Cluster Computing (2019) 22:S4007–S4016
https://doi.org/10.1007/s10586-018-2609-x

Secure and optimal authentication framework for cloud management using HGAPSO algorithm

P. Selvarani[1] · A. Suresh[2] · N. Malarvizhi[1]

Received: 8 March 2018 / Revised: 15 March 2018 / Accepted: 18 March 2018 / Published online: 28 March 2018

Abstract
Data security is the major problem in cloud computing. To overcome this problem in the existing work Password can be used as a key to encrypt and decrypt the data in cloud environment. Some of the limitations having Password system because it is not secured, and easily forgotten. In order to overcome these problems the proposed technique utilizes effective data storage using biometric-based 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. In order to improve the security Extracting the feature value of fingerprint and iris and it is given input to the hybrid Genetic Algorithm and Particle swarm optimization algorithm to find the best solution using Cross over mutation technique. Best solution value can be act as a key for encrypting and decrypting data using Triple Data Encryption Standard Algorithm. Finally encrypted data can be stored in cloud using cloud simulator in the Working platform of net beans in java. Finally randomly tested with 5 fingerprint and 5 Iris image for the purpose of man in the middle attack. After tested with fingerprint and iris proposed Hybrid Genetic algorithm with Particle swarm optimization algorithm having less attack compared with the existing Particle swarm optimization algorithm. So the intruder cannot be able to access the data in cloud environment.

Keywords Data security in cloud · Fingerprint and iris · Particle swarm optimization algorithm · Genetic algorithm · Triple DES algorithm

1 Introduction

Data security is the major problem in cloud computing because hackers can hack Man in the Middle Attack [1] the data like creating, copying, destroying the data without data owner authorization. So authorized will lose millions of dollars due to illegal activities [2]. To overcome these difficulties the data can be encrypted before sending to the third party. In the existing technique password based authentication can be used to encrypt the data. Many of the limitations can be used for password based authentication forgotten, if the intruders know the password can easily hack the data [3]. To overcome this difficulties in our research work biometric based authentication can be used because stable, don't changed, not forgotten, don't sharable; mainly the person should be present at the time of authentication [4]. In this work multimodal biometric like fingerprint and iris is used to generate the key, Generated key is used to encrypt the data.

The new user has given input image of fingerprint and iris. Example, The input file (fp.png, ir.png). In our research work Extracting the feature value of fingerprint and iris by using local binary pattern. Local binary pattern works with the eight neighborhood of a pixel, Center pixel

✉ A. Suresh
prisu6esh@yahoo.com

P. Selvarani
selvarani.meena@gmail.com

N. Malarvizhi
drnmalarvizhi@gmail.com

[1] Department of Computer Science and Engineering, School of Computing, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, Tamil Nadu 600062, India

[2] Department of Computer Science and Engineering, Nehru Institute of Engineering and Technology, T.M. Palayam, Coimbatore, Tamil Nadu 641105, India

value is greater than the neighborhood pixel value becomes 0 other wise 1. Likewise all the pixel value can be calculated by using Local Binary pattern. Finally Binary value can be generated of fingerprint and iris by using LBP. The Binary value can be converted into decimal value. Finally a set of Fingerprint Feature value and iris feature value can be generated [5]. Generated value of fingerprint and iris and it has given input to hybrid Genetic Algorithm and Particle swarm optimization Algorithm for finding best solution. The best solution value act as a key for data encryption and decryption using triple data encryption standard algorithm. The major drawback of this one if you are not finding the best value the intruder can easily Extract the data by using fingerprint and iris image. The main advantage for finding the best value, the intruder does not identify the best value and also which particular portion of fingerprint and iris feature value going to act as a key for data encryption and decryption process. So the intruder cannot be able to access the data in cloud. Figure 1 represents Overall architecture of the research work.

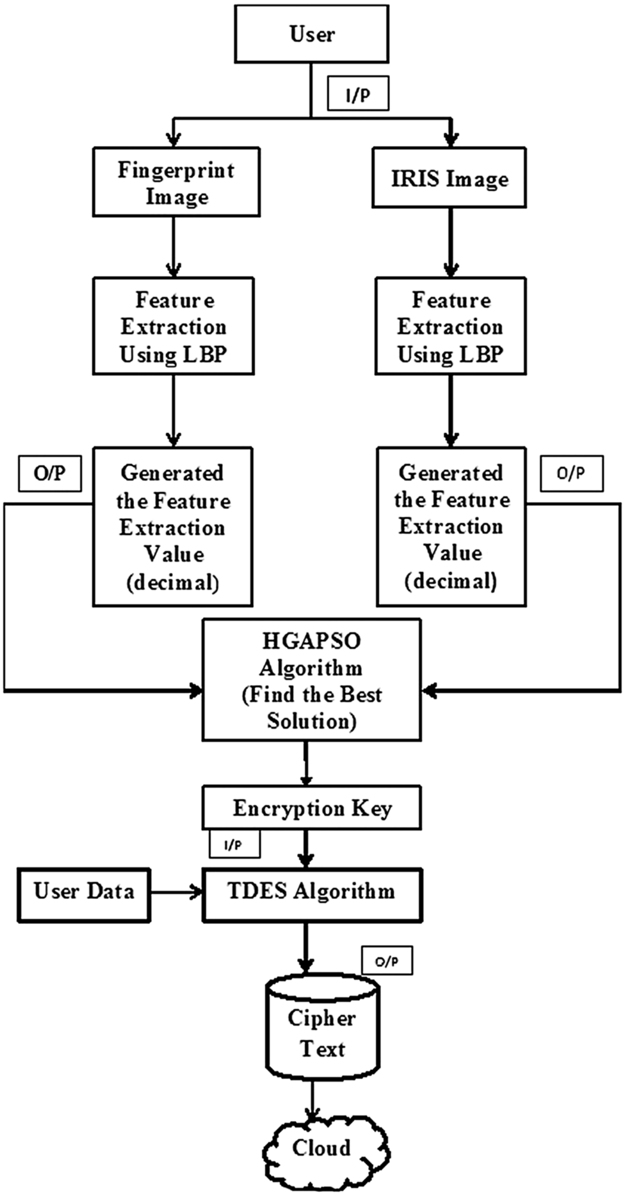

User
I/P
Fingerprint Image
IRIS Image
Feature Extraction Using LBP
Feature Extraction Using LBP
O/P
Generated the Feature Extraction Value (decimal)
Generated the Feature Extraction Value (decimal)
O/P
HGAPSO Algorithm (Find the Best Solution)
Encryption Key
I/P
User Data
TDES Algorithm
O/P
Cipher Text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

Fig. 1 Overall architecture

2 Choosing best value using HGAPSO algorithm

A set of fingerprint feature value and Iris feature value has been combined and it is given input to the hybrid genetic algorithm [6] and Particle swarm optimization algorithm [7–9] for finding the best value. One small example to find out the top most height of two persons. Table 1 represents example for how to find the best solution.

In normal Particle swarm optimization algorithm randomly select the height. Table 2 represents calculate the solution from Table 1 randomly select the persons height. In solution 1 (person 3 and 7) the value of height is 130,130 respectively. In solution 2 (person 2 and 8) the height value 115,165 respectively For finding the purpose of calculating the fitness value. Finally in solution 1 and solution 2 the best fitness value is 280.

So the particle swarm optimization algorithm take the best value and replace the worst value. In the next step take the another solution and combine two value, choose the best value and replace the worst value. Same process can be applied for all the values. Finally one best value can be chosen. In our research work Genetic Algorithm can be added for improving the optimization performance. GA + PSO. Genetic algorithm include the cross over + mutation process. Table 3 represents finding the fitness value using cross over and mutation technique from Table 1.

Particle swarm optimization algorithm finded the best value of 280. In our research work PSO add the GA to find out the best solution is 295. Same process can be applied for finding the best solution of fingerprint and iris. In fingerprint and iris image for finding the best solution Maximum key breaking time can be applied.

2.1 Process of HGAPSO

Step 1: Initialize fingerprint and Iris feature extraction values.

Step 2: Evaluate the feature values using fitness function (task: maximum key breaking time).

Step 3: Choose the best value and update the remaining value.

Step 4: Compare the initialized value with updated value and also calculate the fitness function.

Table 1 Finding best solution example

No of person	1	2	3	4	5	6	7	8	9	10
Height	165	115	130	165	145	120	130	165	125	155

Table 2 Fitness calculation for PSO

Solution	Position	Value	Fitness
Solution 1	3 & 7	130 + 130	260
Solution 2	2 & 8	115 + 165	280
Best solution value: 280			

Table 3 Fitness calculation using cross over mutation technique

Solution	Position	Value	Fitness
Solution 1	3,7	130 + 130	260
Solution 2	2,8	115 + 165	280
Cross over from solution 1 and 2 (3,8 & 2,7)			
Solution 3	3,8	130 + 165	295
Solution 4	2,7	115 + 130	245
Mutation: replace the new value (instead of 8 and 7)			
Solution 5	3,10	130 + 155	285
Solution 6	2,9	115 + 125	240
Best solution of HGAPSO: 295			

Step 5: Repeat the iteration, till to find out the best solution.

Step 6: Finally stop the iteration.

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

2.2 Pseudo code for optimization procedure

```
For each particle
    {
    initialize particle
    }
    end
    (Estimate intensity of particle as an objective)
    do
    or each particle
    {
    calculate Fitness value
    }
    If the fitness value is better than pBest
    {
    Set pBest = Current fitness value
    If pbest is better than gbest
    {
    Set gbest = pbest
    }
    end
    for each particle, calculate particle velocity according to equation of V
    Update particle position according to equation of present x
    }
    end
```

2.3 Calculation for HGAPSO algorithm

To generate the local binary pattern which is needed for the input of the proposed algorithm, it is necessary to find the velocity, fitness and the cross over mutation.

Step 1: Derived the feature extraction values from fingerprint and Iris using local binary pattern.

Step 2: Derived feature value has been given input to the hybrid genetic algorithm with particle swarm optimization algorithm for finding best solution.

Step 3: Calculating the best solution the following techniques has been followed. (I) update the velocity (II) Fitness Function calculation (III) Cross over mutation technique.

Velocity position of the feature extraction value.

Fitness function evaluate the quality of the represented solution.

Cross over and mutation recombined two distinct values and then randomly mixes their parts to form the solution.

Mutation randomly perturbs a candidate's solution.

Step 4: The above mentioned techniques has been followed to find out the best solution. The best solution value act as a key for data encryption and decryption using Triple DES algorithm for more security purpose.

Step 5: Finally encrypted data stored in cloud environment using cloud simulator. So the intruder cannot be able to access the data in cloud environment.

Velocity updation, fitness function calculation, cross over mutation formula is given below.

2.3.1 Calculation of velocity updating

$$\overline{V}_{T+t} = M * \overline{V}_T + \frac{R1 * G * \left(\overline{X}_T - \overline{G}_{best}\right)}{t} + \frac{R2 * L * \left(\overline{X}_T - \overline{L}_{best}\right)}{t} \tag{1}$$

Table 4 PSO versus GA

Factors	Particle swarm optimization	Genetic algorithm
Developed	Dr. Ebhart and Dr. Kenady in 1995	Dr. John Holland in 1975.
Description	Naturally behavior of bird flocking and fish schooling for finding food source	Genetic behavior of parent and child
Method	Velocity updation Position updation	Cross over Mutation
Implementation	Simple easy to implement Computationally efficient	Easy to exploit Support multi objective optimization
Preference	Artificial neural network training, fuzzy system control telecommunications, data mining, combinatorial optimization, power systems, signal processing and many others	Bioinformatics, phylogenetic, computational science, engineering, economics, chemistry, manufacturing, mathematics, physics and other fields
Advantages/ disadvantages	Applied on both Scientific research and engineering Disadvantages Low convergence, weak local search ability	Easily understand, less time required, getting optimal solutions Disadvantages Fitness function must be accurate
HGAPSO	Population based stochastic optimization Random generation Fitness function for evaluating purpose Difference PSO does not have genetic operator like cross over and mutation. But they also have memory	

Table 5 Process of data encryption and decryption

User can upload the data in cloud location PM1, VM2	Your data can be secured. Your account number 481961919. And your password jesus@selva999
Conformation	If the file can be encrypted? Once conformation process is succeed the file can be encrypted using the authentication secret key to encrypt the data
Authentication secret key	0.0321437095
Encrypted data	oPYeNokdzyvhfqsuZHr1QzfS9SSeo/XQvv4qRu4nPOMNSxj3uiVCpvb0KgoVM5iNiJfXuiWzNEiRf Ujj9oGGXOnTswv/fxNP2jkZdapjx5qvekB/TdPEh14whH9XmDOm
Decryption	Decryption process is same as reverse

Table 6 Testing with fingerprint and Iris image

Fingerprint	Iris
Randomly tested with fingerprint and Iris for the purpose of man in the middle attack	
Testing\Fingerprint 109_5.png	Testing\iris 109_1.png
Testing\Fingerprint 109_6.PNG	Testing\Iris 109_2.PNG
Testing\Fingerprint 109_7.PNG	Testing\Iris 109_3.PNG

$$\overline{V}_{T+t} = M * \overline{V}_T + \frac{R1 * G * \left(\overline{X}_T - \overline{G}_{best}\right)}{t * \left|\overline{X}_T - \overline{G}_{best}\right|} + \frac{R2 * L * \left(\overline{X}_T - \overline{L}_{best}\right)}{t * \left|\overline{X}_T - \overline{L}_{best}\right|} + \overline{S}\overline{R}\overline{F} \tag{2}$$

where M is the momentum, $\overline{V}_T$ is the velocity, t is the time, $\overline{X}_T$ is the current position of the particle, $\overline{G}_{best}$ is the global best value, $\overline{L}_{best}$ Local best value, R1 and R2 are two independent random numbers in the range from zero to one.

2.3.2 Calculation of the fitness function

It is used to measure the quality of the represented solution.

Table 7 Testing process with fingerprint image 109_5 and Iris image 109_1 image

<table>
<tr><td colspan="2">1. FINGERPRINT IMAGE 109_5 WITH IRIS IMAGE 109_1 IMAGE</td></tr>
<tr><td colspan="2">Testing\fingerprint 109_5.PNG (Derived the values using Local binary Pattern)</td></tr>
<tr><td colspan="2">4.944565E4/0.00735417/0.0020683603/0.046381414/0.048728343/0.32471168/0.029193828/0.22844587/0.26484066/0.047781214:0.19049808/0.051695082/0.0/0.22190651/0.26149088/0.06643824/0.09899577/0.09157196/0.017403476/0.03.65991E4/0.0014006194/0.0021466778/0.0033150339/0.0025760136/0.0071016327/0.008994932/0.021121902/0.024479168/0.0322424/0.02355715/0.020798141/0.01665259/0.03231278/0.017490147/0.009142737/0.082432434/0.69386965:0.090125285/0.050112613/0.046269707/0.21680743/0.22671734/0.06706081/0.1071509/0.13590935/0.059846565/0.05.192921E4/0.0012804462/0.0018708741/0.0012235375/8.6785795E4/7.540405E4/6.615638E4/7.8960846E4/0.0015223082/0.0020558275/0.0037061803/0.006508935/0.008209082/0.00867858/0.0071847257/0.005513032/0.0047732187/0.0053992146/0.005705099/0.0084936265/0.011659173/0.014092022/0.016852094/0.009375711/0.08616691/0.78613704:0.014433473/0.024563225/0.07188282/0.31168193/0.15819912/0.06293393/0.115574494/0.16066043/0.08007057/0.0</td></tr>
<tr><td colspan="2">Testing\IRIS 109_1.PNG (Derived the values using Local binary Pattern)</td></tr>
<tr><td colspan="2">0.09577621/0.08641012/0.051581375/0.07193113/0.075392514/0.076851726/0.055099316/0.09317452/0.21664178/0.17714131:0.09568571/0.0058481516/0.082089044/0.3778449/0.25263563/0.13093299/0.052429754/0.002533822/0.0/0.00.0659856/0.047491286/0.02552284/0.017863695/0.015260961/0.015708126/0.017886626/0.027391763/0.034053385/0.027930655/0.018643368/0.014355164/0.014229041/0.016510732/0.026141992/0.051848285/0.078242525/0.48493394:0.088332415/0.0029811044/0.02699046/0.30564347/0.29124242/0.17634378/0.100990646/0.0074756923/0.0/0.00.049653634/0.032893207/0.015958436/0.011495188/0.007810684/0.007287647/0.0060323584/0.00557906/0.0065321494/0.008403459/0.010809429/0.015412153/0.02101446/0.017399693/0.012111209/0.009507648/0.008031522/0.0068924637/0.0056487983/0.0059858663/0.0068692174/0.009740109/0.018317914/0.03751918/0.053361382/0.60973316:0.08415082/0.002243247/0.013006183/0.2224069/0.3213771/0.2059138/0.13378121/0.01712074/0.0/0.0</td></tr>
<tr><td colspan="2">Derived the feature values has given input to the hybrid particle swarm optimization and Genetic algorithm for finding best solution</td></tr>
<tr><td>HGAPSO</td><td>PSO</td></tr>
<tr><td>Initialization</td><td>Initialization</td></tr>
<tr><td>[[161, 36], [67, 125], [95, 24], [164, 57], [8, 18], [3, 122]]</td><td>[[34, 110], [97, 3], [62, 115], [133, 159], [55, 143], [36, 4]]</td></tr>
<tr><td>Evaluation</td><td>Evaluation</td></tr>
<tr><td>iteration 2 fitness [0.6458879698301067, 0.32478328366260395, 0.2903911139174377, 0.7703317912553478, 0.6681242128775828, 0.1576585935606088]</td><td>iteration 2 fitness [0.6213610641256965, 0.2523476471243879, 0.6076516160871516, 0.38803072491310886, 0.8524342229491362, 0.4856362886766559]</td></tr>
<tr><td>iteration 3 fitness [0.5302321528431031, 0.7599596867967031, 0.36411068508585215, 0.4411915782743094, 0.20996302038888826, 0.2992518606062702]</td><td>iteration 3 fitness [0.49271020891058986, 0.40550876087372567, 0.580374594599773, 0.24763597134744525, 0.46819737835261815, 0.6077979886862743]</td></tr>
<tr><td>iteration 4 fitness [0.6842290802644126, 0.42111706490856404, 0.6916496063469134, 0.3662684407339656, 0.5894309605905814, 0.40016710130435384]</td><td>iteration 4 fitness [0.46221150841924613, 0.8205825957103097, 0.5081784048538994, 0.6989706403504763, 0.7766567217359331, 0.36711652862282307]</td></tr>
<tr><td>iteration 5 fitness [0.5678118926200735, 0.4114086835521598, 0.2633262357311334, 0.6591654953370836, 0.6515310894362942, 0.30851320765680607]</td><td>iteration 5 fitness [0.8623055736122476, 0.5145038551919403, 0.6688354644650532, 0.11927738939707333, 0.31444097864595266, 0.578883228075799]]</td></tr>
<tr><td>Updation</td><td>Updation</td></tr>
<tr><td>Best Solution [67, 125]</td><td>Best Solution [62, 34]</td></tr>
<tr><td>[0.0084936265, 0.30564347]</td><td>[0.0071847257, 0.017490147]</td></tr>
<tr><td colspan="2">The best value can act as a key for data encryption and decryption using triple DES algorithm. Finally encrypted data stored in cloud environment</td></tr>
</table>

$$\mathrm{f} = \frac{W1 * R1 * F1 + W2 * R2 * F2}{W1 * R1 + W2 * R2} \tag{3}$$

Here

$$\mathrm{w1} = \frac{D1}{D1 + D2} \tag{4}$$

$$\mathrm{w2} = \frac{D2}{D1 + D2} \tag{5}$$

where F1 is the fitness, R1 is the reliability, D1 is the distance.

2.3.3 Calculation of cross over and mutation

The progress value of crossover CP as the gain obtained by

$$\mathrm{CP} = \mathrm{f\_sum}_{\mathrm{S}} - \mathrm{f\_sum}_{\mathrm{P}} \tag{6}$$

Here f_sumS is the fitness sum of the two offspring, f_sumP is the fitness sum of the parent individuals.

Mutation MP is

$$\mathrm{MP} = \mathrm{f}_{\mathrm{new}} - \mathrm{f}_{\mathrm{old}} \tag{7}$$

Table 8 Testing process with fingerprint image 109_6 and Iris image 109_2 image

2. FINGERPRINT 109_6 IMAGE WITH Testing\IRIS 109_2.PNG	
Testing\FINGERPRINT 109_6.PNG (Derived the values using Local binary Pattern)	
3.6910136E4/0.0056270543/7.939161E4/0.029618641/0.020913422/0.32872304/0.022981782/0.25341246/0.29436877/0.04319182:0.21559697/0.061758317/6.9641765E6/0.2554251/0.29649982/0.054689676/0.07470472/0.03787119/0.0034472672/0.03.9414415E4/7.671734E4/9.3609234E4/0.00209741/0.0015625/0.0046030404/0.004469313/0.011247185/0.009360923/0.017898368/0.016061373/0.01702562/0.013492399/0.032179054/0.014336993/0.006559685/0.08532517/0.7616836:0.10257601/0.059396114/0.05777027/0.2623522/0.26673704/0.068165824/0.100133725/0.07631616/0.0065526464/0.01.6361257E4/3.7702025E4/5.762008E4/4.197018E4/3.8413386E4/3.6990666E4/4.268154E4/5.8331434E4/0.0010314705/0.0011595151/0.0015863305/0.002603574/0.0028952311/0.003364728/0.0034927726/0.0031157522/0.0032651378/0.003642158/0.004182791/0.0061674826/0.008813738/0.011459993/0.014333883/0.0064733666/0.088685125/0.8304263:0.016069598/0.028134247/0.087874174/0.37398276/0.18993996/0.07737452/0.12524897/0.094347544/0.0070282267/0.0	
Testing\IRIS 109_2.PNG (Derived the values using Local binary Pattern)	
0.1001199/0.08975838/0.052780416/0.06825483/0.06927288/0.06917108/0.055370796/0.096952625/0.13319533/0.26512375:0.08456631/0.0054069953/0.085052714/0.40257227/0.25085968/0.11803765/0.051434323/0.002070042/0.0/0.00.067648135/0.049635388/0.026405705/0.018161805/0.015295358/0.016006237/0.019193726/0.025499908/0.02712805/0.026554761/0.018505778/0.015421483/0.014045588/0.016854705/0.029249221/0.12937993/0.08134975/0.40366447:0.07789855/0.0026944596/0.02762108/0.33871078/0.28951108/0.16063567/0.0967483/0.0061800587/0.0/0.00.049990702/0.032846715/0.016981265/0.010728068/0.008089636/0.006415919/0.006427542/0.0062648193/0.006741364/0.008496444/0.010635083/0.014679901/0.015714353/0.016074667/0.01184388/0.009065973/0.0076944535/0.005811521/0.0054628295/0.005532568/0.0074619926/0.009461156/0.019363986/0.040564414/0.05483751/0.61281323:0.07387605/0.0023711005/0.011878748/0.24900042/0.32856014/0.19172207/0.12778372/0.014807755/0.0/0.0	
Derived the feature values has given input to the Hybrid Particle swarm optimization and Genetic algorithm for finding best solution	
HGAPSO	PSO
Initialization	Initialization
[[108, 71], [35, 162], [34, 39], [121, 71], [134, 104], [16, 4]]	[[113, 20], [158, 15], [43, 162], [106, 66], [23, 105], [25, 151]]
Evaluation	Evaluation
iteration 2 fitness [0.5167676556729806, 0.519782809121758, 0.7144539838572175, 0.37565185182205973, 0.9103898826112224, 0.7080377726739893]	iteration 2 fitness [0.25087610168138974, 0.58389149599131, 0.3314422215005449, 0.7150479865742847, 0.5883831760664875, 0.1425952158183984]
iteration 3 fitness [0.42908939296133414, 0.37246271880737547, 0.3098336458797569, 0.6672373687834808, 0.22966885907154944, 0.3713477707828624]	iteration 3 fitness [0.8205781053524529, 0.3956118335228041, 0.35024131971739575, 0.2539289119237171, 0.34365435285329504, 0.62151094842666]
iteration 4 fitness [0.6773701685589575, 0.4107245477134548, 0.6347416816879694, 0.2340827842706264, 0.0990752779657057, 0.14818833690032696]	iteration 4 fitness [0.47973694516215026, 0.523909522428062, 0.5759918527544441, 0.6931786022166397, 0.712874510682242, 0.5559084740864527]
iteration 5 fitness [0.8253247215120777, 0.5449561205143703, 0.6632541522403351, 0.09385976748173858, 0.3115995442690484, 0.21596736882006395	iteration 5 fitness [0.36932877513805307, 0.45573786589071863, 0.8351985079684161, 0.9201885963165768, 0.4944282158368228, 0.4598474197012948]
Updation	Updation
Best Solution [162, 16]	Best Solution [20, 43]
[0.32856014, 0.07470472]	[0.0023859798, 0.021825733]
The best value can act as a key for data encryption and decryption using triple DES Algorithm. Finally encrypted data stored in cloud environment	

3 Particle swarm optimization versus genetic algorithm

The Table 4 herewith specifies the comparison factors of particle swarm optimization and genetic algorithm.

4 Data encryption

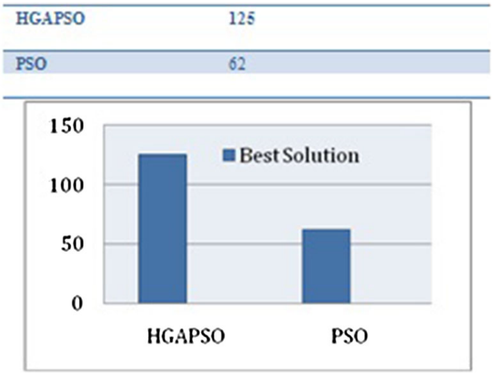
In this research work find out the best solution 0.0321437095 (This value derived from fingerprint and iris).It can be act as a key for encrypting and decrypting the data using triple data encryption standard algorithm. Triple DES algorithm receives 168 bit keys which is divided into three 56 bit keys [10, 11]. Encryption using First Secret Key, Decryption using Second secret key Encryption using third secret key. Table 5 represents process of data encryption and data decryption.

Table 9 Testing process with fingerprint image 109_7 and iris image 109_3 image

3. FINGERPRINT 109_7.IMAGE WITH\IRIS 109_3.IMAGE	
Testing\FINGERPRINT 109_7.PNG (Derived the values using Local binary Pattern)	
7.173102E4/0.0063443645/0.0024235332/0.051284194/0.09347317/0.3064934/0.020502536/0.21848014/0.25743076/0.042850576:0.1824475/0.050761882/0.0/0.20802692/0.22966461/0.043282356/0.092136055/0.16144353/0.032237172/0.00.0023859798/0.0048704953/0.004757883/0.0032657657/0.0020340653/0.0053068693/0.010564471/0.033072915/0.052456364/0.044165257/0.017933559/0.010824887/0.008396678/0.026463963/0.015526464/0.010585586/0.08342483/0.663964:0.09866976/0.05139358/0.0449817/0.2191371/0.19594595/0.021825733/0.047388796/0.16725789/0.1533995/0.00.0039338153/0.0058687115/0.005513032/0.002461302/0.0011879695/7.824949E4/5.4774643E4/7.967221E4/0.0012733326/0.0026320282/0.006224391/0.016048258/0.022037901/0.018893695/0.009333029/0.004289495/0.0024684158/0.002824095/0.003137093/0.004403312/0.0065445025/0.010734407/0.017470976/0.010734407/0.08191299/0.7579459:0.015038129/0.029948212/0.07653511/0.32403824/0.14321078/0.011289267/0.025537787/0.14447701/0.22992545/0.0	
Testing\IRIS 109_3.PNG (Derived the values using Local binary Pattern)	
0.10112665/0.09346862/0.050371025/0.07061898/0.08636487/0.06932944/0.054205693/0.09957694/0.13622686/0.23871092:0.05630967/0.0062327497/0.09371748/0.4211461/0.25460386/0.117743544/0.0482218/0.0020247952/0.0/0.00.07018208/0.05102275/0.02799945/0.019331316/0.016086498/0.015639333/0.018138874/0.02546551/0.031485047/0.026004402/0.017806366/0.015513209/0.014274904/0.017026693/0.07113374/0.055517334/0.08493854/0.42243394:0.049864702/0.0033365437/0.031393323/0.35571456/0.2998647/0.16086498/0.09401944/0.0049417536/0.0/0.00.05204798/0.034532055/0.017341578/0.011239481/0.008566181/0.006694872/0.0065670186/0.006357804/0.0067646103/0.0076944535/0.0110883815/0.014947231/0.018213306/0.016249012/0.011320842/0.00905435/0.0075666/0.006357804/0.0055093216/0.0056952904/0.0071481704/0.010774559/0.019201264/0.038669858/0.057603795/0.6027942:0.0458529/0.0030103677/0.014738017/0.26681855/0.34036914/0.19282626/0.124285184/0.012099586/0.0/0.0	
Derived the feature values has given input to the hybrid particle swarm optimization and Genetic algorithm for finding best solution	
HGAPSO	PSO
Initialization	Initialization
[[83, 81], [130, 99], [83, 123], [110, 103], [71, 106], [138, 124]]	[[13, 43], [130, 20], [85, 54], [6, 26], [124, 161], [63, 18]]
Evaluation	Evaluation
iteration 2 fitness [0.5167676556729806, 0.519782809121758, 0.7144539838572175, 0.37565185182205973, 0.9103898826112224, 0.7080377726739893]	iteration 2 fitness [0.8400636345875165, 0.5726670179061223, 0.4521719106999336, 0.32714574468946533, 0.11001074506635689, 0.5576002702965603]
iteration 3 fitness [0.42908939296133414, 0.37246271880737547, 0.3098336458797569, 0.6672373687834808, 0.22966885907154944, 0.3713477707828624]	iteration 3 fitness [0.19974233100445732, 0.5434174121670008, 0.02431222649250031, 0.8135516844517368, 0.3796602165669181, 0.4552085543252178]
iteration 4 fitness [0.6773701685589575, 0.4107245477134548, 0.6347416816879694, 0.2340827842706264, 0.0990752779657057, 0.14818833690032696]	iteration 4 fitness [0.4558056130442279, 0.6364716204617027, 0.13995685096283939, 0.5305281210795023, 0.6048510047968827, 0.6919186052123951]
iteration 5 fitness [0.8253247215120777, 0.5449561205143703, 0.6632541522403351, 0.09385976748173858, 0.3115995442690484, 0.21596736882006395	iteration 5 fitness [0.5160326418431376, 0.40295738986365104, 0.5862890045541005, 0.37927779318390886, 0.05241726949163483, 0.4436729266811939]
Updation	Updation
Best Solution [106, 99]	Best Solution [20, 43]
[0.02799945, 0.117743544]	[0.0023859798, 0.021825733]
The best value can act as a key for data encryption and decryption using triple DES Algorithm. Finally encrypted data stored in cloud environment	

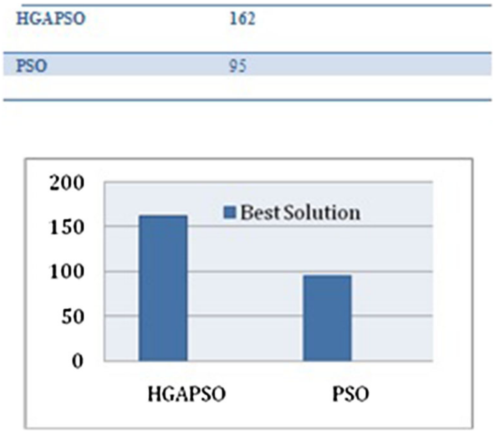
Table 10 Best values for proposed HGAPSO compared with Existing PSO

Biometric Image	HGAPSO	PSO
Fingerprint-109_5.png	Best solution [67, 125]	Best solution [62, 34]
Iris-109_1.png	[0.0084936265, 0.30564347]	[0.0071847257, 0.017490147]
Fingerprint-109_6.png	Best solution [162, 16]	Best solution [95, 87]
Iris-109_2.png	[0. 32856014, 0.07470472]	[0.0054069953, 0.06825483]
Fingerprint-109_7.png	Best solution [106, 99]	Best solution [20, 43]
Iris-109_3.png	[0.02799945, 0.117743544]	[0.0023859798, 0.021825733]



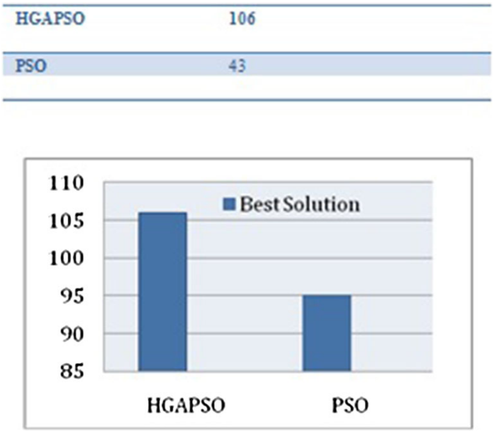
HGAPSO	125
PSO	62

Fig. 2 Best solution for the finger print image 5 and iris image 1



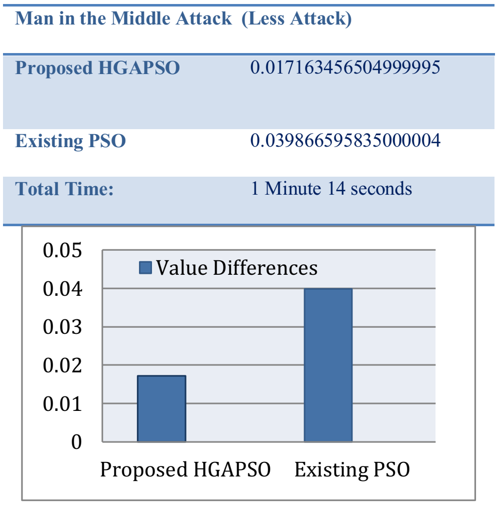
HGAPSO	162
PSO	95

Fig. 3 Best solution for the finger print image 6 and iris image 2



HGAPSO	106
PSO	43

Fig. 4 Best solution for the finger print image 7 and iris image 3



Man in the Middle Attack (Less Attack)	
Proposed HGAPSO	0.017163456504999995
Existing PSO	0.039866595835000004
Total Time:	1 Minute 14 seconds

Fig. 5 Comparison of HGAPSO with existing PSO for best solution

5 Execution of results

Randomly testing fingerprint and iris image to hack encrypted data by using particle swarm optimization algorithm. in our proposed technique Secured the data by using Hybrid Genetic algorithm and Particle swarm optimization algorithm. Therefore hacker couldn't be hacking the encrypted data. Table 6 represents randomly tested with Fingerprint and Iris image. Figures 2, 3 and 4 proves that HGAPSO could be considered as the best solution.

Randomly testing the image of Fingerprint with iris for the purpose of Man in the Middle attack. Initially the user has given input image of fingerprint and iris for feature extraction. Extracting the feature values using local binary pattern. These values can be given input to the HGAPSO algorithm for finding the best solution. First initialize all the fingerprint and Iris Values. Ten evaluating the values to finding the fitness (1–6 iterations can be generated). Choose the best value and replace the worst value, likewise all the values can be calculated to find out the best solution. The best solution value can be act as a key for encrypting and decrypting the data using Triple DES Algorithm. Finally all the best values compared with the algorithm of HGAPSO and PSO. The HGAPSO Algorithm almost finds out the best value compared with existing PSO. And also less attack compared with PSO. Finally encrypted data stored in cloud [12–15]. Table 7 represents testing process for fingerprint image 109_5 with Iris image109_1 image Table 8 represents test with the fingerprint image 109_6 and iris image 109_2 image. Tables 9 and 10 represents Test with the Fingerprint image 109_7 with iris image 109_3. For finding best value and also identifying less attack.

(i) Randomly tested with the fingerprint 109_6 image with the Iris image109_2 image.

(ii) Randomly tested with the fingerprint 109_7 image with the Iris image109_3 image.

(i) Execution 1: Fingerprint image 109_5.png with Iris Image 109_1.png.

(ii) Execution 2: Fingerprint image 109_6.png with Iris Image 109_2.png.

(iii) Execution 3: Fingerprint image 109_7.png with Iris Image 109_3.png.

5.1 Man in middle attack

Randomly tested for the purpose of man in middle attack while comparing with 3 fingerprint and 3 iris. Finally the result concluded as proposed Hybrid Genetic algorithm and Particle swarm optimization algorithm is 0.017163456504999995, Compared with the existing particle swarm optimization then the value is 0.039866595835000004. Comparing both algorithms HGAPSO and Existing PSO Algorithm as shown in Fig. 5 it proves that HGAPSO is less Attacked considering existing PSO. Total Running Time 1 min 14 s.

6 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 min 14 s. It can be more secure less attack and higher data security in cloud.

References

1. Zhu, B., Gong, G.: MD MITM attack and its applications to GOST, KTANTAN and hummingbird-2. *eCrypt* (2011)
2. Lori, M.: Data security in the world of cloud computing. Co-published by the IEEE Computer and Reliability Societies, pp. 61–64 (2009)
3. Bellovin, S.M., Merritt, M.: Encrypted key exchange: password-based protocols secure against dictionary attacks. In: Proc. IEEE Symp. Security and Privacy. IEEE CS Press, pp. 72–84 (1992)
4. Hao, F., Anderson, R., Daugman, J.: Combining crypto with biometrics effectively. IEEE Trans. Comput. **55**(9), 1081–1088 (2006)
5. Trefný, J., Matas, J.: Extended set of local binary patterns for rapid object detection. Proceedings of the Computer Vision Winter Workshop (2010)
6. Goldberg, D.: The design of innovation: lessons from and for competent genetic algorithms. Kluwer Academic Publishers, Norwell (2002). ISBN 978-1402070983
7. Kennedy, J., Eberhart, R.: Particle swarm optimization. In: Proceedings of the IEEE International Conference on Neural Networks, Perth, Australia 1995, pp. 1942–1945
8. Suresh, A., Varatharajan, R.: Competent resource provisioning and distribution techniques for cloud computing environment. Cluster Comput. (2017). https://doi.org/10.1007/s10586-017-1293-6
9. Chinnasamy, A., Sivakumar, B., Selvakumari, P., Suresh, A.: Minimum connected dominating set based RSU allocation for smartCloud vehicles in VANET. Cluster Comput. (2018). https://doi.org/10.1007/s10586-018-1760-8
10. Stallings, W.: Cryptography and network security: principles and practice, 5th edn. Pearson Education/Prentice Hall, Boston (2003)
11. Suresh, A., Reyana, A., Varatharajan, R.: CEMulti-core architecture for optimization of energy over heterogeneous environment with high performance smart sensor devices. Wirel. Pers. Commun. (2018). https://doi.org/10.1007/s11277-018-5504-0
12. Yang, K., Jia, X.: Data storage auditing service in cloud computing: challenges, methods and opportunities. World Wide Web **15**(4), 409–428 (2012)
13. Kyziropoulos, P.E., Filelis-Papadopoulos, C.K., Gravvanis, G.A., Efthymiopoulos, C.: Toward the design of a novel hybrid parallel N-body method in scope of modern cloud architectures. J. Supercomput. (2018). https://doi.org/10.1007/s11227-017-2140-5
14. Nezarat, A., Shams, Y.: A game theoretic-based distributed detection method for VM-to-hypervisor attacks in cloud environment. J. Supercomput. **73**, 4407 (2017). https://doi.org/10.1007/s11227-017-2025-7
15. Jahani, A., Khanli, L.M.: Cloud service ranking as a multi objective optimization problem. J. Supercomput. **72**, 1897 (2016). https://doi.org/10.1007/s11227-016-1690-2

P. Selvarani currently pursuing Ph.D. in the Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sakunthala R&D Institute of Science and Technology, Chennai, Tamil Nadu, India. She was born on 12th February 1981 at Ayilpatty, Namakkal Dist, and Tamil Nadu, India. She obtained B.B.A. Degree from University of Madras, Chennai, and Tamil Nadu, India. M.C.A. Degree from Anna University Affiliated College, Chennai, Tamil Nadu, India. M.Phil. Degree in Computer Science from Bharadhidasan University Affiliated College, Chennai, Tamil Nadu, India. M.E. Degree in Computer Science and Engineering from Anna University Affiliated College, Chennai, Tamil Nadu, India. Her research interests include Cloud Computing, Data Security, Data Mining and Computer Networks.

A. Suresh currently working as the Professor & Head, Department of the Computer Science and Engineering in Nehru Institute of Engineering & Technology, Coimbatore, Tamil Nadu, India. He has been nearly two decades of experience in teaching and his areas of specializations are Data Mining, Artificial Intelligence, Image Processing, Multimedia and System Software. He has published 45 papers in International journals. He has published more than 40 papers in National and International Conferences. He has served as a reviewer for Springer, Elsevier, and Inderscience journals. He is a member of IEEE, ISTE, IACSIT, IAENG, MCSTA, MCSI, and Global Member of Internet Society (ISOC). He has organized several National Workshop, Conferences and Technical Events. He is regularly invited to deliver lectures in various programmes for imparting skills in research methodology to students and research scholars. He has published three books, in the name of Data structures & Algorithms, Computer Programming and Problem Solving and Python Programming in DD Publications, Excel Publications and Sri Maruthi Publisher, Chennai, respectively.

N. Malarvizhi currently working as Professor & Head in the Department of Computer Science and Engineering at Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai-62, Tamilnadu, India. She is having more than 15 years of teaching experience. She has written a book titled “Computer Architecture and Organization”, Eswar Press, The Science and Technology Book Publisher, Chennai. She serves as a reviewer for many reputed journals. She has published numerous papers in International Conferences and Journals. Her area of interest includes Parallel and Distributed Computing, Grid Computing, Cloud Computing, Big Data Analytics, Internet of Things, Computer Architecture and Operating Systems. She is a life member of Computer Society of India (CSI), IARCS and IAENG. She is a Senior Member of IEEE and IEEE Women in Engineering (WIE).