OPTIMAL RSA BASED COST EFFECTIVE OFFLOADING SCHEME IN MOBILE CLOUD COMPUTING

M. S. Premalatha
Research Scholar, Manonmanium Sundaranar University, Abishekapatti, Thirunelveli-12, Tamil Nadu, India.
premalatha_ms@yahoo.co.in

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

ABSTRACT

In the current scenario, there is an immense use of smartphones by the mobile users. There is an increase of problems due to offloading of mobile applications to cloud resource. Limited battery life, less processing speed and low storage capacity of smartphone have various limitations on applications and codes and offloading is the process to overcome these issues by applying mobile to cloud offloading. Due to this the efficiency and performance of the mobile devices are improved. The mobile applications are processed locally on mobile devices or the processing time and the energy of mobile devices are saved by offloading to the cloud servers. Therefore, in this article, security and privacy for the user data to be offloaded are provided through a proposed algorithm named as RSA-ABC. The private key algorithm of RSA is used to obtain an encrypted data that provides security and cost-efficiency for offloading in cloud computing. The Artificial Bee Colony (ABC) algorithm is used to receive the decrypted data. The encryption and decryption process has to be performed properly so that the attacker finds it difficult to obtain the secret data. This paper provides enhancing the security in computation offloading in mobile cloud computing using the RSA-ABC algorithm.

Keywords: - RSA-ABC, mobile cloud computing, computation offloading, encryption, decryption, security

1. INTRODUCTION

Nowadays, the most popular network is social network in both mobile and internet domains. The internet is used in the home, work and public places or self-organizations to communicate with each other or to perform any other social activities through the personal devices such as mobile devices, laptops, tablets and PDAs [1]. Pervasive Social Networking (PSN) is one of the social networking that is utilized at any time and anywhere in a pervasive manner. Based on the connectivity of the internet, mobile networks and ad hoc networks, the PSN support current and online social proceedings [2]. Mobile data offloading is also called mobile cellular traffic offloading. This is beneficial for the communications of complementary networks to transfer the mobile data traffic over the cellular networks [3]. The offloading solution, for offloading mobile traffic for sharing among people, has high potential to significantly reduce the cellular traffic load [4]. The offloading process of cloud computing has some benefits such as execution of code for client applications, minimum delay communications and excellent QoS. Variety of solutions are available for code offloading where extra resources are encouraged to obtain such as power,

memory and high capacity for computations [6]. In pervasive and current manner PSN is able to receive useful environmental information. This type of social network gives a better experience for mobile users [9].

Pervasive technology provides information about the creation of transparent services and empowerment services [5]. Its ablility to perform at any time and anywhere gives the social networking platform to adopt the needs of social communication.This is not only for the socially connected people but also form a social network for instantly connected physical strangers in the vicinity. PSN is very difficult for accessing internet online social networking but for mobile users, it is valuable [7]. The determination of social computing is critical to the interior design of an open social networking. Pervasive computing is clearly used for the real applications of physical and virtual lines blurring between them, determine the connection highness among the people mobility on time. Online social pervasively acceptable community applications are Foursquare, Gowalla and Facebook platforms. They are providing a large communication network for realtime and non-realtime applications. Moreover, mobile or pervasiveness are received from social computing. Thus the creation of social computing is a process [8]. The major benefits of pervasive computing are the generation of mobile devices with more comfortable, digital interior designs with capable to transfer any type of information within the scenarios [10].

2. LITERATURE SURVEY

Mobile system capabilities are increased in mobile cloud computing based on the popular offloading techniques. Some special types of timing attack is unsafe for offloading since requires more time for transmission and gathering. Due to that the **Tianhui Meng** *et al*. [11] have proposed offloading for mobile cloud computing with security and minimum cost which optimizes the performance and security tradeoff of the system. In their work they have some balancing issues during numerical analysis which was addressed by applying a Markov-chain and queuing model with continuous time. These two models were used for security and performance attributes. The hybrid Continuous-time Markov chain was represented as the evolution of condition model. These indicate the characters of the systems established on particular hit and systems structure. It depended on definite safety constraints and job operation processing and the offloading decision was showed by queuing open model. By using that, mobile devices were used to process the job either locally or offloaded. In cloud computing, the offloading safety balancing was enhanced by applying safety and minimal cost offloading method.

Bruno Guazzelli Batista *et al*. [12] have discussed the performance and security of cloud computing based on a QoS-driven approach. In the system, security techniques and methodologies have main influences on the performances since security and performances were two quantities. The two quantities were inversely proportional to each other. Due to this, the computing infrastructure was failed efficiently by the service provider. The interest of

performances neither does nor requires quality through the users, safety and services, numerical assets were utilized effectively. The QoS approach needs numerical assets neither were nor approved for the cloud. This work was addressing a QoS approach in cloud scenario that regularly place on the numerical operations. In that various safety systems were occupied. Another optimization algorithm should be established for these because their approach was unfit for optimization.

Vishal Sharma *et al*. [13] have discussed the computational offloading in pervasive online social networks. The author introduces a common belief executive scheme for pervasive online social networks. This was used for clients to associate hybrid usages in common platform. Trust management framework is able to create maximum assurance values and minimum monitoring cost. It was interacting with various drivers, common performance workers and gateway utilizations with a large number of users and also it was important for providing a trustworthy environment. The consistent, safe and illustrated congruence's were generated information gather and information creators from the trustworthy environment. The author mainly concentrated on minimizing the monitoring cost with trusted users and un-trusted users. They also introduced another approach called Flexible Mixture Model (FMM) used for the process of numerical offloading to minimizing extra usage of constraints across a server in osmotic computing. It has an ability to provide ratings of user effectively with a maximum of low errors in ±2% of range.

Vaishali Y. Baviskar *et al*. [14] have discussed energy-efficient offloading based on the cloud. The author introduced an offloading method for a mobile cloud system using minimum energy. Minimization of energy and maximizing the applications in mobile devices are main challenging problems in a mobile cloud environment. The author mainly focused on energy consumption reduction when displaying a video stream. Preserving of energy is referred to as dual backlight scaling performance. These can limit the usage of energy during the exposure of videos in mobile devices. Finally, they have enhanced their method with minimum constraint energy and enhanced the performance of cloud resources.

Khadija Akherf *et al*. [15] have discussed issues and challenges of computation offloading. In this article, the author addresses the recent offloading structures and numerical offloading methods. Moreover, explains how the capabilities of mobile devices are extended by integrating Mobile computing and Cloud computing through offloading techniques and analyses the various problems in current offloading frameworks. To achieve efficiency various offloading approaches were used that are based on frameworks. Computing resources and services were provided by Cloud computing. It was called as to order arrangement anywhere else to process user's numerical assets. The recent offloading structures deal with many problems and threats for which elevating and executing new structure is required.

3. PROBLEM DEFINITION

Mobile devices have become an essential thing in the world. Normally, it can be used for watching videos, playing games, social networking and other applications. Due to the growth of mobile devices, cloud servers are widely used in mobile computing. The major technique of cloud computing is offloading that enhances the capacity of mobile devices. Based on this offloading technique, the capacity of mobile devices are increased with the integration of mobile computing and cloud computing. The drastic computation application components are transferred to a remote server by applying a task of computation offloading. In this article, many approaches are proposed based on the computation offloading frameworks for the mobile device applications.

- Diversion is the one of the major issues of the current computation offloading frameworks and heterogeneity of smart phone architectures and operating systems.
- Partitioning is done based on the clouds trusted way. Partitioning of task for offloading in to different cloud server leads great difficulties.
- One of the major attributes in MCC is SMDs mobility. The data exchange rates and network bandwidth may vary due to the movement of mobile users. So there is a chance for data loss due to weak connection.
- Financial issues of end users are received from the resources of cloud infrastructure. The cost for offloading process is too expensive.
- The offloading system is vulnerable to timing attacks in which the unauthorized user may access the cloud server.

4. PROPOSED METHODOLOGY

The data and computation is offloaded from the mobile devices to the cloud using an approach called computation offloading approach. The mobile applications are processed based on the available computation capability, execution time and energy on mobile devices. The computation time and battery life is saved with the process of offloading and processing of mobile applications done based on the computation. These methods are beneficial for some applications such as real time multimedia applications and fitness applications. In this scenario, the data should be encrypted before it is forwarded to the cloud server so that the data is secure. These approaches are easily attacked by timing attacks. During the server timing analysis, the attacker could obtain the RSA-ABC private key. Once the attacker receive the code then all the data could be easy to offload. These data are not secure anymore. To overcome these issues, a RSA private key with server measuring and a decryption algorithm named as ABC algorithm are proposed. This approach has a secure and cost efficient offloading. The master secret is easily computed by the client and server when the decrypted message is properly formatted. This

process must be done properly otherwise own random code will be created for a master secret. The proposed method is implemented using JAVA.

4.1 Mobile Cloud Offloading System

The Figure 1 shows the process of mobile cloud computing. The cloud server is used to process the mobile applications. This process is performed with remote controller. In these scenario, offloading approaches are used to process the data computation and offloading. The execution of mobile applications locally in mobile devices are computational intensive and also consume large amount of energy. These issues are overcome by using the technique named as computational offloading.

For the execution of applications on cloud, the computational intensive applications and the tasks of mobile devices are offloaded. According to its resource availability the computation is offloaded to cloud then it is transferred from cloud to mobile devices. This process will save the execution time and energy on the mobile devices. For the mobile users, the cloud is a useful tool for sharing photos, video clips, real time experiences, multimedia and health care applications where offloading approach is an advantage. The health care mobile devices handle pulse rate, blood pressure and the monitoring of patients through the emergency systems. For the security reasons, these data must be encrypted so as to be secured.

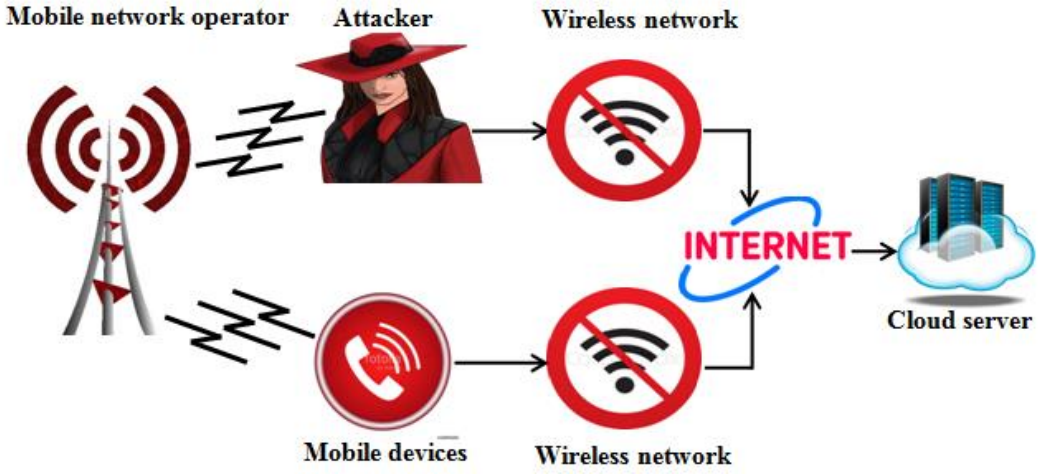

Fig.1. An architecture of mobile cloud computing system.

In the architectural model illustrated in Fig.1, there are mainly three components such as mobile devices, mobile network operator, and cloud. The cloud is also formed by using mobile devices. The mobile devices are referred as mobile terminal. The smart phones, tablet PCs, notebook computers, laptops and PDAs are considered as a mobile cloud. The data centers and servers are included with the cloud structure and also present the IT resource or information service. The cloud consists of three layers such as,

IaaS-Infrastructure as a Service:

It contains all types of components such as server, databases, storage, and parallel computing system.

SaaS- Software as a Service:

Software, applications, information and data are present in this layer.

PaaS-Platform as a Service:

It consists of all types of platforms such as operational, supported, and developmental.

The mobile networks are accessed by the mobile devices in mobile cloud computing. Thus the mobile network needs to transfer the information between cloud and the mobile device through the mobile operator network. During the process of mobile cloud computing all the three layers of cloud deal the problems of security and privacy.

Security challenges during partitioning and offloading process

In the process of offloading, it needs to operate the cloud via the wireless network. In these processing period users does not have any controlling process across the mobile devices. Thus there is difficult in processing the unauthorized operations offloaded information. Instead of using mobile devices, it is considered to use a cloud or edge servers to access the offloaded information during the process of offloading and also enhance the confidentiality and integrity of offloaded information. The challenge of integrity occurs when the offloading process is finished. This offloading process will provide a result and if it is not correct then the mobile device does not verify the correctness of the result. And also various challenges occurs which contains availability attack and malicious content threats. During the process of partitioning jamming attack will occur between data, applications and mobile devices. The availability of cloud services can also affect the offloading. Partitioning and offloading stages contains malicious contents to transgress the users' confidentiality as well as the mobile users' privacy.

4.2 Mobile Applications in Cloud Computing

In recent years, through the mobile devices users utilize the internet. Smart phones and tablet PC are good examples for mobile devices. Mobile equipment consists of limited amount of storage and processing capacity and energy. Thus the receiving side resources does not have highness and the ability of mobile equipment calculation is limited. The mobile devices have poor ability of sustaining battery and data sharing.

Hardware limits breaking

During the process of complex information, the mobile cloud computing gives an energy to the complex data and the big data accessed in the cloud. So the load of calculations and energy on the mobile device is decreased.

Intelligent balance load

This is used to balance the loads and minimize the usage of electricity. The mobile cloud computing has the ability to provide a solution to the battery issues and also increase the life of batteries for mobile devices.

Convenient access data

The convenient access to data for reducing the means of on-demand own services to the cost of management.

4.3 Security in Computation Offloading

Here the design of system and implementations of real systems life time are discussed about. Under the issue of timing attacks the performances and security attributes of the system are analyzed. In the proposed model, the models of offloading, mobile cloud systems and the secret information placed in cloud server are focused. These are used for the processes of encryption and decryption. For encryption process RSA algorithm is used and the decryption process is done by using ABC algorithm. These two algorithms are discussed below.

Encryption using RSA Algorithm

The RSA is a highly used algorithm for the key generation of public encryption technique. The RSA expands as Ron Rivets Shamir and Len Adelman. This was first launched in the year of 1977. The work of RSA algorithm is to encrypt the data that encrypted data must be used only by the user who has the original security code. The RSA and ABC algorithms are analyzed in detailed manner.

1. RSA-Key generation.
2. RSA-Encryption.
3. ABC-Decryption.

The RSA is emerged as an encryption and decryption technique. The public key is forwarded to all the users who need to encrypt the messages and the private key is not shared to the public because it is shared only for the original user. The private key is used for the decryption process.

The major work of RSA is effectively providing an Euler's theorem: $xx\lambda\ (mm)\ mod\ (m) = 1.where,\ abc\ (x,\ m) = 1.$This is required to the calculation of $m = gk.h.$in such a way i.e. $\lambda(mm) = (g_k - 1)(h - 1).$ In this l and c are carefully chosen for the inverse $mod\ \lambda(m).$The encryption of data is denoted as an $EM.$ It is needed to the public key receiver side $g_{kw} = \{mm,\ ll\}.$ Cr is referred to as cipher text $Cr = EM\ ll\ mod\ (m),$ where $0 \leq EM \leq mm.$ The cipher text C_r is less than the *modulus mm.* Here, g_{kr} is used for decryption where $g_{kr} = \{mm, cc\}$ and the estimates $EM = C_r\ mod\ (m).$

Encryption: The encryption is defined as the process of changing to cipher text (data) from the original text (data).

Procedure:

1. If an user intended to save the data in to the cloud. The user only receives the *public key m, l*. from the cloud service provider. The cloud server share public key only to the cloud users.
2. In this scenario, padding approach is referred to as transformable protocol used to connect a user data to an integer.
3. Then the user data is encrypted and $C_r = m, l$ is the representation of cipher text data C_r.
4. Finally, the cloud service provider stores the cipher text data or encrypted data.

Decryption by using ABC algorithm

- **Effectiveness of Producer**

In this section, an operation of ABC decryption algorithm is presented. The producers S_{gk} at "O" process is given below

(i) The zero degree scanning function for producer is,

$$S_f = S_{gk}^o + \pi_1 c_{\max} J_{gk}^o(\varepsilon^o) \tag{1}$$

(ii) The right hand side hypercube scanning function is,

$$S_t = S_{gk}^o + \pi_1 c_{\max} J_{gk}^o(\varepsilon^o + \pi_2 \lambda_{\max/2}) \tag{2}$$

(iii)The hypercube performs the producers scanning task in left-hand side

$$S_t = S_{gk}^o + \pi_1 c_{\max} J_{gk}^o(\varepsilon^o - \pi_2 \lambda_{\max/2}) \tag{3}$$

The general dissemination arbitrary, mean zero and standard deviation is represented by π_1. And π_2 assign the range values for homogeneous distributed arbitrary sequence.

Value range from 0 to 1.

The maximum search angle $\lambda_{\max}$ is given below,

$$\lambda_{\max} = \beta / c^2 \tag{4}$$

Here, the value of C_r is computed as,

$$C_r = round(\sqrt{m=1}) \tag{5}$$

Here, the search space dimension is represented by $\lambda_{\max}$

$$\lambda_{\max} = \beta / m = 1 \tag{6}$$

The calculation of maximum search distance C_{max} is given below,

$$C_{\max} = \left\| c_w - c_v \right\|$$

$$C_{\max} = \sqrt{\sum_{j=1}^{m} (cw - cvj)^2} \tag{7}$$

Here, C_{ui} and C_{ul} represent the lower and upper limits of i^{th} dimension. The better place containing the beneficial resource is attained with the help of equations (9), (10) and (11). The present better place assigns a new better place, this resource is made to be lesser to that in the new location.

$$\varepsilon^{0+1} = \varepsilon^{0} + \pi_2 \mu_{\max} \tag{8}$$

The maximum turning angle is represented as a $\mu_{max.}$ This is calculated by means of $\mu_{max.}$

$$\mu_{\max} = \lambda_{\max/2} \tag{9}$$

Determining of spot superior place is challenging issue to the producers even after the computation. Its head starts to obtain the initial place as given below,

$$\varepsilon^{o+cr} = \varepsilon^{o} \tag{10}$$

- **Effectiveness of scrounger**

In all calculations the number of exception to the producer members are preferred and characterized as a scrounger. The behavior of scrounger also consists of the copying task for place. In the calculation of "o"th performances of place copying scrounger brings out in the structure of producers comfort manner,

$$S^{0+1} = S_j^o + \pi_3 A(S_{gk}^o - S_j^o) \tag{11}$$

- **Effectiveness of ranger**

Usually the ranger placed in the residual member's front of the group that is replaced in their own previous places. The ranger has able to place in the resources in the sense of arbitrary walks and an orchestrated analysis performances. For dissemination process the resources are placed

during the arbitrary walks. Based on the arbitrary walk the head angle and ranger distances are produced. An adaptive genetic algorithm is an advanced algorithm for the ranger performances.

5. RESULT AND DISCUSSION

In this section, the proposed methods are discussed and analyzed. The proposed method is simplified by using JAVA programming language. Here, some data sets that are from the research community are used.

5.1 Explanation of Datasets

The datasets used is census-incoming UCI machine learning datasets (KDD). This dataset has number of records and characters such as 299285r, 40c.This is obtained from U.S in the year of 1994 to 1995 by conducting population surveys. This type of data sets is used for some special calculations with the accepted benchmark. The primary sets of data are used only for the testing of special character algorithms. The removal of missing data presented records and twisted distribution records are used as a de facto benchmark. These data sets are called as sanitized data sets. Out of 40 original characters, we are choosing 12 characters, in that 9 will be quasi identifiers and 3 will be sensitive characters.

5.2 Analysis of Proposed Methods

To ensure the effectiveness of proposed method, different analysis is carried to collect results. A real-time analysis is performed to obtaining a secure data from cloud server. The user data and mobile cloud computing system are tested during the analysis to collect the secured data. In mobile cloud computing, the RSA-ABC is executed in the operational platform of JAVA. Finally, the cloud server performance is ensured in minimizing the timing attack and simultaneously increasing the security of user data.

The results performance of time between the mobile devices and cloud servers are shown in Table 1. In Table 1 it is observed that the time 6254secs for a file size 10kb, time 8245secs for file size of 20kb, file size of 30kb got 10127secs and finally, for 40kb file size the time is 13248secs. The Fig.2 shows the time in sec and file size in kb for the proposed method.

Table. 1. Size of files in kb with time in sec for RSA-ABC

File size(kb)	Time(sec)
10	6254
20	8245
30	10127
40	13248

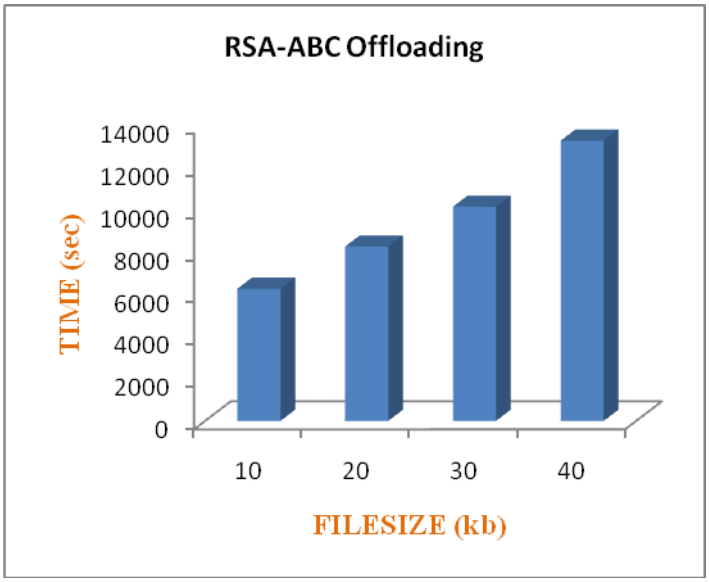

Figure 2. RSA-ABC time in sec with file size kb

Table.2. files size in kb with memory size in kb for RSA-ABC

File Size (kb)	Memory(kb)
10	1102154
20	1236887
30	1321415
40	1411257

Table 2 shows the memory size of the cloud server. In the estimation table the 1102154kb size of memory for 10kb file size, 20kb file size contains 1236887kb memory size, 30kb file size consists 1321415kb of memory size and the size of 40kb file consists of 1411257kb memory size.

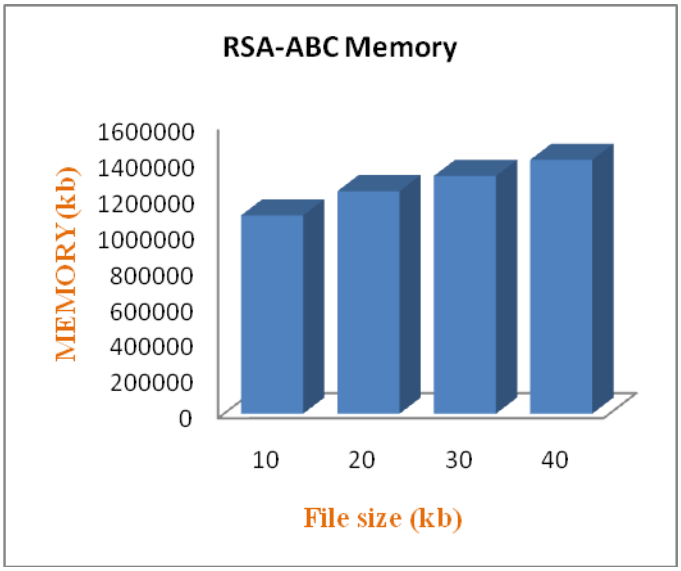

Fig.3. RSA-ABC memory size in kb with file size in kb

The processing of the above presented methods are discussed. This consists of four tables that contain values of encryption, decryption and memory space for different size of files. If the attacker sends a request to the server, then the time of encryption will increase gradually. The decryption time is low when the attacker sends a request. The Table 2 illustrates the memory space for different size of files. If the authorized user sends a request to server, then the processing of encryption time is minimum. Similarly, the mobile users increase the utilization of memory space.

5.3 Analysis between Existing and Proposed Methods

From Table 3 the comparison time in sec and file size in kb for the proposed and existing method is obtained. In this article 'of' method as RSA and the time for 'of' method is high compared to proposed method RSA-ABC. The newly proposed method gives excellent efficiency without timing attack.

Table 3: Size of files in kb with decryption time in sec for RSA-ABC

Methods	RSA-ABC Proposed	RSA Existing
File size(kb)	25	25
Time(sec)	9468.5	9484.8

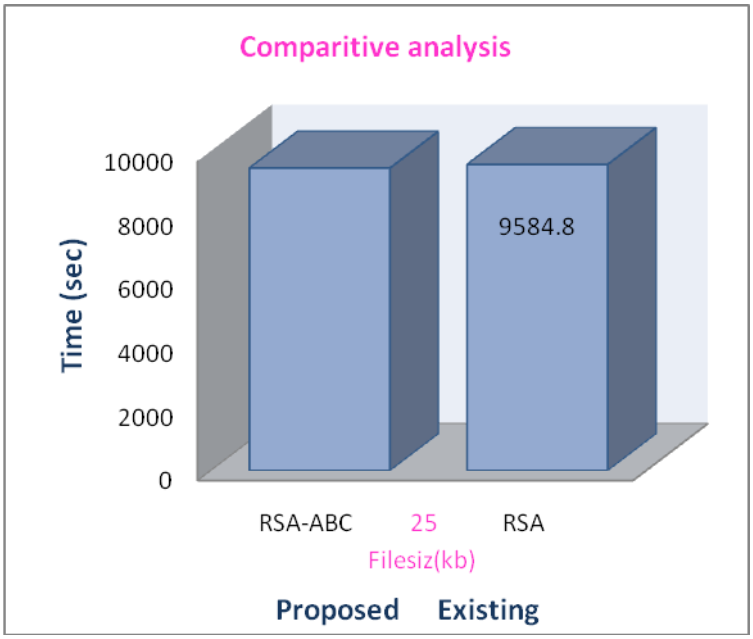

Fig.4: Comparative analysis between RSA-ABC and RSA

5.4. Result Analysis

The Table 3 consists of the analysis results between of method and newly presented method. The new method is processed by using encryption of files. The analysis between RSA-ABC and RSA shows if the file size for encryption is increased then the processing time is also increased. From the Table 5 by using RSA-ABC method the maximum time for encryption is low as 9468.5secs but the RSA have maximum time for encryption as 9484.8secs. The above analysis done based on the size of files, when the size of the file in kb is minimum then the memory size in kb is also minimum. The size of file is 10kb then the time for encryption is minimum 2658secs for the proposed method. Likewise, the memory usage of the presented method is given in Table 2. Finally, this shows that our presented method perfectly provide security and privacy for the users information compared with the RSA method.

6. CONCLUSION

In this article, a secure based cost efficient offloading for cloud computing using RSA-ABC algorithm is presented. This method is used to protect the user data from the attackers. Here, highly used public key technique RSA is utilized for encryption. A secure based cost efficient offloading for cloud computing using RSA-ABC algorithm is presented. The RSA algorithm has capability to save the data from the attacker. It only responds to the request from original data owner and it neglects the request from the attackers. It is able to easily identify the data owners by the secret code. The ABC algorithm is implemented for decryption process. In this work, secret data is stored in cloud server and before transferring the secret data from user to cloud server, the data should be offloaded. This process is back for encryption and decryption. The encrypted data is saved in cloud service provider and decryption is done in receiver side. All these processes are implemented using JAVA. As per the findings the proposed RSA-ABC

algorithm provides better solution to protect data from the attackers with cost efficient offloading.

REFERENCES

[1] M. Chen, Y. Hao, Y. Li, C. F. Lai and D. Wu, "On the computation offloading at ad hoc cloudlet: architecture and service modes", IEEE Communications Magazine, Vol.53, No.6, pp. 18-24, 2015.

[2] Yan, Zheng and Mingjun Wang , "Protect pervasive social networking based on two-dimensional trust levels", IEEE Systems Journal, Vol. 11, No.1, pp. 207-218, 2017.

[3] Bo Han, Pan Hui, V.S. Anil Kumar,Madhav V. Marathe, Jianhua Shao and Aravind Srinivasan, Fellow, "Mobile data offloading through opportunistic communications and social participation." IEEE Transactions on Mobile Computing, Vol.11, No.5, pp. 821-834, 2012.

[4] Xiaofei Wang, Zhengguo Sheng, Shusen Yang, and Victor C. M. Leung, "Tag-assisted social-aware opportunistic device-to-device sharing for traffic offloading in mobile social networks", IEEE Wireless Communications, Vol.23, No.4, pp.60-67, 2016.

[5] Applin, Sally A., and Michael D. Fischer, "Pervasive Computing in Time and Space: The Culture and Context of 'Place Integration", Intelligent Environments (IE), in process of 7th International Conference, pp.285-293, 2011.

[6] Ferreira, Luis Lino, Guilherme Silva, and Luis Miguel Pinho, "Service offloading in adaptive real-time systems", Emerging Technologies & Factory Automation (ETFA), in process of IEEE 16th Conference, Vol.431, 2011.

[7] Z. Yan, W. Feng and P. Wang, "Anonymous Authentication for Trustworthy Pervasive Social Networking,"in process of IEEE Transactions on Computational Social Systems, Vol. 2, No. 3, pp. 88-98,2015.

[8] M. Endler, A. Skyrme, D. Schuster and T. Springer, "Defining Situated Social Context for pervasive social computing," in process of International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), Seattle, WA,pp. 519-524, 2011.

[9] C. Huang, Z. Yan, N. Li and M. Wang, "Secure Pervasive Social Communications Based on Trust in a Distributed Way, "IEEE Access, Vol. 4, pp. 9225-9238, 2016.

[10] D. Angelo, Gianni, Salvatore Rampone, and Francesco Palmieri, "Developing a trust model for pervasive computing based on Apriori association rules learning and Bayesian classification", Soft Computing, Vol.21, No.21, pp. 6297-6315, 2017.

[11] Tianhui Meng, Katinka Wolter, Huaming Wu and Qiushi Wang, "A secure and cost-efficient offloading policy for Mobile Cloud Computing against timing attacks", Pervasive and Mobile Computing, Vol.45, pp. 4-18, 2018.

[12] Bruno Guazzelli Batista, Carlos Henrique Gomes Ferreira, Danilo Cost Marim Segura, Dionisio Machado Leite Filho , Maycon Leone Maciel Peixoto, "A QoS-driven approach

for cloud computing addressing attributes of performance and security", Future Generation Computer Systems, Vol.68, pp. 260-274, 2017.

[13] Vishal Sharma, Ilsun You, Ravinder Kumar and Pankoo Kim, "Computational offloading for efficient trust management in pervasive online social networks using osmotic computing", IEEE Access, Vol.5,5084-5103, 2017.

[14] Vaishali Y. Baviskar, Snehal Mandlik, Supriya Patil,Pallavi Sinha,Pooja Gopale, "Cloud–Based Energy Efficient Offloading Transcoding Service Policy" ,International Journal of Computer Science and Information Technologies, Vol.6, No.6, pp. 4898-4900, 2015.

[15] Akherfi, Khadija, Micheal Gerndt, and Hamid Harroud, "Mobile cloud computing for computation offloading: Issues and challenges", Applied computing and informatics, Vol.14, No.1, pp. 1-6, 2016.

Authors

M. S. Premalatha received BSc degree in Computer Science from Nesamony Memorial Christian College, Marthandam. She received Master of Computer Applications from Bishop Heber College, Thiruchirapalli and Master of Philosophy in Computer Science at Manonmanium Sundaranar University, Thirunelveli. She is currently working as Assistant Professor in the Department of Computer Applications, Nesamony Memorial Christian College, Marthandam. She is a Research Scholar in Computer Applications at Manonmanium Sundaranar University, Thirunelveli. Her field of interest is Mobile communications, Green computing and Cloud computing.

Dr. B. Ramakrishnan is currently working as Associate Professor in the Department of Computer Science and research Centre in S.T. Hindu College, Nagercoil. He received his M.Sc degree from Madurai Kamaraj University, Madurai and received Mphil (Comp. Sc.) from Alagappa University Karikudi. He earned his Doctorate degree in the field of Computer Science from Manonmaniam Sundaranar University, Tirunelveli. He has a teaching experience of 30 years. He has 23 years of research experience and published more than 50 research articles in reputed international journals (12 Science Citation Index Expanded research articles at Springer Journals and 22 SCOPUS indexed research articles). Further, he has authored a book titled “Vehicular Ad Hoc Network and Web Vehicular Ad Hoc Network an Overview” published by the International book publisher LAP Lambert Academic Publishing with the ISBN:978-3-330-02628-5. His research interests lie in the field of Vehicular networks, mobile network and communication, Cloud computing, Green computing, Ad-hoc networks and Network security.