A secured best data centre selection in cloud computing using encryption technique

A. Prabhu*

PSG Institute of Technology and Applied Research,
Neelambur, Coimbatore – 641 062, India
Email: aprabhu0484@gmail.com
*Corresponding author

M. Usha

Department of Computer Science and Engineering,
Sona College of Technology,
Salem-5, India
Email: ushaanu@yahoo.com

Abstract: In this work, we have proposed an approach for providing very high security to the cloud system. Our proposed method comprises of three phases namely authentication phase, cloud data centre selection phase and user related service agreement phase. For the purpose of accessing data from the cloud server, we will need a secure authentication key. In the authentication phase, the user authentication is verified and gets the key then encrypts the file using blowfish algorithm. Before encryption the input data is divided into column-wisely with the help of pattern matching approach. In the approach, the encryption and decryption processes are carried out by employing the blowfish algorithm. We can optimally select the cloud data centre to store the data; here the position is optimally selected with the help of bat algorithm. In the final phase, the user service agreement is verified. The implementation will be done by cloud sim simulator.

Keywords: authentication key; blowfish; bat algorithm; pattern match; cloud data centre selection.

Reference to this paper should be made as follows: Prabhu, A. and Usha, M. (2019) 'A secured best data centre selection in cloud computing using encryption technique', *Int. J. Business Intelligence and Data Mining*, Vol. 14, Nos. 1/2, pp.199–217.

Biographical notes: A. Prabhu obtained his Bachelor of Science degree in Computer Science from the K.S.R. College of Arts and Science, Periyar University, Salem, India in 2004. Then, he obtained his Master of Computer Application degree in K.S.R. College of Arts and Science, Periyar University, Salem, India in 2007. Then, he obtained his Master of Engineering in the K.S.R College of Engineering and PhD in Computer Science and Engineering in Cloud Security, from Anna University, India in 2009. He is currently working as an Assistant Professor at PSG Institute of Technology and Applied Research, Coimbatore. His specialisations include cloud computing, theory of computation, compiler design, operating system and computer graphics.

M. Usha received his BE (ECE) degree from the Madras University, Coimbatore, India in 1984, ME (CSE) degree from the College of Engineering, Anna University, Chennai, India, in 1994, and PhD degree from the Anna University, Chennai, India, in 2008. She worked as a Lecturer at the Coimbatore Institute of Technology. She is currently working as a Professor in the Department of Computer Science and Engineering at Sona College of Technology. Her research interests are in internet of things QoS and intelligence in networking, network security, wireless sensor networks, embedded architecture, operating systems, and mobile e-learning. He serves as a member in IEEE, life member in ISTE, and life member in CSI.

1 Introduction

It is heartening that the sophistication in the computing has reached such a saturation state that it is being metamorphosed into an appealing pattern encompassing an assortment of services which are commoditised and handed in a platter, just like the time-honoured utilities like the water, electricity, gas, and the telephony. In the relative patterns, the users emerge as the kingpins with the carte blanche of enjoying 24/7 swift access to services anchored in their penchants without making any hue and cry about the places from which the relative services approach them to give extreme delight or the way they are delivered. In this regard, a feast of computing paradigms offer a ray of hope by flooding the valued clients with several options to offer them the related utility computing vision which bring under its umbrella various endearing services such as the cluster computing, grid computing, and the latest innovation being the inimitable cloud computing (Buyyaa et al., 2009). The cloud computing in quintessence represents a novel technique of handing over the computing resources, rather than an innovative methodology.

In this connection, the cloud computing may be defined as "the mega distributed computing paradigm which is motivated by economies of scale, in which a flood of abstracted virtualised, dynamically-scalable, managed computing power, storage, platforms, and services are showered based on the requirements to the outdoor clients over the web" (Christodorescu et al., 2009). The fundamental points forming part of the captioned definition are furnished as follows. At the outset, the cloud computing represents a dedicated distributed computing model, which follows a divergent trajectory from the conventional techniques as illustrated below:

1 It is extraordinarily scalable.

2 It is capable of being summarised as an abstract entity endowed with the requisite skills of offering a varied spectrum of services to clients outside the cloud.

3 It is invariably motivated by the economies of scale (Silvestre, 1987).

4 The services are animatedly designed by means of virtualisation or other parallel techniques and showered as and when required.

In the process of offering a safe cloud computing solution, an important facet to be prudently considered is the decision regarding the category of the cloud to be performed. As of now, three distinct kinds of the cloud deployment patterns provided which include the public, private (Ramgovind et al., 2010) and the hybrid cloud (Jensen et al., 2009). Further, the cloud computing glisten with the sheen of possessing five key distinctive technological traits as detailed below:

1 the titanic computing resources

2 the superior scalability and elasticity

3 the shared resource pool (both the virtualised and physical resources)

4 the animated resource scheduling

5 the wide-ranging targets.

Especially, the cloud computing effectively offers the computing resources in the edition of on-demand services hosted at far-off locations, availed over the Web, and habitually billed on a per-use base.

The live instances of the cloud computing are found in the Web 2.0, with the giants such as the Google, Yahoo and Microsoft, making their august appearance on the arena as the appealing service providers, exciting their dedicated clients with the browser-based enterprise service applications in the garb of the webmail and remote data backup. Of late, the cloud computing has elegantly established itself as an endearing, feasible and close at hand platform, a consortium of clients from several scenarios such as the financial institutions, educators, or cybercriminals are vying with one another in sharing the virtual machines to carry out their day-to-day deals. With the result, it has become highly essential to offer an implied level of confidence as together with an overt level of watchfulness to so as to achieve unfailing success (Kaufman, 2009). In the domain of the cloud computing world, the implicit scenario enables the users access the computing power which is far in excess of what they have in their own physical worlds. In order to have an access to this virtual world, it is not essential to have an awareness regarding the precise locality of their data or the parallel sources of the data jointly amassed with theirs (Kaufman, 2009). In fact, all the data safety approaches are rooted on the confidentiality, integrity and accessibility of the captioned three fundamental principles. The confidentiality, in turn, relates to the supposedly-concealed real data or information, particularly in the military and other sensitive areas, the confidentiality of data on the further tough requisites (A Platform Computing Whitepaper, 2010).

In the case of the cloud computing, as the data is amassed in the 'data centre', the safety and secrecy of the user data assumes zooming significance. In fact, the self-styled integrity of data in any state must have the essential pre-requisites to ensure against the illegal erasure, alteration or destruction. By the term the 'availability of data' what is meant is that the user can expect to have free access to the usage of data by means of empowerment of the related capability (Yuefa et al., 2009). With an eye on guaranteeing the data confidentiality, integrity, and availability (CIA), the service provider has to provide the minimum capabilities such as a tested encryption schema to guarantee that the shared storage scenario protects the entire data, together with stern access controls to avert the illegal access to the data as well as the scheduled data backup and safe storage of the backup media (Kaufman, 2009). The data security essentially includes the encryption of the data in addition to guaranteeing that suitable stratagems are imposed for the purpose of the data sharing (Hamlen et al., 2010). In the cloud computing, the safety aspect is concerned with two layers in the software stack. The first one is that the workloads of diverse users have to be operated free from one another, in order that a particular malevolent user is disabled from exerting any impact or spying on the workload of another user. Further, each user also has various anxieties regarding the safety and secrecy of his own workload, particularly if it is revealed over the internet such as in the case of a web service or internet application (Christodorescu et al., 2009). Some of the data classification techniques (Pratama et al., 2015b, 2016e) widely used in cloud computing. The objective of data classification is to find out the required level of security for data and to protect data by providing sufficient level of security according to the risk levels of data. General classification techniques are recurrent fuzzy neural network classifier (Pratama et al., 2016b), fuzzy classifier (Pratama et al., 2016a, 2016d; Lughofer and Pratama, 2017; Lughofer and Pratama, 2017; Venkatesan et al., 2016), scaffolding classifier (Pratama et al., 2014; Pratama et al., 2016c), multi label classifier (Venkatesan et al., 2016) and recurrent classifier (Pratama et al., 2015a).

2 Related work

The universal ubiquity of cloud computing is likely to expose the sensitive personal data of the clients to the significant privacy and security challenges. A vital issue for the cloud computing industry is to attain the confidence of the clients by guaranteeing sufficient secrecy and privacy for the sensitive consumer data. A concise assessment of several hi-tech works associated with the safety problems and their solutions in the cloud scenario are beautifully pictured in the following section.

The regulation of the consumer privacy and security together with the challenges thrown by the government enforcement of data safety laws were devised with the national borders in mind. From the standpoint of data secrecy, King and Raja (2012) resourcefully assessed the significant functioning of the regulatory frameworks setup in the Europe and the USA which effectively safeguarded the safety and secrecy of the sensitive consumer data in the cloud. They were successful in making useful suggestions for the regulatory reform with the aim of shielding the sensitive data in the cloud computing scenarios and to eliminate the regulatory challenges which restrict the development of the exciting new industry. A major motive of the reform was to setup a regulatory framework anchored in the confidence of the client that his sensitive personal data is preserved as safe and confidential in the cloud. Their various reforms comprised:

1 The enlargement of the legal definitions of sensitive data which were eligible for sharp data protection.

2 The cut down in the regulatory restrictions which then restricted the EU and US businesses from exploiting the merits of the cloud computing.

Mackay et al. (2012) brilliantly brought to limelight a novel concept for an innovative integrated platform to reinforce the integrity and safety of cloud services and it was applied this in the backdrop of the critical infrastructures to locate the key requisites, components and facets of the relative infrastructure. Further, they were successful in illustrating the method by which the cloud computing and the end-to-end networking could be logically being made sufficient protected to help the critical infra-structure providers. Moreover, they intelligently introduced an open architecture for CI support in clouds and recognised the fundamental modules of a safety ‘toolbox’ that cloud providers were competent to execute and utilise for the simplification of the relative procedure.

Sood (2012) significantly synthesised a novel structure encompassing diverse approaches and specific processes which was capable of effectively shielding the data right from the start to the end, in other words, from the owner to the cloud and ultimately to the user. In the innovative technique, the classification of the data was performed based on the three cryptographic constraints offered by the user such as the confidentiality (C), availability (A) and the integrity (I). The new approach was adopted for the guarding the data employing several measures like the secure socket layer (SSL) 128-bit encryption and was also capable of being enhanced to the 256-bit encryption if necessary, as well as the message authentication code (MAC) which was effectively employed for the purpose of integrity check of data, searchable encryption and segmentation of data into three sections in the cloud for storage. The segmentation of data into three sections effectively ensured the additional defence and easy access to the data.

The modern research enthusiasm in designing the software engineering methods to prop up the techniques is mainly rooted in the cloud, as a large majority of the modern techniques miserably find a waterloo in furnishing a methodical and well thought-out technique which lent a helping hand to the software engineers to detect the safety and secrecy requisites and choose an appropriate cloud service provider anchored in the relative requisites. Mouratidis et al. (2012) were instrumental in bringing to limelight an innovative structure which was able to bridge the resultant gap. Their novel structure has integrated a modelling language and it furnished an ordered procedure which helped the elicitation of safety and secrecy requisites and the choice of a cloud provider as per the satisfiability of the service provider to the relative safety and secrecy requisites.

Ryan (2013) remarkably evaluated the thorny issues in the cloud computing safety. The fact that data was shared with the cloud service provider was recognised as the fundamental scientific issue which separated the cloud computing security from other subjects related to the computing safety. The author was able to appraise certain investigation activities which successfully tackled the central issue of the cloud computing safety such as the probable access by the cloud provider to the data of the customers. He effectively investigated the manner in which the novel solution was competent to effectively function for the running instance. Nevertheless, it was worth remembering that the cloud computing is very diverse, and several instance possessing entirely different traits.

One of the vital safety constraints was the dearth of auditability for several facets of safety in the cloud computing scenario. Rasheed (2013) remarkably dealt with the problem of the cloud computing security auditing from three outlooks such as the user auditing requisites, technological approaches for the (data) security auditing and the existing cloud service provider skills for satisfying the audit requisites. The author skilfully segmented the specific auditing problems into distinctive types like the infrastructure security auditing and data security auditing. Further, it was discovered eventually that in spite of a host of approaches offered for successfully tackling the user auditing concerns in the data auditing domain, and hence the cloud providers invested their attention mainly on the infrastructure security auditing concerns (Lughofer et al., 2015).

Wei et al. (2014) wonderfully launched an innovative privacy cheating deterrent and safe evaluation auditing technique, known as the SecCloud, which was the debutant protocol linking the safe storage and secure evaluation auditing in the cloud and attaining the privacy cheating deterrent by means of the designated verifier signature, batch verification and probabilistic sampling methods. A comprehensive investigation was carried out to achieve an optimal sampling size to considerably cut down the cost. Another key contribution was that they had constructed a practical secure-aware cloud computing test scenario known as the SecHDFS, as a test bed to perform the SecCloud. Moreover, the test outcomes amply illustrated the efficiency and efficacy of the innovative SecCloud (Foster et al., 2008).

3 Problem definition

Cloud computing has produced important attention in both academia and industry, but it's still an evolving paradigm. One of the most vital challenges of the cloud computing is concerned with the data safety. By moving data into the cloud, an organisation is relinquishing custody of that data to the cloud provider. The common problem in existing cloud security and privacy approaches are given below:

- In existing method, we were not able to include large number of factors that have been shown to manipulate the technology. It is only centre of attention on a single level of analysis.
- Cost and effectiveness is the major problem of the existing security and privacy approaches.
- The main problem existing cloud security and privacy approaches is security problem.
- An existing security and privacy computing have one drawback that is the cloud ventures cannot have much incentive to do some sampling if they can improve the efficiency at the same time it will reduce the accuracy.
- The cloud computing is maybe the more cost effective method to use preserve and enhance also it have a possible to break, security issues, cost effective, and inflexibility.

These are the main drawbacks of various existing works, which motivate us to do this research on Security and privacy approaches in cloud computing.

4 Proposed method

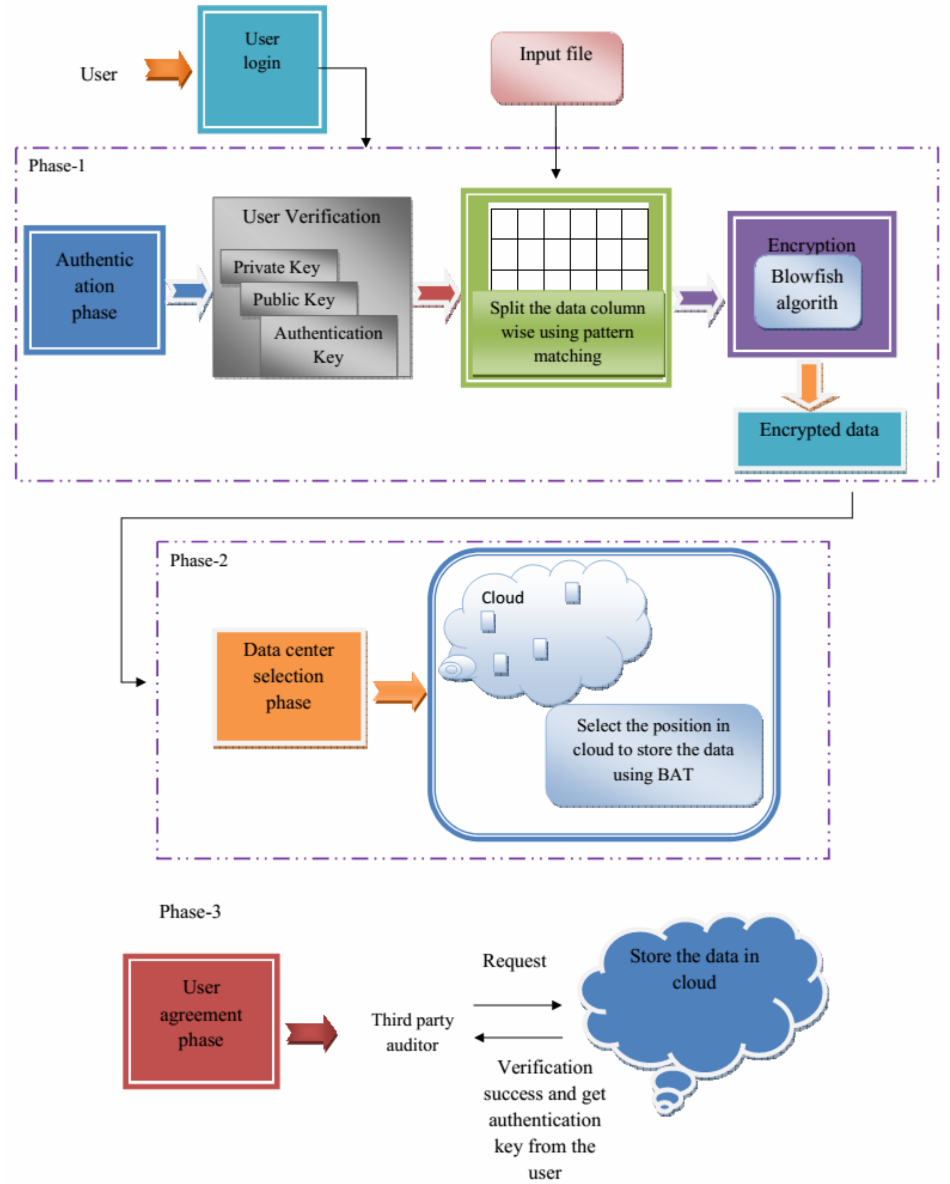
In the cloud system, the data transaction is performed with elevated security. In the document, our objective is to launch an effective method to safeguard the data. In the innovative technique, there are three distinct phases such as:

1 authentication phase

2 cloud data centre selection phase

3 the user related service agreement phase.

Figure 1 The block diagram of the proposed method (see online version for colours)



For accessing the data from the cloud server, it is highly essential to have a safe authentication key. In the initial phase, the authentication task is carried out by means of the blowfish technique. In order to secure the authentication, the proposed method is used to split the input file column wisely by means of pattern matching approach. In the subsequent phase, the cloud data centre is shortlisted to stockpile the data, which is performed with the help of optimisation technique. For the purpose of storing the data in the cloud, we resort to the selection of the optimal position by means of the BAT technique. The final phase is concerned with the authentication of the user related service agreement. The comprehensive function of the novel technique is effectively exhibited in the block diagram appearing in Figure 1.

The protected data transaction in the cloud flows through three phases like the authentication phase, cloud data centre selection phase and the user related service agreement phase. In the authentication phase, the user data is confirmed for the purpose of authentication and subsequently the data is encrypted for the securing procedure, by utilising the blowfish approach. The encrypted data are furnished to the subsequent phase namely the cloud data centre selection phase, in which the positions for stockpiling the data in the cloud are selected by means of the bat technique. In third and last phase, the third party auditor is allowed access to the user data, after getting nod from the user for the eventual authentication of the data. Following the above processes, the secure data transaction is realised in our document. A comprehensive account of the document is elegantly exhibited as follows.

4.1 Phase 1: authentication phase

In the initial phase, a safe data transaction is carried out in the cloud by employing an appropriate technique. The data owner has to invariably encrypt the file for the subsequent storage in the cloud. In the event of a stranger downloading the file, he is capable of going through the document if he is in possession of the key employed to decrypt the encrypted file. This strange predicament is likely to crop up thanks to the amazing advancement of the technology and the heinous efforts of the unscrupulous hackers. It is in successfully outwitting this sophisticated challenge that the significance of the authentication phase plays a decisive role by authenticating the user data in the cloud in the initial stages. In fact, the user furnishes the relevant data like the user name, id and password for generating the database in the cloud. And this is accompanied by the automatic creation of the private and public keys intended for the user. On successful verification, the user takes possession of the authentication key:

a private key

b public key

c authentication key.

Now the user achieves his account in the cloud, it is essential the file containing his data is safely stored in the cloud, after it is encrypted. To improve the authentication the proposed method is split the input data into column wisely by means of pattern matching approach.

4.1.1 Pattern matching approach

The input data is subdivided column wise by employing the pattern matching technique, in which the issue of the pattern matching takes into account a data (D) of length n and a pattern of length m with the intention of subdividing the entire data into the columns (Faust et al., 2013), which are subsequently stockpiled in diverse locations of the cloud, by evaluating the outcomes. In the paper, the pattern matching technique is utilised to split the data from the input file. The process of pattern matching technique is described as below:

1 In the input data, each column is combined with the other columns based on their desire meaning of the word or data.

2 After that, the threshold value is fixed for grouping the data presented in the columns. Based on the threshold value, we have formed the groups like, group 1, group 2, etc.

3 The corresponding data are checked and grouped belongs to their corresponding threshold values of group 1 or group 2.

4 The above steps (1–3) are repeated for grouping the data presented in all columns. The similar way of analysis is used in the paper for splitting the data into columns.

Finally, the column wise splitted data is fed to the encryption process. The proposed method uses the blowfish algorithm for encryption process. The step by step procedure of encryption algorithm is shown in beneath:

a encryption and decryption process

The encryption represents the task of transforming the basic text data into the sophisticated cipher text. Conversely, the decryption is entrusted with the function of transforming the cipher text back to the original plaintext. The encryption process involving titanic amount of data is achieved by means of the symmetric encryption. In the document, the encryption function is performed with the help of the mighty blowfish technique.

4.1.2 Utilising blowfish algorithm for encryption process

The blowfish technique has been effectively and extensively employed for the purpose of achieving the symmetric key cryptography. In the ground-breaking technique, the blowFish approach is elegantly employed for both the encryption and decryption. It encompasses the 64 bit block size and key length from 32 bit to 448 bits. There is the presence of the P-array and four 32 bit S-boxes. The P-array, in turn, comprises 18 of 32 bit sub keys and each S-box is home to 256 entries (Ravali et al., 2014). The blowfish technique flows through two vital processes such as the key expansion and the data encryption. The key expansion is entrusted with the task of effectively carrying out the transformation of the input key (448 bit) into sub key (4168 bytes) arrays. The data encryption employs the 16 round feistel network, with each round endowed with a key dependent permutation and a key dependent substitution. All the functions represent those of the XOR and the additions on 32 bit words in the blowfish technique.

4.1.2.1 Sub keys of blowfish algorithm

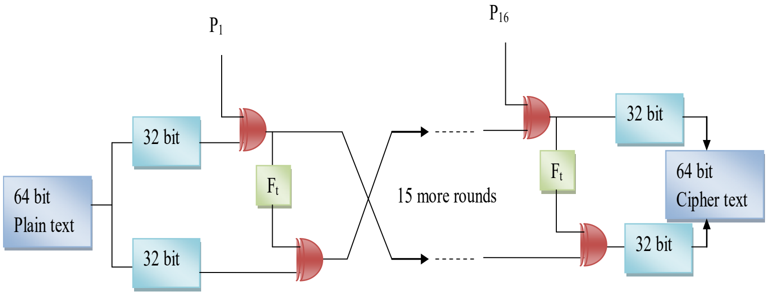
A gigantic number of sub keys are deployed in the novel blowfish technique, and they have to be invariably pre-computed before carrying out the encryption and decryption processes.

- P-array consist of 18 of 32 bit sub keys
- four 32 bit S-box contains 256 entries

a Encryption

The encryption represents the task of transforming basic text into the sophisticated cipher text. In the epoch-making technique, the input used is the 64 bit data, which, in the initial round, is divided into two 32 bit halves, which are labelled as the left halves (LH) and right halves (RH). In the innovative blowfish algorithm, the first 32 bit left halves and the P-array perform the XOR function and the outcomes are furnished to the function (Ft). Subsequently, execute the XOR function for both left halves and the next 32 bit right halves elegantly. This is followed by the swapping of both the outcomes. Thereafter, the rest of the round continues until the attainment of the 16 round. The specific procedure is effectively exhibited in Figure 2.

Figure 2 The detailed encryption process (see online version for colours)



b Process of F_t function

The F_t function deploys four 32 bit S-boxes, with each one encompassing 256 entries. In the novel blowfish technique, the initial 32 bit left halves is subdivided into four 8 bit blocks such as m, n, o and p.

The formula employing the F_t function is elegantly exhibited in the ensuing equation (1).

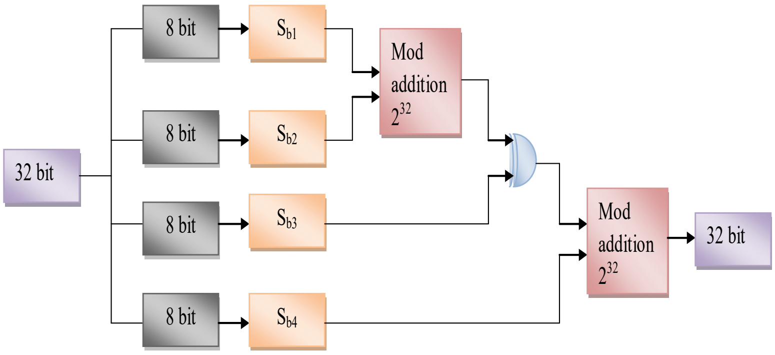
$$F_t\left(L_H\right)=\left(\left(S_{b1,m}+S_{b2,n} \bmod 2^{32}\right)\oplus S_{b3,o}\right)+S_{b4,p} \bmod 2^{32} \tag{1}$$

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

c Decryption

The decryption procedure of the blowfish technique is identical to that of the encryption, though in the former, the P-array is employed in the reverse. 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 public and private keys the file undergoes the function of encryption and gets uploaded into the cloud. In the above task, the client is validated with the username and password, earlier furnisher by him. The modus operandi of the data centre selection phase is brilliantly briefed below.

Figure 3 Working process of ft function (see online version for colours)



4.2 Phase 2: data centre selection phase

In data centre selection phase, the locations are optimally selected for stockpiling the data in the cloud, which is recognised by means of the bat technique (Raghavan et al., 2007). The comprehensive procedure of the innovative bat technique is effectively elaborated in the ensuing section.

4.2.1 Bat algorithm for finding the optimal location to store the data

The innovative bat algorithm represents a meta-heuristic technique, stimulated by the echolocation conduct of the micro-bats. It is effectively employed to find the optimal location in the cloud (Ardagna et al., 2007). Recounted below is a concise account of the novel bat algorithm.

Step by step procedure of bat algorithm

Step 1: At the outset, the bat population si (i=1,2,…,n) is initialised.

Step 2: Thereafter, the pulse frequency (f) and velocity (v) are defined.

Step 3: It is followed by the initialisation of the pulse rate (r) and loudness (L)

Step 4: Now, the fitness is evaluated by means of Equation 2.

$$fitness = maximum\ matched\ data \tag{2}$$

Step 5: Create the new solution by adapting the frequency and updating the velocity with the help of the following Relations.

$$\begin{aligned} f_i &= f_{\min} + (f_{\max} - f_{\min})\gamma \\ v_i^x &= v_i^{x-1} + (s_i^x - s_0) f_i \\ s_{new} &= s_{old} + EL^x \end{aligned} \tag{3}$$

where i = {1,2,…N} N denote the number of bats. E and γ represent an arbitrary number E & $\gamma \in [0, 1]$. S0 symbolises the existing global best location. Lx = <Lix> refers to the average of loudness.

Step 6: If the arbitrary number exceeds the pulse rate

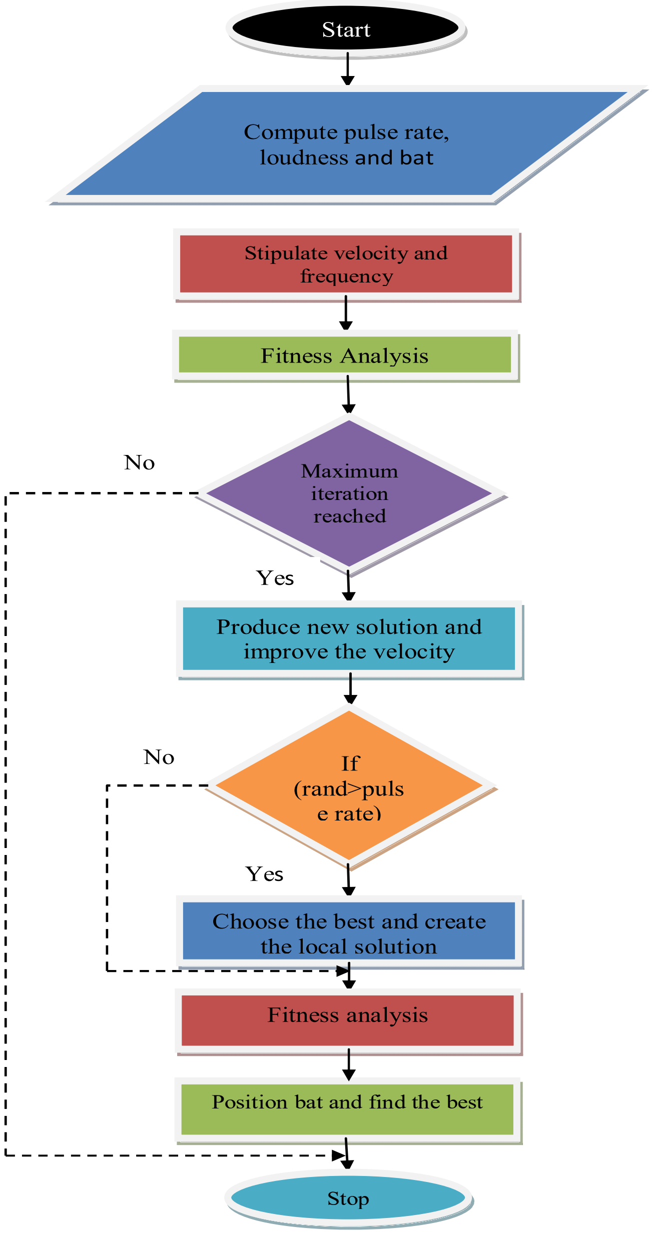
Step 7: Choose the solution from among the best and create a local solution around the best solution by flying arbitrarily

Step 9: Now the fitness is evaluated

Step 10: if (rand<Li and f(si)<f(sn)), Accept new solution by enhancing the pulse rate and reducing the loudness.

Step 11: Step 11: Find out the best location. The flowchart for the novel bat technique is beautifully pictured below.

Figure 4 Flowchart for bat algorithm (see online version for colours)


Start
Compute pulse rate, loudness and bat
Stipulate velocity and frequency
Fitness Analysis
Maximum iteration reached
No
Yes
Produce new solution and improve the velocity
If (rand>puls e rate)
No
Yes
Choose the best and create the local solution
Fitness analysis
Position bat and find the best
Stop

By means of the above-cited procedures, the optimal locations are found out and subsequently phase-3 is performed.

4.3 Phase 3: 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, which is used by the third party auditor for the purpose of scrutiny and subsequent editing of the relevant document? In due course, the third party auditor decrypts the document by making use of the login credentials tendered by the user. In the document, the runtime, memory utilisation and the outlay are evaluated and scaled down for propping the excellence of the new-fangled technique. The ever-cheering outcomes emerge as the convincing credentials for the superlative efficiency in performance of the milestone method, by comparing and contrasting its efficiency with those of the peer competing approaches (SECES, 2008).

5 Results and discussion

This section gives the detailed view of the result that is obtained by our proposed method of secured data transaction. To develop a secure data transactions blowfish algorithm is used in our method. Blowfish algorithm is applied for encryption and decryption process. For selecting the data centre our method use the bat algorithm. The implementation will be done by using cloud sim simulator. The experimental result and the performance of the proposed method are given below in detail.

5.1 Experimental result

The experimental result of the proposed method is shown in below. At first, the user registers their details in the cloud server. The new registration of the user is shown in Figure 5. After the registration, the client generates their own public and private key. The screen shot for the signup process is shown in Figure 6. Then open the login window of the corresponding user.

5.2 Performance analysis

The performance analysis of our method is shown in the below section. Here, Table 1 shows various file size and the corresponding encryption and decryption time. In our method, we take the file size as 5 kb, 10 kb, 15 kb and 20 kb. To encrypt the file contain 5 kb it takes the 25 milliseconds and if the file size vary the time consumption to encrypt the file also vary (Wang et al., 2009).

Figure 5 New registration of the user (see online version for colours)

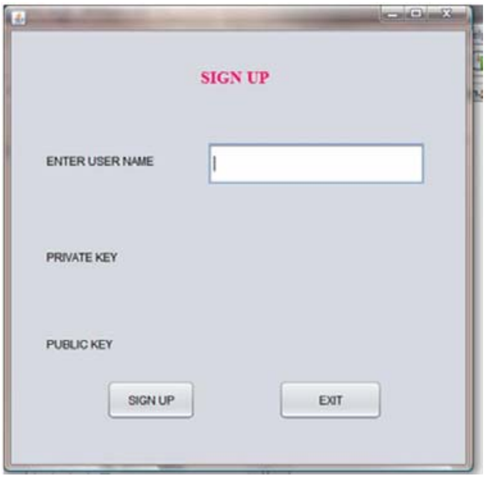
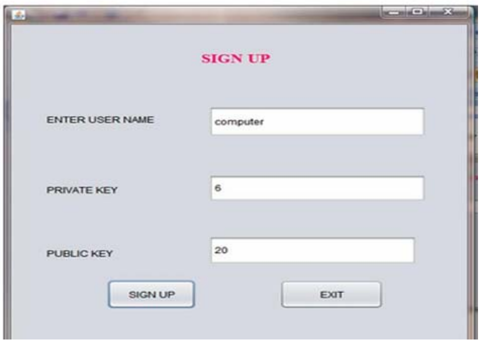


Figure 6 The signup process (see online version for colours)

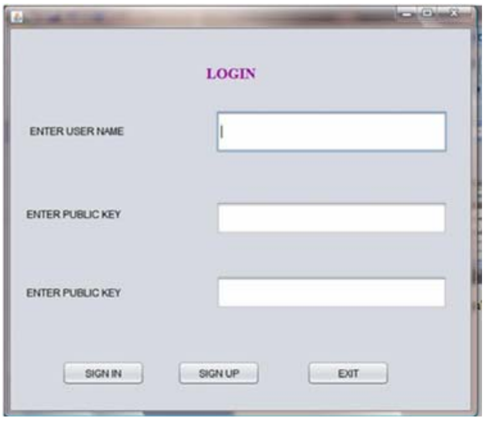


ENTER USER NAME computer

PRIVATE KEY 6

PUBLIC KEY 20

Figure 7 Login window of the corresponding user (see online version for colours)



Figures 8 and 9 represent the graph for encryption and decryption time with various file size. Figure 8 shows the encryption time versus the file size in terms of milliseconds. The time is proportional to that of file size. It is shown in below section.

Table 1 Encryption and decryption time for various file size

File size	*Encryption time*	*Decryption time*
5 kb	25	24
10 kb	40	42
15 kb	51	52
20 kb	63	54

Figure 8 Graph for encryption time vs. file size (see online version for colours)

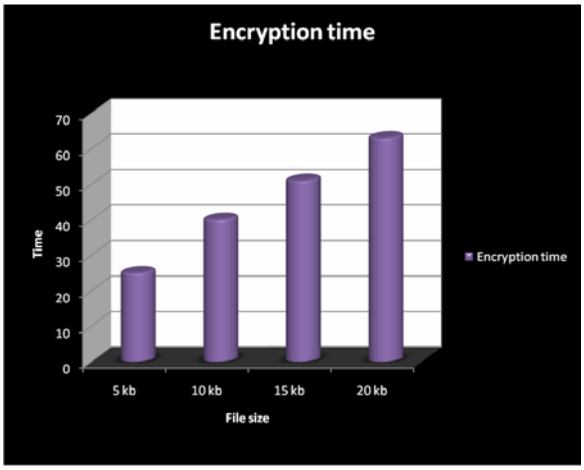
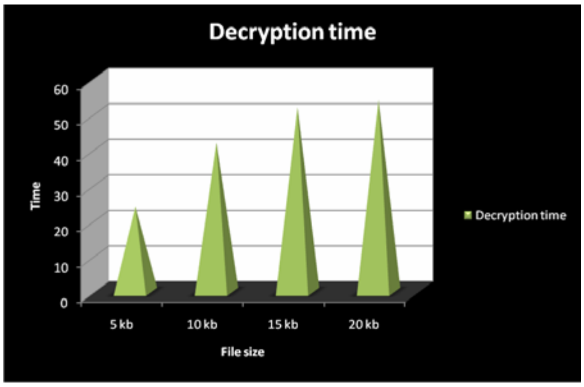


Figure 9 Graph for decryption time vs. file size (see online version for colours)



In our proposed technique, Table 2 shows the overall memory value and execution time of the proposed method. In Table 2, we vary the number of iteration and evaluate the memory value and execution time. Table 2 shows in the below section. Figures 10 and 11 show the graph value for no of iteration with memory value and execution time.

Table 2 Memory and execution time for no. of iteration

No. of iterations	*Memory*	*Time*
10	472976	11
20	563576	17
30	654072	25
40	744512	34
50	834952	40

Figure 10 No. of iteration vs. memory value (see online version for colours)

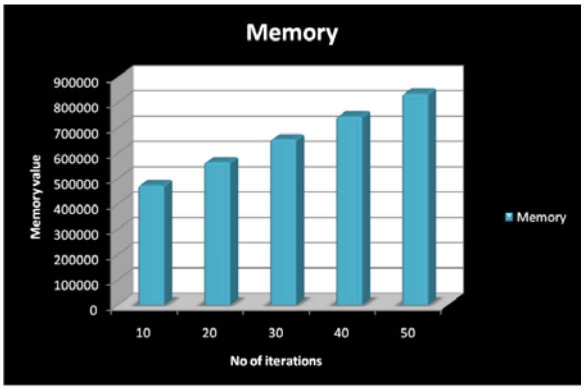
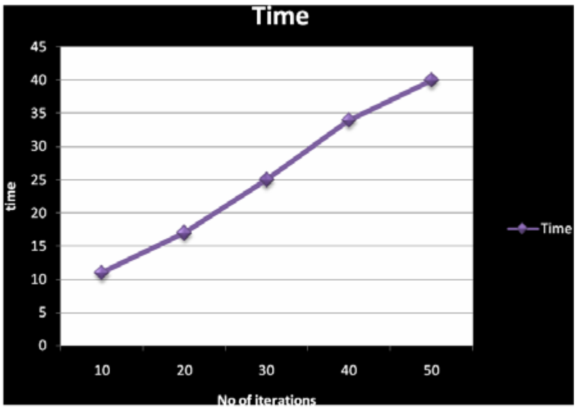


Figure 11 No. of iteration vs. execution time (see online version for colours)



5.3 Comparative analysis

The comparative analysis of our proposed method is compared with the various existing method is tabulated and the result are plotted given below. Table 3 shows the encryption and decryption time of the proposed method is compared with the existing method. For comparing the encryption and decryption time in terms of milliseconds, we have to choose the file size is 5 KB for both proposed and existing technique.

Table 3 Comparative analysis for encryption and decryption time

File size	*Proposed method*		*Existing method (Raghul et al., 2015)*		*Existing method (Vidhate and Shinde 2015)*	
	Encryption time	*Decryption time*	*Encryption time*	*Decryption time*	*Encryption time*	*Decryption time*
5 KB	25	24	1,924	53	64	57

To encrypt the 5 kb file size the proposed method takes 25 ms for encryption and 24 ms for decryption. In existing method (Raghul et al., 2015) uses homomorphic technique for encryption method, this method takes nearly 1,924 ms for encryption and 53 ms for decryption. Existing method (Vidhate and Shinde, 2015) use AES method to encrypt the file, here AES takes 64 ms for encryption and 57 ms for decryption which means our proposed method encrypt and decrypt the 5 kb file with minimum time when compared to the existing method.

6 Conclusions

In this research work, optimal blowfish algorithm based on secured data transaction is proposed. The proposed method is implemented by using CloudSim. At this point, encryption and decryption is carried out with the help of blowfish algorithm and the best possible location of data centre is selected by way of bat algorithm. To prove that the suggested technique yields enhanced results, the performances of the suggested technique is evaluated, investigated, and compared with those of existing systems. From the outcomes of the results, the superior quality of the proposed method is proved and the proposed method demonstrates its efficacy with its presented features and evaluated with the existing technique. In future, the researchers can carry out their research with their individual optimisation practices and can perform improved research.

References

A Platform Computing Whitepaper (2010) 'Enterprise cloud computing: transforming IT', *Platform Computing*, p.6, viewed 13 March.

Ardagna, D. and Pernici, B. (2007) 'Adaptive service composition in flexible processes', *IEEE Trans. on Software Engineering*, Vol. 33, No. 6, pp.369–384.

Buyyaa, R., Yeo, C.S., Venugopal, S., Broberg, J. and Brandic, I. (2009) 'Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility', published in *Journal Future Generation Computer Systems*, June, Vol. 25 No. 6, pp.599–616.

Christodorescu, M., Sailer, R., Schales, D.L., Sgandurra, D. and Zamboni, D. (2009) 'Cloud security is not (just) virtualization security', *Proceeding CCSW '09 Proceedings of the 2009 ACM Workshop on Cloud Computing Security*, pp.97–102.

Faust, S., Hazay, C. and Venturi, D. (2013) 'Outsourced pattern matching', in *Automata, Languages, and Programming*, pp.545–556.

Foster, I., Zhao, Y., Raicu, I. and Lu, S. (2008) 'Cloud computing and grid computing 360-degree compared', *Grid Computing Environments Workshop*, pp.1–10.

Hamlen, K., Kantarcioglu, M., Khan, L. and Thuraisingham, B. (2010) 'Security issues for cloud computing', *International Journal of Information Security and Privacy*, Vol. 4, No. 2, pp.39–51.

Jensen, M., Schwenk, J., Gruschka, N. and Iacono, L.L. (2009) 'On technical security issues in cloud computing', *IEEE International Conference on Cloud Computing*, pp.109–116.

Kaufman, L.M. (2009) 'Data security in the world of cloud computing', *IEEE Security & Privacy*, Vol. 7, No. 4, pp.61–64.

King, N.J. and Raja, V.T. (2012) 'Protecting the privacy and security of sensitive customer data in the cloud', *Journal of Computer Law and Security Review*, June, Vol. 28, No. 3, pp.308–319.

Lughofer, E. and Pratama, M. (2017) 'On-line active learning in data stream regression employing evolving generalized fuzzy models with certainty sampling', *IEEE Transactions on Fuzzy Systems*, online and in-press.

Lughofer, Edwin, Cernuda, C., Kindermann, S. and Pratama, M. (2015) 'Generalized smart evolving fuzzy systems', *Evolving Systems*, Vol. 6, No. 4, pp.269–292.

Mackay, M., Baker, T. and Yasiri, A.A. (2012) 'Security-oriented cloud computing platform for critical infrastructures', *Journal of Computer law and Security Review*, Vol. 28, No. 6, pp.679–686.

Mouratidis, H., Islam, S., Kalloniatis, C. and Gritzalis, S. (2012) 'A framework to support selection of cloud providers based on security and privacy requirements', *The Journal of Systems and Software*, Vol. 86, No. 9, pp.2276–2293.

Pratama, M., Anavatti, S.G. and Lu, J. (2015a) 'Recurrent classifier based on an incremental meta-cognitive-based scaffolding algorithm', *IEEE Transactions on Fuzzy Systems*, Vol. 23, No. 6, pp. 2048-2066.

Pratama, M., Anavatti, S.G., Joo, M. and Lughofer, E.D. (2015b) 'pClass: an effective classifier for streaming examples', *IEEE Transactions on Fuzzy Systems*, Vol. 23, No. 2, pp.369–386.

Pratama, M., Joo, M., Anavatti, S.G., Lughofer, E., Wang, N. and Arifin, I. (2014) 'A ovel meta-cognitive-based scaffolding classifier to sequential non-stationary classification problems', in *Proceedings of the 2014 IEEE Conference on Fuzzy Systems (FUZZ-IEEE)*, pp.369–376.

Pratama, M., Lu, J. and Zhang, G. (2016a) 'Evolving interval type-2 fuzzy classifier', *IEEE Transactions on Fuzzy Systems*, Vol. 24, No. 3, pp.574–589.

Pratama, M., Lu, J., Anavatti, S., Lughofer, E. and Lim, C.P. (2016d) 'An incremental meta-cognitive-based scaffolding fuzzy neural network', *Neurocomputing*, Vol. 171, pp.89–105.

Pratama, M., Lu, J., Lughofer, E., Zhang, G. and Anavatti, S. (2016e) 'pClass+: a novel evolving semi-supervised classifier', *International Journal of Fuzzy Systems*, Vol. 3, No. 19, pp.863–880.

Pratama, M., Lu, J., Lughofer, E., Zhang, G. and Joo, M. (2016b) 'incremental learning of concept drift using evolving type-2 recurrent fuzzy neural network', IEEE *Transactions on Fuzzy Systems*.

Pratama, M., Lu, J., Lughofer, W., Zhang, G. and Anavatti, S. (2016c) 'Scaffolding type-2 classifier for incremental learning under concept drifts', *Neurocomputing*, Vol. 191, pp.304–329.

Raghavan, B., Ramabhadran, S., Yocum, K. and Snoeren, A.C. (2007) 'cloud control with distributed rate limiting', *Proc. 2007 ACM SIGCOMM*, pp.337–348.

Raghul, H., Ramagopal, R.N., Saravanan, B., Guhapriya, T. and Anitha, R. (2015) 'data security in federated cloud environment using homomorphic encryption technique', *International Journal of Emerging Technology and Advanced Engineering*, Vol. 5, No. 4, pp.137–141.

Ramgovind, S., Eloff, M.M. and Smith, E. (2010) 'The management of security in cloud computing', *Information Security for South Africa*, pp.1–7.

Rasheed, H. (2013) 'Data and infrastructure security auditing in cloud computing environments', *International Journal of Information Management*, Vol. 34, No. 3, pp.364–368.

Ravali, S.V.K., Neelima, P., Sruthi, P., Dileep, P.S. and Manasa, B. (2014) 'Implementation of blowfish algorithm for efficient data hiding in audio', the *Journal of Computer Science and Information Technologies*, Vol. 5, No. 1, pp.748–750.

Ryan, M.D. (2013) 'Cloud computing security: the scientific challenge, and a survey of solutions', *The Journal of Systems and Software*, Vol. 86, No. 9, pp.2263–2268.

SECES (2008) *Proc. First International Workshop on Software Engineering for Computational Science and Engineering, in Conjuction with the 30th International Conference on Software Engineering (ICSE2008)*, Leipzig, Germany, May.

Silvestre, J. (1987) 'Economies and diseconomies of scale', *The New Palgrave: A Dictionary of Economics*, Vol. 2, pp.80–84.

Sood, S.K. (2012) 'A combined approach to ensure data security in cloud computing', *Journal of Network and Computer Applications*, Vol. 35, No. 6, pp.1831–1838.

Venkatesan, R., Joo, M., Dave, M., Pratama, M. and Wu, S. (2016) 'A novel online multi-label classifier for high-speed streaming data applications', *Evolving Systems*, pp.1–13.

Vidhate, R. and Shinde, V.D. (2015) 'Secure Role-based access control on encrypted data in cloud storage using raspberry PI', *International Journal of Multidisciplinary Research Development*, Vol. 2, No. 7, pp.20–27.

Wang, C., Wang, I., Ren, K. and Lou, W. (2009) 'Ensuring data storage security in cloud computing', *17th International Workshop on Quality of Service*, pp.1–9.

Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y. and Vasilakos, A.V. (2014) 'Security and privacy for storage and computation in cloud computing', *Journal of Information Sciences*, Vol. 258, pp.371–386.

Yuefa, D., Bo, W., Yaqiang, G., Quan, Z. and Chaojing, T. (2009) 'data security model for cloud computing', *Proceedings of the 2009 International Workshop on Information Security and Application*.