INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Effective Renewal and Signing Method to Achieve Secure Storage and Computation Using Hybrid RSA-MABC Algorithm

Anju Malik[1*], Vinod Kumar Jain[2]

[1]*College of Engg. Roorkee, Uttrakhand, India*
[2]*Devi Ahilya University, Indore and UTU, Dehradun, India*
*Corresponding author's Email: anjumalik0881@gmail.com

Abstract: Cloud providers offer several storage services for their users in efficient manner. Cloud users are allowed to store their data in cloud. The data leakage, lack of proper security control policy, and weakness in the data security are the main worries of the companies. We intended to propose a secure cloud storage system RSA-ABC algorithm for encryption and decryption process. Initially the user will login with the aid of private key and public key. Then send a request to the data base administrator for upload a file in a cloud. In this phase we will give one time password and keys. Then the DBA will verify that data and accept that file and encrypt that file and stored in to the cloud server. If the user want that file means they send a request to DBA continue the same process after they will decrypt the file and send to the user.

Keywords: RSA-ABC; DBA; Encryption; Decryption.

1. Introduction

The cloud computing has emerged as a gifted technique intended to promote the growth of mega-scale, on demand, flexible computing infrastructures [1]. It constitutes one of the most significant and emergent conceptions for both the developers and the users [2]. It elegantly metamorphoses the Internet into a novel computing platform, and represents a business pattern which is competent to attain the services of purchase on-demand and pay-per-use in the network, and has a wide-ranging growth potential [3]. It effectively provides several services which enable a user outsource for carrying out his calculation and thereby save his data to the cloud servers by deploying the Internet [4]. Further, the cloud computing represents an Internet-based pattern for facilitating trouble-free, on-demand network access to a shared collection of configurable computing resources [5]. Moreover, it effectively leads to the decrease in IT expenses and step up the skills and accessibility of the offered services [6]. In the cloud scenario, resources are shared among all the servers, users and individuals. Consequently, the result files or data stored in the cloud are thrown open to all [2].

As a rule, the cloud providers offer three categories of services such as the Software as a Service (SaaS), Platform as a Service (PaaS) and the Infrastructure as a Service (IaaS) [7]. The clouds are competent to furnish various categories of services like the applications (e.g., Google Apps, Microsoft online), infrastructure [8]. The cloud computing is intended for various applications connected with the consumer electronics (CE) virtualization of consumer storage, Cloud TV platforms which furnish access to a host of Web applications like the social networking, user created video games, and all that [9]. The clouds must not be aware of the query but have to competent enough to restore the records which meet with the query [10]. Boundless storage for the clients is one of the vital merits offered by the cloud computing which goes a long way in considerably cutting down the anxieties regarding the quantum of residual memory [11]. The effective search also emerges as a significant challenge in the clouds. Moreover, the user secrecy is highly indispensable to ensure that the cloud or other users are not aware of the identity of the user [8]. Further, safety constitutes one of the major worries for the deployment of cloud computing. Thus, security has become a key issue linked to several facets [12].

As a rule, three safety requisites are taken due care of, which include the secrecy, honesty, and accessibility for a large majority of the Internet service providers and cloud users [13]. The relative safety aspect is segmented into various elements and one of the most significant elements is concerned with the guaranteeing of the user validation procedures and regulation of accesses when the users outsource the sensitive data and share on the public or private cloud servers [11]. The most significant safety needs encompass the user recognition and verification [14]. The verification is intended to examine the identity of the user, to ensure that the person is the same as he claims to be [15]. The verification effectively takes into account the hub of security in the cloud computing [4]. The user verification in the cloud computing scenarios is segmented into two vital procedures as follows. The investigation of the distinctive identifiers of the users in the course of the preliminary registration stage. The user verification and validation of the user legal identities and obtaining their access control privileges for the cloud-based resources and services during the service operation stage [11].

The keywords are forward to the cloud encrypted, and the cloud sends back the outcome unaware of the real keyword for the search. The challenge here is that the data records must have keywords linked with them to facilitate the search. The accurate records are restored only when a search is made with the precise keywords [10]. It has brought a lot of gains particularly in the omnipresent services where anybody is competent to access computing services by means of the Internet [5].

2. Related Work

A number of methods have been launched by several authors related to the Security Authentication in Clouds and certain important related works are detailed below:

Q. Wang *et al* [16] wonderfully addressed the challenge of ensuring the integrity of data storage in the Cloud Computing. Especially, they investigated the process of permitting a third party auditor (TPA), as the representative of the cloud client, to authenticate the integrity of the vibrant data stored in the cloud. Their innovative structure was intentionally devised to achieve those two vital objectives simultaneously keeping the efficiency feature in mind. At the outset, they detected the hassles and probable safety issues of direct extensions with entirely vibrant data updates from the earlier works.

The fingerprint identification emerged as one of the most well-known and efficient techniques for priori authorizing the users and safeguarding the data contents in the course of transmission. J. Yang *et al* [17] was instrumental in envisaging an innovative fingerprint identification approach rooted in a set of assembled invariant moment (geometric moment and Zernike moment) features to facilitate the protected transmission.

S. Sundareswaran *et al* [18] significantly launched a highly decentralized information accountability structure to monitor the authentic utilization of the user data in the cloud. Especially, they envisaged an object-centered technique which facilitated enclosing their logging system with the user data and policies. Their novel method enabled the data owner audit their content and also impose well-built back-end shield if necessary

The safe preservation of log records over elongated duration of time is very vital to the effective functioning of any organization. I. Ray *et al* [19] remarkably introduced a perfect mechanism to safely outsource log records to a cloud provider. They evaluated the current solutions and located the issues in the accessible operating system based logging services like the syslog and practical hassles in certain obtainable secure logging methods.

R. Ranjith *et al* [20] resourcefully launched a safe cloud storage by offering access to the files with the policy based file access employing the Attribute Based Encryption (ABE) technique with the RSA key public -private key amalgamation. The Private Key, in turn, represented the integration of the user credentials so as to ensure superior safety. Further, they envisaged the time based file Revocation approach for file-assured deletion. On expiry of the time limit of the file, the file is mechanically revoked and is not accessible by anyone in future.

G. Yan *et al* [21] excellently envisaged the safety issues of an innovative outlook of the VANETs, which included taking VANETs to clouds. At first, they brought in the safety and confidentiality issues which VC computing networks habitually encountered, in addition to successfully tackling the probable safety solutions. Even though certain solutions were capable of leveraging the modern safety approaches, still certain distinctive issues persisted.

V. Varadharajan *et al* [22] winningly launched a safety design which effectively offered safety as a service pattern which a cloud provider was capable of providing to its manifold tenants and clients of its tenants. Their innovative technique furnished a baseline protection to the provider to safeguard its own cloud infrastructure, in addition to offering flexibility to the tenants to have extra safety functionalities which tailored their safety requisites.

A two-layer encryption based technique was green-signaled by M. Nabeel and E. Bertino [23] so as to order to tackle the issue by delegating a huge quantity of access control enforcement tasks which was viable to the Cloud simultaneously bringing down the data disclosure risks on account of the conspiring Users and Cloud. The data owner effectively performed coarse -grained encryption under their technique where as the cloud carried out a fine- grained encryption on top of the owner encrypted data.

F. Fatemi et *al*. [24] fantastically formulated an effective and scalable user verification method for the cloud computing scenario. A client-based user verification agent was brought in to substantiate the identity of the user in the client-side. Moreover, a cloud-based software-as-a-service application was employed to validate the procedure of authentication for the unregistered tools. There were two separate servers for amassing the authentication and cryptography resources from the major servers to significantly scale down the dependency of user.

Problem Definition

The cloud computing has increased by leaps and bounds, commensurate with the extensive utilization of the Internet services. It elegantly offers easy access to the documents and pictures and media on the cloud storage through the Internet. With the unprecedented advancements in the technology market, the specialists are immensely worried about the zooming safety requirements for the cloud computing. Certain challenges faced by the modern cloud safety techniques are effectively detailed as follows.

- ❖ In the cloud computing, there is a greater hurdle to construct a hybrid technique, because if the providers hold up the service then all the cloud users will be adversely affected because of the relative deficiency.
- ❖ A modern safety and privacy computing [18] namely, the Accountable Map Reduce enables accountability for Map Reduce and furnishes demonstrable proof founded on replication. A vital deficiency is that the cloud vendors do not have any motivation to perform certain sampling. Though they are competent to enhance the efficiency it leads to the decrease in the accuracy simultaneously.
- ❖ In the privacy anxieties, the modern accomplishment permits access to log records which are indirectly recognized by upload-tag values [19].
- ❖ In [20] they have carried out a single authority based attribute based encryption. The demerit of the related approach is the fact it causes a number of erroneous hits in the course of validation.
- ❖ In [19] they have envisaged the safe data storage and access data in the cloud and the deficiency of the technique is that the owner invariably does not possess any authority to manage the data.

3. Objective of the Research

The vital deficiencies of several modern techniques have given us the necessary impetus to carry out the current investigation on the Cloud Security.

- An appropriate cryptography technique is suggested to attain safe data storage and transaction in the cloud computing.
- The data privacy problem faced in the course of the third party auditing cannot be steered clear of completely with the encryption technique, though it may be just converted into the composite key management domain.
- The data safety guaranteed by means of the Privacy-Preserving Public Auditing is colorfully pictured in [25], where, the TPA is elegantly employed to usher in superior levels of effectiveness. Still, the efficacy of their technique in the course of manifold auditing functions is far from satisfactory. Further, it was clearly established that the protection and effectiveness achieved through their work fail miserably, when a wide-ranging exploration is conducted.
- It may not be easily possible for any user to access the entire data of significance from the cloud data center. Because several cloud service providers amass the needed data. Therefore, a gloom of doubt pervades the users, when the data is accessed through the medium of the cloud service providers.

4. Proposed Methodology during the tenure of this Research

The cloud computing constitutes a certain category of the computing which is basically dependent on sharing computing resources moderately having local servers or personal devices to address the applications. In the cloud computing the cloud users are competent to access the services through the internet 24/7 from any nook and corner of the cosmos. The cloud computing services offer incredibly effective facilities which can be quickly enjoyed by various entities just like a shot in the arm for them. Though the upkeep of proper data protection is the fundamental constraint at present, the cloud computing infrastructure is well-endowed with the skills of significantly stepping up the total safety. With an eye on ensuring efficient protected storage and safe calculation, an innovative technique for addressing safety and secrecy facets in the cloud security and privacy is proudly presented in the document. The key target behind the novel method is to bring in an efficient renewal technique and signing approach. At the time of demanding a cloud service, the client has to initially get registered for the same, and the registered data has to be furnished to the system operator, who, in turn, will acknowledge it and part with a security key to him.

In the usual signing procedure, the user signature is utilized. However, in our novel technique, a designated verifier signature is envisaged for the purpose. Here, a novel signing algorithm is introduced for the cloud user, who signs for identification by the cloud server or verifier agency. Subsequently, the user pre-computes the period key. On account of the Bilinear Diffie-Hellman (BDH) problem, the period key is resilient against the ambushes by the unscrupulous assailant. At the end, the user conveys the data and the related signature pairs, which are effectively encrypted by the corresponding session key to the cloud server provider, when the CSP obtains and decrypts the packet. Further, an innovative and safe data transmission is brought in namely, the RSA algorithm with modified Artificial Bee Colony optimization algorithm (MABC), for the relative encryption and decryption procedures, if the encryption key is public and kept confidential. Subsequently, a safe cloud executed protocol is performed for secure auditing. Further, the renewal procedure for download the key is also designed which ensures that on expiry of time prescribed the user is competent to renew the secret key as and when the files are required for renewal. The innovative technique is performed in the Cloud simulator in the working platform of Java software

4.1. Security Issues in Cloud Computing

The cloud computing is home to various applications, platforms and infrastructure modules. Each module elegantly executes diverse functions and provides several products for businesses and individuals across the globe. The business applications encompass the Software as a Service (SaaS), Utility Computing, Web Services, Platform as a Service (PaaS), Managed Service Providers (MSP), Service Commerce and the Internet Integration. In fact, the cloud computing habitually encounters a host of safety problems, as it includes a feast of sophisticated methodologies encompassing the networks, databases, operating systems, virtualization, resource scheduling, transaction administration, load balancing, concurrency management and the memory organization. Hence the safety problems of the captioned techniques are relevant to the cloud computing also. For instance, the network which links the systems in a cloud has to be indispensably safe and mapping the virtual machines to the physical machines has to be performed in a much protected manner. The data safety is concerned with the encryption of the data in addition to seeing to it that fitting stratagem is implement for the data sharing. Recounted below is certain vital safety aspects habitually encountered in the domain of the cloud computing.

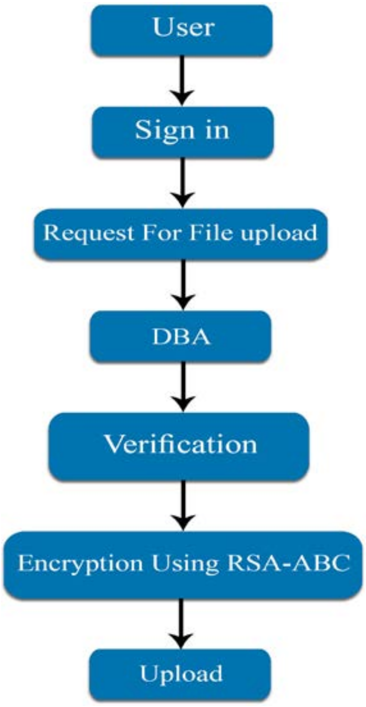


Figure.1 Proposed diagram for Hybrid RSA-MABC

4.1.1. Different models of cloud computing

As a rule, the cloud services may be categorized into three types such as the Software as a Service (SaaS), Platform as a Service (PaaS), and the Infrastructure as a Service (IaaS).

Software-as-a-Service (SaaS): SaaS is defined as the procedure by which the Application Service Provider (ASP) offers diverse software applications over the Internet. With the result, the client is given the facility to shun the setting up and performing the application on his own computer and to steer clear of enormous burden of software preservation, long-lasting functioning, safeguarding and support.

Infrastructure as a Service (IaaS): Infrastructure as a service (IaaS) relates to the sharing of hardware resources for performing services employing the Virtualization technique. Its supreme motive is focused on facilitating the resources like the servers, network and storage further easily available by applications and working mechanisms.

Platform as a Service (PaaS): "PaaS represents the deliverance of a computing platform and solution stack as a service devoid of the software downloads or setting up for the developers, IT managers or end-users. It effectively offers an infrastructure with a superior level of integration so as to perform and evaluate the cloud applications.

Generally, there are four diverse cloud deployment patterns like the Private cloud, Public cloud, Hybrid cloud and the Community cloud, which are beautifully depicted below.

Private Cloud: It may be owned or leased and administered by the organization or a third party and can be located at on-premises or off-premises. It is further costly and protected in relation to the public cloud. Here, there are no supplementary safety rules, legal requisites or bandwidth constraints which are existent in a public cloud scenario. By effectively deploying this type of cloud, the cloud service providers and the clients get optimized regulation of the infrastructure and superior safety.

Public Cloud: Generally, a cloud infrastructure is offered to several clients who is administered by a third party and is located outside the company firewall. A number of enterprises are competent to work on the infrastructure furnished concurrently and the clients are competent to energetically provision the resources. This type of the clouds is entirely hosted and administered by the cloud provider with the full responsibilities of installation, administration, provisioning, and preservation. The clients are levied only for the resources they have utilized, thereby effectively eliminating the under-utilization. As the client have no control over the infrastructure, procedures needing dominant safety and regulatory conformity are not often an excellent option for the public clouds.

Hybrid Cloud: It represents a structure of multiple cloud deployment models which is connected in such a way that data transfer is effectively carried out between them without having any impact on each other. This category of clouds is characteristically generated by the enterprise and management tasks which are split between the enterprise and the cloud provider. In the technique, a company is competent to feature the targets and requisites of the services. The vital deficiency of the hybrid cloud is concerned with the complications in efficiently generating and managing the related solution. Further, it is essential to get the services from diverse quarters and provision them so as to appear that they emanate from a solitary locality. Moreover, the interfaces between the private and public components can make the performance further difficult.

Community Cloud: This type of cloud infrastructure is shared by various entities and backs up a specified community which possesses common interests such as the mission, safety requisites, policy, and conformity obligations. It can be administered by the entities themselves or by a third party and is likely to exist on premise or off premise.

4.2. File uploading Process

At the outset, the client is validated with the username and password, which consists of the private key and public key and thereafter the corresponding keys are furnished to the authentication procedure. The database administrator is entrusted with the task of effectively addressing the related authentication procedure. After completion of authentication procedure, the user is issued a one-time password and key. Then a file is l uploaded with the assistance of the RSA technique, followed by the decryption of the file by means of the ABC technique. Thus by means of the relative decryption procedure, the file is easily uploaded to a specific node. In the current investigation, there are four options such as 'view your files', 'view other files', 'message from DBA' and 'get space' which are detailed as follows.

View your files: This option allows the user to view his files.

View other files: By using this option, it is easy to view other files. For the purpose, a request has to be preferred with the DBA, which thereafter examines and issues the necessary approval to view other files.

Message from DBA: This procedure is carried out for the purpose of safety. The DBA examines the user details and issues an approval to the user to the files.

Get Space: This option is employed for the space allocation. To enable the uploading of a file, sufficient space is allotted to upload the file. If additional space is required, additional space is allotted by splitting.

4.3. RSA Algorithm for Encryption

The RSA has emerged as a highly utilized Public-Key technique. The RSA is the abbreviation for Ron Rivest, Adi Shamir and Len Adleman, who initially publicly launched it in the year 1977. In the current investigation, the RSA algorithm is elegantly employed to encrypt the data to furnish security in order that only the appropriate user is competent to access it. In the following section, the RSA algorithm is discussed in detail.

The RSA technique proceeds through three fundamental phases as shown below.

1. The Key Generation
2. The Encryption
3. The Decryption

The most extensively employed Public Key technique is known as the RSA, which derives its name from its inventors Rivest, Shamir, and Adelman of the MIT. The RSA represents fundamentally an asymmetric encryption/decryption technique. The Public key distributed to all the clients through which they are competent to encrypt the message and private key which is employed for the purpose of decryption is kept confidential and is not disclosed to all. It is invariably dependent on the exponentiation in a restricted field over integers modulo a prime number.

The RSA effectively employs the Euler's Theorem: $aa\emptyset$ (nn) mod (n) = 1 where gcd (a,n) =1. In the RSA it is essential, at the outset, to evaluate n = p.q in such a manner that $\emptyset$ (nn) = (p-1)(q-1) to carefully chose e and d are selected with due care as the inverses mod ø(n). For the purpose of encryption of a message M, it is necessary to attain the public key of the recipient Pu = $\{nn, ee\}$ for computing the cipher: C = $MMee$mod (n), where 0≤M<n. It is significant to note that the message M has to be lesser than the modulus n. identically, for the purpose of decryption the recipient effectively employs his private key Pr = $\{nn, dd\}$ and calculates: M = $CCdd$mod (n).

Encryption: The encryption represents the procedure of transforming the original plain text (data) into the cipher text (data).

Steps:

1. The cloud service provider has to furnish or hand on the Public- Key (n, e) to the user who intends to store the data with him.
2. At this juncture, the user data is mapped to an integer by effectively employing an approved reversible protocol termed as the padding scheme.
3. The data is encrypted and the consequential cipher text (data) C is represented as: C = me (mod n).
4. The corresponding cipher text or encrypted data is now stockpiled with the Cloud service provider.

4.4. ABC Algorithm for Decryption

- **Producer performance**

In the course of performance of the ABC technique, the action of the producer Z_p at 's' iteration is represented below.

(i) The producer carries out the scanning function at zero degree.

$$Z_z = Z_p^s + \varepsilon_1 d_{\max} L_p^s\left(\Psi^s\right) \qquad (1)$$

(ii) The producer carries out the scanning function at the right hand side hypercube

$$Z_r = Z_p^s + \varepsilon_1 d_{\max} L_p^s\left(\Psi^s + \varepsilon_2 \,{}^{\Phi_{\max}}\!/_{2}\right) \qquad (2)$$

(iii) The producer executes the scanning task at the left hand side hypercube

$$Z_l = Z_p^s + \varepsilon_1 d_{\max} L_p^s\left(\Psi^s - \varepsilon_2 \,{}^{\Phi_{\max}}\!/_{2}\right) \qquad (3)$$

Where, ε_1 represents a usually disseminated arbitrary number with zero mean and unity standard deviation and ε_2 indicates the homogeneously distributed arbitrary sequence which assumes values in the range of 0 and 1.

The maximum search angle $\Phi_{\max}$ is illustrated by means of Equation 4 shown as follows.

$$\Phi_{\max} = \frac{\pi}{c^2} \qquad (4)$$

Now, the constant *c* is illustrated as per the following Equation 5

$$C = round(\sqrt{n+1}) \qquad (5)$$

Where, n represents the dimension of the search space.

$$\therefore \Phi_{\max} = \frac{\pi}{n+1} \qquad (6)$$

The evaluation of maximum search distance d_{max} is carried out by means of Equation 7 shown below.

$$d_{\max} = \left\| d_U - d_L \right\|$$

$$d_{\max} = \sqrt{\sum_{i=1}^{n}(d_{Ui} - d_{Li})^2} \qquad (7)$$

Where, d_{Ui} and d_{Li} illustrate the upper and lower limits of *i*th dimension, correspondingly.

The best location consisting of the most advantage resource is attained with the help of equations (9), (10) and (11). The present best location assumes a new best location, if its resource is found to be inferior to that in the new location. Otherwise, the producer preserves its location and turns its head in accordance with the head angle direction which is randomly created by means of the following Equation (16).

$$\Psi^{s+1} = \Psi^{s} + \varepsilon_2 \tau_{\max} \qquad (8)$$

Where, τ_{max} illustrates the maximum turning angle which is effectively evaluated by means of Equation 9 shown below.

$$\tau_{\max} = \frac{\Phi_{\max}}{2} \qquad (9)$$

When the producer finds it very difficult to spot a superior location even after the conclusion of *m* iterations, its head begins to regain its initial location as expressed in the following equation (11).

$$\Psi^{s+c} = \Psi^{s} \qquad (11)$$

- **Scrounger performance**

In all the iterations, many members with the exception of the producer are selected and labelled as the scroungers. The scrounging behavior of the habitually includes the area copying task. In the course of the *s*th iteration, the function of area copying which the *i*th scrounger carries out may be shaped as a movement to arrive at the producer in an intimate manner, which is illustrated by means of the following Equation 19.

$$Z^{s+1} = Z_i^{s} + \varepsilon_3 o(Z_p^{s} - Z_i^{s}) \qquad (12)$$

Where, o specifies the Hadamard product which evaluates the product of the two vectors in an entry-wise manner and ε_3 denotes a uniform random sequence lying in the interval of (0, 1). The *i*th scrounger continues its searching activity to make a choice of the better occasion for linking. The designing of the scrounging action involves the turning of the head in the ith scrounger to a novel and arbitrarily generated angle as illustrated in equation (16).

- **Ranger performance**

The rangers stay behind as the residual members of the group, which are relocated from their existing position. They are also capable of effectively locating the resources by means of arbitrary walks or an orchestrated investigation process. The arbitrary walks are desired in cases, where the resources are located for the purpose of dissemination. The head angle and the distance related to the ranger are produced in an arbitrary manner. As a substitute for the ranger performance an innovative Adaptive genetic algorithm is elegantly launched.

5. Results and Discussion

The innovative cloud data security with the aid of RSA and AANN algorithm is performed in the working platform of Java with cloud sim. The time and memory values are also estimated and its average values are contrasted with that of the current method. The table appearing below illustrates the file size value of our proposed study. Table 1th reveals the time for encryption and decryption for each file in kb. To finish each file, the innovative techniques taken size is given in the table. The corresponding time taken for finishing the encryption and decryption process in every file is explained. Time taken for encryption process in the 1th file is 156 and decryptionn time is 163. In the time taken for encryption and decryption process in the 2th file is 213 and 198. In the time taken for encryption and decryption process in 3th file is 265 and 241. In the time taken for encryption and decryption process in 4th file is 368 and 317.

Table 1. No of time taken for the Encryption and Decryption for our proposed method

File size	Encryption time	Decryption time
10 kb	156	163
20 kb	213	198
30 kb	265	241
40 kb	368	317

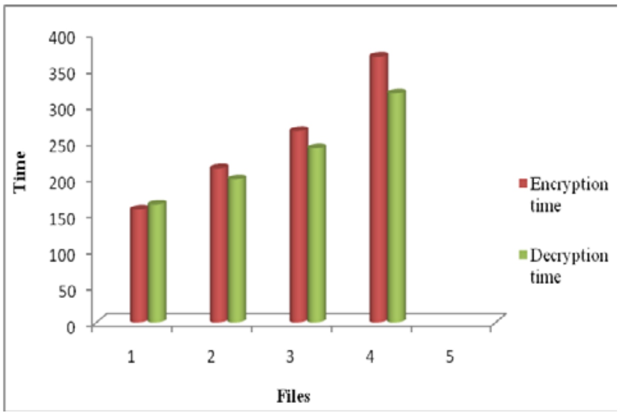


Figure.2 Encryption and Decryption Time taken for our proposed Method

Table 2 reveals the throughput value for each file. To finish each file, the innovative technique taken throughput value is given in the table. The corresponding value for finishing the uploading and downloading in the time taken for 1th file is 1687 and 1589. The novel approach finishes the 2th file is 1842 and 1941. The novel approach finishes the 3th file is 2007 for file uploading 2237 for file downloading. The novel approach finishes the 4th file is 2415 for uploading and 2574 for downloading. The graphical illustration is exhibited in Figure.6.

To finish each file storage, the innovative technique taken memory is given in the table. The corresponding value for finishing the 1th file for memory space is 538741 and the file size is 10 kb. The value for finishing the 2th file for memory space is 687412 and the file size is 3754. The value for finishing the 3th file for memory space is 745854 and the file size is 4369. The value for finishing the 4th file for memory space is 846511 and the file size is 4981. The value for finishing the 5th file for memory space is 964745 and the file size is 5631. The graphical illustration is exhibited in Figure.4.

Table 2. No of time taken for the uploading and Downloading for our proposed method

File size	Uploading time	Downloading time
10 kb	1687	1589
20 kb	1842	1941
30 kb	2007	2237
40 kb	2415	2574

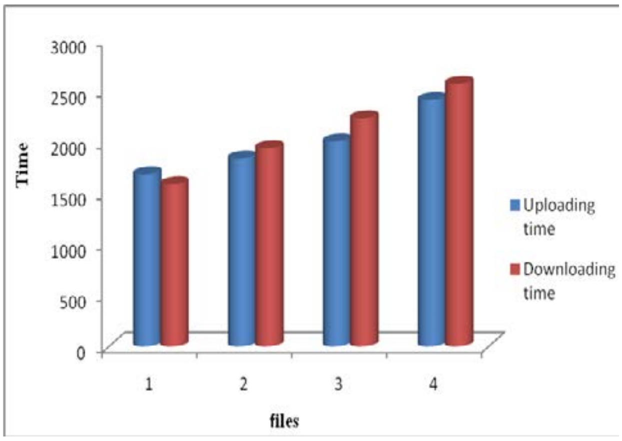


Figure.3 Uploading and Downloading Time taken for our proposed Method

Table 3. No of memory space taken for file storage

No of Iterations	Memory	File size
10	538741	10 kb
20	687412	20 kb
30	745854	30 kb
40	846511	40 kb
50	964745	50 kb

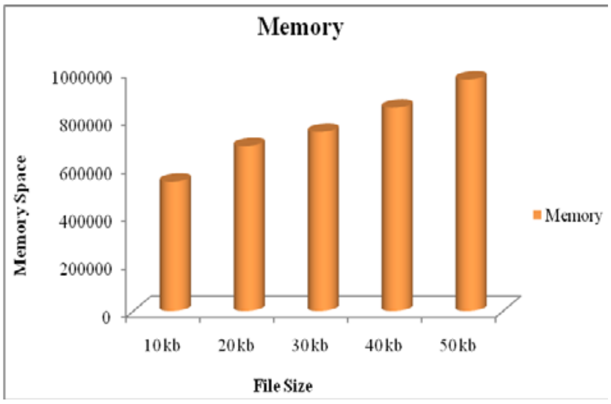


Figure.4 Encryption and Decryption Time taken for our proposed Method

Table 4. Encryption time for our proposed and existing method

Files	Existing Method	Proposed Method
10 kb	250	156
20 kb	350	213
30 kb	400	265
40 kb	500	368

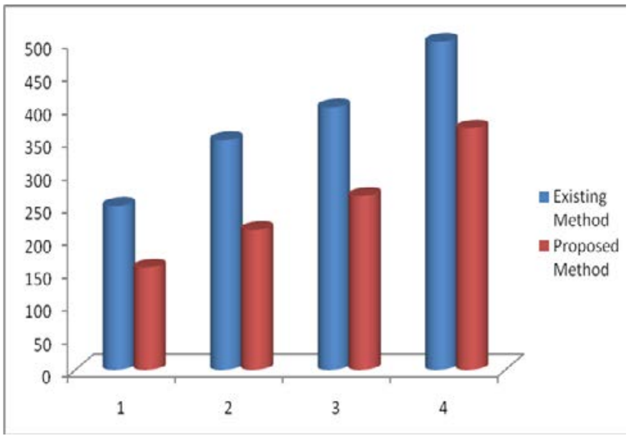


Figure.5 illustrates the graphical representation of comparative analysis. It is shown in below,

5.1. Comparative Analysis

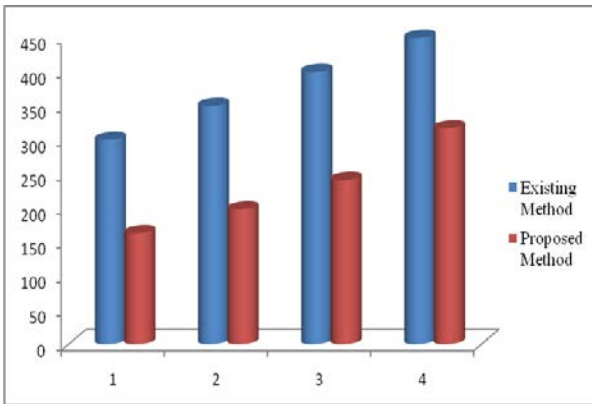
Here the existing works are compared with our proposed work, in order to prove the proposed work is better one. For this existing method is taken to compare the result with our method RSA-ABC. The following table is shown the comparative result. The graphical representation of comparative analysis is shown in figure.5.

From our results of comparison, we can say that our proposed work rescues the encryption time. The existing work 10KB file completes the encryption withnin the time 250 ms, our proposed RSA-ABC takes minimum encryption time as 156. In the second file if the existing method gives 350 ms to complete the encryption process in the file of 20kb but in our proposed method gives 213 ms. In the third file if the existing method gives 400 ms to complete the encryption process in the file of 30kb but in our proposed method gives 265 ms. In the fourth file if the existing method gives 500 ms to complete the encryption process in the file of 40kb but in our proposed method gives 368 ms. From these existing works, we can say that our proposed reduces the encryption time when compared to the existing method. It is clear that the total computation time for encryption of our proposed RSA-ABC is less than that of ordinary RSA. From the figure 5 it is observed that our proposed method had shown a great performance.

Table 5. Decryption time for our proposed and existing method

Files	Existing Method	Proposed Method
10 kb	300	163
20 kb	350	198
30 kb	400	241
40 kb	450	317

Here Figure.6 illustrates the graphical representation of comparative analysis. It is shown in below



From our results of comparison, we can say that our proposed work rescues the decryption time. The existing work 10KB file completes the encryption withnin the time 300 ms, our proposed RSA-ABC takes minimum encryption time as 163. In the second file if the existing method gives 350 ms to complete the encryption process in the file of 20kb but in our proposed method gives 198 ms. In the third file if the existing method gives 400 ms to complete the encryption process in the file of 30kb but in our proposed method gives 241 ms. In the fourth file if the existing method gives 450 ms to complete the encryption process in the file of 40kb but in our proposed method gives 317 ms. It is clear that the total computation time for decryption of our proposed RSA-ABC is less than that of ordinary RSA. From the figure 5 it is observed that our proposed method had shown a great performance. When we compared to the existing method. We can say that our proposed reduces the encryption time

6. Conclusion

In this secure data cloud data storage are proposed at the outset with the aid if RSA-ABC algorithm for encryption and decryption process. In cloud servers, processors are more vulnerable to soft errors caused by either on-purpose attack or system mistakes with the continuous operations. The encryption time of the authors have systematically studied for security and privacy issues in cloud computing based on RSA-ABC algorithm. Our proposed secure cloud storage system RSA algorithm for encryption and the ABC algorithm for decryption process. We have identified the most illustrative security/privacy attributes (e.g., integrity, confidentiality, privacy-preservability, availability, and accountability), as well as discussing the vulnerabilities, which may be exploited by adversaries in order to perform various attacks. We believe this review will help shape the future research directions in the areas of cloud security and privacy.

References

[1] R. Piplode and U. K. Singh, "An Overview and Study of Security Issues & Challenges in Cloud Computing", *IEEE International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 2, No. 9, pp. 115-120, Sep 2012.

[2] K. W. Nafi, T. S. Kar, S. A. He and Dr. M. M. A Hashem, "A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture", *In proceeding of IEEE International Journal of Advanced Computer Science Applications*, Vol. 3, No. 10, pp. 181-186, 2012.

[3] X. Tan and B. Ai, "The Issues of Cloud Computing Security in High-speed Railway", *In proceeding of IEEE International Conference on Electronic & Mechanical Engineering and Information Technology*, Vol. 8, pp. 4358-4363, Aug 2011.

[4] A. A. Yassin, H. Jin, A. Ibrahim and D. Zou, "Anonymous Password Authentication Scheme by Using Digital Signature and Fingerprint in Cloud Computing", *In proceeding of IEEE International Conference on Cloud and Green Computing*, pp. 282-289, Nov 2012.

[5] R. K. Banyal, P. Jain and V. K. Jain, "Multi-factor Authentication Framework for Cloud Computing", *In*

proceeding of IEEE International Conference on Computational Intelligence Modelling and Simulation, pp. 105-110, Sept 2013.

[6] A. Behl and K. Behl, "An Analysis of Cloud Computing Security Issues", *In proceeding of IEEE International Conference on Information and Communication Technologies*, pp. 109-114, Oct 2012.

[7] R. P. Padhy, M. R. Patra and S. C. Satapathy, "Cloud Computing: Security Issues and Research Challenges", *IEEE International Journal of Computer Science and Information Technology & Security*, Vol. 1, No. 2, pp. 136-146, Dec 2011.

[8] S. Ruj, M. Stojmenovic and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds", *In proceeding of IEEE International Symposium on Cluster, Cloud and Grid Computing*, pp. 556-563, May 2012.

[9] R. Sánchez, F. Almenares, P. Arias, D. D. Sánchez and A. Marin, "Enhancing Privacy and Dynamic Federation in IDM for Consumer Cloud Computing", *IEEE Transactions on Consumer Electronics*, Vol. 58, No. 1, pp. 95-103, Feb 2012.

[10] S. Ruj, M. Stojmenovic and A. Nayak, "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds", *IEEE Transaction on Parallel and Distributed Systems*, Vol. 25, No. 2, pp. 384-394, Feb 2014.

[11] F. F. Moghaddam, S. G. Moghaddam, S. Rouzbeh, S. K. Araghi, N. M. Alibeigi and S. D. Varnosfaderani, "A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments", *In proceeding of IEEE Region of Symposium*, pp. 508-513, April 2014.

[12] J. Chen, X. Wu, S. Zhang, W. Zhang and Y. Niu, "A Decentralized Approach for Implementing Identity Management in Cloud Computing", *In proceeding of IEEE International Conference on Cloud and Green Computing*, pp. 770-776, Nov 2012.

[13] F. Zhao, C. Li and C. F. Liu, "A cloud computing security solution based on fully homomorphic encryption*", In proceeding of IEEE International Conference on Advanced Communication Technology*, pp. 485-488, Feb 2014.

[14] B. Zwattendorfer and A. Tauber, "Secure Cloud Authentication Using Eids", *In proceeding of IEEE International Conference on Cloud Computing and Intelligent Systems*, Vol. 1, pp. 397-401, Nov 2012.

[15] A. H. M. Emam, "Additional Authentication and Authorization using Registered Email-ID for Cloud Computing", *IEEE International Journal of Soft Computing and Engineering*, Vol. 3, No. 2, pp. 110-113, May 2013.

[16] Q. Wang, C. Wang, K. Ren, W. Lou and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", *IEEE Transactions on Parallel and Disributed Systems*, Vol. 22, No. 5, pp. 847-859, May 2011.

[17] J. Yang, N. Xiong, A. V. Vasilakos, Z. Fang, D. Park, X. Xu, S. Yoon, S. Xie, and Y. Yang, "A Fingerprint Recognition Scheme Based on Assembling Invariant Moments for Cloud Computing Communications", IEEE Systems Journal, Vol. 5, No. 4, pp. 574-583, Dec 2011.

[18] S. Sundareswaran, A. C. Squicciarini and D. Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud", *IEEE Transactions on Dependable and Secure Computing*, Vol. 9, No. 4, pp. 556-568, July 2012.

[19] I. Ray, K. Belyaev, M. Strizhov, D. Mulamba, and M. Rajaram, "Secure Logging As a Service—Delegating Log Management to the Cloud", *In proceeding of IEEE Systems Journal*, Vol. 7, No. 2, pp. 323-334, Jun 2013.

[20] R. Ranjith and D. Kayathri Devi, "Secure Cloud Storage using Decentralized Access Control with Anonymous Authentication", *IEEE International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 2, No. 11, pp.4262-4266, Nov 2013.

[21] G. Yan, D. Wen, S. Olariu, and M. C. Weigle, "Security Challenges in Vehicular Cloud Computing", *IEEE Transactions on Intelligent Transportation Systems*, Vol. 14, No. 1, pp. 284-294, Mar 2013.

[22] V. Varadharajan and U. Tupakula, "Security as a Service Model for Cloud Environment", *IEEE Transactions on Network and Service Management*, Vol. 11, No. 1, pp. 60-75, Mar 2014.

[23] M. Nabeel and E. Bertino, "Privacy Preserving Delegated Access Control in Public Clouds", *IEEE Transaction on Knowledge and Data Engineering*, Vol. 26, No. 9, pp. 2268-2280, Sep 2014.

[24]F. F. Moghaddam, S. G. Moghaddam, S. Rouzbeh, S. K. Araghi, N. M. Alibeigi, and S. D. Varnosfaderani, "A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments", *IEEE symposium*, *Kuala Lumpur*, Malaysia, pp. 508-513, 2014.

[25] C. Wang, S. S. M. Chow, and Q. Wang, "Privacy-Preserving Public Auditing for Secure Cloud Storage", *In the Proceeding of IEEE Transaction on Computers*, Vol. 62, No. 2, pp. 362-375, Feb 2013.