Design and Implementation of Crypt Analysis of Cloud Data Intrusion Management System

Dinesh Elangovan and Ramesh Muthiya
Department of Electronics and Communication Engineering, Anna University, India

Abstract: *Cloud computing is the method of employing a set-up of isolated servers to be hosted on the web to accumulate and supervise information instead of an area server or a private laptop. Storage of data in cloud sometimes creates security issues in the data stored so, security in provided for the stored cloud data. In order to provide secured cloud data transaction, our proposed method initially verifies the authentication of the user followed by splitting the information of the user using pattern-matching technique. The blowfish computation is used to encrypt the alienated data. After encryption, resorting to the selection of the optimal position of a data center by means of the cross grey wolf optimization and firefly technique is done. Finally, the encrypted data are stored at an optimal location in the cloud. Then the data split column wise and separated at an optimal location in the cloud, this method is highly secured since the user cannot retrieve the file without authentication verification.*

Keywords: *Cloud computing, Pattern Matching Technique, Blowfish Algorithm, Hybrid Grey Wolf Optimization, Firefly Technique*.

Received July 11, 2019; accepted May 10, 2020
https://doi.org/10.34028/iajit/17/6/8

1. Introduction

In the past years, people used to run applications or programs from the software downloaded on a physical computer or server, with little processing output. In order to overcome this crisis, the cloud services platform is formed [3, 5]. Appropriated figuring security is the course of action of control-set up together advances and concerning request movement of enlisting control, record amassing, applications and Information Technology (IT) resources through the cloud organization's methodology by methods for the web with the resuscitate as-you-go evaluating. Its advantages include scalability, resilience, flexibility, efficiency and outsourcing non-core activities. Disseminated processing offers a creative game plan for relationship to grasp IT organizations without candid endeavour [24, 32]. More associations are enduring the cloud arrange in light of its focal points and organizations. According to examiners at the advancement research firm Gartner, by one year from now 20 percent of all associations will never again have their own one of a kind servers and the rate is likely going to create in the exceptional years and disseminated processing is most likely going to build up much speedier in years.

As appropriated figuring is accomplishing broadened all inclusiveness and the distinction in the IT scene passes on with it new issues transmitting from the general idea of redistributing and from its fundamental assets. These issues handle association disrupting impacts and effect powerlessness to the cloud providers to suit structures. Regardless, the top weight that affiliations have with dispersed enrolling, rehashed examinations have found that it is attested in light of current conditions [14, 30]. Since a passed on figuring stage gives benefits by sharing gigantic assets, satisfactory utilization of these focal points can be drilled by guaranteeing that the stage can counter security risks which may isolate its showcase and unfaltering quality [29]. Exactly when all is said in done, the cloud stage is equipped with world class server machines, brisk aggregating gadgets and an effective structure [10]. The cloud clients can interface with the system through cell phones, workstations or present day work locales. Since the server machines are related using an internal framework, any kind of attack on the framework may cause a blocking impact as correspondence delays or the framework may finish up hard to reach. Also, the ambushes on virtual machines and hypervisors have appeared to genuinely crack the security for toxic purposes [18, 22]. Many cloud suppliers don't think about security an extreme need, with respect to a report discharged in Gregorian timetable month by Cloud advances and besides the Pokémon Association. The cloud organizations are similarly disposed to security threats as they contain programming which has been defenceless against hacks and security attacks various periods. These attacks may cause encroachment of data confirmation and in this manner cause detachment of organizations to all of the clients [21, 26].

A part of the estimations used for cloud security are commonly moderate computation, Message-Audit (Extraordinary imprint) counts, impelled encryption standard figuring, etc., [7, 27].

reasonably moderate figuring is for open key cryptography and incorporates an open and a private key. The open key is for encoding messages. Customer information handles coding and customer affirmation frameworks before limit or recuperation and building secure channels for data transmission. RSA is slower than its private key accomplices, similarly may be weak against emulate and is normally repetitive in a lone customer condition [19, 28]. Message Digest Algorithm-5 (MD5) count is a by and large used hash work, making a 128-piece hash a motivating force with specific limitations, for instance, security blemishes, vulnerabilities and is less secure standing out from the Secure Hash Algorithm-1 (SHA-1) computation [6, 23]. Advanced Encryption Standard (AES) is a symmetric encryption count with hindrances that it needs all the all the more taking care of and more modifies of correspondence when appeared differently in relation to Data Encryption Standard (DES) [9].

2. The Related Work

In PC frameworks, security and execution are commonly conversely corresponding. Batista *et al.* [1] have characterized Quality of Service (QoS)-driven methodologies for cloud situations based on the exhibition assessment of an administration comprising of various security components. These instruments force additional overhead on the presentation of the administration and so as to counter this, an undertaking was made to shift machine assets powerfully and on-the-fly. Guaranteeing QoS in a cloud situation was not a paltry undertaking since there were various kinds of customers with different administration necessities in the web based condition. In view of the after-effects of the examinations, they have confirmed that the QoS-driven methodology embraced in the Vertical condition gave the satisfaction characterized in the administration level understandings, with slight varieties in the administration costs.

Li *et al.* [15] have proposed security and cost mindful planning calculation for heterogeneous assignments including logical work process in mists. This calculation depended on meta-heuristic advancement procedure, Molecule Swarm Improvement, the coding technique concocted to limit the all out work process execution cost, complying with the time constraint and hazard rate limitations. Another coding methodology for tackling the multi-dimensional and multi-limitation streamlining issue was proposed. Expansive preliminaries using three genuine consistent work process applications speak to the practicality of this figuring.

Casola *et al.* [2] have proposed affirmation of-thought application that builds up on standard risk evaluation devices and grasps state of-craftsmanship Security Control Structures and a novel Security Service Level Agreement (SLA) model for the security necessities depiction. They gave a security-by-structure approach for the event of cloud applications that predominantly depends upon the SLA as a procedure to correct their security necessities. The strategy sought after to make a Security SLAs includes the machine of a peril examination technique furnished towards perceiving the most risks and licenses the countermeasures to consider design time. They focused on the methods inciting the time of per-part SLA and presented a SLA age application and different supporting instruments for its utilization.

Cotroneo *et al.* [4] have proposed a structure containing a channel and a choice tree to address gigantic volumes of security alarms and to help the mechanized particular proof of the concealed drivers of the cautions. The structure grasps term coefficient and dynamic group approaches to manage fill the opening between the unstructured issue alerts and the resistance of the choice tree. They evaluated the framework by separating two security datasets in a creation saas cloud, delivering a typical volume of 800 cautions for every day. The structure joins a decision tree to help the Identity Document (ID) of the fundamental drivers of the alerts held by the channel. A principle driver was a human-sensible portrayal of the events that caused the enacting of an alert. The unmistakable evidence of the principle drivers was developed through a determined clustering approach, which recognizes the general structure of the alert.

The benefits of appropriated processing go with the condition that the Cloud Organization Customers (CSC) need to accept the Cloud Service Providers (CSP) with their data. From this, it is understood that it was critical for CSC to acknowledge what security affirmations the CSP can guarantee by having the choice to quantitatively or emotionally balance CSPs offer with yielding with their very own needs. In order to address these Cloud security examination issues, Modic *et al.* [20], proposed a new Cloud security evaluation framework called Moving Between Times Strategy (MTS). It offers both precision and high computational capability and advises the most ideal approach to make the current Quantitative Different leveled Technique (QDLT) strongly beneficial. They have modified the QDLT, by applying principal numerical principles and have improved its presentation.

Kritikos and Massenet [12] have proposed a cloud-based Model-driven structure (MDE) approach that can try to push toward getting to be security-careful. The meta-model gets both high-and low-level security necessities and has capacities to drive application sending and security-masterminded flexibility rules to control application reconfiguration. The model is in like manner joined with Thing Constraint Language (TCL) goals actualizing the security space semantics. A system to make re-usable security segments empowering quick

security model specific following the meta-model is also proposed, to diminish the draftsman's exhibiting effort.

Zhang *et al.* [31] have proposed a system called organize then-unscramble, in which a planning stage is exhibited before the deciphering stage. This technique tackles the reason of figuring excellent parts in figure works, which were used to test that if the property private key matches the disguised access approach in unravelling compositions without disentangling. For speedy disentangling, special trademark fragments were made which grant mixture of pairings during unscrambling. They showed a puzzling Obscure trademark Based Encryption (OBE) improvement and got a security-redesigned extension reliant on one-time checks. In the proposed advancements, the estimation cost of a trademark organizing test was shy of what one interpreting task, which simply needs somewhat relentless number of pairings. Expansive execution examinations show that the methodology facilitate then-unscramble can improve interpreting viability in strange OBE.

Kritikos *et al.* [13] have orchestrated a model-driven philosophy and structure that confirms multi-cloud stages and moreover enables customers to have their own one of a kind non-open house. The procedure also engages changing a model based storage facility into a multi-inhabitant store on which access to affiliation express information is kept. This change joins abusing existing accommodation as for affirming the Chief Data Officer (CDO) model-based store which fathoms the Passage Metadata-Database module, mapping each from a huge amount of unequivocal occupations to a particular default set of access control strategies and controls the segment of access to the connection clients to the alliance's own exceptional data assets. The outcome pushes the sharing of information with perhaps various frameworks therefore improving the action of Relational relationship as the focal center empowering getting sharing.

Han *et al.* [8], have proposed an amazing and checked access control contrive for shared data to handle issues including key escrow, in turn around security and inefficiency issues. The point refines the protection of existing plans. Specifically, key escrow and end issue was tended to by secluding the key age center into a couple circled semi-trusted in parts. Cipher text-Plan quality base Encryption is a capable cryptographic approach to manage administers achieves a fine-grained data access control on dispersed point of confinement systems. Appropriated multi-parts key age estimation was gotten by the approach to manage the input issue. They have improved backward riddle with capability characteristics repudiation figuring. In switch puzzle was outfitted by their arrangement with denied attributes and re-encoded figure content. They have given point by point security and execution examination as well, which shows that the arrangement was both secure and capable.

Lyu *et al.* [16] have proposed, an insurance defending Data Sharing Arrangement to totally satisfy customers' security necessities. Social applications were getting the chance to be a champion among the most notable applications to share data and pass on the web. These applications impact stores of non-open data. Their methodology contains a fine-grained get to the administrator’s point which is a dynamic social trademark organization model and a multi-customer available puzzle making subject. To get the data owner's private data, people at first send the requesting message and addition the passageway power message from the conveyed stockpiling server. After endorsement, they can unravel the substance key of ABE and get the key for mixed data records. They have demonstrated that the proposed arrangement is versatile and profitable for recognizing checked data sharing for social applications.

3. Problem Definition

- Distributed computing has produced intrigue largely however, it is yet an advancing worldview. One of the principal contemplations of distributed computing is security. The basic issues in existing cloud security are as given beneath.
- Cost and adequacy is one of the serious issues of existing security and protection approaches.
- The clients worry about hacking dangers whether inside or remotely and the infeasibility of scrambling all information without thinking about its classification degree.
- The point of Intrusion Detection System (IDS) is to locate the assaults and produce right reaction. In any case, the current mark based interruption location strategy cannot identify the new or variation of known assaults.
- More time is required to recognize the assaults in a current interruption location framework.
- These downsides propel us to do this examination on Cloud Security Storage and interruption discovery framework. We look forward to propose a reasonable technique to accomplish secure information stockpiling and interruption discovery in distributed computing.

4. Proposed System

In the cloud framework, the information exchange is performed with raised security. In the inventive system, there are three unmistakable stages, for example, the authentication phase, cloud Data Center Selection Phase and the User Related Service Agreement Phase. For getting to the information from the cloud server, it is fundamental to have a sheltered verification key. In the underlying stage, the confirmation undertaking is completed by methods for the Blowfish strategy. To verify the

validation, the proposed technique is utilized to part the info document section shrewdly by methods for example coordinating methodology. In the resulting stage, the cloud data center is shortlisted to store the data, which is performed with the help of the progression methodology. To store the data in the cloud, we resort to the decision of the perfect position by techniques for the creamer Gray wolf progression and firefly framework. The last stage is stressed over the approval of the customer related organization understanding. The broad limit of the novel strategy is sufficiently shown in the square outline appearing in Figure 1 exhibited as pursues,

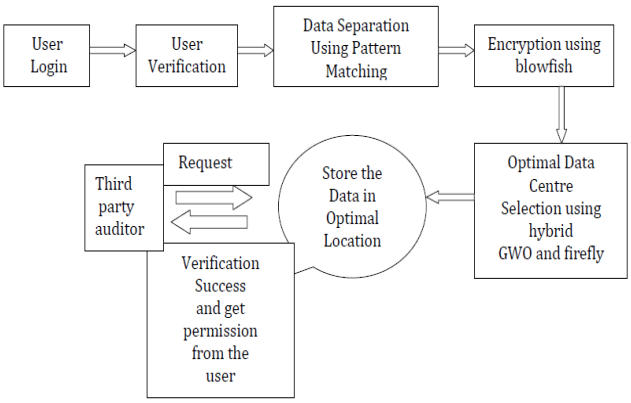


Figure 1. The overall semantic structure.

The verified data trade in the cloud courses through all the three phases. In the check organize, the customer data is certified with the ultimate objective of affirmation and as such, the data is mixed for the confirming framework, by utilizing the Blowfish approach. The scrambled information are outfitted to the ensuing stage in particular the cloud server farm choice stage, in which the situations for amassing the information in the cloud are chosen by methods for the half and half Gray wolf advancement and firefly strategy. In the third and last stage, the outsider evaluator is enabled access to the client information, in the wake of getting approval from the client for the inevitable confirmation of the information. Following the above procedures, the safe information exchange is acknowledged in our archive.

4.1. Authentication Phase

In the underlying stage, a protected information exchange is completed in the cloud by utilizing a proper procedure. The information proprietor needs to perpetually encode the document for capacity in the cloud. In the event that an outsider downloading the record, he is fit for, experiencing the report in the event that he is in control of the way to unscramble the scrambled document. This is probably going to manifest gratitude to the stunning progression of the innovation and the endeavors of the corrupt programmers. It is outmaneuvering an advanced test that the noteworthiness of the confirmation stage assumes a significant job by validating the client information in the cloud. Actually, the client outfits the applicable information like the client name and secret key for creating the database in the cloud. What's more, the programmed making of the private and open keys proposed for the client joins this. On fruitful confirmation, the client claims the validation.

a) Private key.
b) Public key.

Presently the client accomplishes his record in the cloud, it is fundamental that the document containing the information is securely put away in the cloud after it is scrambled. To improve the verification, the proposed strategy parts the info information into segment by methods for example coordinating methodology.

- **Example Coordinating Methodology**

The information is separated section savy by utilizing the example coordinating procedure, in which the example coordinating considers information of length and an example of length with the goal of subdividing the whole information into segments [11], which are thusly amassed in assorted areas of the cloud, by assessing the results. In the paper, the example coordinating system is used to part the information from the info record. The procedure of example coordinating system is depicted underneath,

1. In the information, every segment is joined with different sections dependent on their craving significance of the word or information.
2. After that, the limit worth is fixed for gathering the information displayed in the segments. In light of the limit esteem, we have framed gatherings like gathering group 1, group 2 and so on.
3. The relating information are checked and gathered has a place with their comparing limit estimations of group1 or group 2.
4. The above advances (1-3) are rehashed for gathering the information exhibited in all sections. The comparable method for examination is utilized in the paper for part the information into segments.

Finally, the segment adroit split data is supported to the encryption technique. The proposed methodology uses the Blowfish estimation for the encryption system. The very much arranged procedure of encryption figuring is showed up underneath,

- **Encryption and Decryption Process**

The encryption addresses changing the key substance data into propelled figure content. Then again, the unraveling is associated with the limit of changing the content along with the first plaintext.

The encryption limit is performed with the help of the Blowfish method.

- **Utilizing the Blowfish Algorithm for the Encryption Process**

The Blowfish procedure has been adequately busy with the standard of accomplishing the symmetric key cryptography. In the dynamic method, the Blow Fish technique is secured for both the encryption and the translating. It solidifies 64-bit square estimation and key length from 32 bits to 448 bits. The P-bundle and four 32-bit S-confines like way happen. The P-bunch incorporates 18 of 32-bit sub keys and each S-box is home to 256 entryways [25].The key advancement is a representative by the task of actualizing the change of the information key (448 Bytes) into sub key (4168 Bytes) exhibits. The information encryption takes up 16 round Feistel framework, among each surrounding invested by a key dependent blend and a changeover. Every single assignment connotes the XOR and the embellishments on 32-bit words in the blowfish technique.

- **Sub Keys of Blowfish Algorithm**

An incredibly enormous number of sub keys are conveyed in the Blowfish procedure, and they must be perpetually pre-registered before completing the encryption and decoding forms.

- P-exhibit has (18) out of (32)-Bit sub keys.
- Four (32) Bit S-box has (256) records.

- **Encryption**

The encryption implies the task of redesigning central content into the Figure 2 content. In the age making strategy, the information utilize is a 64-bit information, which, in the fundamental enclosing, is isolated into twofold 32 bit cut up, set apart as the Left Hand (LH) and the Right Hand parts (RH). In the first blowfish calculation, the essential 32 bit left parts and the P-cluster complete the XOR task and the outcome is conveyed to a specific capacity (F) which is appeared in Figure 2. Next to that point, finish the XOR task similarly for left half and 32-bit right half. Thus, the remaining will drag out until the accomplishment of the 16 rounds.

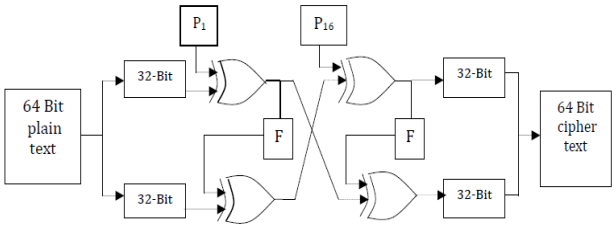


Figure 2. Blowfish structure of the suggested technique.

- **Procedure of the F Function**

The F function deploys the four (32) bit S-boxes, with each one subsuming (256) records. In the new blowfish technique, the initial (32) bit left halves are subdivided into four (8) bit blocks as m, n, o and p. The mathematical relationship employing the Ft function is exhibited in the ensuing Equation (1).

$$F(L_H) = ((S_{b1,m} + S_{b2,n} \bmod 2^{32}) \oplus S_{b3,o}) + S_{b4,p} \bmod 2^{32} \quad (1)$$

The detailed working process of F function is shown in the Figure 3.

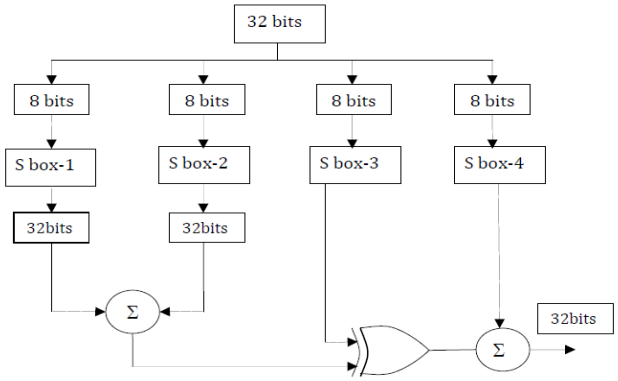


Figure 3. The working procedure of F function.

- **Decryption**

The decryption system of the blowfish method is alike to that of the encryption, even if in the earlier, the P-array is engaged in the repeal. The productivity of the blowfish method accumulates the folder in the cloud, which is arranged at the input of the second segment. By the support of the communal and personal keys, the folder experiences the task of encryption and acquire uploaded into the cloud in the algortihm 1

Algorithm 1: Proposed Blowfish

1. *Read the 64bit system data Y*
2. *System data Y divided into two equal parts* Y_1 *and* Y_2
3. *For* $j = 1 \text{ to } 16$
   $Oy_1 = y_1 \; XOR \; p_1$
   $Oy_2 = f(Oy_1) \; XOR \; y_2$
4. *Exchange* Oy_1 *and* Oy_2
5. *Again do the process until it reaches the 16th round*
6. *Combine the two equal parts*

The S-Boxes and P-Boxes are initiated by standards from the hex digits of pi. The variable length user input key is then XOR by P-entries. Subsequently, a mass of zeros are encrypted, and this outcome is utilized for P1 and P2 access. The output of the blowfish technique saves the file in the cloud, which is deployed as the input of the second phase. With the assistance of the secret keys, the file undergoes the function of encryption and gets uploaded into the cloud. In order to upload the data, the suggested technique selects the optimal data centre. The modus

operandi of the data centre selection phase is brilliantly briefed below.

- **Data Center Selection**

In the data centre selection phase, the locations are optimally selected for stockpiling the data in the cloud, which is recognized by means of the hybrid Grey wolf optimization and firefly technique. The comprehensive procedure of the innovative technology is effectively elaborated in the ensuing section,

- **Hybrid Grey Wolf Optimization and Firefly Technique**

Grey Wolf Optimizer (GWO) is a distinctive swarm-intelligence series that is impressed by the management hierarchy with looking mechanism of gray wolves in nature. Grey wolves are measured apex predators; they enclose a typical group range of about five to twelve. In the GWO algorithm, the gathering of grey wolves is alienated into following groups: omega (ω), alpha (a), beta (β) and delta (δ). In each iteration, the first three best applicant solutions are named as α, β and δ. The remaining of the grey wolves are reviewed as ω and are guided by α, β and δ. In the order of GWO, alpha (α) is considered the most mastering member among the cluster. The remaining of the subordinates of α are beta (β) and delta (δ), which is to manage the majority of the wolves in the order that are considered as omega (ω). The wolves are of lower positioning in the progressive system. So as to improve its presentation, the firefly calculation is crossover with dim wolf advancement. The Firefly (FA) calculation is a met heuristic calculation, enlivened by the glimmering conduct of fireflies. The main role of a firefly's glimmer is to go about as a sign frame to pull in different fireflies. This firefly calculation is takes three suppositions,

- All fireflies region are unit sexual all together, with the end goal that one firefly will be attracted to every extraordinary firefly.
- Attractiveness is matching to their intensity, and thinking about any 2 fireflies, the more splendid one however the splendor will diminish as the separation increments will pull in the less splendid one.
- If there aren't any fireflies more splendid than a given firefly, it'll move heedlessly.
- The well ordered procedure of the dim wolf improvement calculation is referenced underneath,

- *Step* 1: Preliminary process
  Instate the quantity of server farm and the comparing coefficient vectors $x, y, and\ z$.
- *Step* 2: Strength evaluation
  Assess the Strength execution based on the condition (2) and pick the best outcome.

$$\mathrm{Str}_{\mathrm{i=max\ matched\ data}} \tag{2}$$

- *Step* 3: Separate the arrangement dependent on the Strength
  At present, the particular outcome is found based on the Strength esteem. Consider the principal best Strength result as J_a, the second best Strength result as J_β and the third best Strength arrangements as J_δ.
- *Step* 4: Revise the position
  We accept that the alpha (best competitor arrangement), beta and delta have improved their insight about the potential area of the prey to replicate numerically the chasing conduct of the dim wolves. For redundancy, the new arrangement or information $J_P(t+1)$ reevaluated by utilizing the formulae referenced underneath.

$$\vec{K} = |\vec{z} J_p(t+1) - J_p(t)| \tag{3}$$

Where,

$$\vec{K}^{\alpha} = |\vec{z}_1.J_{p\alpha} - J_p|, \quad \vec{K}^{\beta} = |\vec{z}_2.J_{p\beta} - J_p|, \quad \vec{K}^{\delta} = |\vec{z}_3.J_{p\delta} - J_p|$$

$$J_P(t+1) = (J_{P1} + J_{P2} + J_{P3})/3 \tag{4}$$

Where,

$$J_{P1} = J_{P\alpha} - \vec{y}_1.(\vec{K}^{\alpha}), J_{P2} = J_{P\beta} - \vec{y}_2.(\vec{K}^{\beta}), J_{P3} = J_{p\delta} - \vec{y}_3.(\vec{K}^{\delta})$$

$$\vec{y} = 2\vec{x}r_1 - \vec{x} \quad \text{And} \quad \vec{z} = 2r_2 \tag{5}$$

Where t speaks to the emphasis number, p (t) speaks to the situation of the prey, y and z speaks to the vector coefficient, is diminished straightly from 2 to 0, and speaks to the arbitrary incentive in the array [0, 1].

The alpha, delta, and beta evaluate the situation of the prey and furthermore different wolves update their positions self-assertively incorporating the prey. Investigation and misuse are positive by methods for a versatile estimations of x and y. The versatile estimations of x and y grant GWO to effortlessly transition between investigation and abuse. With the lessening y, half of the emphases are focused on the examination and the other half is committed to its use. Encasing the lead, the resulting conditions are used remembering the ultimate objective to give numerical mode.

- *Step* 5: Firefly update

n the firefly algorithm, the new solution is updated by means of the equation below,

$$J_{ix}^{new} = J_{ix} + A(J_{jx} - J_{ix}) + \alpha(\delta - 1/2)$$
$$A_t = A_{t0}\, e^{-\beta d_{ij}^2} \tag{6}$$

Where,

A_{t0} refers to the present attractiveness

β - represents the radiance absorption coefficient

d_{ij}- denotes the space between the two centers

Here, α and δ depict the uniformly disseminated values in the range of 0 to 1. Hence, the modernized values encourage the data centre to inch towards the current best Strength value. The best data centre is updated in the first fireflies by substituting the existing old data centre. Thereafter, all the fireflies are updated by performing these processes.

- *Step* 6: Strength calculation

Calculate the Strength of the new search solution using Equation (2) and then store the best solution.

- *Step* 7: Stopping criteria

Reiterate step 3 to 6, until highest number of iterations are obtained. Based on the above-described process, the optimal data centre location should be attained.

- **User Related Service Agreement Phase**

Here, the third party auditor performs his duty of perusing and, if necessary, editing the document of the use, after getting the requisite nod from the user, as it is simply impossible for the third party to access the data for scrutiny or editing sans the concurrence of the users. Thus if a third party auditor wants to peruse or edit the document, he has to be invariably authenticated beforehand. In the event of successful completion of the authentication, the user hands in the authentication key to the third party auditor, this does the third party auditor for the purpose of scrutiny and subsequent editing of the relevant document use. In due course, the third party auditor decrypts the document by making use of the login credentials tendered by the user. The runtime, memory utilization are evaluated and scaled down for the performance of the new-fangled technique.

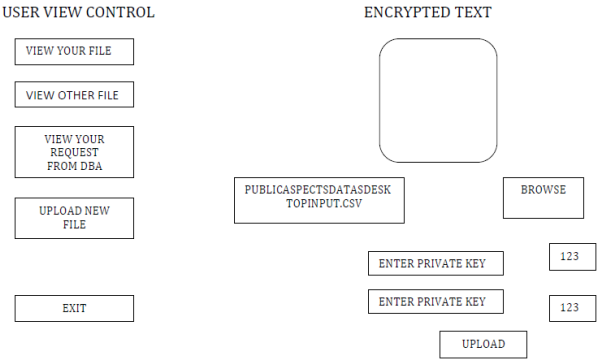
5. Result and Analysis

This section gives a detailed view of the result that is obtained by secured data transaction process in the cloud. This work is implemented in java with CloudSim simulator in Intel (R) Core i7 processor, 3.2 GHz, 4 GB RAM with operating system platform as Microsoft Wnidow7 Professional.

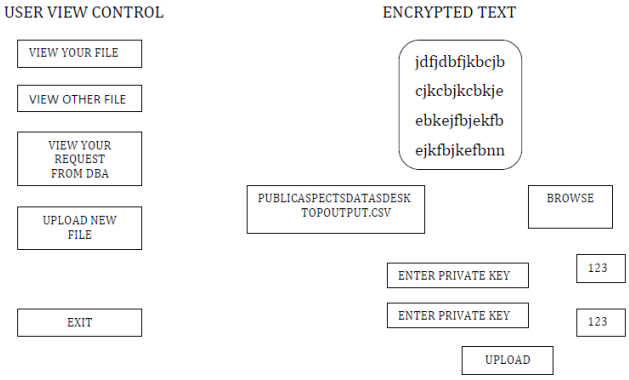
- *Assessment Frameworks*: This section provides the performance analysis of encryption time and memory usage at different file size.
- *Memory Usage*: Java effectively organizes the memory. New objects are generated and positioned in the stack. The memory usage of the suggested technique is computed in bytes.
- *Execution time*: The execution time in Java with Cloud Sim program is evenly rooted based on the database values. The time duration is computed in milliseconds (ms).
- *Encryption and decryption time*: The time taken to complete the encryption and decryption method. Here the progression time is computed in milliseconds (ms).

5.1. Experimental Results

Initially, the user selects the data from the input file afterwards the encryption process is carried out. The data selection of the user window is exposed in Figure 4-a and the screenshot for the data encrytpion process is exposed in Figure 4-b.



a) User window.



b) Data encryption process.

Figure 4. Cloudsim data selection and process window.

5.2. Performance Analysis

The Tables 2, 3, and 4 shows the performance analysis of the proposed encryption method .The performance is analysed with the assessment frameworks such as file size after encryption and decryption, encryption time and decryption time for existing and our proposed method, memory usage and run time for overall execution of each file for existing and our proposed method and convergence time for a range of iterations. When we look into the performance analysis the encrypted file size is increased from the original file size and the same file range is obtained after decryption. Here, in our proposed system the encryption and decryption time decreases when compare with the existing method. Based on the iterations in each file range the convergence time for our proposed system is less when compared with GWO and Firefly.

Table 1. Encryption time for different file size.

File range(Kb)	Existing System Encryption Time(ms)	File size after Encryption (Kb)	Proposed System Encryption Time(ms)
5	36153	8 Kb	31356
10	34324	13 Kb	29748
15	35214	19 Kb	30659
20	41283	24 Kb	34812

Table 1 shows the number of file sizes 5 kb, 10 kb, 15 kb, and 20 kb. The recommended technique requires 31356ms,29748ms,30659ms,34812ms for encryption.

Table 2. Decryption time for different file size.

File range (Kb)	Existing System Decryption Time (ms)	File size after Decryption (Kb)	Proposed System Decryption Time (ms)
5	**36217**	**5**	**31545**
10	**39512**	**10**	**32256**
15	**37613**	**15**	**35581**
20	**54216**	**20**	**36437**

Table 2 shows the number of file sizes 5 kb, 10 kb, 15 kb, and 20 kb. The recommended technique requires 31545ms,32256ms,35581ms,36437ms for decryption.

Table 3. Memory and execution time for various file size.

File range(Kb)	Existing System Memory Usage	Proposed System Memory Usage	Existing System Run Time(ms)	Proposed System Run Time(ms)
5	10482357	11788588	173246	185544
10	11254613	12358455	193215	202585
15	12326714	13488477	224219	236598
20	14153148	15259766	241846	259452

From Table 3 it becomes apparent that the 5 kb document length is 11788588 copies for the storage occupied and 12358455 pixels for the 10 kb device volume, 13488477 pixels for the 15 kb memory occupied and 15259766 pixels for the 20 kb document volume. The data size of the 5 kb file time is 185544ms and the execution period for the file size 10 kb is 202585ms. The execution time for the file size 15 kb is 236598ms and for the file size of 20 kb, it is 259452ms respectively. The execution time is 259452ms.

Table 4. Convergence time for various file size.

No of Iterations	Convergence Time (ms) Firefly	Convergence Time (ms) GWO	Convergence Time (ms) (Firefly+GWO)
10	9	10	7
20	19	20	18
30	30	28	24
40	36	33	24

Table 4. shows the convergence time for various file sizes, based on the number of iterations.

- **Comparative Analysis**

The file size taken for our proposed work before encryption and after encryption is shown in Figure 5.

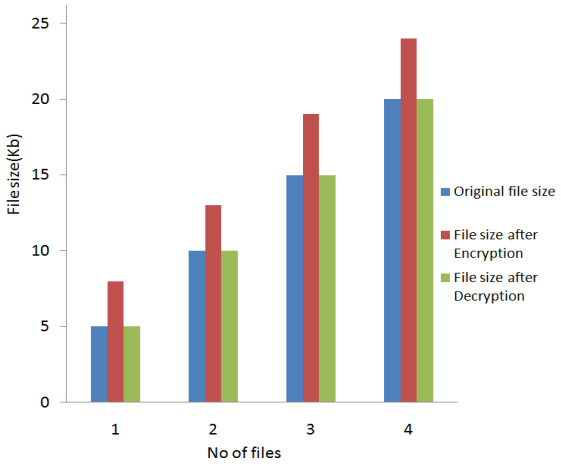


Figure 5. File size taken for the proposed method.

After the blowfish encryption, the file size is changed, initially, the file size we are taking is 5(kb) but after the encryption, the file size is changed to 8 (kb). The file size 10 (kb), 15(kb) and 20(kb) size is changed after the encryption is 13(kb), 19(kb) and 24(kb) respectively. Then the encrypted file is stored in the cloud using the optimal data centre selection. To view the file, we must decrypt the file after the download. Hereafter the encrypted file is changed to the original size.

For comparison existing Advanced Encryption Standard (AES) method [17] is taken to compare the result with encryption method using blowfish. The following Figure 6 shows the comparative result of encryption with decryption scheme for both proposed and existing technique.

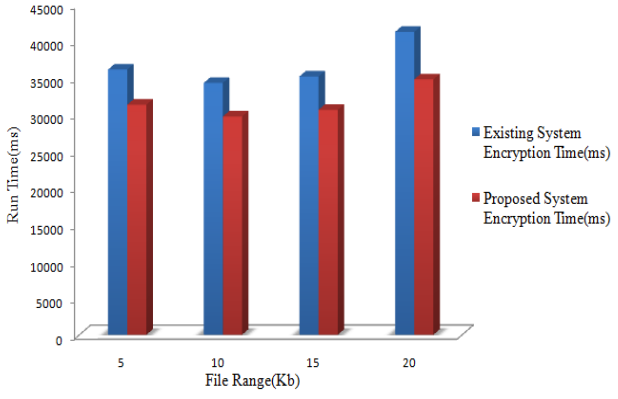


Figure 6. The comparative analysis of encryption.

From the analysis it is shown that our planned method has better encryption with decryption time when compared to the existing methods. The graphical version of the comparative analysis for decryption time for proposed and existing method is shown below Figure 7,

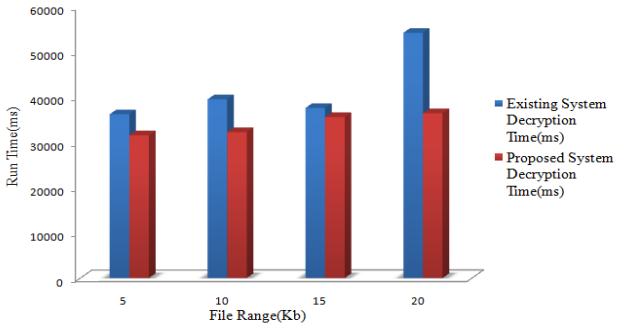


Figure 7. The comparative analysis of decryption.

When analyzing the Figures 6 and 7, the suggested technique attains the minimum encryption and decryption time when compared to the existing techniques. The hybrid GWO used for selecting the optimal location based firefly algorithm, since it reduces the convergence time of the recommended techniques. The convergence time comparison for the proposed method and existing methods is shown in Figure 8.

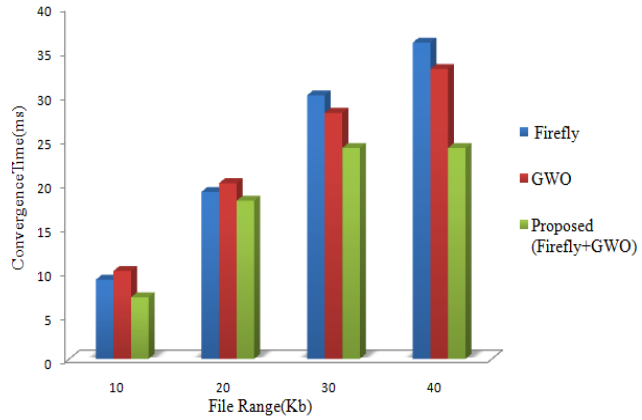


Figure 8. Convergence time comparison for proposed versus existing methods.

Finally, the optimal location in the cloud is selected and stored as the encrypted data. It is highly secured and thus the proposed method serves the best security.
The memory usage and execution time increases while comparing with the existing method but the data security is increased. This is shown in Figures 9 and 10.

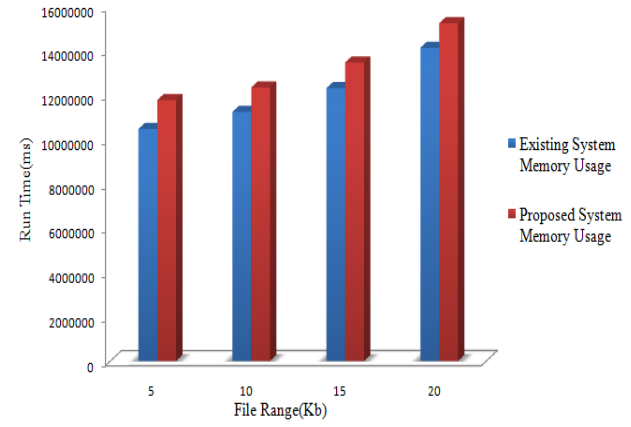


Figure 9. Memory usage comparison for proposed versus existing methods.

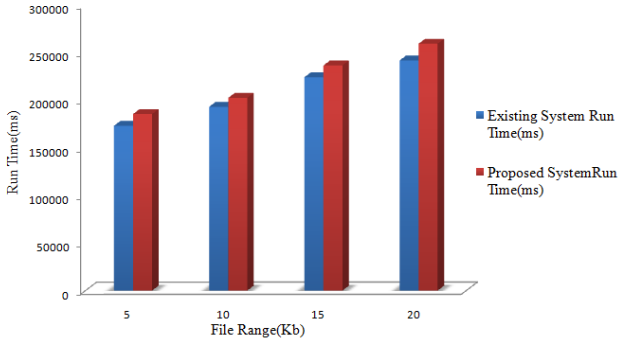


Figure 10. Execution time comparison for proposed versus existing methods.

Finally, the optimal location in the cloud is selected and stored as the encrypted data. It is highly secured and thus the proposed method serves the best security.

6. Conclusions

In the projected method once the user logins, the authentication of the user is firstly verified. After verification, the information of the user is split column wise using a pattern matching technique. The separated data are encrypted using the blowfish algorithm. The encrypted data are stored at an optimal location in the cloud. For this purpose, the optimal data centre in the cloud is selected using hybrid grey wolf optimization and firefly technique. Finally, the encrypted data are stored at an optimal location in the cloud. The routine of the method is evaluated in terms of memory, encryption and decryption time. The investigational results show that the method is highly preferable than the existing methods. Since the data is split column wise and separated at the optimal location in a cloud, this method is highly secured. The user cannot retrieve the file without authentication verification hence this method is highly secured. In future efficient algorithms could be used for increasing the speed of the overall process.

References

[1] Batista B., Ferreira C., Segura D., Filho D., and Peixoto M., "A QoS-Driven Approach for Cloud Computing Addressing Attributes of Performance and Security," *Future Generation Computer Systems*, vol. 68, pp. 260-274, 2017.

[2] Casola V., Benedictis A., Rak M., and Rios E., "Security-by-Design in Clouds: A Security-SLA Driven Methodology to Build Secure Cloud Applications," *Procedia Computer Science*, vol. 97, pp. 53-62, 2016.

[3] Chang V., Kuo Y., and Ramachandran M., "Cloud Computing Adoption Framework: A Security Framework for Business Clouds,"

Future Generation Computer Systems, vol. 57, pp. 24-41, 2016.

[4] Cotroneo D., Paudice A., and Pecchia A.,"Automated Root Cause Identification of Security Alerts: Evaluation in A Saas Cloud," *Future Generation Computer Systems*, vol. 56, pp. 375-387, 2016.

[5] Cusack B. and Ghazizadeh E.,"Evaluating Single Sign-on Security Failure in Cloud Services," *Business Horizons*, vol. 59, no. 6, pp. 605-614, 2016.

[6] Grobauer B., Walloschek T., and Stocker E., "Understanding Cloud Computing Vulnerabilities," *IEEE Security and Privacy*, vol. 9, no. 2, pp. 50-57, 2011.

[7] Gupta P. and Kumar S., "AComparative Analysis of SHA andMD5 Algorithm," *International Journal of Computer Science and Information Technologies*, vol. 5, no. 3, pp. 4492-4495, 2014.

[8] Han K., Li Q., and Deng Z., "Security and Efficiency Data Sharing Scheme for Cloud Storage," *Chaos, Solitons and Fractals*, vol. 86, pp. 107-116, 2016.

[9] Iqbal S., Kiah L., Dhaghighi B., Hussain M., Khan S., Khan M., and Choo K., "On Cloud Security Attacks: A Taxonomy and Intrusion Detection and Prevention As A Service," *Journal of Network and Computer Applications*, vol. 74, pp. 9-120, 2016.

[10] Kalpana P. and Singaraju S., "Data Security in Cloud Computing using RSA Algorithm," *International Journal of Research in Computer and Communication Technology*, vol. 1, no. 4, pp.143-146, 2012.

[11] Khan M., "A Survey of Security Issues for Cloud Computing," *Journal of Network and Computer Applications*, vol. 71, pp. 11-29, 2016.

[12] Kritikos K. and Massenet P., "An Integrated Meta-model for Cloud Application Security Modeling," *Procedia Computer Science*, vol. 97, pp. 84-93, 2016.

[13] Kritikos K., KirkhamT., Kryza B., and Massenet P., "Towards a Security-Enhanced Paas Platform For Multi-Cloud Applications," *Future Generation Computer Systems*, vol. 67, pp. 206-226, 2017.

[14] Kuyoro S., Folami I., and Oludele A., "Cloud Computing Security Issues and Challenges," *International Journal of Computer Networks*, vol. 3, no. 5, pp. 247-255, 2011.

[15] Li Z., Ge J., Yang H., Huang L., Hu H., Hu H., and Luo B., "A security and Cost Aware Scheduling Algorithm for Heterogeneous Tasks of Scientific Workflow in Clouds," *Future Generation Computer Systems*, vol. 65, pp. 140-152, 2016.

[16] Lyu C., Sun S., Zhang Y., Pande A., Lu H., and Gu D., "Privacy-Preserving Data Sharing Scheme over Cloud for Social Applications," *Journal of Network and Computer Applications*, vol. 74, pp. 44-55, 2016.

[17] Mahendran N., "Collaborative Location Based Sleep Scheduling with Load Balancing in Sensor-Cloud," *International Journal of Computer Science and Information Security*, vol. 14, pp. 20-27, 2016.

[18] Mahendran N. and Priya R., "Sleep Scheduling Schemes Based on Location of Mobile User in Sensor-Cloud," *International Journal of Computer, Electrical, Automation, Control and Information Engineering, World Academy of Science, Engineering and Technology*, vol. 10, no. 3, pp. 615-620, 2016.

[19] Mal W., Han Z., Li X., and Liu J., "A Multi-Level Authorization Based Tenant Separation Mechanism in Cloud Computing Environment," *China Communications*, vol. 13, no. 5, pp. 162-171, 2016.

[20] Modic J.,Trapero R., Taha A., Luna J., Stopar M., and Suri N., "Novel Efficient Techniques for Real-Time Cloud Security Assessment," *Computers and Security*, vol. 62, pp. 1-18, 2016.

[21] Niu S., Tu S., and Huang Y., "An Effective and Secure Access Control System Scheme in the Cloud," *Chinese Journal of Electronics*, vol. 24, no. 3, pp. 524-528, 2015.

[22] Ravali K., Neelima P., Sruthi P., Dileep P., and Manasa B., "Implementation of Blowfish Algorithm for Efficient Data Hiding in Audio," *Journal of Computer Science and Information Technologies*, vol. 5, no. 1, pp. 748-750, 2014.

[23] Sachdev A. and Bhansali M., "Enhancing Cloud Computing Security using AES Algorithm," *International Journal of Computer Applications*, vol. 67, no. 9, pp. 19-23, 2013.

[24] Shah P. and Javheri S., "Data Security in Cloud Storage using Role-Based Access Control and Time-Based Assured Deletion," *International Journal of Computer Application*, vol. 5, no. 6, pp. 1-5, 2015.

[25] Shanmugam S. and Iyengar S., "Improving Energy Efficiency and Impairing Environmental Impacts on Cloud Centers by Transforming Virtual Machine into Self-Adaptive Resource Container," *The International Arab Journal of Information Technology*, vol. 16, no. 4, pp. 617-623, 2019.

[26] Singh S., Jeong Y., and Park J., "A survey on Cloud Computing Security: Issues, Threats, and Solutions," *Journal of Network and Computer Applications*, vol. 75, pp. 200-222, 2016.

[27] Srivastav S. and Verma N., "Improving Data Security in Cloud Computing using RSA Algorithm and MD5 Algorithm," *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 4, no. 7, pp.

5450-5457, 2015.

[28] Suresh K. and Prasad K., "Security Issues and Security Algorithms in Cloud Computing," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, no. 10, pp. 110-114, 2012.

[29] Vasudevan S., Vivek C., and Srivathsan S., "An Intelligent Boxing Application through Augmented Reality for two users-Human Computer Interaction Attempt," *Indian Journal of Science and Technology*, vol. 8, no. 34, pp. 1-7, 2015.

[30] Vasudevan S. and Vivek C., "An Intelligent Attempt to Export Files into Cloud in Handheld Devices through Gesture Recognition," *Indian Journal of Science and Technology*, vol. 8, no. 34, pp. 1-8, 2015.

[31] Zhang Y., Chen X., Li J., Wong D., Li H., and You I., "Ensuring Attribute Privacy Protection and Fast Decryption for Outsourced Data Security in Mobile Cloud Computing," *Information Sciences*, vol. 379, pp. 42-61, 2017.

[32] Zissis D. and Lekkas D., "Addressing Cloud Computing Security Issues," *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583-592, 2012.

Dinesh Elangovan obtained his Bachelor's degree in Electronics and Communication from Anna University, Chennai. Then he obtained his Master's degree in Applied Electronics and PhD doing in Information & Communication majoring in Cloud Computing, Big Data Analytics and Networking both from Anna University, Chennai, Tamilnadu, India. He has also obtained Computer Networking professional qualifications. Currently, he is a SeniorAssistant Professor at the Faculty of Electronics and Communication Engineering, M.Kumarasamy College of Engineering, Karur. His specializations include Cloud Security, networking, and Virtual Reality. His current research interests are Cloud Data Security Formation, Public Key Infrastructure, Network Security, Authentication Server, Virtual Simulation, Virtual Reality and Cryptographic Techniques.

Ramesh Muthiya received the B.E. degree in Electronics and Communication Engineeringfrom National Institute of Technology (Formerly REC), Trichy, India, in 2001 and the M.E. degree in Applied Electronics from the Anna University, Chennai, India, in 2004. He was awarded his Ph.D. degree in Information and Communication Engineering from Anna University, Chennai, India, in 2012.; He is currently working as Professor in the Department of Electronics and Communication Engineering at K.P.R Institute of Engineering and Technology, Coimbatore, India. He has published 69 articles in international and national journals and more than 33 papers in international and national conferences. His current research focuses are in Image processing, VLSI design, Embedded systems and Wireless networks. He is a life member of the ISTE, a member of the IAENG and a life member of the IETE.