TDWOA: Effective Triple DES with Whale Optimization Algorithm for Trust Based Offloading System

M. S. Premalatha, B. Ramakrishnan

***Abstract:** In Mobile Cloud Computing (MCC), offloading may be a fashionable scheme projected to reinforce the characteristics of portable devices by extenuating complex calculations to capable cloud servers. Efficiency in security and energy consumption point of view, offloading is most important. It actually demonstrates the new disputes over security vulnerabilities by the unauthorized users. Among doable security problems are temporal arrangement threads that aren't secured by ancient scientific discipline security. Therefore, the first intension is to propose secure and economical offloading approach to writing methodology to be performed with the assistance of Triple DES rule personal key by activity server and also the optimum key choice is completed by the "Whale Optimization algorithm (WOA)". The experimental results are presented to ensure the efficiency of this research. The proposed TDWOA technique is analyzed with various existing algorithms to ensure the security over computational offloading in cloud.*

***Keywords:** Offloading, Trust Management, encryption, Whale Optimization, Triple DES*

I. INTRODUCTION

Cloud computing is the mostly used term since a long time back imagined vision of computing as an efficacy. The cloud gives strong, on-ask for brains access to a united gathering of configurable figuring assets that can be rapidly sent with phenomenal effectiveness and inconsequential organization overhead [4]. The name was awakened by the cloud picture that is frequently used to address the Internet in stream graphs and charts. An obvious movement to the clouds has been stirring above late years with end customers, "a modest piece at any given moment" trusting up a multimedia data on distant servers open by means of a framework [1]. Another safe adaptable cloud benefit design is important to address the requirements of customers in their stand-out operational condition. By and large, adaptable customers can be benefitted incredibly from cloud administrations for computationally genuine data planning and gathering, for instance, data seek, information dealing with, information mining, mastermind status checking and field distinguishing [5]. A "Trusted Authority (TA)" is accepted to oversee security keys and authentications for adaptable customers [5].

Cloud stockpiling is a critical administration of cloud computing. It facilitates data administrator to have their data in the cloud and rely upon cloud servers to give "all day every day/365" information access to customers (information buyers) [6].

The "computation offloading" in distributed computing is used to address the characteristic issues in portable processing by using asset providers other than the mobile phone itself to have the execution of flexible function. Mobile device is such that the processing and storage of data can be done outside the device [2]. In distributed environment, many architectures are obtainable to ensure the efficacy [7]. Offloading of mobile data through an optimal opportunistic mobile network is used to enhance the capacity of network and nodes of network. But this is used to reduce the issue of data offloading optimization. The cloud offers several advantages like fast organization, pay-per-use, cut down costs and scalability. Enormous integrity, confidentiality and privacy are the primary obstruction to broad espousal [4], inescapable framework access, greater adaptability, hypervisor assurance against framework attacks, ease disaster recuperation and information storage engagements, on-demand security controls, real time location of framework interfering and fast re-constitution of facilities [3].

Encryption contrives which integrates the cryptographic strategies with RBAC. Several cloud based security and savvy offloading strategies are presented in existing articles and a segment of the methods are analyzed. The RBE plot allows RBAC approaches to be maintained for the scrambled data set away out in the open mists [9]. An expressive, beneficial and revocable information access control plot for multi-authority distributed storage frameworks, where there are diverse authorities concur and each authority can issue attributes autonomously [10, 11].

An epic open auditing mechanism for the uprightness of shared data in light of capable customer revocation [12]. Out sourcing computation into IBE suddenly and propose a revocable IBE plot in the server-aided setting [13]. A measurement by using a trust display measures the security quality and procedures trust value. A trust value includes various parameters that are necessary measurements in which protection of cloud services can be calculated [14]. The real-time video applications of offloading have some challenges and opportunities such as common force efficient offloading and dynamic wireless rules made small particles offloading by using an adaptive scheduling algorithm [15, 21, 22].

Revised Manuscript Received on February 05 2019.

M. S. Premalatha, Research Scholar, Manonmanium Sundaranar University, Abishekapatti, Thirunelveli – 12, Tamil Nadu, India.

Dr. B. Ramakrishnan, Associate Professor, Department of Computer Science and Research Centre, S.T. Hindu College, Nagercoil, Tamil Nadu, India.

II. Related Works

Li et al. [16] have presented a savvy cryptography approach. In their method the cloud benefit administrators can't straightforwardly achieve halfway information. Their methodology segments the record and independently stores the information in the scattered cloud servers. An elective methodology was expected to describe whether the information parcels need a split in order to truncate the activity time. Their introduced shows that it was fundamentally supported by their proposed calculations. Their trial evaluation have surveyed both protection and viability exhibitions and the trial results depict that their methodology can successfully monitor fundamental dangers from mists and requires an adequate calculation time.

Yan et al. [17] have described a plan to control information access in cloud figuring dependent on trust assessed by the information proprietor and additionally notorieties produced by different notoriety centers in a versatile way by applying “Attribute-Based Encryption and Proxy Re-Encryption”. In their work they coordinate setting aware trust and notoriety assessment into a cryptographic structure in order to help different control situations and procedures. The security and execution of their plan were assessed and legitimized through wide investigation, security affirmation, examination and usage. Their outcomes exhibit that the profitability, versatility and practicality of their plan for information get to control in cloud enrolling.

Talal H. Noor et al. [18] have displayed the arrangement and execution of a notoriety based trust the board system. A novel convention to exhibit the validity of trust criticisms and save customers' security, ii) a versatile and solid believability for estimating the validity of faith inputs to shield cloud administrations from malevolent customers and to analyze the reliability of cloud administrations, and iii) an accessibility model to deal with the accessibility of the distributed usage of the trust the executives benefit.

Li et al. [19] have exhibited another characteristic based information sharing plan reasonable for confined versatile customers in cloud figuring. Their displayed plan takes out a dominant part of the calculation errand by including structure open parameters other than moving incomplete encryption calculation detached. What's more, an open figure content test stage was performed before the unscrambling stage that dispenses with a vast bit of calculation overhead in light of ill-conceived figure compositions. For information security, a Chameleon hash work was used to create a quick figure message, that was blinded by the separated figure compositions to acquire the last online figure writings.

Yuchuan Luo et al. [20] have displayed a novel open groping plan for the loyalty of reported data to efficient course of action safe customer repudiation. Additionally they extend their exhibited plan to help safe signature and confirmation re-appropriating that permit greater efficiency for social event customers and the examiner. The numerical investigations and test results exhibit that their plan was protected and exceptionally proficient. The redistributing calculations make the marks age and confirmation process increasingly proficient and reasonable for phones.

In a distributed cloud, where the users data will be placed in social networks with minimization of operational cost for cloud service provider was a major problem. The variety of data centers was placed at various environment. These were interrelated with the internet. So the **Qiufen Xia** et al. [23] have introduced the algorithm named as a fast scalable algorithm. It was used to reduce the data location issues. In their article they focused to connect the user’s social network to various locations, same communication location for the same user with user’s data in data centers, connecting user’s data into a near and far data centers that were used for communication purpose. The user’s data with their updating rates of reading and location was changed by using extra time. The efficiency of an algorithm was evaluated based on the three real social network datasets such as Twitter, Facebook and Wiki vote. The algorithm was used for the functional cost reduction and increasing the speed of runtime.

In MCC applications, many data want to communicate with customer mobile device and cloud due to which cellular networks traffic will be increased. So in this article they focused on reducing the offloading problems in any Wi-Fi network with limited difficult data types. For considerations in communication capacity, offloading before the limited time period was possible. To overcome that issues Guoju Gao et al. [24] have introduced an offloading algorithm for offline data. It was used to achieve a similar rate. And also the author have introduced the other algorithm to obtain a competitive ratio of 2 and an offloading algorithm for dual type data to clear up the issues in common environments. These are applicable for dual cost Wi-Fi transmission scenarios.

III. PROBLEM DEFINITION

Several issues occur within the offloading process of cloud [25, 26]. Some of them are mentioned here.

- Preventing information replication in order to expand the degree of learning accessibility since any of information focused down can cause the disappointment of information recoveries.
- Maltreatment and despicable consumption of distributed environment by the unauthorized users.
- Accuracy and performance of streamlining the trust of the executive’s administration is appallingly low.
- Direct trait repudiation in data sharing for asset limited clients in distributed computing is one among the issue in cloud environment.
- Based on the size of the changed data, the dividing schema, and furthermore the system collected the postponement.
- Testing of framework in an exceptionally goliath scale connected with various gadgets is furthermore a standout amongst the most drawback of cloud environment.

IV. PROPOSED METHODOLOGY

"Offloading in MCC" is a famous procedure proposed to expand the abilities of portable frameworks by alleviating complex calculation to ingenious cloud servers. Although this might be advantageous from the execution and vitality point of view, it unquestionably displays new difficulties as far as security because of expanded information transmission over systems with conceivably obscure dangers. Among conceivable security issues are timing assaults which are not counteracted by customary cryptographic security. The numerical outcomes dependent on test information demonstrate that the security execution exchange off is enhanced through the proposed plan. Additionally, a secure and proficient offloading approach is the encryption procedure to be performed with the guide of Triple DES calculation private key by estimating server. And the Whale optimization algorithm is used for optimal key.

Triple DES

TDES is one of the important encoding technique. It has 3 types of keys for encryption process such as 1) a block cipher with symmetric key 2) a key with 64 bits length and 3) a key with length either 56 or 112 or 168 bits. Because of this triple encryption it is much slower than Conventional DES. The decoding process is the reverse process of encoding. The input key length is 64 bits in which the original size is 56 bits only. Because, the right most least significant bit of each byte is considered as parity.
So the actual strength of the key in Triple DES is only 168 bits. While doing the encoding process the parity bits in each 3 keys remain unused.

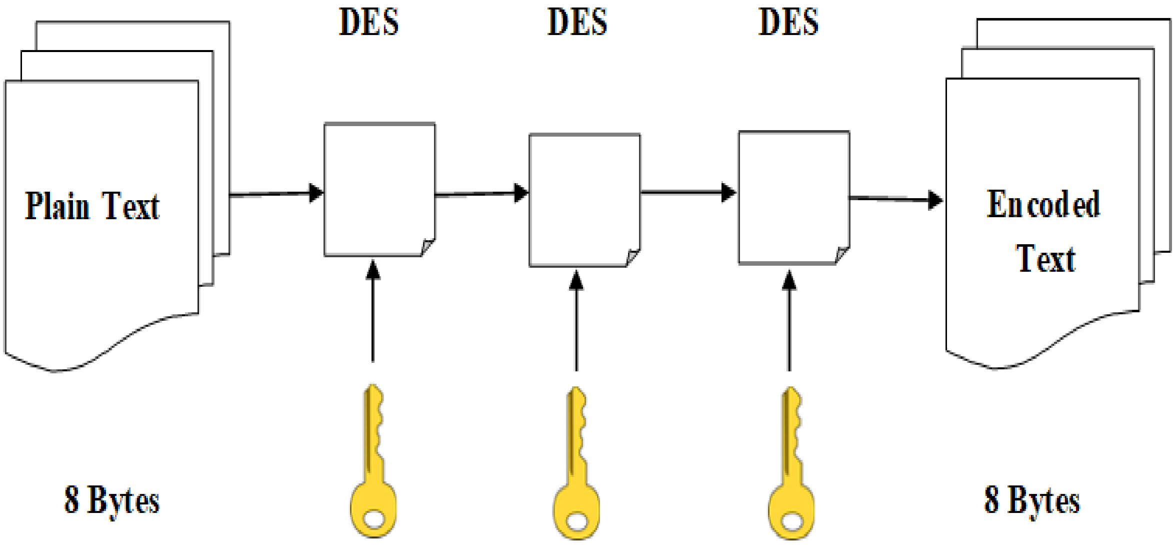


Fig. 1 64 Byte Structure of Triple DES

"Triple Data Encryption Standard (TDES)" is an automated encryption algorithm in which the encoding is done thrice for each data chunk and it is presented in Fig. 1. To ensure high security the key size is increased automatically. Three types of keys with size 56 bits is used to encode each data block. The process of TDES is explained in Fig. 2.

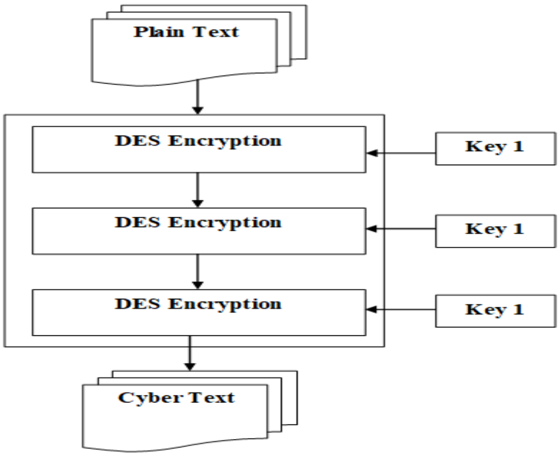
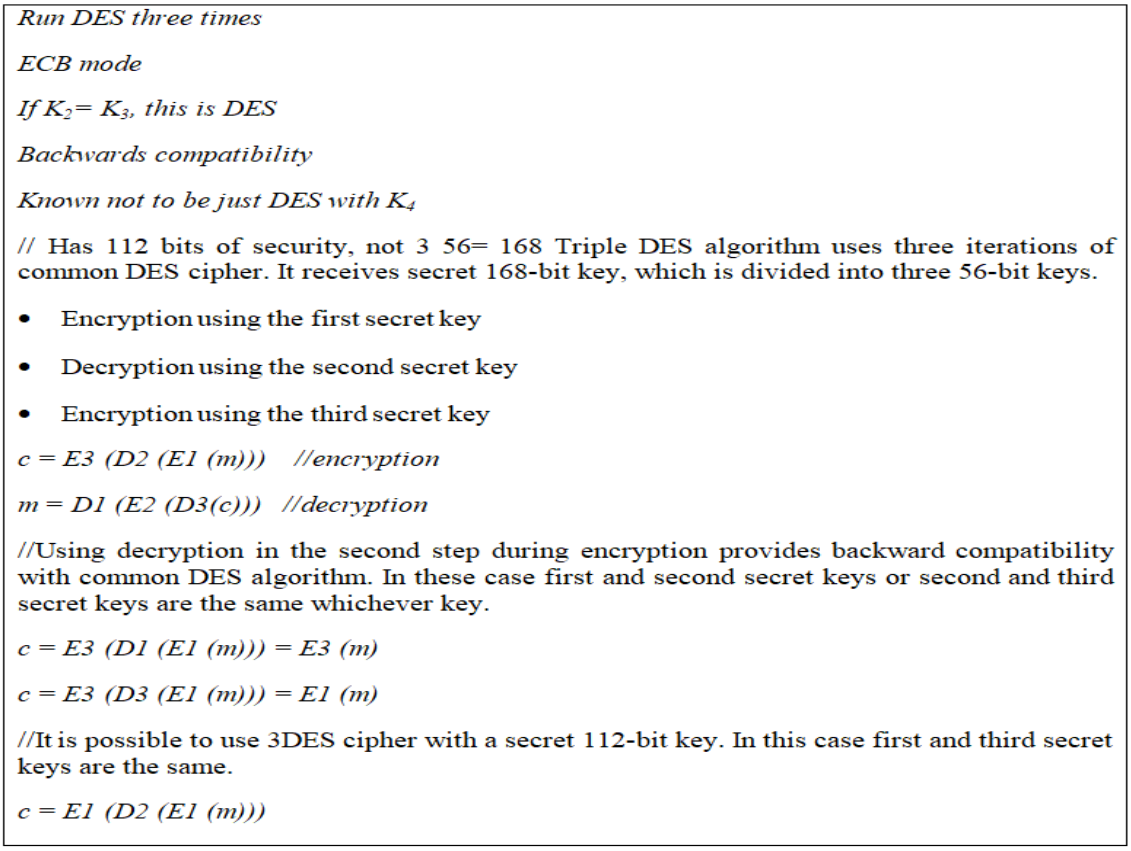


Fig. 2 Process of TDES

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Algorithm:



Run DES three times

ECB mode

If $K_2 = K_3$, this is DES

Backwards compatibility

Known not to be just DES with K_4

// Has 112 bits of security, not 3 56= 168 Triple DES algorithm uses three iterations of common DES cipher. It receives 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

c = E3 (D2 (E1 (m)))　//encryption

m = D1 (E2 (D3(c)))　//decryption

//Using decryption in the second step during encryption provides backward compatibility with common DES algorithm. In these case first and second secret keys or second and third secret keys are the same whichever key.

c = E3 (D1 (E1 (m))) = E3 (m)

c = E3 (D3 (E1 (m))) = E1 (m)

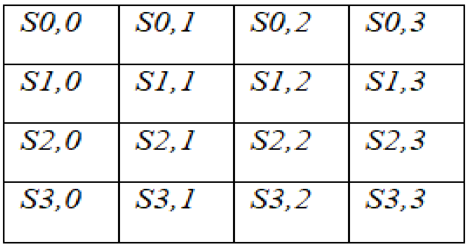
//It is possible to use 3DES cipher with a secret 112-bit key. In this case first and third secret keys are the same.

c = E1 (D2 (E1 (m)))

TDES is one of the most efficient encryption algorithm in which 3 types of keys with different sizes are used to encrypt a data block. This differentiates TDES from other encryption or cryptographic algorithms. TDES is the replica of DES in which the process is repeated thrice. For more flexibility and compatibility the key size is increased as 64 bits.

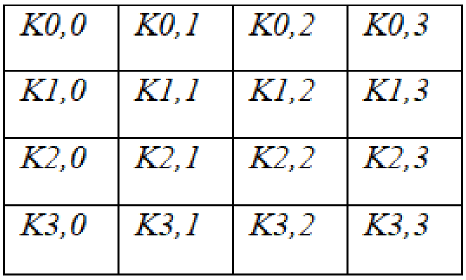
AES

AES is an encoding algorithm with key length 128 bits. But varying key sizes are also allowed. Ten rounds of execution with 128 bit keys are used in Encoding process. All the rounds are unique other than last 4 rounds. A state array is presented as a 4*4 matrix which is the input block for encoding. A state of the proposed work is represented as given below.



S0,0	S0,1	S0,2	S0,3
S1,0	S1,1	S1,2	S1,3
S2,0	S2,1	S2,2	S2,3
S3,0	S3,1	S3,2	S3,3

With 128 bit key length the corresponding 4*4 matrix of keys for state array is given below.



K0,0	K0,1	K0,2	K0,3
K1,0	K1,1	K1,2	K1,3
K2,0	K2,1	K2,2	K2,3
K3,0	K3,1	K3,2	K3,3

Encryption:

The encoding procedure consists of 4 operations which are described below.

“Sub-bytes”:

This process is based on the state array autonomously. The S-box is generated based on 2 transformations such as,

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

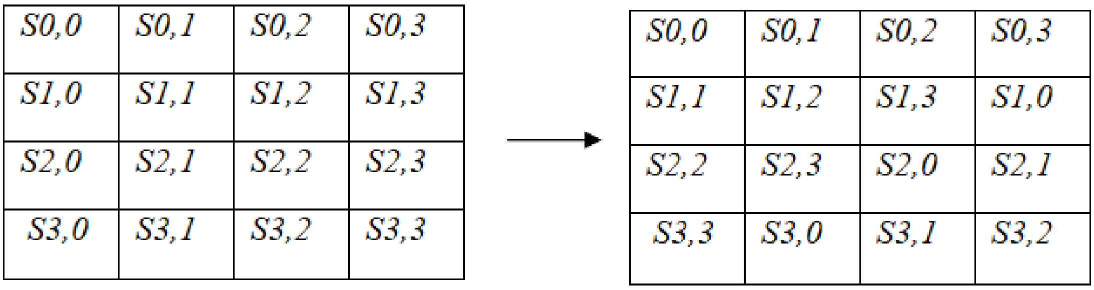
(i)Take the multiplicative inverse in Rijindael's finite field

(ii)Apply the affine transformation, they has been recorded in the Rijindael's documentation.

Pre-estimation is necessary if S-box is input undependable. The value of each byte in the S-Box is replaced with corresponding indexes based on following equation.

S(i,j)=SBox[s(i,j)]

"Shift Rows": In this process, each column is consistently moved to one side based on the indices of the data.



S0,0	S0,1	S0,2	S0,3
S1,0	S1,1	S1,2	S1,3
S2,0	S2,1	S2,2	S2,3
S3,0	S3,1	S3,2	S3,3

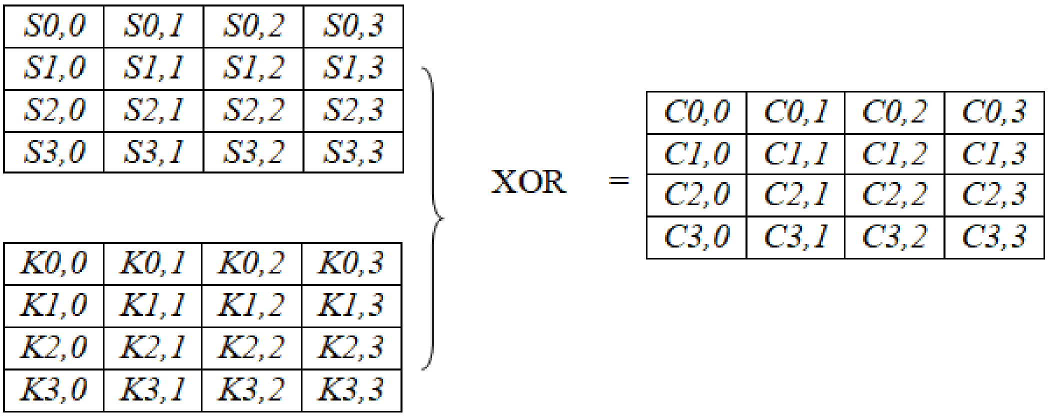
S0,0	S0,1	S0,2	S0,3
S1,1	S1,2	S1,3	S1,0
S2,2	S2,3	S2,0	S2,1
S3,3	S3,0	S3,1	S3,2

"Mix-Column"

This is a column-wise process in which each column is treated as 4th order polynomial. The intension of this process is to give dispersion of the bits over numerous rounds. It is accomplished by increasing one section at any given moment. Each incentive in the segment is increased beside each line evaluation of a standard lattice.

"Add Round Key":

In this process, perform bitwise XOR operation. Based on the key schedule and cipher key, the round key can be extracted.



S0,0	S0,1	S0,2	S0,3
S1,0	S1,1	S1,2	S1,3
S2,0	S2,1	S2,2	S2,3
S3,0	S3,1	S3,2	S3,3

K0,0	K0,1	K0,2	K0,3
K1,0	K1,1	K1,2	K1,3
K2,0	K2,1	K2,2	K2,3
K3,0	K3,1	K3,2	K3,3

C0,0	C0,1	C0,2	C0,3
C1,0	C1,1	C1,2	C1,3
C2,0	C2,1	C2,2	C2,3
C3,0	C3,1	C3,2	C3,3

Basically it can be written as $C_{ij}=S_{ij}\, XOR\, K_{ij}$

From that process, encrypt the user message and send the scrambled information to the updation specialist. In updation specialist the decoding process is completed. Based on the above operations, encode the user input data and transfer the cipher text to receiver. The decoding is completed there and the original data is retrieved.

Optimal key selection using "Whale optimization algorithm (WOA)":

This algorithm is accomplished the life style of whales. The whales are the most intelligent animals with emotion. Amongst the most type of whales, humpback whales have distinctive hunting method. Humpback whales hunt the prey in the surface of the sea using the bubble net feeding behavior. In this hunting method, humpback whales generate bubbles around the prey along a 9-shaped path or circular path.

Prey Encircling: Humpback whales cannot diagnose the optimal position of the prey at the outset. Hence they consider the current position as the optimal candidate solution. Once the best solution is defined, the other search agents update their position to the best candidate solution. This behavior is defined as follows,

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

$$\vec{A}(t+1)=\vec{A}_{best}(t)-\vec{K}\cdot\vec{F}$$

$$\vec{F}=\left|\vec{L}\cdot\vec{A}_{best}(t)-\vec{A}(t)\right|$$

Where, t describes the present iteration, $\vec{A}_{best}$ and $\vec{A}$ denote the optimal position and position vector respectively. $\vec{K}$ and $\vec{L}$ represent the coefficient vectors and defined as follows,

$$\vec{K}=2\vec{k}\cdot\vec{r}-\vec{k}$$

$$\vec{L}=2.\vec{r}$$

Where, $\vec{k}$ is reduced to 0 and $\vec{r}$ describes a arbitrary vector.

Bubble net hunting behavior: This hunting behavior embraces two phase such as shrinking encircling prey and Updation of spiral position. These phases are termed as follows:

Method of shrinking encircling prey: In this phase, encircling prey is shrunk by reducing the value of $\vec{k}$. As a result $\vec{K}$ in the range [-$\vec{k}$, $\vec{k}$] is also reduced by $\vec{k}$ where $\vec{k}$ is reduced from 2 to 0.The new position is calculated ie, the predictable positions of the agent from the original position (A, B) to the current best agent position (A_{best}, B_{best}) that can be accomplished by $1\geq K\geq 0$ in two-dimension (2D) space.

Updation of spiral position: Humpback whale at the position (X, Y) circumscribes the prey at the position (A_{best}, B_{best}) by the way of the helix-shaped path as revealed in figure 4. Thus the spiral equation between (A, B) and (A_{best}, B_{best}) is defined as follows,

$$\vec{A}(t+1)=\vec{F}'.e^{cn}.\cos(2\pi n)+\vec{A}_{best}(t)$$

Where, c and n are represented as a constant value of the number in the range [-1, 1] twisting shape and a random respectively. $\vec{F}'$ represents the distance between the prey (best solution) and the whale and is defined as:

$$\vec{F}'=\left|\vec{A}_{best}(t)-\vec{A}(t)\right|$$

Based on the above two bubble net hunting methods, whales hunt the prey simultaneously. So, 50% probability is assumed to select either one of the two Updation methods.

$$\vec{A}(t+1)=\begin{cases}\vec{A}_{best}-\vec{K}.\vec{F} & if\ q<0.5\\ \vec{F}'.e^{cn}.\cos(2\pi n)+\vec{A}_{best}(t) & if\ q\geq 0.5\end{cases}$$

Prey searching: In this phase, whales are searching for prey (best solution) randomly. This approach also utilizes a variation of the $\vec{K}$ with the random values between -1 to 1. The location of the search agent is restructured by choosing the search agent arbitrarily rather than the optimal search agent. It is described below

$$\vec{A}(t+1)=\vec{A}_{rand}-\vec{K}.\vec{F} \qquad for\left|\vec{K}\right|\geq 1$$

$$\vec{F}=\left|\vec{L}.\vec{A}_{rand}-\vec{A}\right|$$

Where, $\vec{A}_{rand}$ denotes the random point vector of the search agent.

Decryption: In decoding process, the activities are backward demand that stand out from their demand in encryption mode. Along these lines it begins with a basic round, trailed by nine cycles of a converse run of the initial round and closes with an “Add Round Key”. A reverse common round comprises of the going with tasks in an explicit request. After the decoding procedure, the original message is retrieved by the receiver. So that the proposed technique uses the system where a whale optimization technique (WOA) for optimal key selection is included.

V. Experimental Results

In this section, the experimentation and results are analyzed for the proposed research. The proposed cloud based secure and cost effective technique is performed in the working stage of JAVA. The time and memory values are also estimated and its normal values are contrasted with that of the present technique. The table shown beneath illustrates the record size estimation of the proposed technique; here each file size in kb. Table I reveals the time for memory for Triple DES Whale optimization algorithm (**TDWOA)**. Table I is tabulated in the below section.

The results performance of time between the file sizes and cloud memory are shown in Table I. The time 61385secs for a file size 10kb, time 79865secs for file size of 20kb, file size of 30kb takes 10025secs and finally, time 12456secs is obtained for 40kb.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Table.1 Size of files in kb with time in sec for TDWOA.

File size	Time	Memory
10kb	61385	1101259
20kb	79865	1225448
30kb	10025	1314587
40kb	12456	1411152

The Figure 3 shows the time in sec and file size in kb for the proposed method. When the file size increases the time for the presented method is decreased. If the file size is minimum then the time of the presented method is high.

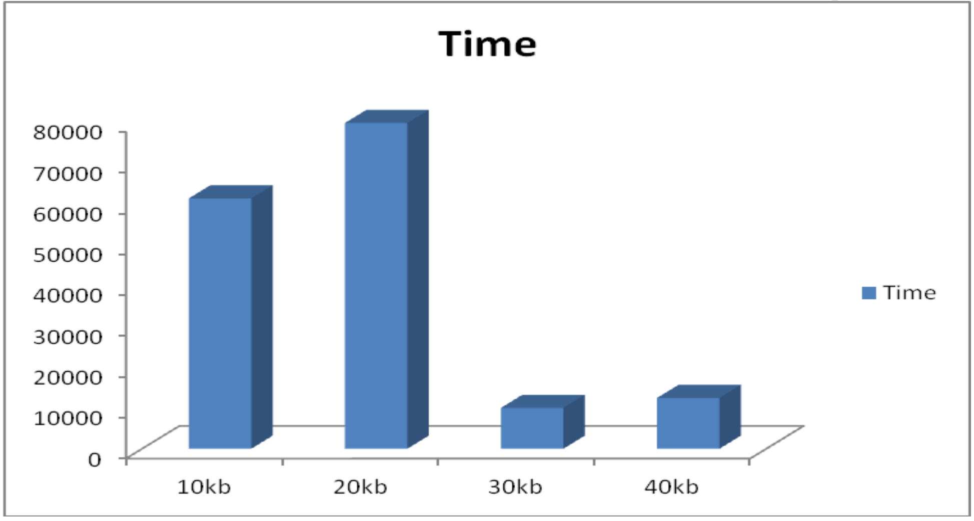


Fig. 3 TDWOA time in sec with file size kb

The figure 4 shows the memory and file size in kb for the proposed method. When the file size increases the memory size for the presented method is also increased. If the file size is minimum then the time of the presented method is low.

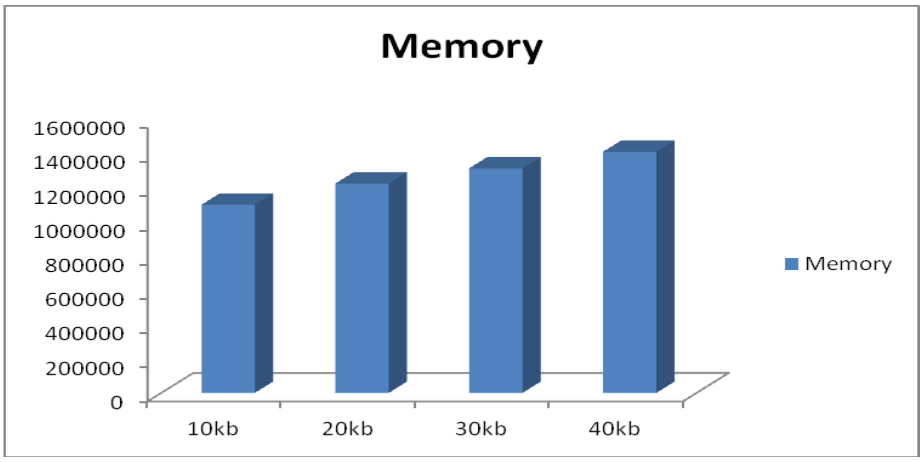
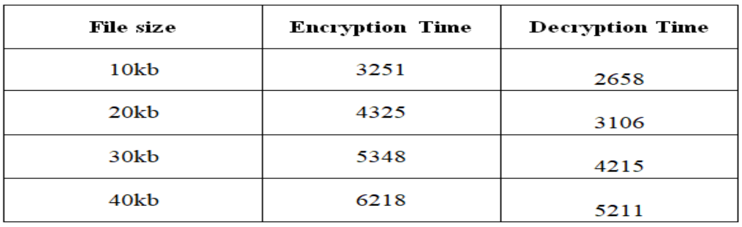


Fig. 4 TDWOA memory size and file size in kb

Table II shows the time analysis of encoding process of the cloud server. The decryption time for the presented method is minimum. In the estimation table the Time of encryption is 3251 and decryption is 2658 for 10kb file size, 20kb file size takes 4325 for encryption and 3106 for decryption.

The 30Kb file size takes 5348 for encryption and 4215 for decryption and the size of 40kb file size consumes 6218 for encryption and 5211 for decryption.

Table. 2 Encryption and Decryption Time Analysis



File size	Encryption Time	Decryption Time
10kb	3251	2658
20kb	4325	3106
30kb	5348	4215
40kb	6218	5211

The figure 5 shows the encryption time in sec and file size in kb for the proposed method. When the file size increases the encryption time for the presented method is also increased. If the file size is minimum then the encryption time of the presented method is low.

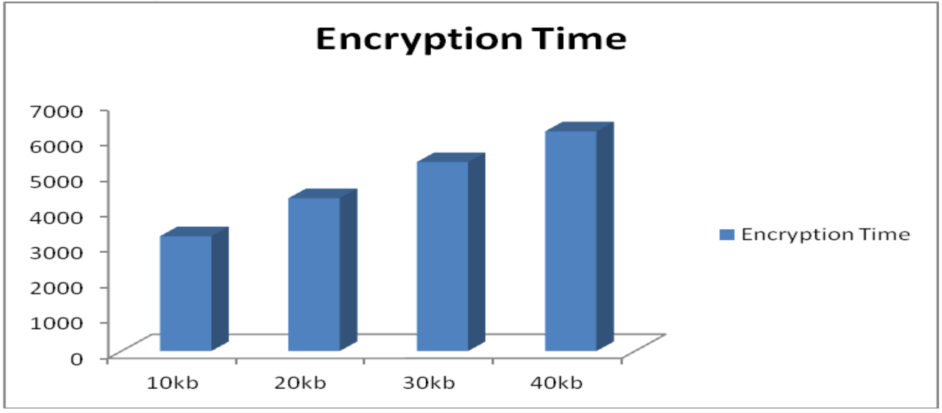


Fig. 5 TDWOA Encryption Time analysis

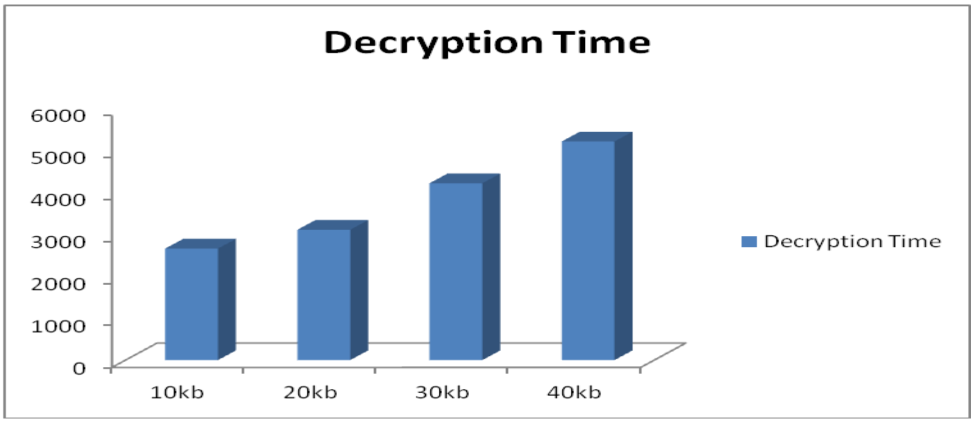


Fig 6. TDWOA Decryption time analysis

The figure 6 shows the decryption time in secs and file size in kb for the proposed method. When the file size increases the decryption time for the presented method is also increased. If the file size is minimum then the decryption time of the presented method is low.

Comparative Analysis

The proposed methodology is compared with other existing techniques in terms of decryption time. Here the comparison is done with conventional RSA, RSA with ABC algorithm and RSA with Oppositional ABC. Among these, the proposed TDWOA gave better outcome. It is presented in Table III.

Table. 3 Decryption Time Comparison

Methods	RSA-ABC	RSA Existing	RSA-OABC(Proposed)	TDWOA
File size(kb)	25	25	25	**25**
Time(sec)	9468.5	9484.8	5261	**3872**

VI. Conclusion

In this research, a secure and cost effective offloading for distributed computing utilized Triple DES and Optimization algorithm. This procedure is accustomed to shielding the client's information from the assailants. It surely displays new difficulties as far as security because of expanded information transmission over systems with possibly obscure dangers. Over that the security threats are timing attacks which are not forestalled by customary cryptographic security. For ensuring security Triple DES is proposed. By utilizing the new technique the security computation offloading performance is improved. In addition, the fluctuation of arbitrary postponements is the essential impacting component to the relief viability of irregular cushioning and that the additional number of assessment an assailant needs to develop with the standard deviation of the irregular deferrals. To resolve the issue Triple DES whale optimization algorithm is utilized. The TDWOA is used for optimal encoding in which the whale optimization is connected for the optimal key identification. The customer and server can enter a common ace mystery at the point when the decoded data is organized legitimately. In the event that the decoded data isn't legitimately arranged, the server creates its own irregular incentive for figuring an ace discharge. According to the work proposed Triple DES whale optimization algorithm provides better results for secure offloading from the attackers with expense effectively.

REFERENCES

1 Zissis, Dimitrios, and Dimitrios Lekkas, "Addressing cloud computing security issues," Future Generation computer systems , Vol.28, No. 3, pp 583-592, 2012.

2 Fernando, Niroshinie, Seng Wai Loke, and Wenny Rahayu, "Dynamic mobile cloud computing: Ad hoc and opportunistic job sharing," In process of IEEE 4th International Conference on Utility and Cloud Computing (UCC 2011), pp. 281-286, 2011.

3 Subashini, Subashini, and Veeraruna Kavitha, "A survey on security issues in service delivery models of cloud computing." Journal of network and computer applications, Vol. 34, No. 1, pp. 1-11, 2011.

4 Ren, Kui, Cong Wang, and Qian Wang. "Security challenges for the public cloud," IEEE Internet Computing, Vol. 16, No. 1, pp. 69-73, 2012.

5 Huang, Dijiang, Zhibin Zhou, Le Xu, Tianyi Xing, and Yunji Zhong, "Secure data processing framework for mobile cloud computing, " In Computer Communications Workshops (INFOCOM WKSHPS), In process of IEEE Conference, pp. 614-618, 2011.

6 Yang, Kan, Xiaohua Jia, Kui Ren, Bo Zhang, and Ruitao Xie, "DAC-MACS: Effective data access control for multi authority cloud storage systems." IEEE Transactions on Information Forensics and Security, Vol. 8, No. 11, pp. 1790-1801, 2013.

7 Khan, Abdul Nasir, ML Mat Kiah, Samee U. Khan, and Sajjad A. Madani.,"Towards secure mobile cloud computing: A survey," Future Generation Computer Systems , Vol. 29, No. 5, pp. 1278-1299, 2013.

8 Xiao, Zhifeng, and Yang Xiao, "Security and privacy in cloud computing." IEEE Communications Surveys & Tutorials, Vol.15, no. 2 , pp. 843-859, 2013.

9 Zhou, Lan, Vijay Varadharajan, and Michael Hitchens, "Achieving secure role-based access control on encrypted data in cloud storage," IEEE transactions on information forensics and security, Vol. 8, No. 12, pp. 1947-1960, 2013.

10 Yang, Kan, and Xiaohua Jia, "Expressive, efficient, and revocable data access control for multi-authority cloud storage," IEEE transactions on parallel and distributed systems, Vol.25, No. 7, pp.1735-1744, 2014.

11 Baek, Joonsang, Quang Hieu Vu, Joseph K. Liu, Xinyi Huang, and Yang Xiang, "A secure cloud computing based framework for big data information management of smart grid," IEEE transactions on cloud computing, Vol. 3, No. 2, pp. 233-244, 2015.

12 Wang, Boyang, Baochun Li, and Hui Li, "Panda: Public auditing for shared data with efficient user revocation in the cloud," IEEE Transactions on services computing , Vol.8, No. 1, pp. 92-106, 2015.

13 Li, Jin, Jingwei Li, Xiaofeng Chen, Chunfu Jia, and Wenjing Lou,"Identity-based encryption with outsourced revocation in cloud computing," Ieee Transactions on computers, Vol. 64, No. 2, pp. 425-437, 2015.

14 Shaikh, Rizwana, and M. Sasikumar,"Trust model for measuring security strength of cloud computing service," Procedia Computer Science, Vo. 45, pp. 380-389, 2015.

15 Lin, Hui, Li Xu, Yi Mu, and Wei Wu, "A reliable recommendation and privacy-preserving based cross-layer reputation mechanism for mobile cloud computing." Future Generation Computer Systems, Vol. 52, pp. 125-136, 2015.\

16 Li, Yibin, Keke Gai, Longfei Qiu, Meikang Qiu, and Hui Zhao,"Intelligent cryptography approach for secure distributed big data storage in cloud computing," Information Sciences, Vol. 387, pp.103-115, 2017.

17 Yan, Zheng, Xueyun Li, Mingjun Wang, and Athanasios V. Vasilakos, "Flexible data access control based on trust and reputation in cloud computing." IEEE Transactions on Cloud Computing , Vol. 5, No. 3, pp. 485-498, 2017.

18 Noor, Talal H., Quan Z. Sheng, Lina Yao, Schahram Dustdar, and Anne HH Ngu, "CloudArmor: Supporting reputation-based trust management for cloud services," IEEE transactions on parallel and distributed systems, Vol. 27, No. 2, pp. 367-380, 2016.

19 Li, Jin, Yinghui Zhang, Xiaofeng Chen, and Yang Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," Computers & Security, Vol. 72, pp.1-12, 2018.

20 Luo, Yuchuan, Ming Xu, Kai Huang, Dongsheng Wang, and Shaojing Fu, "Efficient auditing for shared data in the cloud with secure user revocation and computations outsourcing," Computers & Security, Vol. 73, No. 492-506, 2018.

21 Saab, Salwa Adriana, Farah Saab, Ayman Kayssi, Ali Chehab, and Imad H. Elhajj, "Partial mobile application offloading to the cloud for energy-efficiency with security measures," Sustainable Computing: Informatics and Systems, Vol. 8, pp. 38-46,2015.

22 Khan, Abdul Nasir, ML Mat Kiah, Mazhar Ali, and Shahaboddin Shamshirband, "A cloud-manager-based re-encryption scheme for mobile users in cloud environment: a hybrid approach," Journal of Grid Computing, Vol.13, No. 4, pp. 651-675, 2015.

23 Xia, Qiufen, Weifa Liang, and Zichuan Xu, "The operational cost minimization in distributed clouds via community-aware user data placements of social networks", Computer Networks, Vol. 112, pp. 263-278, 2017.

24 GuojuGao, Mingjun Xiao,Jie Wu, Kai Han,Liusheng Huang,and Zhenhua Zhao, "Opportunistic mobile data offloading with deadline constraints", IEEE Transactions on Parallel and Distributed Systems, Vol. 28, No.12, pp.3584-3599,2017.

25 Muhammad Shiraz, Abdullah Gani, Azra Shamim , Suleman Khan , Raja Wasim Ahmad, "Energy efficient computational offloading framework for mobile cloud computing" , Journal of Grid Computing, Vol.13, No.1, pp. 1-18, 2015.

26 Muhammad Shiraz, Mehdi Sookhak, Abdullah Gani, Syed Adeel Ali Shah, "A study on the critical analysis of computational offloading frameworks for mobile cloud computing", Journal of Network and Computer Applications, Vol. 47, pp.47-60, 2015.