LEADER K-MEANS CLUSTERING BASED INTRUSION DETECTION IN MOBILE CLOUD COMPUTING COMPUTATION OFFLOADING

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.
ramsthc@gmail.com

ABSTRACT

The mobile applications are processed based on the computation or execution time and energy on mobile devices that are saved with the process of offloading. These methods are beneficial for some applications such as real time multimedia applications and fitness applications. The proposed method requires efficient identification of intrusions before offloading the details to the server. After intrusion detection, the tasks are offloaded between server and device. In this method, the tasks are clustered initially. This will identify the intrusion ie task from unauthorized users and non intrusion. After the clustering the data is encrypted using Oppositional Artificial Bee Colony (OABC) based RSA algorithm. Here Leader based K-means clustering (LKC) is used to find the intrusion. In this scenario, the data should be encrypted before it is forwarded in to the cloud server so that the data is secured. The effectiveness of the algorithms are analyzed by comparing with other existing methods.

Keywords: - K-means clustering algorithm, optimization, Opposition-Based Learning (OBL), mobile cloud, encryption, offloading, decryption.

1. INTRODUCTION

Recently cloud computing turns into master piece in data storage and computing services with the help of Internet [1]. Using cloud service provider, all the requested processes and services are managed. The cloud will allow the third parties to access all the software and hardware services via internet. Security is the major issue in both public and private cloud. During the third party authentication, there is a chance of illegal attacks. Privacy and protection of sensitive data is more important in cloud [2]. Due to increasing cloud users, novel networking attacks and hacking tools have also increased. An effective Intrusion Detection system (IDS) is one of the best way of handling abnormal activities in the cloud network [3]. IDS will identify the authorized and malicious users to ensure confidentiality, integrity and availability [4].

In the mobile devices, mobile offloading is a promising technique to help compacted resources. The mobile application performances and efficiency of energy are increased by applying task of computational offloading [5]. Mobile applications as computational intensive and latency sensitive provide worst performances during used on smartphones e.g., image processing and chess gaming, etc. [6]. The non-real time applications have deferred naturally to minimizing the mobile data traffic and thus the operation cost also minimized.The mobile data offloading has main advantage is that there is no cost for opportunistic communications which is clearly known through the Bluetooth and Wi-Fi technologies [10]. Offloading of mobile data through an optimal opportunistic mobile network is used to enhancing the capacity of network and nodes of network. But this is used to reduce the issue ie. data offloading optimization [7]. The joint resource partitioning and offloading in two-layers cellular network is reduced by applying a common and tractable framework. It also provides a plan for partitioning and offloading for joint resources [8]. The real-time video applications of offloading have some challenges and opportunities such as common force efficient offloading and dynamic wireless rules made small particles offloading by using an adaptive scheduling algorithm [9]. The main aim of this research is to provide a better detection technique to detect the intrusion from the dataset by solving the issues that currently exist in the literary works. Hence, it is intended to propose a new detection method for the intrusion detection system.

2. LITERATURE SURVEY

Warley Junior *et al*. [11] have discussed the Mobile Cloud Computing (MCC) infrastructure. MCC environments were affected by assets security, unlimited energy and minimal network in the wireless scenario. In the cloud environment, mobile application user shift from a cloud to other cloud have been included. So the author has introduced an efficient mapping study. That describing and addressing of mobile approaches in the mobile cloud computing environment. But that method was unfit for LBS, because energy and accuracy is an important issue for LBS.

Muhammad Shiraz *et al*. [12] has introduced a framework named as a numerical based offloading structure with minimum energy. That framework was generated to perform an accelerated mobile application in mobile cloud computing environment. It was concentrated in cloud data centers to the operation of using an application. But that has the minimum detail of numerical comprehensive processing time for component movement. From that analysis, on the wireless network medium, the communication size of data was minimized in 84% and usage of energy level also minimized in 69.9% for various prototype offloading systems. Since numerical offloading, communication data size and cost for usage of energy minimized for mobile cloud computing. But their method was unfit for restricted area mobile devices, remotely operated cloud servers node, execution of perfect mobile applications in a cloud environment.

In computational offloading, resources intensive procedures were simplified by contemporary Computational Offloading Frameworks (COFs). To overcome that, **Muhammad Shiraz** *et al.* [13] have analyzed the resource numerical offloading approach for mobile cloud computing.

SMDs require slit approach for performing an application of numerical clouds. In computational clouds, the real mobile cloud computing with prototype applications for the evaluation of various computation intensifies. The distributed applications were used on additional computing resources. Distributed performance processing time as 31.6% extra energy was used, 39% extra period was taken and in various numerical cloud components of mobile applications were receive 13241.2KB of information. The reduction of overhead during runtime in computational offloading using lightweight procedures was complex.

In a distributed cloud, where the users data will be placed in social networks with minimization of operational cost for cloud service provider was a major problem. The variety of data centers was placed at various environment. These were interrelated with the internet. So the **Qiufen Xia** *et al.* [14] have introduced the algorithm named as a fast scalable algorithm. It was used in reducing the data location issues. The article focused on connecting the social network of user to various locations, same communication location for the same user with the data in data centers, connecting data of user into a near and far data centers were used for communication purpose. The user data with their updating rates of reading and location was changed by using extra time. The efficiency of an algorithm was evaluated based on three real social network datasets such as Twitter, facebook and Wiki vote. The algorithm was used for the functional cost reduction and increasing the speed of runtime.
In mobile cloud computing applications, the data want to communicate from customers mobile to cloud due to which cellular networks traffic is increased. So in this article it is focused on reducing the offloading problems in any Wi-Fi network with limited difficult data types. In any considerations in communication capacity, offloading of before the limited time period was possible. To overcome that issues Guoju Gao et al. [15] have introduced an offloading algorithm for offline data. It was used to achieve a similar rate. And also, the author have introduced the other algorithm to obtain a competitive ratio of 2 and a offloading algorithm for dual type data for clear up the issues in common environments. These as applicable for dual cost Wi-Fi transmission scenarios.
Muhammet Baykara and Resul Das [16] has presented the improved honeypot server application which was developed with IDSs to tested data in real-time and to control effectively. Additionally, by integrating the benefits of low and high-interaction honeypots, a better hybrid honeypot system was achieved.

3. PROBLEM DEFINITION

Mobile device applications are split up based on the levels of granularities and the remote processing of mobile devices improve the capacity of SMDs. Remote processing is done by transferring the application components to remote servers. Thus several issues are present in the computation offloading mechanisms. Due to that, some of the security challenges existing in mobile cloud offloading scenarios are listed below.

- During the period of processing, the settling of which application components need to be offloaded is one of the major conflicts of mobile cloud computing.
- The attacks occur in the communication between the server side and client side in the mobile cloud offloading environment.
- Energy consumption of mobile devices is minimized based on maximizing types of mobile applications. This is the main issues in applications of multimedia streaming.

- Intrusion detection is the major issue in computation offloading.

4. PROPOSED METHODOLOGY

In mobile devices, very less amount of processing speed, power and energy are allowed to perform tasks. So it is necessary to transfer the tasks to the remote server which is known as computation offloading. During this process, security is the major issue. The unauthorized access of third party server will be detected by an efficient intrusion detection system. Our proposed method requires efficient identification of intrusions before offloading the details to the server. After intrusion detection, the tasks are offloaded between the server and device.

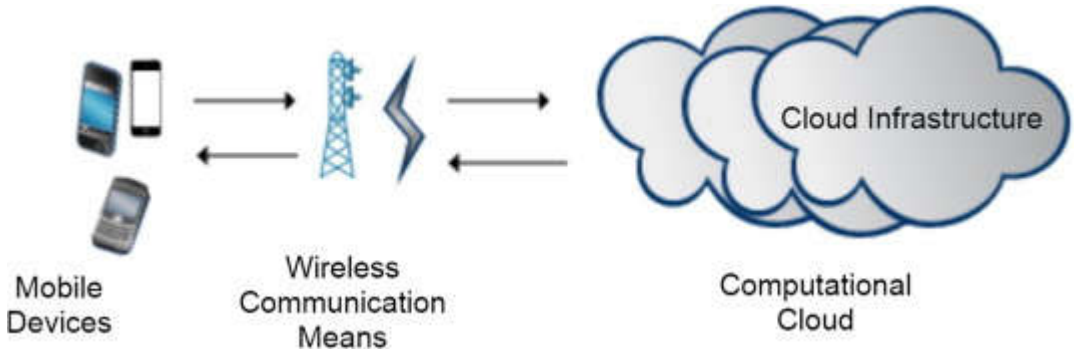

Fig. 1: Offloading architecture

In this method, we have to cluster tasks initially. This could identify the intrusion ie, task from unauthorized users and non intrusion. After the clustering, we can encrypt the data using ABC based RSA. In our method, Leader based K-means clustering is used to find the intrusion. In this scenario, the data should be encrypted before it is forwarded to the cloud server so that the data is secured. These approaches are easily attacked by timing attacks. During the server timing analysis, the attacker obtains the RSA-ABC private key. Once the attacker receives the code then all the data could be easy to offload. These data are not secure anymore. To overcome these issues, we are proposing a RSA private key with server measuring.

4.1 Timing Attacks

In cloud environment, the occurrence of offloading time is defined as the sum of utilized time for communication and computing performances. The execution time of mobile device must be minimal for improving the performance.

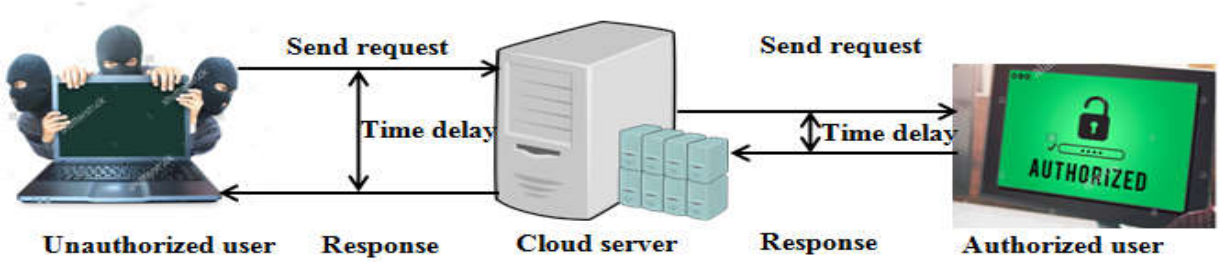

Fig.2. Timing Attack with intrusion

A timing attack has been exploited during the communication between the sender and cloud. When the request is transferred by the authorized user then the cloud checks the request with the original message and compares it with current time and measures the time elapsed from the first forwarding of the message. Then the cloud server observes the time of all messages exchanged between the user and the cloud and focuses on communications. If the incoming message is original then the user can decrypt their data with a minimum time delay. Otherwise the time delay will be increased. The time delay is high then the server identifies that data is from an attacker.

4.2 Problems of Safety And Secrecy in Mobile Cloud Network

In this part, some safety and secrecy problems present in mobile cloud network are analyzed. Security issues in mobile network arise when the mobile networks provide mobility to extend the network nodes and users access way. In these mobile networks contain the smart phones, tablet PCs and PDAs. The mobile device has large number of ways to get accessed such as phone service for users via smart phones, Short Messaging Service (SMS) and 3G networks for internet services. Thus the 3G networks and Bluetooth are used to access the smart phones. The malicious attacks and sensitive data leakage creates many security problems.

For example, different types of people in general places such as cafe, restaurant and airport are given free Wi-Fi, and maximum number of people operates a laptop and access Internet via free Wi-Fi. In these scenarios, the potential data leakage will occur. Due to the weakness of Wi-Fi encryption mechanisms above mentioned issues affects public Wi-Fi and also affects the private Wi-Fi. Hence these are protected from the security issues. Moreover, mobile devices and mobile cloud services interact between them giving a various interfaces frequently. This can incite many security problems too.

Security issues in mobile cloud

The user data having high concentration will attack the cloud. First, the important information is deprecated by the malicious attack. The deprecation is the target for malicious attack. These attacks start from the outside of malicious attack to users legal cloud computing and to cloud computing operators. Then the malicious attack target is to close the cloud service. The users face many data loss when the user transfers all the data to the cloud servers without access to backup and recovery of disaster services. Nowadays these problem arises in cloud providers. For that, the recent security technologies must be integrated with cloud provider which are used to protect the cloud services.

Security issues in application level

The application level security is defined as the hardware and software use of resources to give security to applications. In these environments the attacker does not get any control access to those applications and it will make some changes in their formats. In recent years, the attackers are classified as trusted users and the system also keep them as trusted users which the attacker and affected parties are allowed to access. But a security policy does not allow to access the attacker with random IP address. Where the security policies are applied that allows only authorized users with the proper IP address. These type of security policies are obsolete in processing period with highness technology. The trusted user access the system during that time

the security of that system is exceeded. Due to that all the data are easily corrupted and that imitates the original user with the help of recent technologies.

Privacy issues

In mobile cloud computing privacy protection is the most important problem. On a hand, the ownership data and management data are split because the users own data creates worries and these are the obstacle in mobile cloud computing. In all over the world the user data are stored approximately in sharing manner. But the users do not know their stored location. So receiving the private information of the user has increased the risk.

Authorized users concentrate on the risk of privacy issues of data. In cloud, wireless network and online social network contain privacy preserving techniques. In this work, privacy preserving algorithms are run between cloud and the mobile users. Due to that, in both sides the computation and storage are sufficient. Otherwise these algorithms are prohibited at the end devices. Techniques such as RSA algorithm for decryption can be used to allow privacy-preserving aggregation at the cloud.

4.3 Leader Based Clustering Algorithm for Intrusion Detection

Algorithm 1 : leader based k-means clustering method (S,T)

$L=0$
for each $x \in S$ do
Find a leader $l \in L$ such that $\|(l)-(x)\| \le T$ /*
where
$\|(L)-(x)\|$ can be computed using the Equation
if there is no such a or when $A=0$ then
$L=L\cup\{x\}$;
$count(x)=1$;
$followers(x)=\{x\}$;
else
$count(l)=count(l)+1$;
$followers(l)=followers(l)\cup\{x\}$
end if
end for
Output:
$L^*=\{<l, count(l), followers(l)> l \text{ is a leader}\}$

Fig. 3: Algorithm for leaders based clustering method

K-means clustering is one of the finest clustering algorithm in data mining. But the algorithm has a major drawback in which choosing a K value in high dimensional datasets. To solve the issue, Leader K-means algorithm to speed up the process is used. In this algorithm, the large dataset is divided in the smaller chunks by single scan method. The size of these groups or chunks are

denoted by T . Each chunk is represented by pattern which is known as leaders and the remaining are followers. At initial stage, some of the leaders are empty which are gradually increased. When a leader among group of leaders, the distance between a data x and leader l is less than the size T means the data points similar to that pattern are grouped into one cluster. Each pattern in that chunk is known as follower of that leader. Based on the patterns in the search space, each group is known by the leader. The theory of this algorithm is linear time complexity over large dataset.

Encryption using Oppositional ABC based RSA algorithm

The RSA is a highly used key generation of public encryption technique. The RSA expands as Ron Rivets Shamir and Len Adelman, This was very first launched in the year of 1977.The work of RSA algorithm is to encrypt the data so that the encrypted data is used only by the user who has the original security code. Here 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 people, 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 keys are used only 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. $\lambda(mm) = (g_k\text{-}1)(h\text{-}1).$ In this l and c are carefully chosen for the inverse $mod\ \lambda(m).$The encryption of data is denoted as a 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 we are using g_{kr} for decryption, g_{kr} = {mm, cc} and the estimates $EM = C_r\ C_r\ mod\ (m).$

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

Procedure:

1. If an user intended to save the data in to the cloud. They only receive 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 connecting a user data into 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 OABC algorithm

The Oppositional Artificial Bee Colony Optimization algorithm is used for the decryption process of RSA algorithm. ABC is the bio-inspired optimization algorithm which belongs to the intelligent swarming nature of honey bees. Three colony of bees are used such as employee bee, Onlooker bee and Scout bee. The major contribution of the proposed work is to use Opposition learning behavior in initialization process. The opposition-based learning (OBL) will generate the reverse solutions in the search space, which improves the performance of the ABC algorithm during decryption.

From the "Opposition based learning (OBL)", the initial and the dependable reverse solution is created. This will increase the effectiveness of the proposed algorithm to convalesce the accuracy of solutions.

The pseudo code for OABC decryption is described below

For Each

Generate the initial population $S_i, \quad i = 1,2,....n$

Compute opposite food source using OBL

Evaluate the fitness (Fit) of the population

Set cycle to 1

Repeat:

For each employed bee do

Assign a solution;

Update the solution $S_{ij} = X_{ij} + \Psi_{ij}\left(X_{ij} - X_{kj}\right)$

Calculate the fitness function

End For

For each solution Si do

Calculate the probability $P_i = \dfrac{Fit_i}{\sum_{n=1}^{SN} Fit_n}$

End For

For each onlooker bee do

Select a solution from employed bees based on its probability;

Update the solution by local search procedure and evaluate it;

End For

For each solution Si do

If limit i> threshold then

Abandon solution;

Construct a new solution by scout bee and evaluate $X_{ij} = X_{\min,j} + rand\,[0,1]\left(X_{\max,j} - X_{\min,j}\right)$

End For

Fig. 4: Pseudo code for OABC

5. RESULT AND DISCUSSION

This section discusses and analyzes about the proposed methods. The proposed method is simplified by using JAVA programming language. Here, some data sets which are from the research community is used.

5.1 Explanations of datasets

In this work, census-incoming UCI machine learning datasets (KDD) are used. This data set 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 to the 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, 12 characters are chosen, in that 9 will be quasi identifiers and 3 will be sensitive characters.

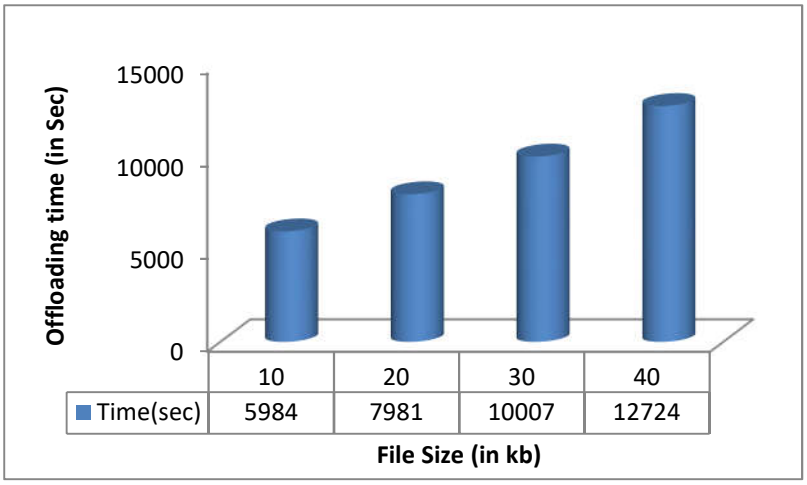

Fig. 5: Offloading time analysis

Fig. 5 shows the offloading time of task with varying file sizes. Table I shows the encryption time for the proposed system. The file size of 10kb takes 3251secs for encryption, 20kb file size takes 4325secs for encryption, 30kb file size takes 5348secs for encryption and 40kb size of file takes 6218secs for encryption. It is graphically shown in Fig. 6.

Table I. Size of files in kb with encryption time in sec for RSA-OABC

Size of Files(kb)	Time for Encryption(sec)
10	3251
20	4325
30	5348
40	6218

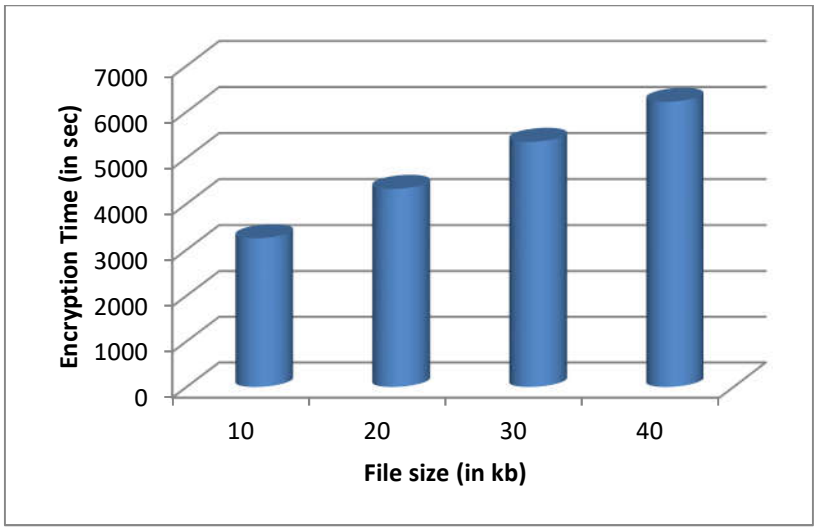

Fig. 6. RSA-OABC encryption time in sec with file size in kb of presented method

Table II shows the decryption time of presented system. The file size of 10kb takes 2658secs for decryption, 20kb file size takes 3106secs for decryption, 30kb file size takes 4215secs for decryption and 40kb size of file takes 5211secs for decryption. It is graphically shown in Fig. 7.

Table II: Size of files in kb with decryption time in sec for RSA-OABC

File size(kb)	Decryption time(sec)
10	2658
20	3106
30	4215
40	5211

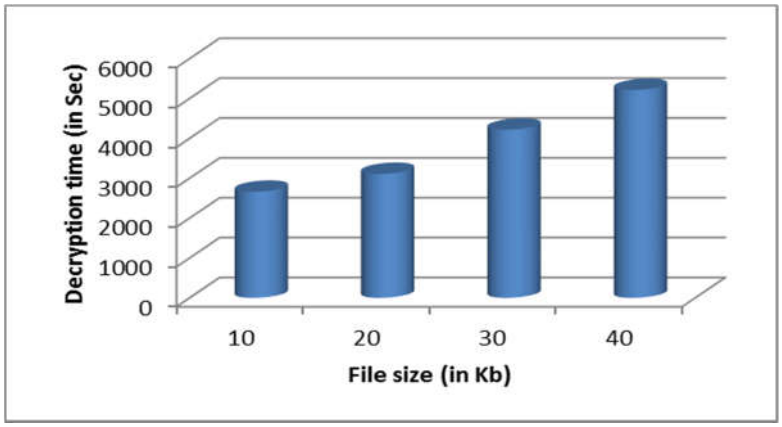

Fig.7. RSA-OABC decryption time in sec for proposed method

From table and figure, it is observed that when the file size is increased, the encryption and decryption time also increases. The major intension of this research is to detect the intrusion before offloading. Leader based K-means will be used for this process. The clustering accuracy is described in Fig. 8.

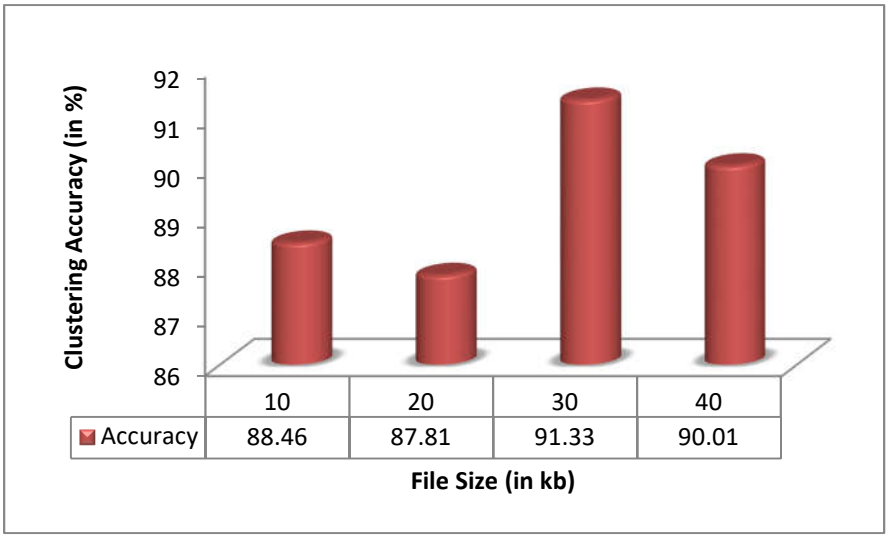

Fig. 8: Clustering accuracy with various file size

Comparative Analysis

The intrusion detection using clustering algorithm is evaluated using clustering accuracy which is compared with other clustering algorithms such as K-means and FCM. The leader based K-means will give better accuracy which is shown in Fig. 9.

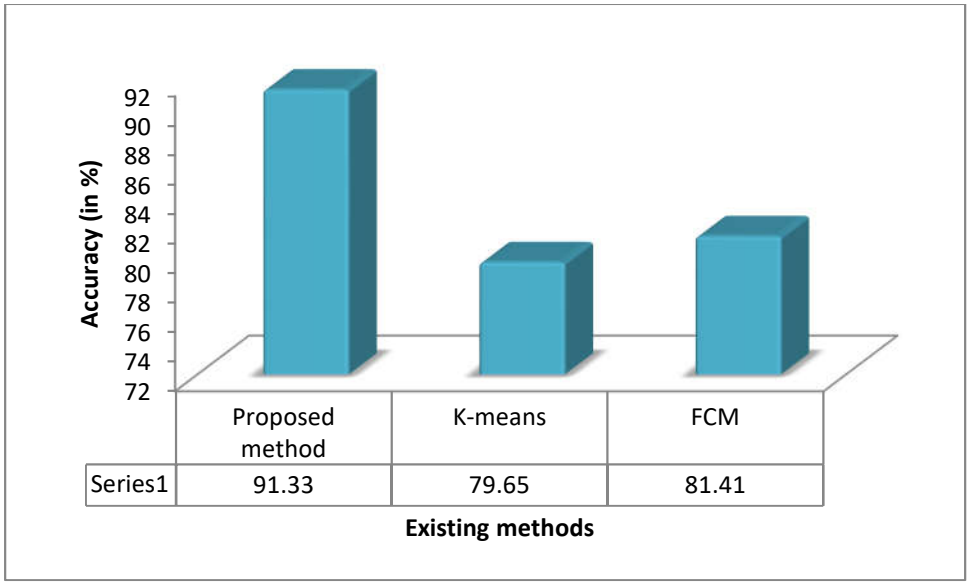

Fig. 9: Clustering accuracy comparison

Table III: Decryption time comparison

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

From the table, it is observed that the proposed RSA-OABC with Leader based clustering algorithm has less decryption time when compared to other existing researches.

6. CONCLUSION

Security in Computation offloading is one of the major worries because of different attacks and vulnerabilities in the mobile cloud. As a result, attack detection is an imperative segment in system security. A combination of RSA-OABC, and leader based k-means clustering generate new IDS which are presented in this paper. Different training subsets are produced by leader based k-means clustering method. This methodology is used to protecting the user data from the attackers. In this article, highly used public key technique RSA is utilized for encryption. The experimental results using the KDD CUP 1999 dataset demonstrates the effectiveness of this approach which provides better precision than the existing method. In future, the security of the data will be improved using cryptographic algorithms.

REFERENCES

[1] Anthony T. Velte, Toby J. Velte and Robert Elsenpeter, “Cloud Computing – A Practical Approach”, Tata McGrawHill Edition, ISBN: 978-0-07-162695-8.

[2] Mell, Peter, and Tim Grance, “Effectively and securely using the cloud computing paradigm” NIST, Information Technology Lab 2009.

[3] Adel Nadjaran Toosi and Mohsen Kahani, "A new approach to intrusion detection based on an evolutionary soft computing model using neuro-fuzzy classifiers",journal of computer communications, vol. 30,pp. 2201–2212, 2007.

[4] H. Debar, M. Dacier and A. Wespi, “Towards a taxonomy of intrusion detection systems”, journal of computer networks, vol. 31, pp.805–822, 1999.

[5] Huber Flores, Rajesh Sharma, Denzil Ferreira, Vassilis Kostakos,Jukka Manner, Sasu Tarkoma, Pan Hui, Yong Li,"Social-aware hybrid mobile offloading", Pervasive and Mobile Computing, Vol. 36, pp.25-43,2017.

[6] Y. Zhang, E. Pan, L. Song, W. Saad, Z. Dawy and Z. Han, "Social Network Aware Device-to-Device Communication in Wireless Networks,"IEEE Transactions on Wireless Communications, Vol. 14, No. 1, pp. 177-190, 2015.

[7] Wei Cao, Gang Feng, Shuang Qin and Mu Yan, "Cellular offloading in heterogeneous mobile networks with D2D communication assistance." IEEE Transactions on Vehicular Technology, Vol.66, No.5, pp. 4245-4255, 2017.

[8] Singh, Sarabjot, and Jeffrey G. Andrews, "Joint resource partitioning and offloading in heterogeneous cellular networks", IEEE Transactions on Wireless Communications, Vol.13, No.2, pp. 888-901, 2014.

[9] Lei Zhang, Di Fu, Jiangchuan Liu, Edith Cheuk-Han Ngai,and Wenwu Zhu, "On energy-efficient offloading in mobile cloud for real-time video applications." IEEE Transactions on Circuits and Systems for Video Technology, Vol. 27, No.1, pp.170-181, 2017.

[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] Junior, Warley, Bruno Silva, and Kelvin Dias, "A systematic mapping study on mobility mechanisms for cloud service provisioning in mobile cloud ecosystems", Computers & Electrical Engineering, pp. 1-18, 2018.

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

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

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

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

[16] Muhammet Baykara and Resul Das, "A novel honeypot based security approach for real-time intrusion detection and prevention systems", journal of information security and application, vol.41, pp.103-116, 2018

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 70 research articles in reputed international journals (14 Science Citation Index Expanded research articles and 25 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.