Optimization of Secret Key using cuckoo Search Algorithm for ensuring data integrity in TPA

S.Raja shree
Research Scholar, Faculty of CSE, Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, India
rajijce@gmail.com

M.Rajesh
School of Maritme Studies
Vistas,Chennai

A.Chilambu Chelvan
Department of Electronics and Instrumentation Engineering, R.M.D Engineering College, Chennai, India
Chill97@gmail.com

Abstract: **Optimization plays an important role in many problems that expect the accurate output. Security of the data stored in remote servers purely based on secret key which is used for encryption and decryption purpose. Many secret key generation algorithms such as RSA, AES are available to generate the key. The key generated by such algorithms are need to be optimized to provide more security to your data from unauthorized users as well as from the third party auditors(TPA) who is going to verify our data for integrity purpose. In this paper a method to optimize the secret key by using cuckoo search algorithm (CSA) is proposed.**

Key word: Cuckoo search, Secret key, Cloud Computing, TPA

I INTRODUCTION

Cloud Computing plays a major role in today's internet world where it reduces all the burden of the users such as storage and maintenance of the data. Users can easily store and retrieve their data from cloud based on access permission. Millions of users store their data in cloud by trusting the system. Cloud providers such as Amazon, Google Cloud provide security to the user's data to a great extent. However there is a lack in trust by the user because of the data loss and data theft often occur in cloud. If the user want to feel empty handed without any data tension they have to trust the provider by means of their service level agreements. Encryption and decryption of data plays a major role in the security of data. In that secret keys both public and private key plays a significant role .In this paper a method is proposed to optimize that secret key to provide better security to the data.

II RELATED WORK

Cuckoo search algorithm was investigated by many researchers and implemented in many fields including mobile networks, power systems, cryptanalysis etc. Cuckoo search algorithm was developed by Yang and Deb in 2009. In conjunction with Levy flights, this algorithm is focused on a parasitic nature of some cuckoo species. [1]. Cuckoo birds enlarge its community by laying its eggs in the host nest and hatches the best egg. Optimization plays an important role in this technical world. Always we need the best solution. Cuckoo starts with some initial population and produces its effective society by optimizing its egg [2].Cuckoo Search algorithm got implemented in many areas because of its simplicity and it requires only one parameter P_a other the population size.[3].Users store their data in the cloud based on the service level agreement provided by the service provider. User may unaware of that where the data get stored and how it is protected from the unauthorized user. The security of the data by the integrity checker such as third party leads to big question mark [4].Data integrity plays a major role in storing and retrieving the data .In order to provide the integrity of the data the optimization of the key was done [5].Cryptanalysis uses the cuckoo search algorithm by evaluating the fitness of the cipher text by means of bigrams and trigrams. [6].Optimization of an algorithm increases its efficiency, convergence rate and accuracy [7]. Optimization of a key produces better security when compared to normal secret key. Selection of public key and private key plays a major role in data encryption. Small values of private keys leads to a path to security breaches .Hence the keys should be optimized to enhance the security of the data [8].

978-1-7281-4514-3/20/$31.00 ©2020 IEEE

III AN INTRODUCTION TO CUCKOO SEARCH ALGORITHM

Cuckoo- a brood parasitic behavior species lays its egg in the host nest and wait for its hatchment by the host bird. Cuckoo having the capability of mimic the color of the eggs of the host bird. So that the host bird not able to find the intruder egg and hatches the cuckoo egg along with its own egg. If the host bird found that intruder either it throws out that or else vacate the nest and build the nest in a new place. Cuckoo search algorithm mainly based on levy flight so that the cuckoo can easily find the next step based on random walk by levy flight. [9].

IV CUCKOO SEARCH ALGORITHM – OPTIMIZATION

Optimization always produce the best output from the so called outputs. Cuckoo birds. Cuckoo lays and hatches its egg in the host nest and the process continues until it forms the best cuckoo community. After some generations the cuckoo moves to one best place with maximum number of best eggs and with good food. There will be a significant lose in the cuckoo egg which is less than 5%.

V DATA STORAGE IN CLOUD

Users want to store their data in cloud means they have to choose a secure cloud service provider who provides more security to their data. Normally users trust the providers based on the service level agreements. Data want to store by the users in the cloud get encrypted by a suitable encryption algorithm based on the service providers. Google cloud uses AES 256 for the data encryption purposes. Different service providers uses different encryption algorithms. The encrypted data get stored in the cloud server. Whenever the users request the data, it gets decrypted by a secret key and provided the data to the user in a readable form. Suppose the user wants to check the integrity of the data such that whether their data get lost or theft they can send a verification request to the provider. The data gets verified by a third party auditor.

The data stored by the user cannot be viewed as it get encrypted. After getting the request from the user, the auditor audits the file using the secret key shared. The auditor audits the content without knowing the actual data. So we need to optimize the key with the help of of hybrid optimization technique [9].

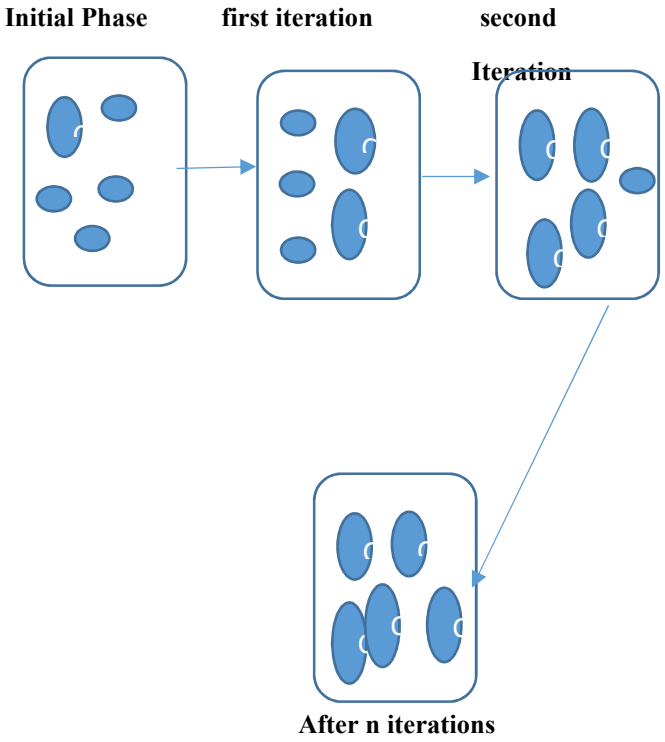

Fig: 1 Cuckoo Search Optimization process

VI OPTIMIZATION OF SECRET KEY

Entire security of the data depends upon the secret key. So it is to be optimized to get a better security to our data

A .Why Cuckoo Search

Cuckoo search algorithm is used to optimize the key because

(i) Of its simplicity
(ii) It can be used to adopt solutions to dynamic circumstances
(iii) Broad applicability-can be applied to any type of problem
(iv) It can be easily combined with other traditional optimization problem
(v) Cuckoo search outperforms other meta heuristics algorithm in terms of the quality of the output produced and the reliability [10].
(vi) Comparing with other population or agent based meta-heuristic algorithm such as PSO, there is essentially only a

single parameter P_a other than the population size 'n'[11].

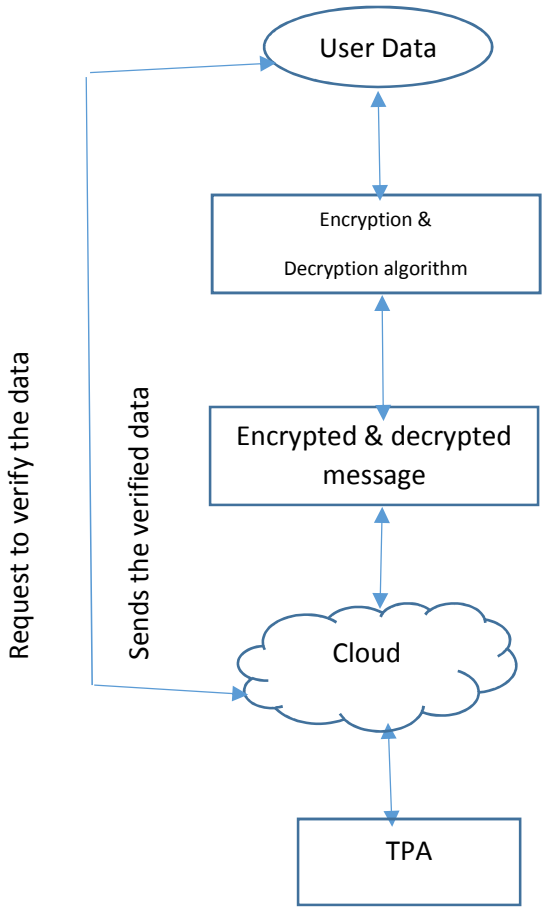

Fig: 2 Data transmission and verification process

B.Secret Key optimization using CSA

Security of the data purely depends upon the secret key generated. Tiny keys can easily be breakable by hackers and also the random selection of the keys can lead to infinite values. A set of keys are generated by applying RSA.The fitness of the keys are evaluated. The key with more fitness value is used to encrypt the message.

(i)Initialize the population of cuckoo with randomly generated keys $P^k(\{P_1^k, P_2^k, P_3^k \ldots P_n^k\})$ for CS (k=0)

For a total number of iterations k=2.gen.

(ii)Each egg in $P_i^k (i \in [1 \ldots N])$ represents a key generated by RSA.

(iii) The fitness function f (P I k) measures the consistency of each egg P I k, whose final iteration gives the optimized key to encrypting the data.

Three different operations involved in the evolution of cuckoo search key optimization 1.Generate the random number of keys using RSA and are distributed using Levy flight. 2. Replacement of existing one by new ones 3. Best key selection strategy

a) Levy flight

Cuckoo search is implemented in combination with levy flight to generate a new set of keys. Under this method, a new key, $\mathbf{P}_i^{k+1}$ ($i \in [1 \ldots N]$), Is created by tormenting the current Pi k with position change Q i. A symmetric Levy distribution generates a random move, s I to get Q I.

b) Replacement

Under this process, a set of individual keys (eggs) are selected and replaced with a new key. Each key, $\mathbf{P}_i^k$ ($i \in [1 \ldots N]$), can be selected with a probability of $p_a \in [0,1]$. In order to implement this process, a uniform random number, g_1, is generated within the range [0, 1]. If g_1 is less than p_a, the individual $\mathbf{P}_i^k$ is selected and modified according to (1) Otherwise, $\mathbf{P}_i^k$ remains without change. This operation can be resumed by the following model:

$$P_i^{k+1}=P_i^k + \text{rand}\,(P_{d1}^k - P_{d2}^k) \quad \text{-- (1)}$$

Where d_1 and d_2 are two random numbers between 1…n

c)Best key selection strategy

After finding $\mathbf{P}_i^{k+1}$, it must be compared with its past value $\mathbf{P}_i^k$. If the fitness value of $\mathbf{P}_i^{k+1}$ is better than $\mathbf{P}_i^k$, then $\mathbf{P}_i^{k+1}$ is accepted as the final solution. Otherwise, $\mathbf{e}_i^k$ is retained. This procedure can be resumed by the following statement:

$$P_i^{k+1}=\begin{cases} P_i^{k+1}, \text{ if } f(P_i^k)<f(P_i^{k+1}) \\ P_i^k, \text{ otherwise} \end{cases} \quad \text{----(2)}$$

VII PERFORMANCE EVALUATION:

This section describes in detail the simulation model used to test the efficiency of the proposed Secret Key Optimization Algorithm. The data integrity in the

cloud environment using third-party auditor using RSA with Cuckoo Search Algorithm (CSA) found five different data file sizes for simulation.

	DES	***RSA***	***Proposed RSA+CSA***
10	0.482	0.535	0.615
20	0.571	0.578	0.625
30	0.608	0.579	0.635
40	0.682	0.590	0.665
50	0.709	0.689	0.730

TABLE 1: EVALUATION OF ENCRYPTION TIME

The performance of the proposed method is assessed using the time taken by the algorithms to perform input file encryption and decryption. There are three important parameters which include the execution time for encryption and decryption and the performance. The table I displays the files ' five different sizes and their corresponding execution time for encryption, taken in seconds by proposed and traditional algorithms.

Input file size (KB)	**Decryption time (in seconds)**		
	DES	***RSA***	***Proposed RSA+CSA***
10	0.732	0.735	0.625
20	0.771	0.778	0.745
30	0.778	0.779	0.565
40	0.782	0.79	0.705
50	0.809	0.89	0.75

TABLE 2: EVALUATION OF DECRYPTION TIME

Table 2 displays the files ' five different sizes and their respective decryption execution time taken in seconds by proposed and traditional algorithms. Table 3 displays the files ' five different sizes and their respective throughput by comparing their private key lengths.

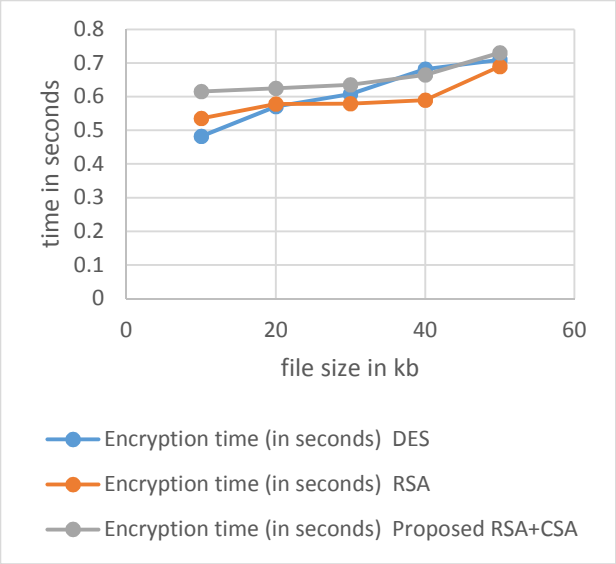

Fig 3: Comparison of encryption time with DES and RSA

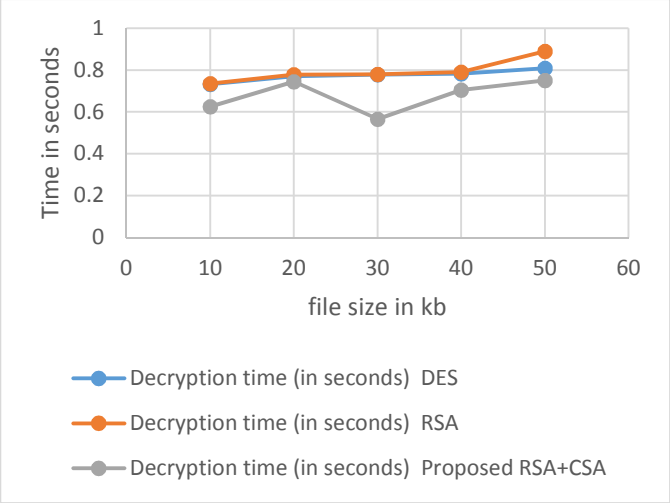

Fig 4: Comparison of decryption time with DES and RSA

TABLE 3: THROUGHPUT BY VARYING THE PRIVATE KEY LENGTHS

Input file size (KB)	**Private key length (128 bits)**	**Private key length (256 bits)**	**Private key length (512 bits)**
10	0.118	0.1	0.2
20	0.134	0.13	0.23
30	0.125	0.25	0.35
40	0.114	0.22	0.38
50	0.15	0.34	0.42

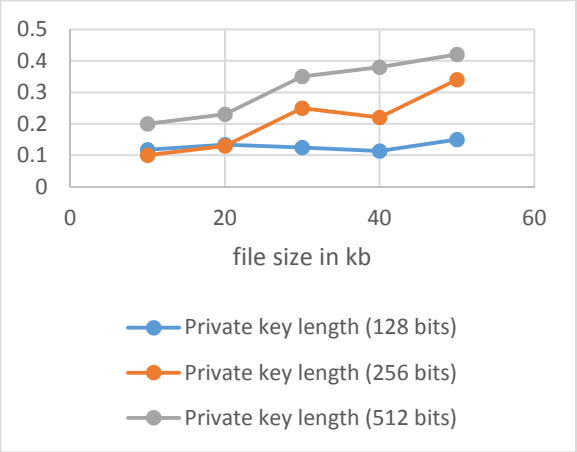

Fig 5: Throughput for various key length

VIII CONCLUSION

In this paper cuckoo search algorithm is used to optimize the collection of secret key to improve the security of the cloud-saved data. The consumer tests data integrity in the cloud with the help of third party auditors. The customized keys are given to the TPA here, so the data is more secure than traditional methods are. The approach proposed achieves less execution time than traditional methods like RSA and DES and provides better security.

REFERENCES:

[1] Yang, X. S. & Deb, S. (2009), "Cuckoo Search via Lévy Flights", in Proc. of World Congress on Nature & Biologically Inspired Computing, pp. 210-214.
[2] R. Rajabioun, Cuckoo optimization algorithm, Appl. Soft Comput. 11 (2011)5508–5518.
[3].S.Joshi, Kulkarni," Cuckoo Search Optimization- A Review", ICAAMM-2016- Materials Today: Proceedings 4 (2017) 7262–7269
[4] Arjun Kumar, Byung Gook Lee, HoonJae Lee," Secure Storage and Access of Data in CloudComputing", DOI: 10.1109/ICTC.2012.6386854
[5] S.Rajashree, A.ChilambuChelvan, M.Rajesh," An efficient RSA cryptosystem by applying cuckoo search optimization algorithm", Concurrency Computatational Practice Experience.2018; e4845 https://doi.org/10.1002/cpe.4845.
[6] Morteza Heydari *et al*, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.1, January- 2014, pg. 140-149
[7] **Geeta, Varma,"** Cuckoo Search Optimization and its Applications: A Review", **International Journal of Advanced Research in Computer and Communication Engineering-** Vol. 5, Issue 11, November 2016
[8] Kota, Padmanabhuni,• Kishor Budda," Authentication and Encryption Using Modified Elliptic CurveCryptography with Particle Swarm Optimization and CuckooSearch Algorithm", J. Inst. Eng. India Ser. B
https://doi.org/10.1007/s40031-018-0324-x
[9] S.Rajashree, A.ChilambuChelvan, M.Rajesh," **Improving the security in cloud using CSA by varying the key length",** International Journal of Pure and Applied Mathematics
Volume 119 No. 18 2018, 2133-2145
[10] M.I. Solihin, M.F. Zanil, Performance comparison of Cuckoo search and differential evolution algorithm for constrained optimization, in: Intrnational Enginering Research and Innovation Symposium (IRIS), vol. 160(1), 2016, pp. 1–7.
[11] M.A. Adnan, M.A. Razzaque, A comparative study of particle swarm optimization and Cuckoo search techniques through problem – specific distance function, in: 2013 International Conference on Information and Communication Technology (ICoICT), Bandung, Indonesia, 2013.)