Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/13S141

Improving Security In Cloud By Key Enhancement In Advanced Encryption Standard Using Particle Swarm Optimization

*Venkata Koti Reddy. G *, Srihari. K and Karthik. S*

Department of Computer Science and Engineering, SNS College of Technology, Tamil Nadu, India.

Received: 3 Nov. 2018, Revised: 4 Jan. 2019, Accepted: 5 Mar. 2019
Published online: 1 Oct. 2019

Abstract: Cloud computing is an internet based service to provide the database storage, applications sharing and utilization of the IT resources for either by pay or at a free cost. When the services are at free cost the access to the resources are in a limited manner. The reason behind the development of cloud computing technology is to easy access of all resources with less cost. This technology is classified based on the service and architecture. Based on architecture, the cloud computing is classified as a private, public, hybrid and community cloud. Based on the services, it is classified as Infrastructure as a Service, platform as a Service and software as a service. A private cloud is one in which all infrastructures and the designed group accesses resources. The resources, which are common for all, and access based on money is called public cloud. Hybrid cloud is the one in which uses the private cloud for storage and public cloud for maintenance during high demand. In IaaS the third party for access provides the resources to the customers over the internet. The application and tools are developed by the third party host and provide as a service to the customer is PaaS. In SaaS the software model is used for the access. In cloud, a variety of data is stored such as the personal information, official data and other high confidential data. In such cases, the data integrity is an important one, the data is preserved by employing the security to the data in the cloud. The security is provided by encrypting the information before and after the process in the cloud. The encryption provides the user for its own information control and prevent from the third party access. In general, encryption methods are AES, RSA or blowfish is employed. In this paper, the AES encryption is improved by changing the key based on the input of the user using PSO algorithm. Here this type of AES-PSO encryption protects the users from third party access, because the key is changing one hence the data cannot be easily cracked by the malicious users.

Keywords: Cloud architecture, Services, Data protection, Encryption, PSO and AES

1 Introduction

Data integrity is important in all the aspects of communication. Especially, in the cloud the data preserving is an important one because it stores all the types of information from personal to confidential ones. In that scenario, the data is protected by employing security techniques to the cloud before and after passing services to the cloud. Fernandes, D et al., [1] presented an overview about the cloud architectures, types of services, types of providers based on each layer or service. The types of security issues occur in all services and infrastructures. It addressed about all types of threats based on the infrastructure, platforms, service and client side. The solutions and its integrity capacity provided by various researcher's for all the threats.

Particle Swarm Optimization (PSO) is one of machine learning models [2,3]. Sreelaja and Vijayalakshmi (2009) [4] proposed a technique for improving encryption by using the key generated by PSO algorithm in stream cipher encryption method called as PSO Key Generation Algorithm (PKGA). PKGA employed PSO for the Generation of keys and it is XOR operation takes place with the plain text to form a cipher text. This technique overcomes the drawback of other stream cipher and ACO algorithm. The security of the PKGA is still facing a problem because the key is based on the character encode table and the cipher text is formed through XOR operation. Daemaen, and Rijmen [6]. Here the advanced encryption standard concept is introduced to improve the data security by encrypting and decrypting the data in the

* Corresponding author e-mail: venkatakotireddyphd@gmail.com

form of blocks by symmetric keys. The key is a common one so which can be hacked by the third party users but the operation to produce a cipher text is processed in the form of blocks. V Surya, et al., [22] has proposed the AES algorithm for cloud security. Here the owner accesses the cloud storage with a fixed verification key and the third party cannot access without the key. The drawback in this method is that the user assigns the security key once in the cloud unit, since if third party may know the key. Therefore, the proposed enhancement in AES is the automatic key generation technique and it gives more security for the cloud data. The multi-cloud server is secured by using AES and MD5 encryption method [25]. The traditional AES algorithm is applicable for cloud storage [23].

These two concepts PKGA and AES give the motivation to develop an encryption algorithm, which provides the client with high data security, as well as to prevent from the hackers. To beat the drawbacks of both the techniques, a new concept is introduced PSO based AES encryption in this paper. The reason behind choosing the AES algorithm is that it is mostly used for messaging apps and social media content. Therefore, when the AES is improved it provides security to dual purposed one is for the data in cloud and for the other platforms where this type of encryption is applies. The PSO based AES algorithm is used for enhancing the security approach.

The objective of this paper is to provide the security to the cloud customers by preserving the data integrity and protecting from hacking. The PSO-AES key generation is depends on the user data. Therefore, the reliable of data will achieve by introducing the key generated using PSO and safety of data will accomplish by block encryption procedure in AES. The paper is organised in the form of stating various methods to provide security in the cloud, working of the proposed method, results and to conclude the paper based on the results. Section II describes the literature review related to this method. Section III is the existing method of AES in cloud storage. Section IV is the proposed methodology. Section V is the evaluation result analysis of key retrieval process and cloud storage unit. Finally, the paper is concluded in section VI.

2 Literature Survey

Dogra and Sharma [7] proposed a PSO based optimization of AES and Blowfish encryption. The suggestions given by this paper, the key will be generated through the ECDH algorithm and encrypted by both AES and Blowfish methods. The particle swarm optimization is used for the decision of cipher text. The experimental works are not carried out and only the text file is considered for the processing. Due to the two-encryption algorithms, the workload will be increased.

Gupta, et al., [8] proposed a multilevel encryption for the data security in the cloud. In this, the two level of encryption takes place on the data 1. Blow fish encryption and 2. AES encryption. Similarly, the decryption process is a reverse of it. The method will enhance the security but the blowfish algorithm operates on 64-bits basis, which is not suitable for large data. As well as the user has to remind the three keys to decrypt the data. The computational time will increase for larger datasets and complexity will also increase.

The security of the cloud is improved by using AES algorithm for the encryption of data in the cloud by Sachdev and Bhansali [9]. In this, the advanced encryption standard is employed for the data preserving and the results were best in terms of execution when compared to the other algorithms like DES, Triple DES and RC2. The implementation of AES on images instead of text requires less time compared to RC4, blowfish and RC6.

Subashini and Kavitha [10] explained about the service models and the security issues in that service. The security problems in SaaS data related issues, security in the web application, etc. In PaaS the provider has to be strong in terms of data leakage when the intrusion occurs between the host and the application. In IaaS the data is passed through various third party infrastructures so, the data has to be sent with good encryption policies and routing protocol to reach the receiver. Here the survey of security cloud is described with various related works. Tsai et al., [11] proposed a four-tier framework for improving the web application security. Open grid forum gives instructions about the infrastructure details for the cloud storage. Brindha and Shaji [13] explained about the security based on the cloud infrastructures. Almorsy, M et al., [15] also addressed the security issues in cloud services.

Brindha and Shaji [12] proposed a secured method for the fetching of data from the cloud using conditional Source Encryption based Data Transactional Security. In this the request from the client is processed as conditional attributes and it is encrypted before searching in the cloud through the CSEDTS algorithm and mapping the process using bilinear function for transaction. While retrieving the data the decryption process is performed to decode the value from the cloud. In this the request alone is encrypted not the data in the cloud is considered as an encrypted environment.

D'souza and Panchal [19] designed a hybrid approach for the improvement of AES algorithm. The key for cipher text creation is prepared by the logging time of the user and this key is synchronized with the receiver side for the decryption process. The S-Box and inverse S-Box is updated based on the key. Due to this dynamic nature of key and S-box, the AES encrypting nature is improved.

V Surya., et al., [22] has proposed the secured cloud storage system using AES encryption method. 128-bit AES is used for data security and its confidentiality. Here the AES is used for encrypting the data and short message service for the alert mechanism to avoid the third party access. The drawback in this method is in the key retrieval process. The verification key is fixed in the database and

only the owner accesses it. This may theft by unauthorised/third party. Since the proposed methodology uses an automatic key generation AES technique.

Smitha Nisha Mendonca [24] has proposed the secured cloud storage, which is protected by Advanced Encryption Standard Algorithm. Here the general AES algorithm is proposed for providing the security to the cloud storage and it is the most widely used symmetric cryptographic algorithm. Some data security issues are occurred in cloud computing that is data protection, data integrity, data location and relocation, data availability, and identity management. While transmitting the data through the cloud service, the cloud service provider offers the better service for transmission. Before the transmission process, the uploaded data is encrypted using AES and sent to the next resource. If the receiver needs requisition for accessing the data, the decryption process is performed. Both this encryption and decryption use verification key for protecting the cloud data.

Schneier [14] proposed a 64-bit block cipher algorithm called blowfish to encrypt the data through symmetric key approach. In this, the key can be expand to 448 bits and the data is processed of 64- bits as a block. It encrypts the data through the 16 round feistel cipher network. The cryptography and network security algorithm uses feistel-cipher network structure. The drawback of this algorithm is not suitable for the larger data. Sometimes, the key may be asymmetric.

Zhao et al., [16], propose a homomorphic encryption for the improvement for data security in the cloud. This encryption process is applied from the starting query from the client to the retrieval of the data. A homomorphic encryption is based on the additive and multiplication processes of the data with a key. Hence, when the data is of large size, the complexity of encryption increases and the key is leaked, it can easily decode because of simple additions for encrypting. This homomorphics is used for allowing the data to encrypt based on its function.

Bih-Hwang Lee, et al., [21] has proposed the data security system using AES algorithm in HEROKU Cloud environment. The data security protection uses cryptography algorithm for handling the cloud storage. Here the HEROKU cloud is the container system for integrating the data services. The AES security algorithm performs the first stage of selecting substitute bytes, shifting the rows of S-Box and adding the round key. The HEROKU cloud environment is the PaaS cloud service. Here the data is viewed as a symbol not as an exact text.

Samarati et al., [17] discussed the security issues on the cloud based on three types that are confidentiality, integrity and availability. The issues discussed in this are to protect the data when it is not in used condition, securing the query and user details through encryption techniques. Limit the access to the data by authorized owner, execute necessary operations to fetch the data, provide the secured feel between the users in the shared environment. An agreement and auditing is to provide by the cloud owner for the data privacy. Goyal [18] also discussed about the security issues of cloud model and services.

Namitha N.Pathak, and Meghana Nagori. [25] has proposed the secured multi-cloud stage system. This method uses AES algorithm and MD5 method. Here the verification is done for two cloud servers. Here the verification key is generated with round key process and add round key. The substitute bytes are (S-Box) shifted and mixed for encrypting the data. Here the MD5 is the encryption algorithm and it performs hashing to the verification key. The general frame work is designed and discussed about the AES and MD5 encryption.

Ramgovind et al., [20] discussed how the cloud security can be managed through cloud governance, cloud transparency and cloud security impact. The paper first gives an overview about the cloud model, services in the cloud and security issues in the cloud. The cloud providers should follow the guidelines for protecting the privacy of the data in cloud is discussed in cloud governance. Here the SLA (Service Level Agreement) has to be revised and it is accessible to both the client and the providers to know their level of security and confidentiality of the data. The client should access or store the data in secured websites and avoid phishing websites, which is the reason for the data hacking. Based on the above analysis of advantages and disadvantages of various methods, the AES and PSO based encryption produces the best result individually. Hence, in this paper, advanced encryption standard is improved by key enhancement using PSO. The automatic key generation is the proposed technique used for reducing the unauthorised access. The other details are explained in the proposed Methodology.

3 Traditional AES Algorithm

The Advanced Encryption Standard (AES) is involved with encrypting the electronics data. The Rijndael cipher text block is the subset of AES, which is created by cryptography technique. The AES is applicable for both software and interconnected hardware. Rijndael block cipher-text algorithm is used for the advancement of DES algorithm. In an encryption process, the plain text is converted into cipher text format. The AES S-Box is arranged for substitute byte transformations and the key is retrieved by using the decryption technique. The drawback in traditional AES algorithm is not a reliable security algorithm because, the verification key is fixed and it is stored in the database. Since unauthorised party may access the key. Therefore, in the proposed enhancement in PSO based AES algorithm, automatically the key is generated and it is arranged based on the input image using PSO. The cost function of the key is less than the 255 valued. The automatic key generation process rectifies the unauthorized access. The proposed method is efficient in the way of providing the automatic key generation technique. Therefore, we can access the data

securely. The various security parameters are selected for encrypting the data. The traditional AES algorithm is one which the efficient encryption technique for cloud storage. Here the traditional AES algorithm is modelled and it is compared with the proposed enhancement in the PSO based AES algorithm. The computational time of the proposed enhancement in Particle Swarm Optimization algorithm based AES encryption achieves the best results when compared to the existing traditional AES algorithm.

4 Proposed Methodology

The major goal of this key research is to ensure the safety of data in the cloud from the hackers. For this purpose, an enhanced AES encryption is used to encrypt the data before saving into the cloud and decrypt the data while retrieving. The AES algorithm is improved by using the PSO algorithm for optimizing the Key for the process of cipher text creation. The proposed methodology is shown below:

4.1 Steps for The Proposed Method

1.The sender will send the data to be store in the cloud.
2.Before storing in the cloud, the data will be process to produce the key based on the particle swarm optimization (PSO) algorithm.
3.The key and data will be sending to the encryption process and AES algorithm steps are performed to produce the cipher text.
4.This cipher text is stored in the cloud.
5.At the receiver side, when the user fetch the data from the cloud.
6.The same key generated in step 2 has to give to retrieve the data.

4.2 Sender Side

In the sender side, the clients will login with their credentials and send the data to be stored in the cloud. The data can be in any form like text or images. This raw data will be converted into decimals, which is easy for further processing and can facilitate the format for the machines.

4.3 Key Generation

The key will be generated based on the user's input using the Particle swarm optimization algorithm. The upper and lower bounds are the maximum and minimum of the data given by the user. The dimension of the variable is 16 for AES-128 and it is 32 for AES-256. PSO algorithm is inspired from the behaviour of bird flocking, which is proposed, by Kennedy, J and Eberhart, R [5].

The PSO algorithm works on the concept of group of birds finding the best way to search the food. In this, each bird is considered as a "particle ". Each particle has fitness values, which are optimized by its fitness function. These particles have velocities and fly in the problem space. Here, the PSO is initialized as 16 or 32 particles based on the type of encryption and then searches for the optimal solutions by updating each time. The two best values are calculated called as pbest and gbest. The pbest is the best solution reached by the particle in that iteration and gbest is the overall best particle. The velocity and the position of the particle is updated after finding the best values with the below equations (1) and (2).

$$v[] = v[] + c1 * rand() * (pbest[] - present) * c2 * rand() * (gbest[] - present[]) \quad (1)$$

$$present[] = present[] + v[] \quad (2)$$

Where $v[]$ is the particle velocity, Present [] denotes solution of the current particle, Pbest [] and gbest [] are the best solution, rand () is the random number between 0 and 1 and $c1$, $c2$ are learning factors. The pseudo code of the PSO algorithm for the key generation is given below:

Initialize $pop = 50; c1 = 1.5; c2 = 2.0$.
Initialize lower bound and upper bound based on input.
For each particle
Initialize particle
End
Do
For each particle
Calculate fitness value
If fitness value better than pbest
Set pbest as current value
End
Calculate gbest
For each particle
Calculate and update equations 1 and 2
End
While maximum iterations or minimum error is not reached

4.4 Cipher Text Generation

In this part, the cipher text is generated from the data and key generated through the PSO algorithm. The reason for choosing AES is stronger and faster than Triple-DES. The number of rounds for cipher text generation is variable for different key lengths. It uses 10 rounds for 128 bits, 12 rounds for 192 bits and 14 rounds for 256 key bits. The inputs are divided into the form of block of 16 bytes for processing. The encryption steps of AES by Daemaen and Rijmen [6] is explained below.

1.Plain text and round keys are given as input to the AES

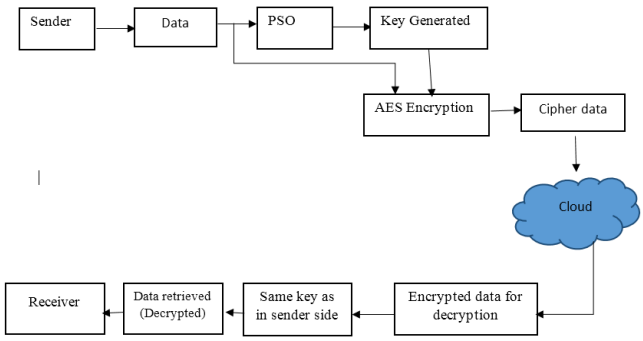

Fig. 1: Block diagram of the proposed methodology

2.The s-box is generated based on the key for the sub bytes process
3.The Byte substitution process takes place for the inputs based on the S-box. The result will be a matrix of four rows and four columns.

$$K[t] : c[n] = K[t-1] : c[n] xor K[t] : c[n] \quad (3)$$

1.The rows of the matrix are shifted in these shift rows process. The steps for shift rows are:
(a)Rows are shifted to the left. If any fall off occurs then it is inserted to the right.
(b)First row is not shifted.
(c)Second row is shifted by one byte to the left.
(d)Third row is shifted by 2 byte to the left.
(e)The result matrix will be shifted 16 matrix values.

$$K[t] : c0 = K[t-1] : c0 xor subyte(K[t-1] : c3 >> 8) xor cipher[n] \quad (4)$$

$$K[t] : c = K1 : c2 xor K2 : c1 \quad (5)$$

Where, K is the verification key, c is the column of S-Box table and n is the routines. The column of input is changed through the mathematical function. This mix column process will not take place in the final round.
2.The 16-byte matrix are XORed with the keys till its round count. When it reaches the final round, the cipher text will be generated.
The final cipher data to be stored in the cloud is produced in this process. This data will be saved in the cloud to protect it from the hackers.

4.5 Receiver Side

In this, the receiver will fetch the data from the cloud. The fetched data will be an encrypted one. This encrypted data is decrypted through the decryption process of AES with the same key.

4.6 Decryption

The decryption of AES is also consists of four Sub-process as in encryption but it is performed in a reverse manner. The steps of decryption are:

1.Cipher text and round keys are given as inputs to the AES.
2.The s-box is generated based on the key for the sub bytes process.
3.The 16-byte matrix is XORed with the keys until its round count. When it reaches the final round, the cipher text will be generated.
4.The column of input is changed through the mathematical function. This mix column process will not takes place in final round
5.The rows of the matrix are shifted in this shift rows process. The steps for shift rows are:
(a)Rows are shifted to the left. If any fall off occurs then it is inserted to the right.
(b)First row is not shifted.
(c)Second row is shifted by one byte to the left.
(d)Third row is shifted by 2 byte to the left.
(e)The result matrix will be shifted 16 matrix values.
6.The Byte substitution process takes place for the inputs based on the S-box. The result will be a matrix of four rows and four columns. The result will be a decrypted data as in the sender side.

5 Experimental Results

The proposed PSO-AES is verified by applying on the text and image data of 128 bit-key size and 256-bit key size. The results are evaluated through the bit error for both the text and images. For images, the PSNR value is calculated for the detection of loss of quality in the image through the proposed algorithm. The results are shown below, the input image is shown in fig 2, which is stored in the cloud database and it is encrypted using AES algorithm. The automatic verification key generated by PSO and the encrypted given image is shown in fig 3.

Fig. 2: Input image

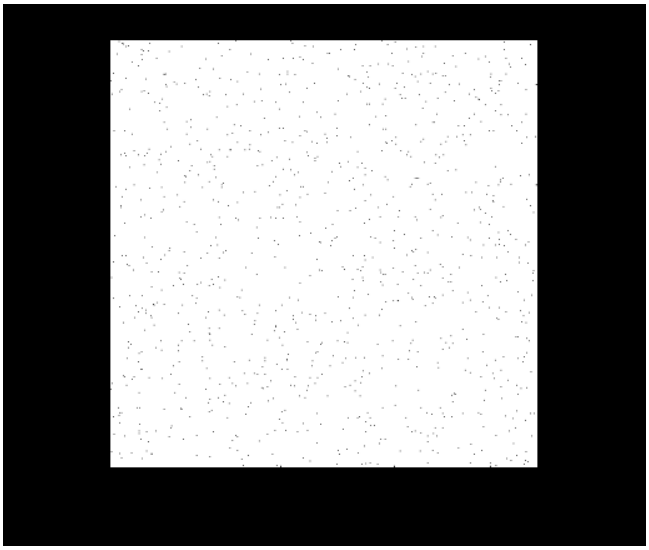

Fig. 3: Encrypted image of 128 key bits

The encrypted image is given for 128 key bits. Here with the use of PSO algorithm in AES, the cost function is set less than 255. The decrypted image for 128 key bits and 256 key bits is evaluated. The decrypted given input image is shown in figure 4 & 5.

Based on bit error rate and peak signal to noise ratio the 128 key bits and 256 key bits are evaluated. Here two types of input data are evaluated that is text and image. Tables 1 & 2 represent the evaluation result of Traditional AES and PSO based AES. In this the bit error rate and peak signal to noise ratio are measured for 128 key bits and 256 key bits. By comparing these two methods, there is not losses/increased error. Because both its same for text data and image data.

The bit error rate is always zero and the peak signal to noise ratio is infinite for image data and zero for text data. Therefore, both the traditional AES and PSO based AES are the same for the bit error rate and PSNR, here there is no extra error occurred using of PSO to the AES algorithm. However, by comparing with the computational time of both this algorithm, the proposed PSO based AES algorithm is efficient one.

The proposed security enhanced PSO based AES algorithm is modelled and it is evaluated. By comparing

Fig. 4: Decrypted image of 128 key bits

Fig. 5: Decrypted image of 256 key bits

Table 1: Evaluation of PSO-AES

Metrics	128 key bits		256 key bits	
	Text	Image	Text	Image
Bit error	0	0	0	0
PSNR	-	Inf	-	Inf

the computational time of cipher text generation, the proposed method reduces the computational time by comparing with the traditional AES algorithm. Both 128 key bits and 256 key bits are evaluated and it is compared.

Table 2: Evaluation of AES

Metrics	128 key bits		256 key bits	
	Text	Image	Text	Image
Traditional AES	0.0399	10.5467	0.0328	19.0566
PSO-AES	0.0273	9.7146	0.0296	16.9034

Therefore the proposed security enhanced PSO based AES algorithm is efficient in the way of security and protection.

6 Conclusion and Future Scope

Nowadays, the cloud-based storage is reached to different types of users due to its main advantage of the reduction in the cost for the IT resources infrastructure and the cloud supporting platforms also increasing day by day. Due to this tremendous reach of cloud computing, the security to the data is need in the cloud. The data in the cloud should not be shared to the third party users and the data should not be hacked by the hackers. It can be prevented by encrypting the data before saving into the cloud. This encryption process should be a stronger one, which cannot be hacked by others. For such a strong encryption, a new PSO-AES algorithm is proposed and its performances are evaluated through the metrics.

The PSO-AES is a stronger encryption method than the traditional AES because the key used for the encryption process is varying every time based on the input, which is optimized through the PSO algorithm. This algorithm computes faster and produces the decrypted output with good quality. This is evaluated by

the PSNR of the decrypted image. The proposed PSO-AES is suitable for both the cloud- computing security and for the other encryption process in social media or messaging apps. In future work, the proposed methodology can be converted into jar files to support in the other platform for the real time scenarios.

References

[1] Fernandes, D. A., Soares, L. F., Gomes, J. V., Freire, M. M., & Inacio, P. R.. Security issues in cloud environments: a survey. International Journal of Information Security, 13(2), 113-170, (2014).

[2] A. Sagheer, M. Zidan and M. M. Abdelsamea, A Novel Autonomous Perceptron Model for Pattern Classification Applications, Entropy, 21(8), 763, 2019.

[3] M. Zidan, A.-H. Abdel-Aty, M. El-shafei, M. Feraig, Y. El-Abou, H. Eleuch and M. Abdel-Aty, Quantum Classification Algorithm Based on Competitive Learning Neural Network and Entanglement Measure, Appl. Sci., 9(7), 1277, 2019.

[4] Sreelaja, NK and Vijayalakshmi, GA. "Design of Stream Cipher for Text Encryption using Particle Swarm Optimization based Key Generation.". Journal of Information Assurance and Security 4, 30-41, (2009).

[5] Kennedy, J., & Eberhart, R, PSO optimization. In Proc. IEEE Int. Conf. Neural Networks . IEEE Service Center, Piscataway, NJ, Vol. 4, 1941-1948 (1995).

[6] Daemen, J., & Rijmen, V., The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media, (2013).

[7] Dogra, R., & Sharma, A. Improvement of Cloud Security Efficiency by Reducing Data Size and Computational Time Using ECDH, AES, BlowFish & PSO Algorithm. International Journal of Innovations in Engineering and Technology (IJIET) ,Vol. 2, Issue8,(2017).

[8] Gupta, U., Saluja, M. S., & Tiwari, M. T., Enhancement of Cloud Security and removal of anti-patterns using multilevel encryption algorithms. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 5, Issue 1, 55-61, (2018).

[9] Sachdev, A., & Bhansali, M.. Enhancing cloud computing security using aes algorithm. International Journal of Computer Applications, 67(9), (2013).

[10] Subashini, S., & Kavitha, V., A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11, (2011).

[11] Tsai, W. T., Jin, Z., & Bai, X. Internetware computing: issues and perspective. In Proceedings of the first Asia-Pacific symposium on Internetware (p. 1). ACM, (2009).

[1]. Open Grid forum accessed on july 2015 https://www.ogf.org/ogf/

[12] Brindha, T., & Shaji, R. S. An Efficient Framework for Providing Secured Transaction of Data in Cloud Environment. Indian Journal of Science and Technology, 9(44), (2016).

[13] Brindha, T., Shaji, R. S., & Rajesh, G. P., A survey on the architectures of data security in cloud storage infrastructure. Engineering and Technology (IJET), 5, 1108-1114, (2013).

[14] Schneier,B. Description of a new variable-length key, 64-bit block cipher (Blowfish). In International Workshop on Fast Software Encryption. Springer, Berlin, Heidelberg, 191-204, (1993).

[15] Almorsy, M., Grundy, J., & Muller, I. An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107,(2016).

[16] Zhao, F., Li, C., & Liu, C. F., A cloud computing security solution based on fully homomorphic encryption. In Advanced Communication Technology (ICACT), 2014 16th International Conference on IEEE, 485-488. (2014).

[17] Samarati, P., di Vimercati, S. D. C., Murugesan, S., & Bojanova, I. Cloud security: Issues and concerns. Encyclopedia on cloud computing, 1-14, (2016).

[18] Goyal, S. Security, Privacy, Threats and Risks in Cloud Computing-A Vital Review. International Journal of Applied Mathematics, Electronics and Computers, 4(1), 31-38 (2016).

[19] D'souza, F. J., & Panchal, D., Advanced encryption standard (AES) security enhancement using hybrid approach. In Computing, Communication and Automation (ICCCA), 2017 International Conference on IEEE , 647-652. (2017).

[20] Ramgovind, S., Eloff, M. M., & Smith, E., The management of security in cloud computing. In Information Security for South Africa (ISSA), 1-7, IEEE (2010).

[21] Bih-Hwang Lee., Ervin Kusuma Dewi., and Muhammad Farid Wajdi. Data security in cloud computing using AES under HEROKU cloud. Proceedings in 27th Wireless and Optical Communication Conference., Hualien, Taiwan. IEEE (2018).

[2]. Babitha M P., K R Remesh Babu. Secure cloud storage using AES encryption. Proceedings of the international conference on Automatic Control and Dynamic Optimization Techniques, 9-10 September 2017, Pune, India. IEEE 2017.

[3]. S Delfin, Rachana Sai B, Meghana J V, Kundana Lakshmi Y, Sushmita Sharma. Cloud Data Security using AES Algorithm. International Research Journal of Engineering and Technology. 2018; 5(10): 11898-1192.

[4]. Roshani Raghatate, Sneha Humne, and Roshna Wadhwe. A Survey on Secure Cloud Computing using AES Algorithm. International Journal of Computer Science and Mobile Computing. December 2014; 3(12): 295-301.

[5]. Zhiyi Fang, Yao Sun, Yujing Sun, and Jianming Yang. The Research of AES algorithm and application in cloud storage system. International conf. on Science and Social Research. 2013; 687-690.

[6]. Abha Sachdev, and Mohit Bhansali. Enhancing Cloud Computing Security using AES Algorithm. International Journal of Computer Applications. 67(9); 20-23. April 2013.

[22] V Surya, S Ravichandra, and R Ranjani. Secure Cloud Storage using AES Encryption. Inter. Joural of Innovative Research in Computer and Communication Engineering. 6(6): 6309-6312, (2018).

[23] Nagasai Lohitha Kodumru, and M Supriya. Secure Data Storage in Cloud using Cryptographic Algorithms. Proceedings of the 4th Inter. Conf. on Computing Communication Control and Automation, Pune, India, (2018).

[24] Smitha Nisha Mendonca. Data Security in Cloud using AES. International Journal of Engineering Research & Technology. 7(1), 205-208, (2018).

[25] Namitha N Pathak, and Meghana Nagori. Enhanced Security for Multi Cloud Storage using AES Algorithm. International Journal of Computer Science and Information Technologies,6(6): 5313-5315, (2015).

G Venkatakoti Reddy was born in 1982, India. He received B.E. degree in Computer Science & Engineering from Anna University, Chennai, M. Tech in Computer Networks & Information Security, JNTU, Hyderabad. He has 8 years of teaching experience at various levels. Presently he is Full time Research Scholar in Anna University, Chennai. His current research interests include Cloud Computing, Information Security, Wireless and Mobile communications and IoT. He guided 5 Projects PG,14 UG and published more than 8 papers in National / international journals. Attended 2 national, 5 international conferences, 5 workshops.

K. Srihari received the M.E. and Ph.D. degree from Anna University, Chennai. He is currently working as an Associate Professor in the Department of Computer Science and Engineering, SNS College of Technology, affiliated to Anna University-Chennai, Tamilnadu, India. Dr.K.Srihari published over 30 papers in international journals and his research area includes semantic search engines, big data and cloud computing.

S. Karthik is presently Professor and Dean in the Department of Computer Science and Engineering, SNS College of Technology, affiliated to Anna University-Chennai, Tamilnadu, India. He received the M.E. and Ph.D. degree from Anna University, Chennai. His research interests include network security, big data, cloud computing, web services and wireless systems. Dr.S. Karthik published more than 96 papers in refereed international journals and 125 papers in conferences and has been involved many international conferences as Technical Chair and tutorial presenter. He is an active member of IEEE, ISTE, IAENG, IACSIT and Indian Computer Society.