the fourth line would have a 3-bit shift toward left side. Decoding, this stage includes the same amount of shift to the right side. At the next step, the columns will be mixed in which each column will be processed individually. At the final stage, the status matrix will be XOR via the key. In this way, at each step the key will be developed. AES algorithm is very fast, and as it applies the iterative operations, parallelization is possible. Also, since the environment is inherently a distributed environment with high volume of data, AES algorithm is suitable for cloud data; however, attacks such as side channel have been reported [6, 7].

RAC algorithm is another encryption algorithm whose main idea is creation of several general keys and random selection of one. This will be combined with special key and the main key would be created. Then the key will be XOR by text, and then by checking the left side bytes of the text, the code would be produced, the XOR step will be repeated. But this algorithm has also be the subject of some attacks. Other algorithms such as BLOWFISH, RC6, MARS and the like were also used, but they were also attacked. Among the mentioned algorithms, AES has the optimized efficiency, speed and security. The below figures, illustrate the superiority of AES over other methods.

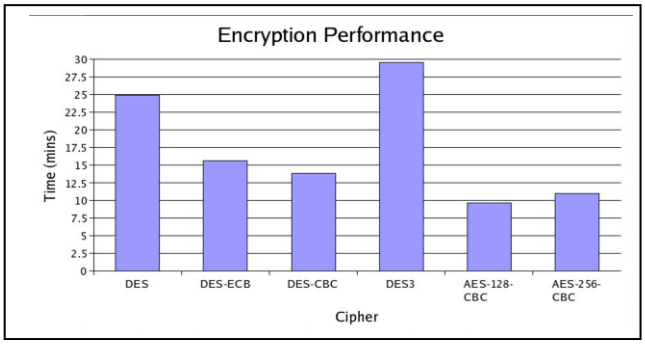

Figure 4. comparison of the speed of encryption algorithms [8]

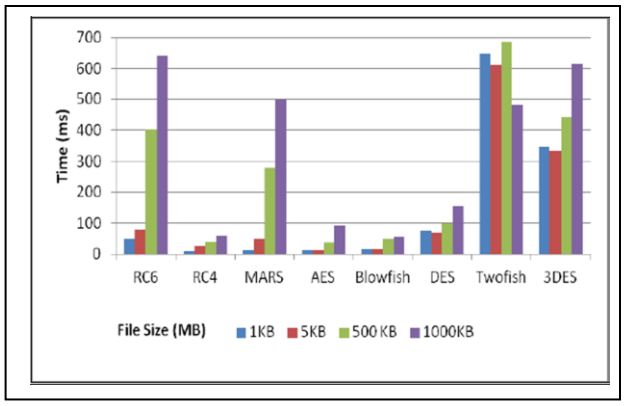

Figure5. comparison of the speed of encryption algorithms [8]

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.

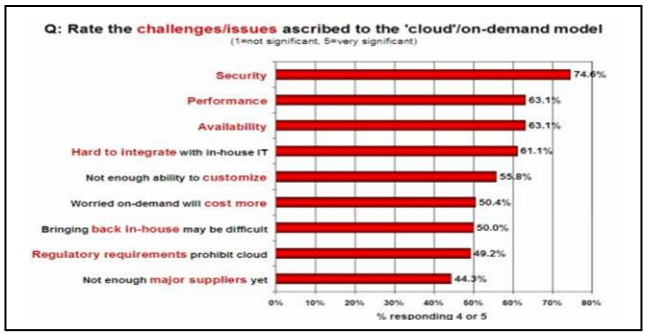

Figure 6. importance of security in cloud [2]

4. ATTACK TYPE

4.1 exhaustive key search attack

This attack is made by having several pairs of the encrypted and main text corresponding to that. This includes testing of all 2m possible key for finding the main key of encryption which is the series key [9,10].

4.2 Complementarity attack

This attack is arisen from Complementarity property. In fact, if X and Y are to binary with the length of n and X+Y=(1,…,1), then two vectors are their Complementarity and we have Y-X′
Now if f is indicative function of code piece and C=f(P,K), then the code has complementarity property if: $\forall P, \forall K$ $f(P',K')=C'$
Now if the key environment of k id divided to two sub-environments of S and S′ where $K=S \cup S$ then the exhaustive key search attack could only be applied in S [10].

4.3 attacks due to being closed

For each piece of code with length of n and a key with length of m, each key indicates a displacement function of binary vectors with length of n. if G shows the series of all these 2m displacements and we have:
H={ Ti*Tj : Ti ,Tj∈G }, and * is the symbol of mapping combinations, then G is closed if H=G in fact, G is closed if for each Ti and Tj in G it is possible to find a Tk in a way that for all the main text we have:
(Ti*Tj)(P) = Tk(P)
But as one of the common methods to increase the security of piece codes id successive encryption of each piece, the code property of being closed, will destroy the repetitive trend and the security will deteriorate. The rest of the attacks on piece codes such as middle meet attack, attacks due to offini property and the like revealed the undesirable properties of piece codes. However, the best and the most effective analyses on this type of codes are linear or deferential attacks which are among the most powerful second and third type attacks on these codes. Therefore, the safety of the piece codes depends on its resistivity toward these two types of attacks. In fact, the main criteria in design of the piece codes is their resistivity toward these types of attacks and the other attacks designed based on the condition of the analyzer and its awareness, and the analysis mentioned in the beginning are applied as the required condition of the design [11,12].

5. PROPOSED APPROACH

The proposed approach is addressed here. The objective is the development and creation of a new algorithm by implication of some changes in the initial key of AES encryption algorithm. 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. However, attacks such as side channels were reported. As it can be seen, AES algorithm is faster and more efficient than the other algorithms, so it is an appropriate choice. Now this proposed model attempts to optimize the security and create a complicated initial key. Stronger the key of the algorithm, more effort is needed to hack. The proposed model also shows that by the changes in AES algorithm and application of parallelization techniques, the speed would remain constant. 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. For construction of the initial key of AES algorithm, two methods from cellular automata along with phase operators were used. The reason for application of phase operators is solving the problem arisen from algebraic and mathematical definitions and production of more precise key [13]. By application of binary cellular automata, several keys will be created and one will be selected randomly. This can be used as the key in AES encryption algorithm. Due to application of phase operators, a more precise and non-repetitive key would be created.

In the proposed method, by application of cellular automata 90 law and substitution of boolean operators with phase operators, the phase 90 law is created. The cellular automata 90 law could be considered as:

a'b'c+a'bc+ab'c'+abc'

Reports and experiments show that by application of the phase laws, the uniform random numbers with desirable quality are obtainable [13]. The possibility of implication of this method in parallel and its high speed along with its desirable quality are among the distinctive features of this method. In the proposed model, the initial key of AES encryption algorithm must be developed by use of cellular automata and phase operator. The reason of application of cellular automata is its high speed and possibility of parallelization and the reason behind the use of phase operators is its accuracy and uniformly distributed random numbers. The mechanism of proposed algorithm is as follows: by application of cellular automata and phase operator several keys are created. In the next step, one key is randomly selected and the rest of steps are like AES algorithm. The decoding operations are not changed and use the same AES algorithm. Regarding these added properties, proposed algorithm resolves the problems and bugs of AES algorithm which makes it an appropriate algorithm in distributed environment of cloud. In fact, proposed algorithm is the same as AES algorithm with this difference that it produces more complicated keys to be more resistant against attacks. As we know, one of the main parts of all algorithms is encryption of their keys. In the proposed model, the key of AES is constructed more resistant and reliable. One of the advantages of proposed encryption algorithm is its speed and efficiency which is inherited from AES algorithm. proposed algorithm can be used in parallel in cloud environment with huge amount of data. The implementation steps of proposed algorithm is as follows: first, by application of cellular automata and phase operation (FAC[1]), several words will be produced. In the next step, one key is randomly selected as the initial key of proposed algorithm, then encryption stages will be started (figure 7).

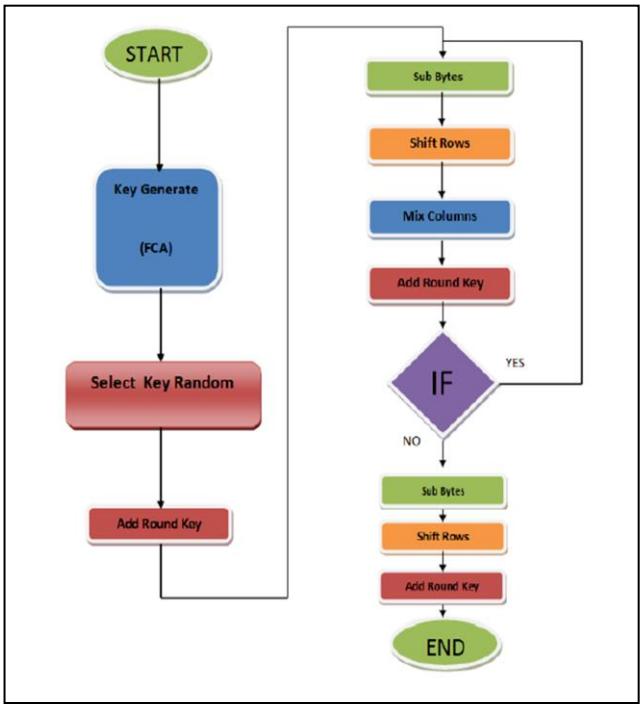

Figure 7. proposed algorithm

[1] Fuzzy Cellular Automata

As it was mentioned before, one of the advantages of the proposed algorithm is its high speed due to use of parallelization technique. Figure 8 shows the number of processors in each step. Due to large numbers of communications between the processors, shift rows stage is implemented in series.

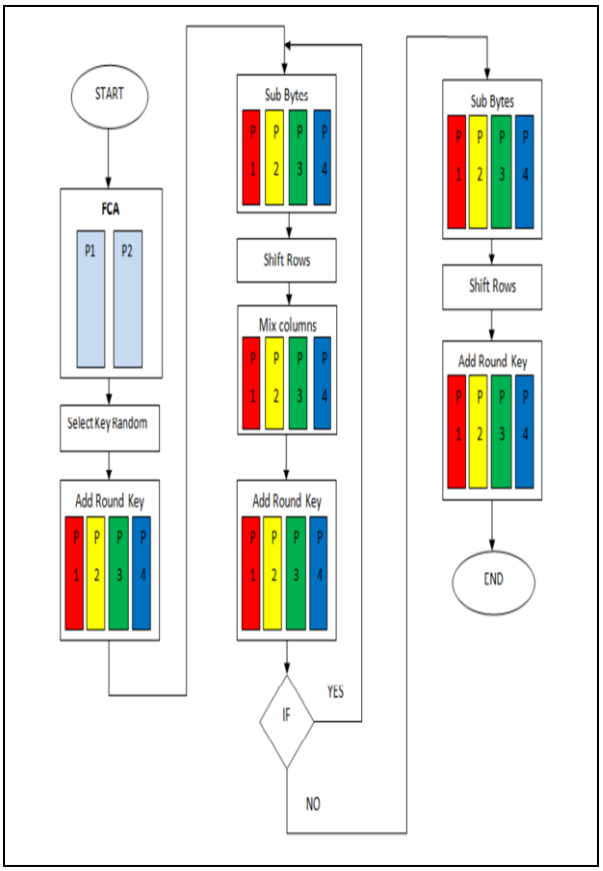

Figure 8. proposed algorithm implemented in parallel

The experiments showed that by addition of phase operators, the efficiency and speed of the algorithm remained unchanged. Because cellular automata random producer and phase logic have the capability to be performed in parallel, therefore, in addition to retaining the algorithm efficiency, its strength against the attacks is improved. By employment of cloudsim simulator, proposed algorithm was tested on several virtual servers and it was proved that the efficiency and speed of the proposed algorithm remained unchanged. Below figure, indicates that.

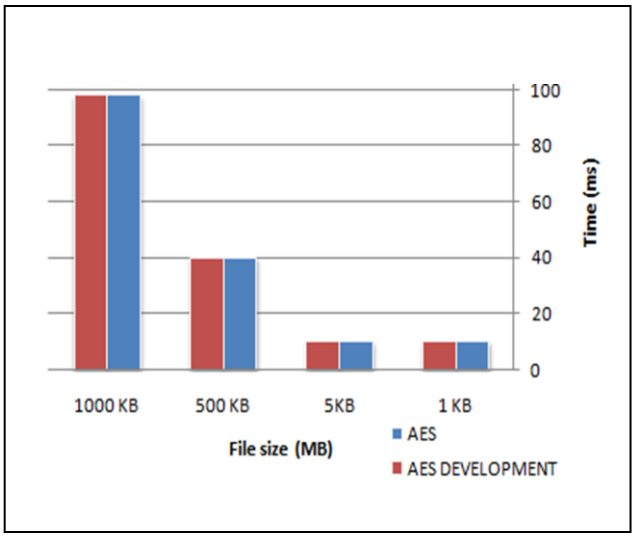

Figure 9. keeping the speed constant in proposed algorithm

Table 1. comparison of the speed of proposed algorithm with other algorithms in cloudsim

algorithm	Speed (ms)	Resistivity against attacks
AES DEVELOPMENT	98	Yes
AES	98	No
DES	150	No
RSA	370	No

Some attacks were imposed on proposed algorithm by use of picklock software. The results showed that proposed algorithm is resistant against attacks. Following figure indicates this issue.

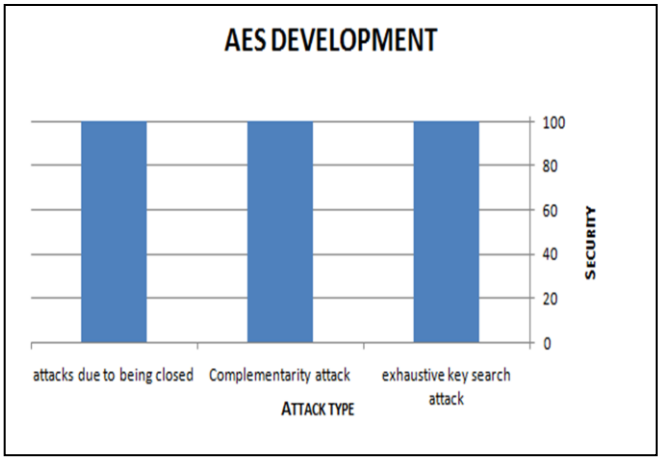

Figure 10. testing proposed algorithm against attacks

As it is clear in figure, proposed algorithm is resistant against attacks and it can be used for protecting the data in cloud.

6. COMPARING PROPOSED ALGORITHM 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, speed and different types of attacks. The results are presented in following table.

Table 2. comparing the efficiency of proposed algorithm with other algorithms

algorithm	efficiency	speed	Attacks
AES DEVELOPMENT	High	High	Resistant
AES	High	High	No resistivity
DES	High	Low	No resistivity
RSA	Average	Low	No resistivity

It is observed that the proposed algorithm has very good results in all tested criteria. proposed algorithm was individually compared with previous algorithms in terms of attacks the obtained results are shown in figure 11.

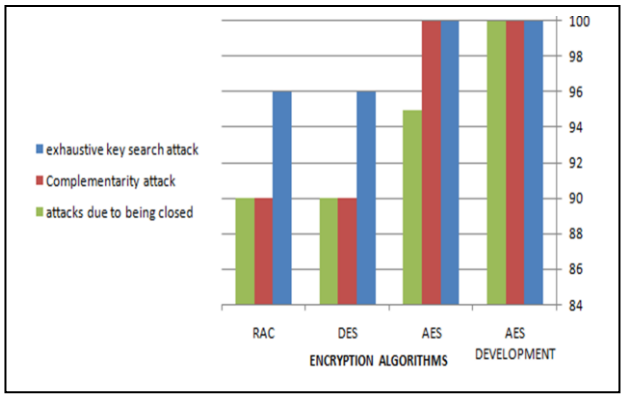

Figure 11.comparing proposed algorithm with the other algorithms.

The obtained results proved that the proposed algorithm can be a good method for protecting the data.

7. 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 and different types of attacks are investigated. After investigation of these methods, a new approach was presented vi development of standard AES encryption algorithm and application of cellular automata along with phase operator, which is entitled as proposed algorithm. This algorithm, which is different from previously presented algorithm, could strengthen the key of AES algorithm by help of phase operators and cellular automata. The results show that proposed algorithm is resistant against different types of attacks. In addition, its speed remains that same. The proposed method reveals that it has optimized speed and resistivity, when compared with other algorithms.

8. 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.

REFERENCES

[1] Gowrigolla,S.,Masillamani,M.(2010). Design and Auditing of Cloud Security,LEEE.
[2] TimMather,M.,SubraKumaraswamy,K and ShahedLatif,l.Cloud Securuty and Privacy
[3] National Institute of Science and Technology(2011)."The NIST Definition of Cloud Computing".p.7.
[4] Narjeet S.,Gaurav, R.,(2012). "Security on BCCP through AES Encryption Technique" .International Journal of Engineering Science & Advanced Technology.
[5] Marko,M.,Franc,N .Hardware Implementation Of AES Algorithm.
[6] Narjeet, S. , Gaurav R,.(2012). "Security on BCCP through AES Encryption Technique" . International Journal of Engineering Science & Advanced Technology
[7] 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, November. 2007, pp.65–68.
[8] Eman.M,Abdelkader.S,Sherif,.E.(2013). Data Security Model for Cloud Computing , The Twelfth International Conference on Networks

[9] Deyan,C., Hong Z.(2012).“Data Security and Privacy Protection Issues in Cloud Computing”. IEEE International Conference on Computer Science and Electronics Engineering.
[10] 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.
[11] Mangard, S., Oswald, E.,and Popp T.,(2007). Power Analysis Attacks: Revealing the Secrets of Smart Cards, Springer – Verlag.
[12]Daemen,J.Rijmen,V.(1999).“Resistance against Implementation Attacks: A Comparitive Study of the AES Proposals ” In Second AES Candidates Conf.
[13] Ayanzadeh,R,Mousavi,Azamshahamatnia,e,. (2012).Fuzzy cellular Automata Based Random Numbers Generation , Academic Journals inc , ISSN 1819-3579.

Naser Attar : Chief of Company Engineering Parta System, Has a master's degree from Mashhad, Iran And has six paper in cloud security and Professional programmer with .NET.