Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2018, 5(11): 858-866

Research Article ISSN: 2394 - 658X

Secure Data Transmission in Cloud Environment Using Criticality with Visual Cryptography and Genetic Algorithm

Mamta[1], Fatima Abdullah[2], Mr. Mayank Deep Khare[3] and Dr. Chandra Shekhar Yadav [4]

[1]Student, CSE, NIET, Greater Noida, India - 201306
[2]Student, CSE, NIET, Greater Noida, India– 201306
[3]Assistant Professor, CSE, NIET, Greater India - 201306
[4]Professor, CSE, NIET, Greater Noida, India - 201306
Kmmahi8@gmail.com

ABSTRACT

Now a day's Cloud Computing is the great concept in the development of an on-demand network which provides access to a common pool of configurable resources. Unique feature of cloud computing is its security. Sharing of data is an imperative functionality in cloud storage.

In Cloud computing environment the sharing of data and transfer has increased exponentially. There are the various factors in data security like integrity, confidentiality, and authentication services. Maintaining secrecy and protection for critical data are highly challenging, particularly when data are stored in memory or send via any communication networks. I have reviewed several papers regarding our concept and what I found is that in some papers, GA has been used for security, In other papers used GA, VC, and Steganography together for enhancing security. But some are providing security quite well, having high overhead. And those which have low overhead, have poor security. Hence for solving this problem, a combination of visual cryptography and genetic algorithm methodology has been proposed, where the genetic algorithm is used for enhancing encryption and decryption, for hiding critical data we are using visual cryptography with a new concept which is named by critical index and extends visual cryptography to support video file as well as audio file. After result analysis we found that visual cryptography with critical index reduce more time as conventional method.

Key words: Cloud Computing, Visual Cryptography, Encryption, Decryption, Secret key, Genetic Algorithm, AES algorithm, Crossover, Mutation, and Critical Index

---

INTRODUCTION

Cloud computing is a technique which provides computing over the internet. A Cloud computing server incorporates highly optimum Virtual data centers [15].

A range of Hardware, software, and infrastructure resources are provided by these data centers whenever needed.

Available infrastructure resources on cloud can be used by organizations on a pay per use basis to avoid capital disbursement on additional infrastructure resources and according to business requisite can be instantly scaled up or scaled down [14].

All the organization is concerned about security, Privacy, unauthorized access and modifications. The security system of clouds should not be vulnerable to unauthorized data manipulation [1].

There are many security issues and concerns which are associated with cloud computing.

These issues are divided into two major categories. The first category is related to social issues which are faced by cloud providers and another one is related to those social issues which are faced by their customers.

The platform, infrastructure, and software are provided by cloud providers and organizations as a service through the cloud [16].

In maximum cases, the provider makes sure the security of infrastructure and protection of their client data and applications while the customer also must ensure that provider took the proper security measure in order to protect their information [17].
There are different types of critical data like company confidential data, national security data, account details etc.
These types of data need more security and confidentiality with special attention [13].We can achieve the secrecy of this type of data by data encryption technique.
Mostly companies or cloud service providers offers public cloud storage, where they place user's critical data on cloud storage space, which plays a big role against the insecurity of public clouds [1].
So it is a new challenge how to store these critical and sensitive data on cloud storage which transmits easily in multiple platforms like cloud, grid, etc.
Hence public cloud storage needs to have secure and reliable encryption mechanism to hold such type of critical data on it.
So for this, we are going to implement a system which uses a genetic algorithm and visual cryptography for storing such type of data on cloud securely.

GENETIC ALGORITHM

It is a search technique to find exact or approximate solutions for designing, optimization or learning.
The primary advantage of the genetic algorithm comes from the crossover operations. In this two pairs of individuals are selected randomly from the current population they are treated as parents to reproduce. These individuals are selected based on the score of their fitness function. Fitness function defines the quality of individuals. Parent will produce the children for the next generation.
This algorithm is secure as it does not utilize the natural number directly.
This uses three rules to introduce next generation.

- Selection rule: In this rule, a parent is selected to produce children for next generation.
- Crossover rule: Now, here the crossing over of genes from two parents occurs resulting into a new set of genes which leads to a next generation.
- Mutation rule: It is an often called sudden change in the base pair sequence of DNA, which results in a new pair of bases which have some unique characteristics.

VISUAL CRYPTOGRAPHY

Visual cryptography is a scheme to hide a secret image by using any number of shadow images called shares.
"It is basically a secret sharing technique that encrypts our secret image into numerous shares but requires neither computer nor calculations to decrypt the secret image. Reconstruction of the secret image is done visually simple by overlaying the encrypted shares then secret image clearly visible [3]."
By using this technology the complexity of encryption and decryption is reduced and also two ways communication can be achieved very steadily.

Access structure scheme for visual cryptography

- (2, 2)-Threshold VCS scheme: In this scheme, we encrypt a secret message into two different shares and on getting these two, our image will reveal.
- (n, n)-Threshold VCS scheme: In this scheme, we encrypt a secreted message into n no of shares and when we get all these shares together our image will be revealed.
- (k, n)- Threshold VCS scheme: In this scheme, secret image is encrypted into n shares when any group of at least k share is overlaid the secret image will be revealed [2].

LITERATURE SURVEY

Many solutions had been proposed for the security of data.
In the first time 1993, for cryptanalysis of substitution cipher, a genetic algorithm based approach was proposed by Spellman R. To discover the key for substitution cipher, a random type search is possible and this possibility was been proposed by this paper.
For cryptanalysis of transposition cipher, an order based genetic algorithm was given by Mathew in the same year.
In 2006, Garg [12] study proposed "genetic algorithm is used to break the S-DES."
In 2006, Nalini [11] compared various attacks of S-DES using optimization heuristics techniques and GA based techniques.
And this gives a result that G.A minimizes the time complexity.
In 2012 [5] a secret key image encryption method based on genetic algorithm has been proposed, to achieve requirements of any encryption method for encrypting the images.

In 2013 [4] a security algorithm has been proposed for wireless Applications by using a genetic algorithm and RSA, according to their work security of any critical data has highly optimized.
In 2015 [2] for the reliability of data transmission, genetic algorithm, steganography, and visual cryptography are combined together.
In the same year [1] a new approach to the security of data has been proposed, in this data has secretly shared in a cloud environment using steganography and genetic algorithm. It uses pixel mapping method and secret key for providing better results in the security of data.
In 2015 [3] another new approach has been proposed where a combination of visual cryptography and the genetic algorithm has been used. This paper securing the shares using genetic algorithm .it uses simple (2, 2) VCS scheme for shares.
After reviewing all these papers we conclude our concept which uses a genetic algorithm and visual cryptography for securing our critical data and securely share these data and store properly in a cloud environment. In our paper, we are going to introduce a new concept in visual cryptography, which is based on the critical Index.

Table -1 Comparative study of Previous Papers

Author Names	**Year**	**Paper Title**	**Proposed Work**
By Ankita Aggarwal[5]	2012[IJARCSSE]	"Secret Key Encryption Algorithm using Genetic Algorithm"	In this paper, they presented "secret key image encryption method" which is based on genetic an algorithm with the features of crossover and mutation.
By G. Prema [4]	2013[IEEE]	"An enhanced security algorithm for wireless applications using RSA and Genetic Algorithm"	In this paper, "a least significant bit (LSB) Based steganography using genetic algorithm and VC" has been proposed. According to their proposed work security feature of steganography are highly optimized using GA and VC. This approach is well-suited with real-time Applications.
By Aayasha Kausar [2]	2015 [IJIRCCE]	"Secure Data transmission by combining G.A and steganography techniques with VC technique"	In this paper, they used G.A for data Encryption. Steganography for hiding encrypted data using LSB Steganography. And apply VC for secure image and data transfer. In this (2, 2), threshold VCS the scheme has been used. It provides a better result in security.
By Anisha mariya [3]	2015 [IJIREEICE]	"Enhancement of security in Visual Cryptography system using G.A"	In this paper, they use VC along with GA. In this system they first generate shares of the secret image using (2, 2) VC scheme. And GA is used to encrypt generated shares to make them secure and prevent unauthorized access to information. In this scheme, the bandwidth and memory usage are very low.
By Subhasish mandal [1]	2015 [IEEE]	"Secret data sharing in a cloud environment Using steganography and encryption using GA."	They proposed a crypto stego Methodology. In this steganography technique embedded confidential data using Pixel Mapping Method (PMM). For encryption and decryption, they use secret session key. This paper gives better encryption and decryption time as compared to DES, AES and RSA.

PROPOSED WORK OR PROCEDURE

Now-a-days all the organizations using cloud services for their storage of data. All the organizations want to secure their data with high security.
So for making high security of data we are using visual cryptography and genetic algorithm as our proposed work.
In our approach we have introduced new approach which is critical index (ci), with the help of critical index we has enhancing our security features. Our approach provides high security with low storage overhead.
Our approach consist three main phases.

- Generating shares with the help of critical index.
- Encryption and decryption of generated shares.
- Share encrypted file to the cloud server.

Our approach focuses on six main functions for implementing above three phases.

(i)Signup (username)
Step-1 initialize u= username;
Step-2 fetches all the usernames from database;
Step-3 for all (users)
{Check
If (username (fetched from database) =u;
{Show error (username is already exist);
} else
{Create database (username);
}}

(ii) Make shares (files)
Step-1 browse file (image, audio, video)
Step-2 initialize with critical index (ci)
a. if ci=6; then output=6;
b. else if ci=5; then output=5;
c. else if ci=4; then output=4;
d. else if ci=3; then output=3;
e. else if ci=2; then output=2;
f. show msgbox=”split successful”;

(iii) Encrypt (part file)
a. Step-1 browse all parts file and encrypt each part file one by one.
b. Set string password= “my key 123”;
c. Get the bytes of the string file.
d. Byte[]bytesToBeEncrypted=file.ReadAllBytes (field);
e. Hast the password with mykey123.
f. PasswordBytes mykey 123.create ().compute Hash (password Bytes);
g. Byte[]bytesEncrpted=AES_Encrypt (bytesToBeEncrypted, passwordBytes);
h. (Crossover operation)
i. For i=1….n; convert each data into its binary form and store it in B.
j. Here, we take two attributes x and y.
k. For example, let secret keys=3 and 5 and do crossover.
l. (Mutation operation)
m. Select mutation attributes as C, like secret key is 4 and we do mutation access all data.
n. Step-3 finally we get encrypted file which is enhanced by genetic algorithm crossover and mutation.

(iv) Share/ upload (encrypt file)
a. Get ftplocation, file, user and password of appropriate server.
b. uploadToFtp (ftplocation, file, user, password);

(v) Download
a. select file from [share] where [Friend] =” ”+label1. Text;
b. Download File (ftp location, file, user, and password); and save file=E:/;

(vi) Merge (files)
Step-1 gets all shares.
Step-2 convert file into Byte array.
Step-3 append all part file with File Mode. Append;

The proposed work is shown in fig 1. In this figure, we first generate the shares of secret data using visual cryptography scheme. If our data is more critical then we assign a high critical index and divide it by a maximum number of shares and if our data is less critical then we assign it low critical index and divide it to a minimum no of shares.
In the next step, a genetic algorithm is used to encrypt the generated shares to make them more secure and preventing it from unauthorized access. Then store this encrypted file into the cloud and share it with an authorized user
At the server side, the user can download encrypted shares from the cloud and decrypt it using genetic algorithm then combine decrypted shares together to form the secret data.
*Critical Index: It is a new term, Introduced by us in visual cryptography. Here, we assign index (ci) from 0 to 5 for the minimum to maximum critical data.

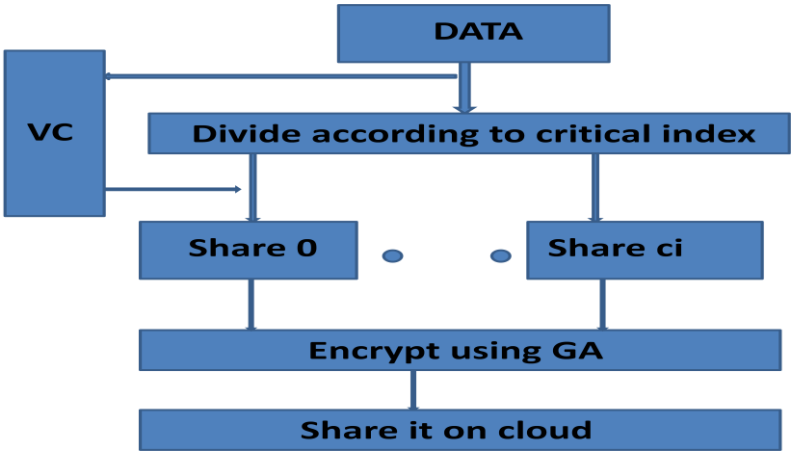

Fig. 1 Proposed Architecture for Sharing Data

RESULTS AND DISCUSSION

We have implemented these approaches in visual studio 2010. We have use c# as front end and Microsoft SQL server 2008 at the backend for the simulation. We have implemented this approach on local server which can be simulated on real world environment.

Table -2 Compare Proposed Model Encryption and Decryption Time with DES and RSA

Algorithm	Packet Size	Encryption Time (sec)	Decryption Time (sec)
DES	100	1.605	1.118
RSA		2.122	2.094
Proposed Method		1.342	1.514
DES	500	5.247	4.739
RSA		10.812	10.500
Proposed Method		4.948	4.726
DES	1000	12.393	11.990
RSA		25.392	21.046
Proposed Method		10.345	10.202
DES	5000	62.49	61.509
RSA		124.166	107.663
Proposed Method		52.089	53.502

Here, we shows the experimental results for encryption and Decryption with DES and RSA algorithm in the table II, which shows comparison of two algorithms DES and RSA with Proposed AES Plus GA based Encryption, using same packet size for three experiments, which shows that our approach is faster and secured with previous encryption methods.

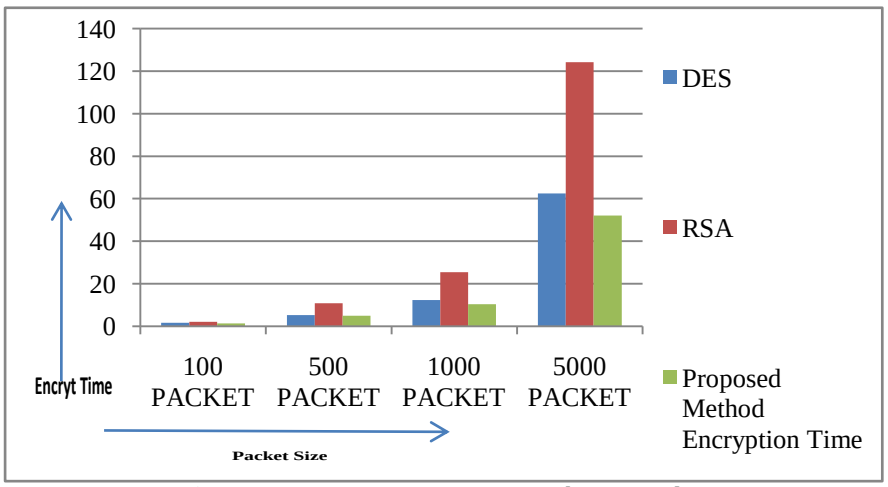

Fig. 2 Compare Encryption time with DES and RSA

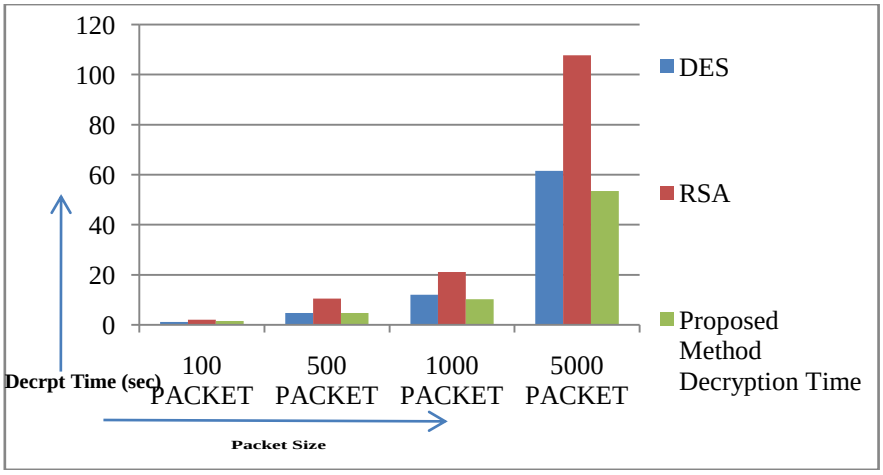

Fig. 3 Compare Decryption time with DES and RSA

Table -3 Comparative Splitting Time of Our Approach with Existing Approach

File Type	Critical Index	Time is taken by existing approach	Time is taken by our approach	Total time saved
Image (183*275) Size=7.21kb	0 2 4 6	10.33ms 10.33ms 10.33ms 10.33ms	0ms 04.52ms 08.23ms 10.33ms	10.33ms 5.81ms 2.1ms 0ms
Video (WMV) Size (25.0mb)	0 2 4 6	16.75ms 16.75ms 16.75ms 16.75ms	0ms 09.51ms 12.77ms 16.75ms	16:75ms 7.24ms 3.98ms 0ms
Audio (mp3) Size=8.02mb	0 2 4 6	12.75ms 12.75ms 12.75ms 12.75ms	0ms 8.89ms 10.82ms 12.72ms	12.75ms 3.86ms 1.93ms 0ms

In the above comparison Table III we have compare our proposed approach with the existing approach, here we take three types of file like image, audio, and video of different sizes what we found here that the overall time of our approach is better than the existing approach because in existing approach the division is fixed for every file type here we assume that the fixed division is '6' but in our proposed approach the division depends on the criticality of the data. If our data is not critical then we only encrypt and send it to the Cloud but if our data critical index is 2, 3, 4, 5, and 6 then we divide it accordingly.

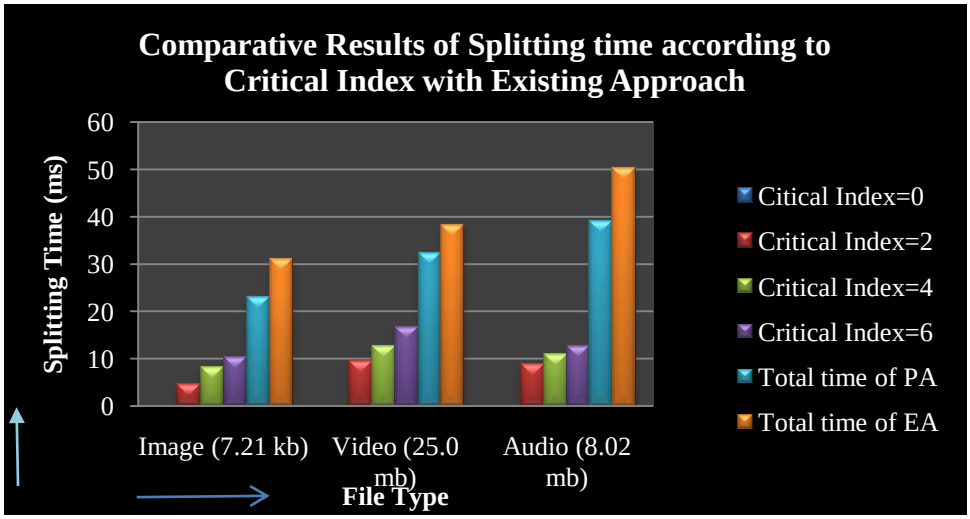

Fig. 4 Comparative Results of Splitting time according to Critical Index with Existing Approach

In the above chart we have given the comparison result on the basis of Critical Index, here we can see that after applying this concept we have save our much time for any multimedia file, after the experimental result of this new approach we have find that this approach reduces our overall storage overhead and save splitting time.

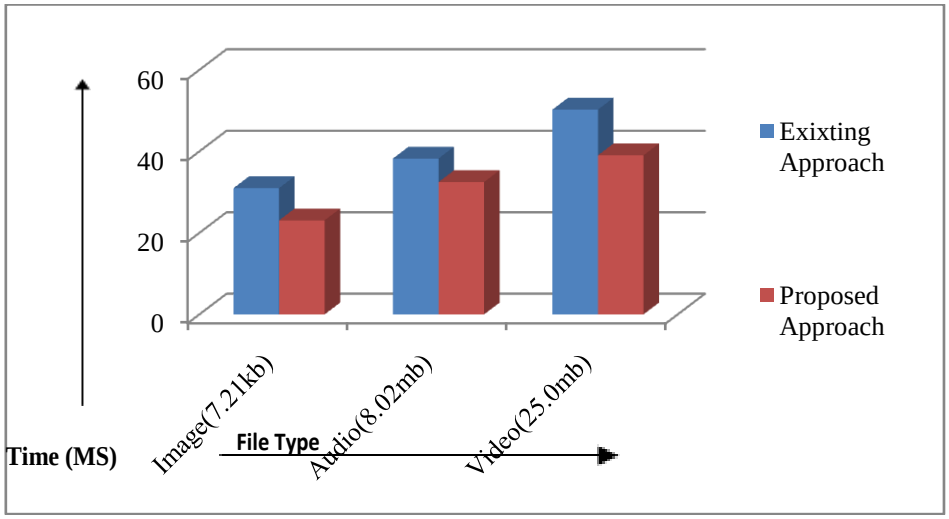

Fig. 5 Compare Total Splitting Time of Proposed Approach with Existing Approach

CONCLUSION & FUTURE WORK

In this paper, we proposed a new concept in visual cryptography methods. According to the priority of confidential data, number of shares can be decided and encrypted by using an AES and genetic algorithm and store it successfully on the cloud. It gives improved results in terms of security and gives overall minimum overhead. Previously visual cryptography is only used for images but here we extend visual cryptography for video and introduced a new term in visual cryptography which is known as a critical index. Basically, critical index defines the criticality of the data means how these data is more critical to user. Our approach provides multilevel security, enhanced bandwidth utilization and secure transmission of multimedia data. We conclude that the security features of the genetic algorithm are extremely optimized using visual cryptography. This technique is very useful for all the user types who want to bother time of or who don't want to bother time. In the future work, there is a planning to design a public key data encryption method based on this technique which will target to use in highly secure multimedia data transmission applications.

Acknowledgements

I take the opportunity to express my heartfelt adulation and gratitude to my dissertation supervisor Dr. C.S Yadav, Professor & Head, Department of Computer Science and Engineering, NIET, Greater Noida, for permitting me to undertake this work.

I express my heartfelt gratitude to my respected Co. Supervisor Mr. Mayank Deep Khare, Assistant Professor, Department of Computer Science and Engineering, NIET, Greater Noida, for his unreserved guidance, and advice in ASP.Net Software and the present research work. He was always there to listen and give advice. The present work is a testimony to his activity, inspiration and ardent personal interest taken by him during course of his work in his present form. I am thankful to him for his dedication and support.

Last but not least, I am grateful to my friends and family member especially my mother, my sisters, and my friend Neetu for their encouragement and tender. Without them, I was unable to have enough strength to finish this dissertation

REFERENCES

[1]. Subhasish Mandal, Secret data sharing in a cloud environment using Steganography and encryption using genetic algorithm, *IEEE international conference on green computing and internet of things (ICGCIOT 2015*, ***2015,*** 978-1-4673-7910-6/15/$31.00, [1469-1474].

[2]. Aayasha Kausar, Secure data transmission by combining genetic algorithm and Steganography techniques with visual cryptography technique, *International Journal of Innovative Research in Computer and Communication Engineering*, **2015**, Vol. 3, Issue 11, November 2015, DOI: 10.15680/IJIRCCE 2015.0311215, [11365-11369].

[3]. Anisha Mariya, Enhancement of security in visual cryptography system using genetic algorithm, *International journal of innovative research in electrical, electronics, instrumentation and control engineering*, **2015**, Vol. 3, Special Issue 1, April 2015, [32-37].
[4]. G.prema, An enhanced security algorithm for wireless applications using RSA and Genetic approach, *IEEE 4th ICCCNT*, **2013,** Tiruchengode, India, IEEE – 31661
[5]. Ankita Aggarwal, Secret key encryption algorithm using genetic algorithm, *International Journal of Advanced Research in Computer Science and Software Engineering*, **2012**, Volume 2, Issue 4, April 2012, [216-218].
[6]. L.M.R.J lobo, Use of genetic algorithm in network security, *IJCA*, **2012**, [0975-8887].
[7]. Soumya paul, Design and implementation of network security using genetic algorithm, *IJRET*, **2013**, ISSN: 2319-1163.
[8]. Gens F (2008) defining "cloud services" and "cloud computing", IDC exchange, 23 Sep 2008.
[9]. Spellman R, Janssen M, Use of Genetic Algorithm in Cryptanalysis of Simple Substitution Cipher, **1993**, Vol.l7, No.4, [367- 377].
[10]. Spellman R, Cryptanalysis of Knapsack Ciphers using Genetic Algorithms, **1993**, Vol7, No.4, [367-377].
[11]. Nalini, Cryptanalysis of Simplified data encryption standard via Optimization heuristics, *International Journal of Computer Sciences and network security*, **2006**, vol 6, No IB, Jan 2006.
[12]. Garg Poonam, Genetic algorithm Attack on Simplified Data Encryption Standard algorithm, *International journal Research in Computing Science*, **2006,** ISSN1870-4069.
[13]. P. Mohan, D. Marin, S. Sultan Medinet: personalizing the self-care process for patients with diabetes and cardiovascular disease using mobile telephony, *International Conference of IEEE Engineering in Medicine and Biology Society*, **2008,** vol.2008, no. 3, [755-758].
[14]. Mayank Deep Khare, Storage cost efficient approach for cloud storage and intermediate data sets in clouds, *IEEE ICGCIOT*, **2015** DOI: 10.1109/ICGCIOT.2015.7380700.
[15]. Aditi Tripathi, Mayank Deep Khare, Efficient and secure approach for faster data availability and restoration in disaster cloud data management, *IEEE ICGCIOT*, **2015**, ICGCIOT, DOI: 1109/ICGIOT.2015.7380628.
[16]. S Sohrabi, A survey on Energy-Aware Cloud, *European Journal of Advances in Engineering and Technology*, **2015,** ISSN: 2394 - 658X, [80-91].
[17]. DIAO Zhe, Study on Data Security Policy Based On Cloud Storage, *IEEE 3rd International Conference on Big Data Security on Cloud*, **2017,** 978-1-5090-6296-6/17 $31.00 © 2017 IEEE DOI 10.1109/BigDataSecurity.2017.12, [145-149].

BIOGRAPHY

Mamta is a student of M.Tech Computer Science and Engineering, Greater Noida. She received her bachelor Degree in computer science & engineering from Indira Gandhi Institute of Technology (IP University), Delhi. She acquired the first position in all her studies. Her research interest includes Cloud Computing and Networking. She has published 3 research papers in international journal and conferences.

Fatima is a student of M.Tech Computer Science and Engineering & Technology, Greater Noida. She received Master of Computer Applications degree. Her research interest is in Cloud Computing and she has taken awards for participated in cultural activities at the university level. And contributed three years in national services scheme (NSS)

Mayank Deep Khare completed M.Tech (Information Technology) from Madan Mohan Malaviya University of Technology, Gorakhpur in 2015. He is working at NIET, Greater Noida for last one year as Assistant Professor in the department of Computer Science & Engineering. He is equipped with an extraordinary caliber and appreciable academic potency. He has published 9 papers in various international and national conferences.

Dr. Chandra Shekhar Yadav is an Associate Professor and Head, Computer Science & Engineering Department at Noida Institute of Engineering & Technology (NIET), Greater Noida. He has about 17 years of experience in teaching. He received Master of Computer Applications degree from Institute of Engineering & Technology (IET), Lucknow in the year 1998, M. Tech (Computer Science & Engineering) from JSSATE, Noida in the year 2007. He received his Ph.D. degree in Computer Science & Engineering from A.P.J. Abdul Kalam Technical University, Lucknow in the year 2016. He has supervised 07 M.Tech theses. He has published 19 research papers in various national, international journals and conferences.