International Journal of Engineering &Technology, *7 (1.7) (2018) 27-33*

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Secure data in cloud with multimodal key generation

P Selvarani [1] *, N Malarvizhi [2]

[1] Research Scholar, Department of Computer Science and Engineering, School of Computing, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai-62, TamilNadu, India
[2] Professor, Department of Computer Science and Engineering, School of Computing, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai-62, TamilNadu, India
**Corresponding author E-mail: selvarani.meena@gmail.com*

Abstract

Data Security is the Major problem in Cloud Computing. In order to overcome the data security problem the proposed technique utilizes effective data storage using biometric-based cryptographic authentication to support the user authentication for the cloud environment. For user authentication here we are considering iris and fingerprint. Initially the feature values are extracted from the iris and fingerprint using local binary pattern and Minutiae extraction respectively. Local binary pattern operator works with the eight neighbors of a pixel, using the value of this center pixel as a threshold. Minutiae points are the major features of a fingerprint image and are used in the matching of fingerprints. These minutiae points are used to determine the uniqueness of a fingerprint image. Based on that the proposed feature values are extracted from the iris and fingerprint image. In order to improve the security, the suggested technique utilizes the optimal features. For selecting the optimal features hybrid particle swarm optimization and genetic algorithm (HPSOGA) is utilized. Particle swarm optimization (PSO) is a population based stochastic optimization technique. The system is initialized with a population of random solutions and searches for optima by updating generations. In PSO, the potential solutions, called particles, fly through the problem space by following the current optimum particles. Genetic Algorithms (GAs) are adaptive heuristic search algorithm based on the evolutionary ideas of natural selection and genetics. In our proposed method these two optimization algorithm is hybrid for more secure. From the optimization algorithm the suggested technique selects the optimal features. and then the optimal features are used to encrypt the input data. For encryption and decryption, the proposed technique utilizes Triple DES algorithm. Finally the encrypted data is stored in cloud. The performance of the proposed technique is evaluated in terms of encryption and decryption time, memory utilization and overall execution time. Our proposed data storage using biometric-based authentication is implemented with the help of Cloud simulator in the working platform of java.

Keywords: *Multimodal Bio Cryptographic Authentication; Local Binary Pattern; Hybrid Particle Swarm Optimization with Genetic Algorithm; Triple DES Algorithm; Cloud Storage Environment.*

1. Introduction

Cloud computing is an emerging computing technology that uses the internet and central remote servers to maintain data and application. Data security becomes more and more important in cloud computing. [1] because hackers can hack the data during data transfer. Hacking means unauthorized user access the data without data owner authorization. [2] So authorized owner will lose billions of dollars due to illegal activities like copying creating and destroying the data without data owner authorization. So it is important to secure the cloud data. Figure 1 Represents Hackers hack the data.

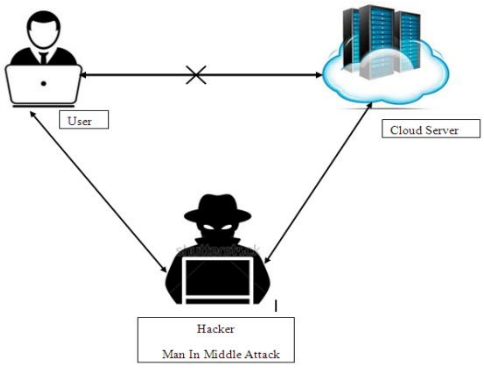


Fig. 1: Represents Meet in Middle Attack.

The user authentication, which is main part of the cloud computing, determines only the authorized user is to access the data. The best way is to encrypt the data before send it to a third party. The problem with storing the data in cloud environment using password system used as a key to encrypt the data, it is not secured, forgotten and easily stolen. [3]. To overcome this problem multimodal bio cryptographic technique [4] can be used to support the user authentication in cloud environment because it is more reliable than password based system, stable, not forgotten, don’t stolen, forgery, copied, shared and distributed etc.,

1.1. Overall process

User authentication here we are considering Fingerprint and iris. Figure 2 represents overall process of our research work. Initially User has given input to the fingerprint image and iris image. Feature can be extracted from the fingerprint and iris image using Local Binary Pattern. Generating feature value can be combined and it can be given input to the Hybrid Genetic and Particle swarm optimization algorithm for finding best solution.
The best solution can be act as a key to encrypt and decrypt the data using Triple DES algorithm. Finally Stored in Cloud Environment. So the intruder cannot be able to access the data.

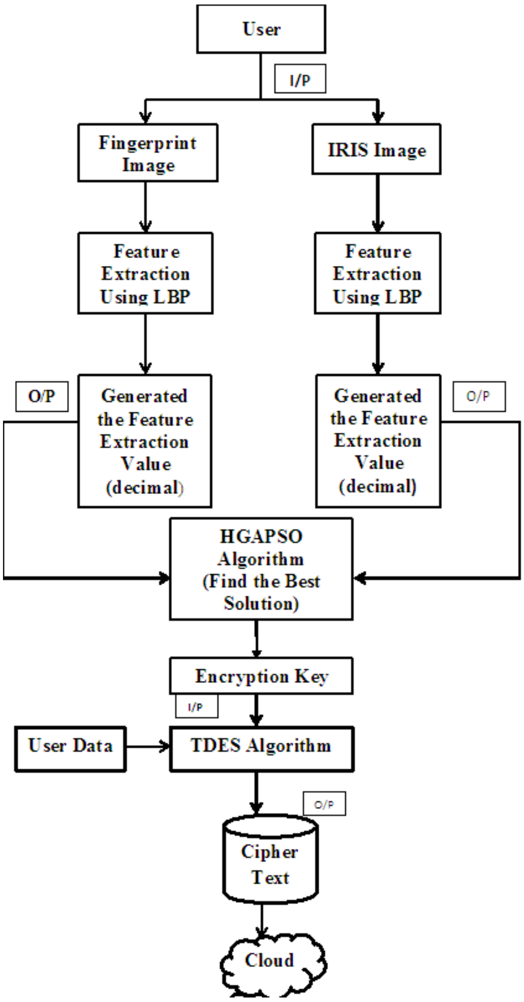

User
I/P
Fingerprint Image
IRIS Image
Feature Extraction Using LBP
Feature Extraction Using LBP
O/P
Generated the Feature Extraction Value (decimal)
Generated the Feature Extraction Value (decimal)
O/P
HGAPSO Algorithm (Find the Best Solution)
Encryption Key
I/P
User Data
TDES Algorithm
O/P
Cipher Text
Cloud

Fig. 2: Overall Architecture.

1.2. Local binary pattern

Local binary pattern operator works with the eight neighbors of a pixel, using the value of this center pixel as a threshold.
Calculate the Fingerprint and Iris Feature Extraction values using LBP. Each pixel Find its LBP. Compare the center pixel value of its neighbor. Center pixel value is greater than the neighbor value becomes 0 other wise 1. [5]. Likewise all the pixel value can be calculated by using LBP. Finally Binary value converted into decimal value. Same process can be used as extracting the feature value of Iris. Figure 3 represents Process of Local Binary Pattern.

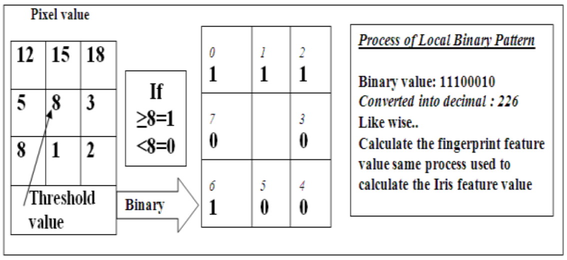
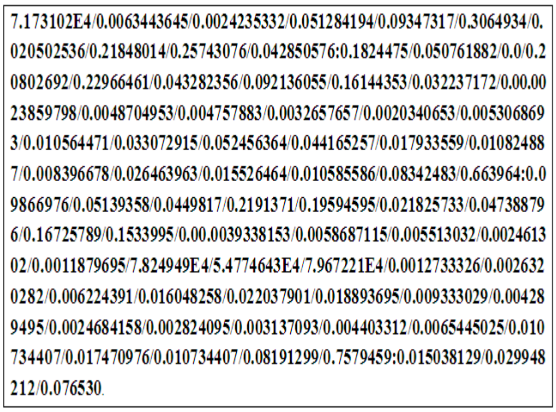

Pixel value
12
15
18
5
8
3
8
1
2
Threshold value
If
≥8=1
<8=0
Binary
0
1
1
1
2
1
7
0
3
0
6
1
5
0
4
0
Process of Local Binary Pattern
Binary value: 11100010
Converted into decimal : 226
Like wise..
Calculate the fingerprint feature value same process used to calculate the Iris feature value

Fig. 3: Process of Local Binary Pattern.

Figure 4 represents Fingerprint feature Values, and Figure 5 represents Iris feature Values by using Local Binary Pattern.

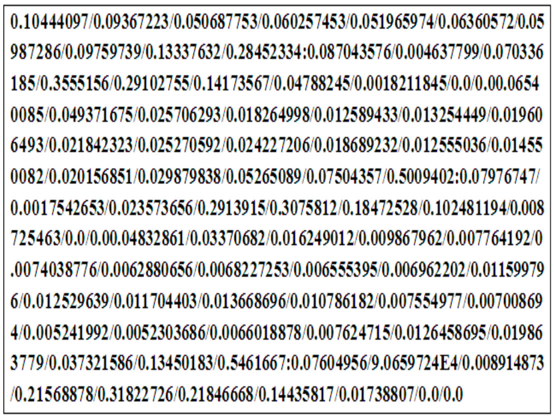
2. Fingerprint feature value using LBP



```
7.173102E4/0.0063443645/0.0024235332/0.051284194/0.09347317/0.3064934/0.
020502536/0.21848014/0.25743076/0.042850576:0.1824475/0.050761882/0.0/0.2
0802692/0.22966461/0.043282356/0.092136055/0.16144353/0.032237172/0.00.00
23859798/0.0048704953/0.004757883/0.0032657657/0.0020340653/0.005306869
3/0.010564471/0.033072915/0.052456364/0.044165257/0.017933559/0.01082488
7/0.008396678/0.026463963/0.015526464/0.010585586/0.08342483/0.663964:0.0
9866976/0.05139358/0.0449817/0.2191371/0.19594595/0.021825733/0.04738879
6/0.16725789/0.1533995/0.00.0039338153/0.0058687115/0.005513032/0.0024613
02/0.0011879695/7.824949E4/5.4774643E4/7.967221E4/0.0012733326/0.002632
0282/0.006224391/0.016048258/0.022037901/0.018893695/0.009333029/0.00428
9495/0.0024684158/0.002824095/0.003137093/0.004403312/0.0065445025/0.010
734407/0.017470976/0.010734407/0.08191299/0.7579459:0.015038129/0.029948
212/0.076530.
```

Fig. 4: Fingerprint Feature Value Using LBP.

3. Iris feature value using LBP



```
0.10444097/0.09367223/0.050687753/0.060257453/0.051965974/0.06360572/0.05
987286/0.09759739/0.13337632/0.28452334:0.087043576/0.004637799/0.070336
185/0.3555156/0.29102755/0.14173567/0.04788245/0.0018211845/0.0/0.00.0654
0085/0.049371675/0.025706293/0.018264998/0.012589433/0.013254449/0.01960
6493/0.021842323/0.025270592/0.024227206/0.018689232/0.012555036/0.01455
0082/0.020156851/0.029879838/0.05265089/0.07504357/0.5009402:0.07976747/
0.0017542653/0.023573656/0.2913915/0.3075812/0.18472528/0.102481194/0.008
725463/0.0/0.00.04832861/0.03370682/0.016249012/0.009867962/0.007764192/0
.0074038776/0.0062880656/0.0068227253/0.006555395/0.006962202/0.01159979
6/0.012529639/0.011704403/0.013668696/0.010786182/0.007554977/0.00700869
4/0.005241992/0.0052303686/0.0066018878/0.007624715/0.0126458695/0.01986
3779/0.037321586/0.13450183/0.5461667:0.07604956/9.0659724E4/0.00891487
/0.21568878/0.31822726/0.21846668/0.14435817/0.01738807/0.0/0.0
```

Fig. 5: Iris Feature Value Using LBP.

3.1. Combined feature value of fingerprint and iris with HGAPSO

Extracted value of Fingerprint and Iris can be combined and it has been given input to the hybrid Genetic Algorithm[6] and Particle swarm optimization algorithm [7] to find the best solution by using cross over mutation technique. Figure 6 Represents Process of HGAPSO Algorithm.

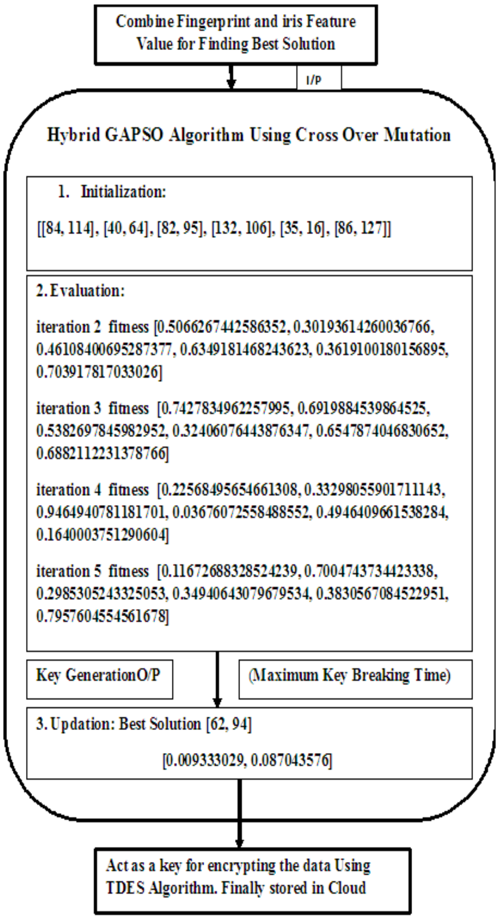

Combine Fingerprint and iris Feature Value for Finding Best Solution
I/P
Hybrid GAPSO Algorithm Using Cross Over Mutation
1. Initialization:
[[84, 114], [40, 64], [82, 95], [132, 106], [35, 16], [86, 127]]
2. Evaluation:
iteration 2 fitness [0.5066267442586352, 0.30193614260036766, 0.46108400695287377, 0.6349181468243623, 0.3619100180156895, 0.703917817033026]
iteration 3 fitness [0.7427834962257995, 0.6919884539864525, 0.5382697845982952, 0.32406076443876347, 0.6547874046830652, 0.6882112231378766]
iteration 4 fitness [0.22568495654661308, 0.33298055901711143, 0.9464940781181701, 0.03676072558488552, 0.4946409661538284, 0.1640003751290604]
iteration 5 fitness [0.11672688328524239, 0.7004743734423338, 0.2985305243325053, 0.34940643079679534, 0.383056708452295l, 0.7957604554561678]
Key GenerationO/P
(Maximum Key Breaking Time)
3. Updation: Best Solution [62, 94]
[0.009333029, 0.087043576]
Act as a key for encrypting the data Using TDES Algorithm. Finally stored in Cloud

Fig. 6: Process of HGAPSO Algorithm.

To improve the optimization performance can be used as Hybrid GA+PSO as more secure by using, (Figure 7 Represents) Cross over Mutation Technique as Selection, Recombination and Mutation.

3.2. Selection

Replicate the most successful solutions found in a population at a rate proximal to their relative quantity.

3.3. Recombination

Decomposes two distinct solutions and then randomly mixes their parts to form novel solution.

3.4. Mutation

Randomly perturbs a candidate's solution.

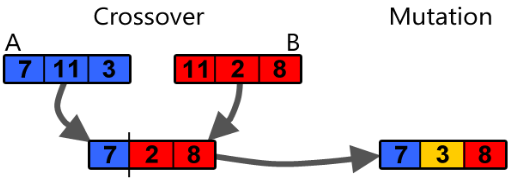


Fig. 7: Cross over Mutation.

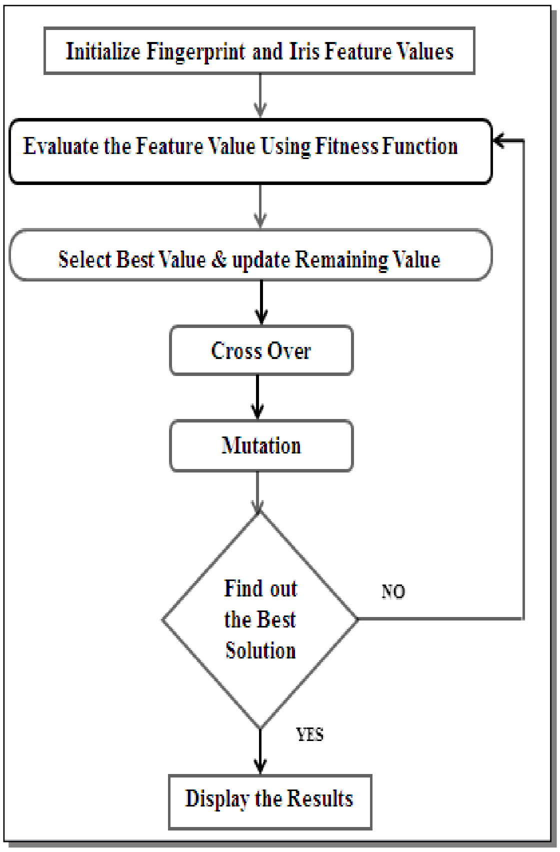
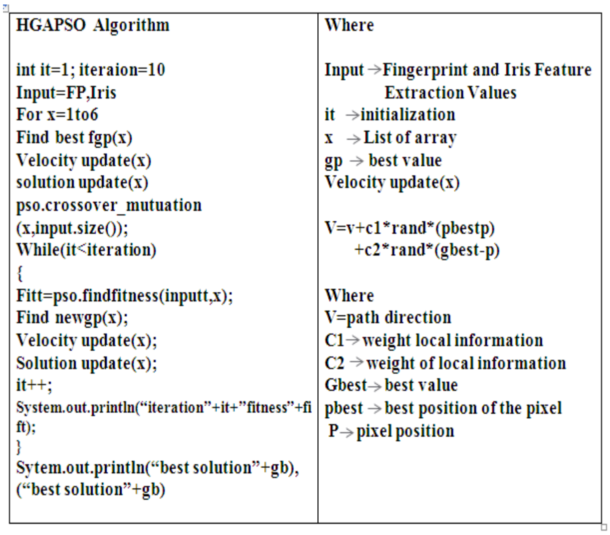

Initialize Fingerprint and Iris Feature Values
Evaluate the Feature Value Using Fitness Function
Select Best Value & update Remaining Value
Cross Over
Mutation
Find out the Best Solution
NO
YES
Display the Results

Fig. 8: Flowchart of HGAPSO Algorithm.

3.5. HGAPSO Algorithm



```
HGAPSO Algorithm

int it=1; iteraion=10
Input=FP,Iris
For x=1to6
Find best fgp(x)
Velocity update(x)
solution update(x)
pso.crossover_mutuation
(x,input.size());
While(it<iteration)
{
Fitt=pso.findfitness(inputt,x);
Find newgp(x);
Velocity update(x);
Solution update(x);
it++;
System.out.println("iteration"+it+"fitness"+fi
ft);
}
Sytem.out.println("best solution"+gb),
("best solution"+gb)
```

Where

Input → Fingerprint and Iris Feature
Extraction Values
it → initialization
x → List of array
gp → best value
Velocity update(x)

V=v+c1*rand*(pbestp)
+c2*rand*(gbest-p)

Where
V=path direction
C1 → weight local information
C2 → weight of local information
Gbest → best value
pbest → best position of the pixel
P → pixel position

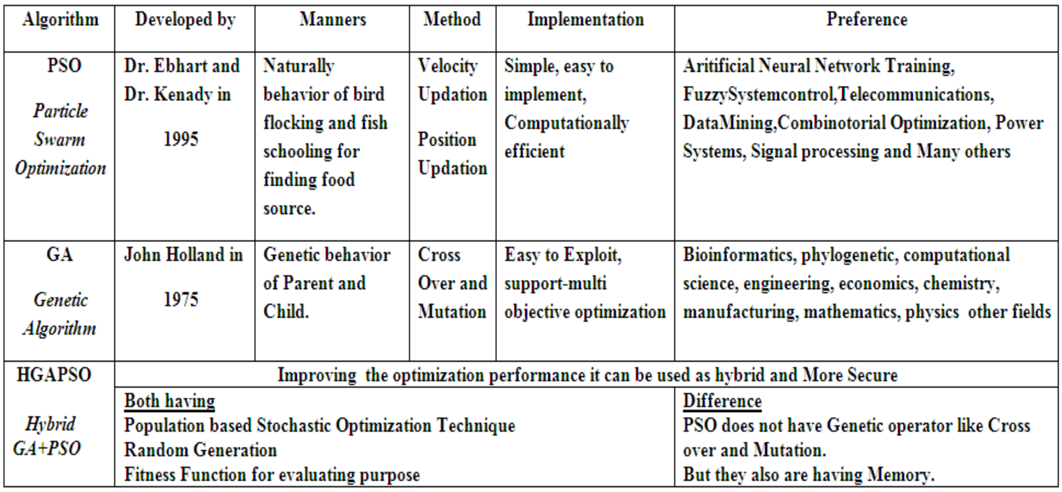
Fig. 9: HAPSO Algorithm.

Initialize Fingerprint and Iris Feature Extraction Values.
Evaluate the Feature Values using Fitness Function.
(Task: Maximum Key Breaking Time
Choose the Best Value and Update the Remaining Value.
Compare the initialized value with updated value and also calculate the fitness function
Repeat the iteration, till to find out the best solution.

Finally stop the iteration. Best solution act as a key for encrypting the data using TDES Algorithm.

Fig. 10: Process of HGAPSO.

To find out the best solution key is 0.0221135095 used as a key for encrypting and decrypting data using Triple DES algorithm.



Algorithm	Developed by	Manners	Method	Implementation	Preference
PSO *Particle Swarm Optimization*	Dr. Ebhart and Dr. Kenady in 1995	Naturally behavior of bird flocking and fish schooling for finding food source.	Velocity Updation Position Updation	Simple, easy to implement, Computationally efficient	Aritificial Neural Network Training, FuzzySystemcontrol,Telecommunications, DataMining,Combinotorial Optimization, Power Systems, Signal processing and Many others
GA *Genetic Algorithm*	John Holland in 1975	Genetic behavior of Parent and Child.	Cross Over and Mutation	Easy to Exploit, support-multi objective optimization	Bioinformatics, phylogenetic, computational science, engineering, economics, chemistry, manufacturing, mathematics, physics other fields
HGAPSO *Hybrid GA+PSO*	Improving the optimization performance it can be used as hybrid and More Secure				
	Both having Population based Stochastic Optimization Technique Random Generation Fitness Function for evaluating purpose				Difference PSO does not have Genetic operator like Cross over and Mutation. But they also are having Memory.

Fig. 11: PSO Vs. GA.

3.6. Cryptographic technique

William Stallings proposed cryptographic technique for the purpose of data security, in the concept of plaintext can be converted to cipher text called encryption and for the reverse process of decryption. There are two types of Cryptographic Algorithm. Symmetric algorithm and Asymmetric algorithm. [8].Same key can be used for symmetric and different key can be used for asymmetric algorithm. Symmetric key algorithm such as DES, AES, 3DES, Blowfish etc., and Asymmetric key algorithm such as RSA, Diffie-helman key exchange etc., for more security purpose
Triple DES algorithm can be used for data encryption and decryption.

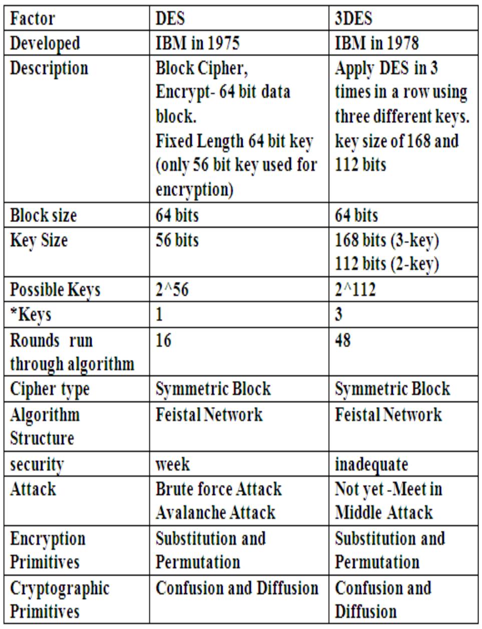
3.7. Triple DES algorithm

Triple DES algorithm uses three iterations of common DES cipher. It receives a secret 168-bit key, which is divided into three 56-bit keys. Encryption using the first secret key Decryption using the second secret key Encryption using the third secret key.

Encryption: c = E3 (D2 (E1 (m)))

Decryption=D1 (E2 (D3 (c)))

In this research work find out the best solution 0.0221135095 (This value derived from fingerprint and iris).It can be act as a key for encrypting and decrypting the data. So the intruder cannot be able to access the encrypted data why because particular portions of fingerprint and iris value can be optimized. So it is more secured.



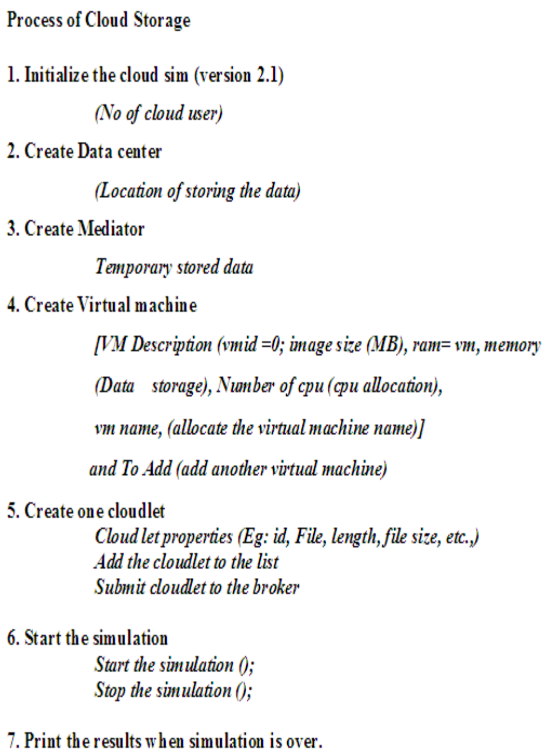
Factor	DES	3DES
Developed	IBM in 1975	IBM in 1978
Description	Block Cipher, Encrypt- 64 bit data block. Fixed Length 64 bit key (only 56 bit key used for encryption)	Apply DES in 3 times in a row using three different keys. key size of 168 and 112 bits
Block size	64 bits	64 bits
Key Size	56 bits	168 bits (3-key) 112 bits (2-key)
Possible Keys	2^56	2^112
*Keys	1	3
Rounds run through algorithm	16	48
Cipher type	Symmetric Block	Symmetric Block
Algorithm Structure	Feistal Network	Feistal Network
security	week	inadequate
Attack	Brute force Attack Avalanche Attack	Not yet -Meet in Middle Attack
Encryption Primitives	Substitution and Permutation	Substitution and Permutation
Cryptographic Primitives	Confusion and Diffusion	Confusion and Diffusion

Fig. 12: Triple DES.

3.8. Testing

Table 4 Represents Randomly Testing fingerprint and iris image to find out the attack by using in the existing technique of Particle Swarm Optimization algorithm with proposed technique of Hybrid Genetic with Particle Swarm optimization Algorithm. It can be find our Less Attack by comparing HGAPSO Algorithm. So it can be concluded as HAPSO is better than PSO.

Images	HGAPSO	PSO
Fingerprint -109_3.png Iris-108_6.png	Best Solution [84, 50] [0.10444097, 0.0017286023]	Best Solution [78, 11] [0.15580185, 0.052767564]
Fingerprint -109_4.png Iris-108_7.png	Best Solution [139, 76] [0.0063461806, 0.08490781]	Best Solution [13, 92] [0.24218619, 0.1362495]
Fingerprint -109_5.png Iris-109_1.png	Best Solution [62, 34] [0.0071847257, 0.017490147]	Best Solution [67, 125] [0.0084936265, 0.30564347]
Fingerprint -109_6.png Iris-109_2.png	Best Solution [95, 87] [0.0054069953, 0.06825483]	Best Solution [162, 16] [0.32856014, 0.07470472
Fingerprint -109_7.png Iris-109_3.png	Best Solution [106, 99] [0.02799945, 0.117743544]	Best Solution [20, 43] [0.0023859798, 0.021825733]



Process of Cloud Storage

1. Initialize the cloud sim (version 2.1)

(No of cloud user)

2. Create Data center

(Location of storing the data)

3. Create Mediator

Temporary stored data

4. Create Virtual machine

[VM Description (vmid =0; image size (MB), ram= vm, memory

(Data storage), Number of cpu (cpu allocation),

vm name, (allocate the virtual machine name)]

and To Add (add another virtual machine)

5. Create one cloudlet

Cloud let properties (Eg: id, File, length, file size, etc.,)
Add the cloudlet to the list
Submit cloudlet to the broker

6. Start the simulation

Start the simulation ();
Stop the simulation ();

7. Print the results when simulation is over.

Fig. 13: Best solution of HGAPSO with PSO.

3.9. Process of cloud storage [9]

Testing Attack HGAPSO with PSO

Proposed HGAP-SO	0.018163456504999995
Existing PSO	0.039866595835000004
Total Time	1 minute 16 seconds

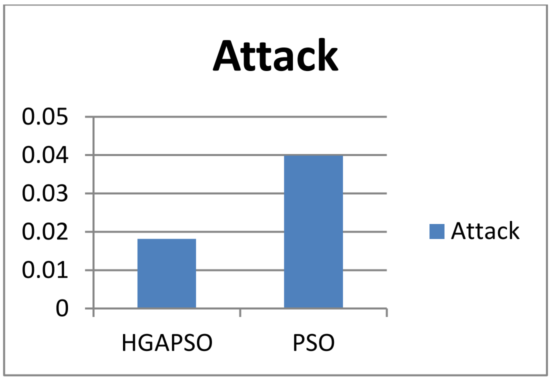
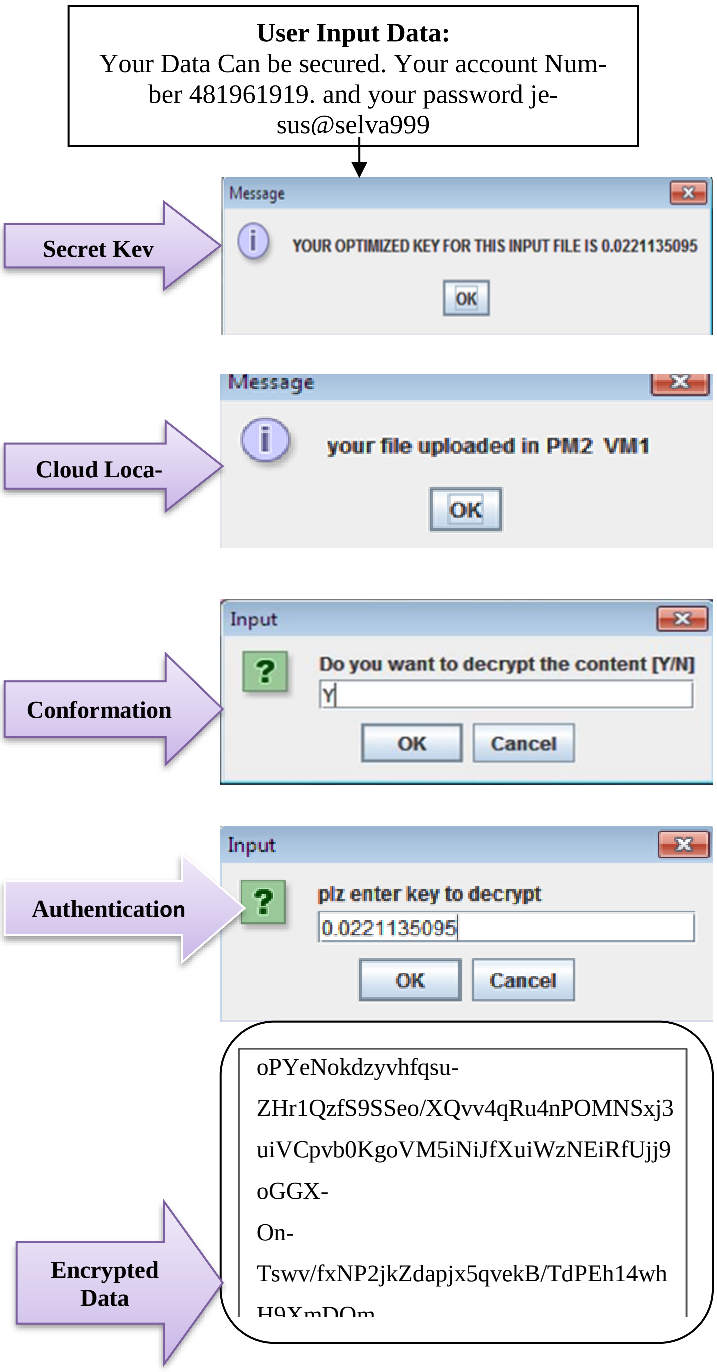


Fig. 14: Less Attack with Comparing PSO.



User Input Data:
Your Data Can be secured. Your account Number 481961919. and your password jesus@selva999

YOUR OPTIMIZED KEY FOR THIS INPUT FILE IS 0.0221135095

your file uploaded in PM2 VM1

Do you want to decrypt the content [Y/N]

Y

plz enter key to decrypt

0.0221135095

oPYeNokdzyvhfqsu-
ZHr1QzfS9SSeo/XQvv4qRu4nPOMNSxj3
uiVCpvb0KgoVM5iNiJfXuiWzNEiRfUjj9
oGGX-
On-
Tswv/fxNP2jkZdapjx5qvekB/TdPEh14wh
H9XmDQm

Fig. 15: Process of Encryption and Decryption.

4. Conclusion

Derived the Best solution from fingerprint and Iris with the help of LBP, HGAPSO algorithm, Cross over Mutation technique, and Triple DES algorithm. (i) Derived the feature value of fingerprint and Iris using LBP. (ii) To find the Best Solution using HGAPSO algorithm with the help of cross over mutation technique. (iii) To Encrypting the data using Triple DES algorithm and it is stored in cloud environment. So the intruder cannot be able to access the data in cloud environment. In this research work at final stage randomly checking the Fingerprint and iris with the help of Proposed HGAPSO algorithm, and also check with the Existing Particle Swarm optimization algorithm. Comparing both algorithms as per the result wise HGAPSO is better than PSO algorithm. The total successful building time is 1 minute 16 seconds. It can be more secure Less attack and higher data security in cloud.

References

[1] M. Lori, “Data security in the world of cloud computing,” Copublished by the IEEE Computer and reliability Societies, pp. 61–64, 2009.

[2] Zhu, Bo; Guang Gong (2011). "MD MITM Attack and Its Applications to GOST, KTANTAN and Hummingbird-2". *eCrypt*.

[3] S.M. Bellovin and M. Merritt, “Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks,” Proc. IEEE Symp. Security and Privacy, IEEE CS Press, 1992, pp. 72-84. https://doi.org/10.1109/RISP.1992.213269.

[4] F. Hao, R. Anderson, and J. Daugman. Combining crypto with biometrics effectively. IEEE Transactions on Computers, 55(9):1081– 1088, 2006. https://doi.org/10.1109/TC.2006.138.

[5] Trefný, Jirí, and Jirí Matas."Extended set of local binary patterns for rapid object detection." Proceedings of the Computer Vision Winter Workshop. Vol. 2010.

[6] Goldberg, David (2002). The Design of Innovation: Lessons from and for Competent Genetic Algorithms. Norwell, MA: Kluwer Ac-

ademic Publishers. ISBN 978-1402070983 https://doi.org/10.1007/978-1-4757-3643-4.

[7] Kennedy, J. and Eberhart, R., “Particle Swarm Optimization,” Proceedings of the IEEE International Conference on Neural Networks, Perth, Australia 1995, pp. 1942-1945. https://doi.org/10.1109/ICNN.1995.488968.

[8] William Stallings, “Cryptography and Network Security: Principles and Practice”, Pearson Education/Prentice Hall, 5 th Edition.

[9] K. Yang and X. Jia, “Data storage auditing service in cloud computing: challenges, methods and opportunities,” World Wide Web, vol. 15, no. 4, pp. 409–428, 2012. https://doi.org/10.1007/s11280-011-0138-0.