Asian Journal of Computer Science and Technology
ISSN: 2249-0701 Vol.7 No.1, 2018, pp. 50-54
© The Research Publication, www.trp.org.in

Data Privacy and Security in Cloud Environment Using Cryptography Approach

Jayashree Agarkhed[1] and Ashalatha R[2]
[1]Professor, [2]Research Scholar,
[1&2]Department of C.S.E, Poojya Doddappa Appa College of Engineering, Kalaburagi, Karnataka, India
E-mail: ashalatha.dsce@gmail.com, jayashreeptl@yahoo.com

Abstract - **Cloud computing environment is a network centered computing technique delivered to the users as a service. It mainly involves computing over the network where the program file or any application, run upon server in various locations at the identical time. Cloud computing accommodates huge data storage and computing capabilities to its users. The cloud storage service is considered to be the best quality cloud maintenance service. Cryptography is known as the skill of securing the confidential information from third party hackers. Both the parties over the insecure network can transfer files with each other by the ways of cryptographic techniques of the sensitive data files for maintaining the security and also privacy. The secrecy and concealment of data are considered an important issue of concern in cloud field.**

Keywords: **Confidentiality, Cloud storage, Cryptography, Privacy preserving, Security**

I. INTRODUCTION

Cloud computing is being considered as a method of computing technology, which includes resources like hardware or software that reside on a remote machine and are conveyed for the sake of end users as services in the network with the utmost proven example being the internet. Major cloud service delivery models include infrastructure services which provide virtual infrastructures like servers and data storage. Platform services provides with user development, web services. In software services, the user is given with running applications in the cloud. Some of the most infrastructure services in the cloud are storage issues and computing services.

The Amazon S3 has been considered as a best example for storage facility in the cloud. Amazon EC2 has been considered for cloud services [1]. Cryptography states the way of undisclosed writing which is used for securing the sensitive information. Two different systems of security have encryption as well as decryption processes. Privacy preservation means the security of personal information of user in cloud area. The communication of sensitive data on an unsecured cloud network uses some of the efficient encryption algorithms. The overall structure of the paper is presented as follows. Section 2 grants the review of literature and section 3 gives the methodology part. Section 4 offers the result analysis and to sum up section 5 ends with the conclusion part.

II. LITERATURE SURVEY

The extensive literature survey is provided for cloud data storing and confidentiality. The data sharing service scheme in the cloud provides dynamic resource access to the data using privacy preserving of data policy methods. The identity encryption methodology allows dynamic operations securely onto the cloud. The policy verifies the security using the generic bilinear model. Data security has been ensured and the privacy of cloud user has been preserved.
Dong, Xin, et al., has used random oracle method for sharing and security of the cloud data. The result examination shows that the given method uses smaller overhead than other methods. The scheme has the hash function using a mapping function for key generation technique and decryption [2]. The attribute used encryption scheme depending upon the cipher text theory can be used for cryptographic systems. Cheng, Yong, *et al.,* has used an attribute union method which is basically used for combining various attributes using arithmetic theorem [3]. Yao, et al., has established a confident storage system in the cloud; a threshold encryption scheme has been offered to meet data robustness and confidentiality. The cryptographic algorithm used is a homomorphic property for storage servers above the cloud [4].

Gai, Keke, *et al.,* has used the dynamic encryption strategy which has been recommended using secrecy grouping methods of data. The model is designed for securing data owner's privacy under certain restrictions [5]. Arya, *et al.,* found a group based key protocol which is implemented for providing authentication and privacy of cloud data. The work uses a group signature method for providing cloud services using access control mechanisms [6]. Using cloud service scheme, the cloud users have the provision to use the data stored in the cloud. Fu, *et al.,* uses cryptographic method known as symmetric encrypting scheme is used for encrypting the user's data. The method uses attribute revocation type for accomplishing the access control over the cloud storage [7]. Prakash, G. L., *et al.,* have made used a secure method for data has been implemented in order to control data in a cloud system. The cryptographic method includes data encryption, data decryption along with key rotation techniques. The cryptographic hash method uses data privacy algorithm for security in cloud computing [8].

Dadhich, *et al.,* has a linear cryptanalysis technique uses four rounds of data encryption standard (DES) algorithm. A cryptanalyst technique provides swarm intelligence for finding optimal key using cryptography. The particle swarm intelligence search scheme is used for obtaining the optimal results [9]. Various procedures and methods for safeguarding socket layer are used for encoding the data. Sood, Sandeep K. *et al.,* has used the message authentication of code (MAC) is provided to prove the reliability of the data. The cloud data are protected in an encrypted manner while transmission. The procedure includes classification index building, encryption and MAC steps. Strong and secure encryption techniques are required for securing the data and for controlling the data access authorization methods are used [10].

III. METHODOLOGY

Privacy of data is considered to be the biggest challenge in cloud computing. The service provider uses encryption technology for security over the cloud data. The sensitive data are protected using an encryption based system for securing the cloud systems. The security and privacy anxieties include various issues such as identity management, protection of data, data privacy and secure operations. Privacy requires encryption and decryption of data files while at rest or while transmitted over the cloud. Strong authentication techniques and secure algorithms will help the confidential data to be secured within the cloud premises. The privacy preserving schemes include access control, encryption strategy, key management, policy, proxy, security, signature and central authority [11]. Encryption is a method of gaining cryptic text using symmetric or asymmetric key based encryption algorithms. The cipher is a cryptographic based algorithm which uses standard mathematical functions. Cryptanalysis is the learning of cipher and crypto systems for converting encrypted text back into plain text using cryptographic keys. Encryption is the simplest way of ensuring confidentiality among the cloud data files [12]. The user's sensitive information can be referred to as privacy of data in the cloud. Cloud threats to privacy and security involve attacks, vulnerabilities and cloud service abuses. Encryption, as well as decryption of data, is applied to avoid un-authorization of confidential information [13].

A. *Data Encryption Standard Algorithm and Firefly Algorithm (FFA)*

The cryptographic encryption algorithm is used as a block cipher for encoding and decoding of the data blocks. The method uses a symmetric algorithm process having 64 bits of data blocks with 64 bits of key size at the rate of 64 bits per second [14]. The encryption process involves converting 64 bits of normal text into 64 bits of cipher values [15]. The algorithm process includes initial permutation, key calculations using 16 rounds and contrary of the initial permutation method. The algorithm uses a cipher key known as fiestel block cipher [16].

DES is a cryptographic algorithm for generating secret codes for cloud data. Encryption is a cryptographic method for transforming the plain text through cipher text which results in an unreadable data form. DES is a type of cryptosystem that was created by IBM Corporation for maintaining people sensitive data and various applications. It is a standard type of block cipher system which uses encryption and decryption algorithms by grouping 64-bit blocks [17]. The major operations of DES algorithm involve the XOR operation, substitution policy and permutation using 16 rounds of operations. The equation 1 denoting the encryption operation is given as follows. The cipher text C is formed by encrypting the clear text with the key used [18].

$$C = DES(P, K) \tag{1}$$

DES approach has been one of the oldest algorithms published in the 1970s for the purpose of securing phone numbers and people conversations made over the phone. It is a type of encryption algorithm which works on particular set of blocks containing normal plain text. The input is taken as 64 bits and which makes 2^{64} possible combinations from it [19]. Therefore, DES uses 16 rounds of the encryption procedure in order to secure the confidential data. The key size can be 64 bits having 56 bits of key and 8 parity bits. The decryption algorithm has 8 total blocks of secret message as input and converts the same back into the original data [20].

DES refers to a block cipher key algorithm which makes use of encrypting and also decrypting processes. The encryption algorithm transforms the series of input plain text into cipher text and decryption algorithm performs the reverse operation by transforming the cipher text back to the block of plain text of the identical length [21]. The method involves initial permutations and the final permutation procedure. The fiestel block cipher system involves 64-bit blocks into two splits using a fiestel function. The procedure involves 16 stages using XOR operation. S-boxes can be used for permutation for transforming two of 32 bit halves randomly [22]. The decryption type algorithm uses subsets of keys to decrypt the cipher text which is just the reverse of the encryption process. The equation 2 for decryption process is given below. The clear text is decrypted back using the cipher text values along with the original key used [23].

$$P = DES(C, K) \tag{2}$$

The firefly species are famous for producing little and musical flashes. The fireflies flash an amazing light during summer sky of tropical regions. In firefly algorithm, the dissimilarity of the light intensity as well as the creation of attractiveness is to be considered. The attractiveness is given by brightness using an encoded function. FFA is basically Meta heuristic algorithm used for the optimization process. The optimizer is used as an engine for searching strategy in cloud process. The firefly is a key optimization algorithm found in the year 2008. This algorithm is a population based type of method used for finding the performance of fireflies. The given algorithm is given for achieving high efficiency for maintaining privacy and preservation in the cloud [24].

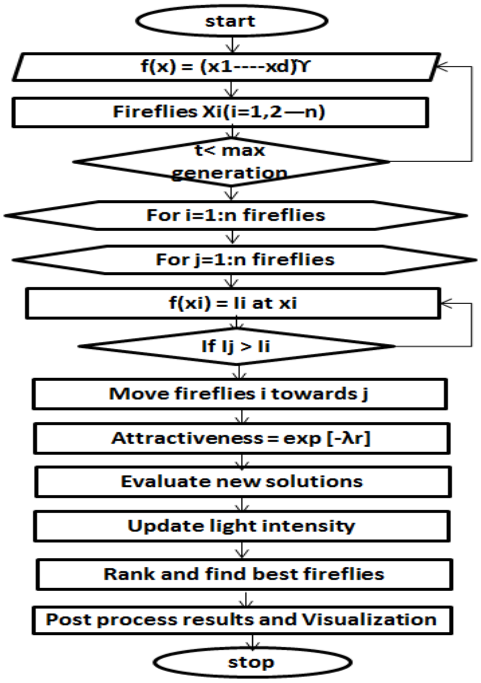


Fig. 1 Firefly algorithm

Firefly algorithm in figure 1 provides desirability of bright and firefly's attractiveness. The algorithm uses the flashing behaviour of swarming fireflies. The definitive theme of the algorithm is to discover the total optimization solution for the given problem. The glow of fireflies shows the quality of solutions using a fitness function for enlargement problem [25]. The assessment of the firefly can be related to objective function's value. Firefly algorithm is used to execute the workload balancing permitted to reduce energy usage of data centers of the cloud. It can also be used as best practice for attaining efficiency in the cloud. This algorithm is mainly used for indicating the ideal feature extraction subset and solution space correctly into the cloud environment [26].

B. Firefly Optimization Equations

The attractiveness can be calculated using equation 3

$$\beta(r) = \beta_0 e^{-\gamma r^2} \tag{3}$$

$\beta \rightarrow attractiveness\ function$
$\gamma \in [0, \infty]$
$r = distance\ between\ the\ two\ fireflies\ i\ and\ j$
The Cartesian distance between X_i and X_j is given in equation 4

$$r_{ij} = \left|\left|X_i - X_j\right|\right| = \sqrt{\sum_{k=1}^{d}(X_{ik} - X_{jk})} \tag{4}$$

Where r_{ij} is the distance defined in the above equation
β_0 is the initial attractiveness at $r = 0$ and γ is an absorption coefficient

The firefly movement between i and j is given in equation 5

$$X_i^{t+1} = X_i^t + \beta_0 e^{-\gamma r_{ij}^2}\left(X_j^t - X_i^t\right) + \alpha_t\,(rand - 1/2) \tag{5}$$

The firefly attraction with brighter fireflies is given in equation 6

$$X_i = X_i + \beta_0 e^{-\gamma r_{ij}^{\mu}}\left(X_j - X_i\right) + \alpha(\sigma - \tfrac{1}{2}) \tag{6}$$

Here X_i is the present location of the firefly.
$\beta_0 e^{-\gamma r_{ij}^{\mu}}\left(X_j - X_i\right)$ is considered as the desirability of firefly to the light power.
$\alpha(\sigma - \frac{1}{2})$ is the arbitrary measure of firefly considered [27].

C. Firefly Key Optimization Algorithm

The firefly key optimization algorithm is defined as follows [28].
Step 1: Firefly Algorithm Objective function f(x), x = (x1 … x_d)^T
Step 2: Generate an initial population of fireflies x_i(i = 1,2 … n)
Step 3: Define light intensity I_i at X_i is determined by f(x_i)
Step 4: Define light absorption coefficient γ
Step 5: while (t <Max Generation)
Step 6: for i = 1: n for all n fireflies
Step 7: for j = 1: i for all n fireflies
Step 8: if I_j>I_i, Move firefly I towards j in d-dimension; end if
Step 9: Attractiveness varies with distance r via exp [−γr]
Step 10: Evaluate new solutions and update light intensity
Step 11: end for j
Step 12: end for i
Step 13: Rank the fireflies and find the current best
Step 14: end while
Step 15: Post-process results and visualization
Step 16: End

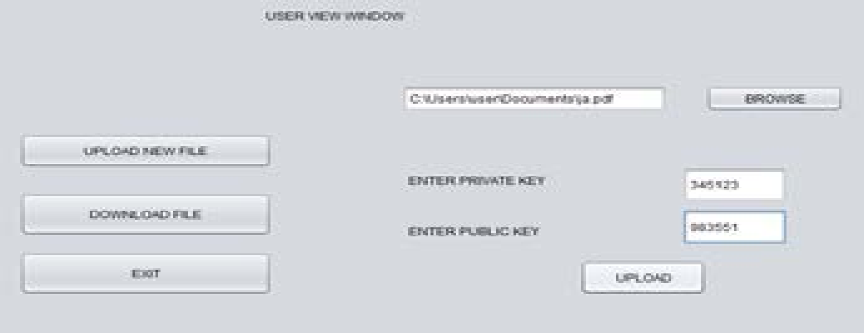
D. Pseudo Code for firefly Algorithm (FA)

The firefly optimization algorithm is used for multimodal optimization problems efficiently [29, 30].

General steps:
Step 1: Initialize firefly agents
Step 2: For each loop, pairwise the firefly comparison.
Step 3: Output the brighter firefly with lower light intensity.
Step 4: Attraction is on short distance fireflies
Step 5: Assign new lower light intensity firefly after the updating
Step 6: Best solution is updated at the end of the each loop.
Step 7: End the loop after all the comparisons.
Step 8: Stop

IV. RESULTS AND DISCUSSION

The proposed work has been analysed for security requirements. The data security and confidentiality over the cloud network has been focussed intently. The scheme uses cryptographic measure using DES block cipher security algorithm which has been combined with the firefly optimization process.



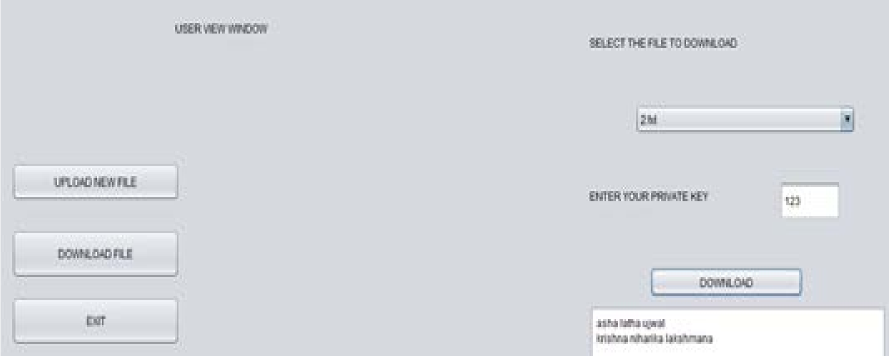
C:\Users\user\Documents\ja.pdf

ENTER PRIVATE KEY 345123

ENTER PUBLIC KEY 983551

Fig. 2 Data encryption process

Figure 2 shows the way of uploading the data to the cloud for confidentiality purpose. The user view window in the figure shows the uploading of the plain text by entering the private and public key values. The encryption process involves DES algorithm along with firefly encryption process which includes key optimization algorithm for security and confidentiality.



SELECT THE FILE TO DOWNLOAD 2.txt

ENTER YOUR PRIVATE KEY 123

asha latha ujwal
krishna niharika lakshmana

Fig. 3 Data decryption process

Fig. 3 shows the downloading data files from cloud storage by making use of cryptographic measures for data confidentiality over the cloud network. The figure depicts the user view window for downloading the data by entering the private key variable. The privacy and authentication have been preserved for data integrity and security issues. The decryption process uses cryptographic security techniques which include DES algorithm and firefly optimization technique process.

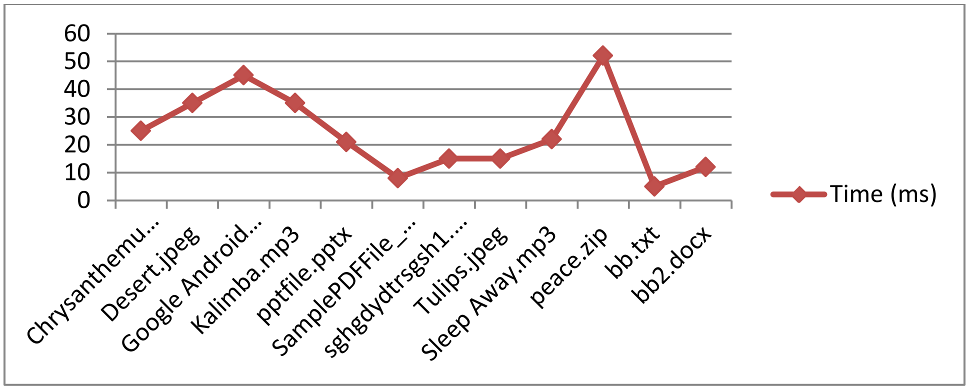


Fig. 4 Auditing time

The auditing time measurement graph is given between the resources and time taken to audit the particular resource. It is the analysis between auditing particular resource and time taken to perform the required computation. Figure 4 depicts the resource access time in milliseconds with a number of the cloud users accessing the data files from the cloud servers. For example, a file called as a p eace.zip file is taking 52 milliseconds for encrypting and decrypting in the cloud server. The resource name along with the time taken by the TPA recorded on the graph. The file names include extensions like JPEG, PDF, pptx, mp3, zip, text and document multimedia files in the cloud server.

V. CONCLUSION

Cloud computing undoubtedly provides unlimited data space for storage to its users. It also serves sharing of data and planned use of heterogeneous resources in distributed systems. The service providers can expand the storage space in a cloud environment. Security is well-thought-out to be the essential attribute in a distributed system. The work comprises of cryptographic technique which is a t ype of method used for securing the data from attackers and eavesdroppers.

REFERENCES

[1] C. Liu, X. Zhang, C. Yang and J. Chen, “CCBKE—Session Key Negotiation for Fast and Secure Scheduling of Scientific Applications in Cloud Computing”, *Future Generation Computer Systems*, Vol. 29, No. 5, pp. 1300-1308, 2013.

[2] X. Dong, J. Yu, Y. Luo, Y. Chen, , G. Xue and M. Li, “Achieving an Effective, Scalable and Privacy-Preserving Data Sharing Service in Cloud Computing”, *Computers & Security*, Vol. 42, pp. 151-164, 2014.

[3] Y. Cheng, J. Ren, Z. Wang, S. Mei and J. Zhou, “Attributes Union in CP-ABE Algorithm for Large Universe Cryptographic Access Control”, in *Cloud and Green Computing (CGC), 2nd International Conference*, *IEEE*, pp. 180-186, November, 2012.

[4] C. Yao, L. Xu and X. Huang, “A Secure Cloud Storage System from Threshold Encryption”, in *Intelligent Networking and Collaborative Systems (INCoS), 5th International Conference*, *IEEE*, pp. 541-545, September 2013.

[5] K. Gai, M. Qiu, H. Zha and J. Xiong, “Privacy-Aware Adaptive Data Encryption Strategy of Big Data in Cloud Computing”, in *Cyber Security and Cloud Computing (CSCloud), 3rd International Conference, IEEE,* pp. 273-278, June 2016.

[6] P. K. Arya, K. Selvamani and S. Kanimozhi, “An Authentication Approach for Data Sharing in Cloud Environment for Dynamic Group”, in *Issues and Challenges in Intelligent Computing Techniques (ICICT), International Conference*, *IEEE*, pp. 262-267, February, 2014.

[7] X. Fu and Z. Wu, “Ciphertext Policy Attribute Based Encryption with Immediate Attribute Revocation for Fine-Grained Access Control in Cloud Storage”, in *Communications, Circuits and Systems (ICCCAS), International Conference, IEEE*, Vol. 2, pp. 103-108, November, 2013.

[8] G. L. Prakash, M. Prateek and I. Singh, “Efficient Data Security Method to Control Data in Cloud Storage System using Cryptographic Techniques”, in Recent Advances and Innovations in Engineering (ICRAIE), *IEEE*, pp. 1-6, May 2014.

[9] A. Dadhich, A. Gupta and S. Yadav, “Swarm Intelligence based Linear Cryptanalysis of Four-Round Data Encryption Standard Algorithm”, in *Issues and Challenges in Intelligent Computing Techniques (ICICT), International Conference*, *IEEE,* pp. 378-383, February 2014.

[10] S. K. Sood, “A Combined Approach to Ensure Data Security in Cloud Computing”, *Journal of Network and Computer Applications*, Vol. 35, No. 6, pp. 1831-1838, 2012.

[11] U. Arjun and S. Vinay, “A Short Review on Data Security and Privacy Issues in Cloud Computing”, in *Current Trends in Advanced Computing (ICCTAC), IEEE International Conference, IEEE,* pp. 1-5, March, 2016.

[12] J. Tang, Y. Cui, Q. Li, K. Ren, , J. Liu and R. Buyya, “Ensuring Security and Privacy Preservation for Cloud Data Services”, *ACM Computing Surveys (CSUR)*,Vol. 49, No. 1, pp. 13, 2016.

[13] S. Dara, “Cryptography Challenges for Computational Privacyin Public Clouds”, in *Cloud Computing in Emerging Markets (CCEM), International Conference, IEEE,* pp. 1-5, October 2013,.

[14] N. Nalini and G. R. Rao, “Cryptanalysis of simplified data encryption standard via optimization heuristics”, in *Intelligent Sensing and Information Processing, ICISIP, 3rd International Conference, IEEE* pp. 74-79, December 2005.

[15] E. F. Schaefer, “A Simplified Data Encryption Standard Algorithm. Cryptologia, Vol. 20, No. 1, pp. 77-84, 1996.

[16] A. Nagamalli, S. S. Krishna and B. KeerthiPriya, “Data Encryption using Counting Bloom Filters for Cloud Security”, 2013.

[17] E. Biham and A. S hamir, “Differential Cryptanalysis of the Data Encryption Standard”, *Springer Science & Business Media*, 2012.

[18] N. Jayapandian, A. M. Z. Rahman, S. Radhikadevi and M. Koushikaa, “Enhanced Cloud Security Framework to Confirm Data Security on Asymmetric And Symmetric Key Encryption”, in *Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), World Conference*, *IEEE*, pp. 1-4, Feb. 2016.

[19] E. M. Mohamed, S. El-Etriby and H. S. Abdul-kader, “Randomness Testing of Modern Encryption Techniques in Cloud Environment”, in *Informatics and Systems (INFOS), 8th International Conference, IEEE*, pp. CC-1, May 2012.

[20] B. Y ang, K. Wu and R. Karri, “Scan Based Side Channel Attack on Dedicated Hardware Implementations of Data Encryption Standard”, In *Test Conference*, *Proc. ITC International,* IEEE, pp. 339-344, October 2004.

[21] S. Landau, “Standing the test of time: The data encryption standard”, Notices of AMS, Vol. 47 No. 3, pp. 341-349, 2000.

[22] M. E. Smid and D. K. Branstad, “Data Encryption Standard: Past and Future, *Proc. of the IEEE*, Vol. 76, No. 5, pp. 550-559, 1988.

[23] R. Davis, “The Data Encryption Standard in Perspective”, *IEEE Communications Society Magazine*, Vol. 16, No. 6, pp. 5-9, 1978.

[24] I. Fister Jr, X. S. Yang, I. Fister, J. Brest and D. Fister, “A Brief Review of Nature-I Nspired Algorithms for Optimization”, arXiv preprint arXiv:1307.4186, 2013.

[25] G. Nithya and G. Jayapratha, “A Multi-agent Brokering Approach and Jumper Firefly Algorithm for Job Scheduling in Cloud Computing”, in *Intelligent Computing Applications (ICICA), 2014 International Conference*, *IEEE*, pp. 52-58, March 2014.

[26] X. S. Yang, “Firefly Algorithm, Stochastic Test Functions and Design Optimisation”, *International Journal of Bio-Inspired Computation*, Vol. 2, No. 2,pp. 78-842010.

[27] A. Gálvez and A. Iglesias, “Firefly Algorithm for Explicit B-Spline Curve Fitting to Data Points”, Mathematical Problems in Engineering, 2013.

[28] X. S. Yang, “Firefly Algorithms for Multimodal Optimization”, in International Symposium on Stochastic Algorithms, *Springer*, Berlin, Heidelberg, pp. 169-178, October 2009.

[29] T. Kanimozhi and K. Latha, “An Integrated Approach to Region Based Image Retrieval using Firefly Algorithm and Support Vector Machine”, Neurocomputing, pp.1099-1111, 2015.

[30] S. Su, Y. Su, F. Shao and H. Guo, “A Power-Aware Virtual Machine Mapper using Firefly Optimization”, in *Advanced Cloud and Big Data*, *3rd International Conference, IEEE,* pp. 96-103, October, 2015.