International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 14 (2015) pp 34485-34489

A new re-encryption scheme with improvised delegation mechanism and homomorphic encryption

[1]S.Kalaivany, [2]Dr.T.Nalini,
[1]Research Scholar, [2]Professor
[1]Department of Computer Science, Vels University, Pallavaram,Chennai
[2]Department of Computer Science & Engineering, Bharath University ,Chennai 600 073

Abstract- A cloud storage system is capable of storing huge data in its storage server. The cloud platform consisting of numerous storage servers that render the storage services for long time. Usually the third party acts an admin for the cloud storage system and that does not provide expected data confidentiality. So the centralized cloud storage system is introduced, however it also has the problem of hackers who eavesdrop or attack the data. General encryption schemes protect data confidentiality. In this paper threshold proxy re-encryption scheme and integrate with Fully Homomorphic Encryption is a promising technique for access control of encrypted data. The proxy re-encryption scheme considers the encrypted messages from the data owner and encodes it as well as forwards towards the receiver or storage server. The overall performance achieves the delegation process with secured access control. The simulation results shows proposed system achieves both forward security and backward security in cloud environment.

Keywords- Cloud storage system, Fully Homomorphic Encryption, Threshold Proxy Re-Encryption.

1. Introduction

A cloud storage system is a large-scale ubiquitous storage system where numerous storage servers are resided and works independently. Every storage systems must have the robustness property. Many methods or system are presented for storage server data storage. Usually the robustness is achieved by using the erasure coding where the transferring message is fragmented into k symbols of n code words [1]. Each code word symbols of a message is stored in the different storage symbol. In order to compute the fragmented code word symbols for a message in a distributed environment, the erasure coding is performed parallel. Once the message symbols are stored in the different storage servers in the distributed environment, the code word symbols are computed independently and stored in the storage servers. This is the traditional encoding and storage process [2].

Later, a set of attributes along the cipher text are labeled and a monotonic key structure long with the decryption key of the user decides which user is authorized for the decryption process. The Coarse Grained Method sends the decryption key to the third party regardless of user's knowledge whereas the FineGrained Method defines that it renders the key for the certified users and is known as centralized authority.This process is known asKey Policy Attribute Based Encryption (KP-ABE) [3]. However, this process lacks in scalability and the flexibility in the attribute management. In order to overcome these drawbacks, the encryptor selects the tree access policy which is encrypted with the cipher text, whereas according to the set of attributes, the decryption key is created. This process is known as Ciphertext Policy Attribute Based Encryptionwhich also has the drawbacks that it does not support the multiple value assignments and the compound attributes. In addition, the data forwarding and the data retrieval also becomes the issue [4].

In this paper a secured decentralized storage system is formed by integrating the secured decentralized code with the Threshold Proxy Re-Encryption Scheme which performs the encoding and forwarding operations on the encrypted and encoded message.The proposed system model constructed with the two servers, one is for message storage and another is for key storage. The message sender encrypts the data and send to the message server where in the encrypted message is encoded and stored. Then the encoded message is forwarded to the receiver using the key from the key server after the proper authentication. The homomorphic property is included in the system model where the arbitrary computation on the encrypted message is performed and the result of the system model bring the delegation process which provide more secured access rights to the authenticated users over the cloud that reduce the overhead.

2. Related Work

The access control and the data security of the data in the cloud is a major issue in recent years. Specially while storing, sharing and retrieving the data. In addition, the scalability, fine grained ness and the confidential data access control becomes danger to the cloud platform and its process. This paper [5] addresses these issues and come with the increasing data qualities with improving secured access policies. This proposed system allows the data owner to do computation in order to improve the fined grained access control where the data content in not visible to the servers where in the data is stored. In order to achieve all this, the decentralized key policy Attribute Based Encryption (KP-ABE) is exploited with highly secured and efficient data sharing and transmission.

The cloud computing environment has the ability of increasing flexibility, scalability, reducing cost and due to this qualities, the cloud computing becomes the hottest research area in recent years. It has many services such as providing information and software to the customers when needed. Even though the resources of the cloud are

distributed in nature, there may the chance of security problems. Therefore the paper [6] analyzes those problems regarding security in the cloud and presents a solution in the form of encryptionwith elliptic curve cryptography and digital signature.

Cloud Computing becomes more familiar technology in recent years and due to the facilities from the cloud, it has got more attention [7]. It improves the cloud platform in cost wise more than five times for consumer applications and more than four times for the business applications. This improvement lead to the efficient client/server model where the large volume of information saved and the files are utilized in the time sharing manner. This process can be made possible by combining the multiple cryptography algorithms.

The standard encryption scheme has the problem of decomposing the data over the cloud computing environment which leads to the security and confidentiality problem. Another most discussing problem is data sharing the access control and the privacy policies are concerned. In addition, the Key escrow is also the problem. Therefore the proposed system [8] provides the solution to the Key escrow problem by issuing the escrow-free key and the proxy encryption is used to provide the user revocation, communication between the data storing center and the key generation center via 2-way communication manner. The RBAC scheme makes the security analyses and the security performance much better by using the third party auditing.

The paper [9] takes a survey about the recent cryptographic techniques in order to protect the cloud storage data and also to access them. Nowadays the information used for the business and any other purpose are mostly stored in the cloud platform and can able to retrieve when needed. This movement of data brings the security issues and decrease the trust in the cloud environment for sharing data.Many researchers introduce new techniques for the purpose for data protection and access the data from remote place.

The cloud computing provides the web services based on the user needs. Cloud computing facilities and the knowledge form it can be used from any place, any time. It provides resilience, high reliability, scalability and cost effective. Therefore many business organizations are using these facilities in which it needs to improvise the protection about the users without accessing authority. Hence the paper [10] reviews different encryption algorithm, its issues, input and output files sizes, its performance comparison with the existing algorithms and each other.

3. Traditional Cloud Storage System

Data centers of different domains are distributed over the network called cloud storage system. These data centers in the cloud platform utilize the cloud computing facilities like virtualization, and render the connectivity for information storage. The information is stored in the cloud storage system via Cloud Service Provider (CSP) and security becomes a major issue while storing the sensitive information. The data to be stored in the cloud may infected by vulnerabilities like attacks. These attacks may be internal or external. The external attacks are introduced because of the security issues that may results in data thefts whereas the internal attacks occurs within the Cloud Storage Provider (CSP) itself [11]. In order to protect the data in the cloud in the event of attacks, the cloud storage system is constructed. Hence the message should be stored confidential in the cloud storage system, so the message are encrypted using some cryptographic methods and encode and store in the Cloud Storage System.

4. Proposed Cloud Storage System

The issues in the traditional cloud storage system and the provision of the confidential to the message in the cloud storage system become a major concern. Hence the threshold proxy re-encryption scheme is proposed along with the homomorphic encryption and the improved delegation mechanism in the cloud environment. The homomorphic encryption involves the operation on the encrypted message without decrypting it whereas Improved Delegation mechanism minimizes the data owner overhead and distribute the access rights over the cloud with proper authentication. The normal encryption and decryption process with the homomorphic property is as follows:

$$Encryption \rightarrow C = E(PK, m1)^{g1} \odot E(PK, m2)^{g2} = E(PK, m1^{g1}.m2^{g2}) \quad (1)$$

$$Decryption \rightarrow D\big(SK, E(PK, m1) \odot E(PK, m2)\big) = m1.m2 \quad (2)$$

Where, D is the decryption function, E is the encryption function, the two message symbols $m1$ and $m2$ are encoded with the coefficients $g1$ and $g2$ in order to get the code word symbol in $m1^{g1}m2^{g2}$ using the pair of private key (SK) and public key (PK).

Once the encrypted message is stored in the message server, the secret key also stored in the key server along with the threshold value referred as t. Initially the messages are divided into k messages symbols; encrypted and stored in the different message servers in the cloud storage system. The cloud storage system with highly secured storage and retrieval mechanism is illustrated in the following session.

Secured Cloud Storage System Using Threshold Proxy Re-Encryption Scheme

The proposed cloud storage system provides the access rights to the authenticated users over the cloud and this process is called as Improved Delegation Mechanism consisting of four stages of message storage and retrieval namely (1) *System Setup, (2) Data Storage, (3) Data Forwarding and finally (4) Data Retrieval.*

(1) System Setup: Initially the message m is divided into k blocks; encrypted and stored in the different servers and the corresponding keys are shared to the key servers considering the threshold t which should not below or equals the number of message blocks and should not be greater than the number of key servers. This stage just constructs the storage system where the basic three operations namely Setup(), KeyGen() and ShareKeyGen() are performed [12]. The Setup operator generates the system parameters. Then the Key Generation operator utilizes the generated system parameters and generates the private and public key. Finally the share the key generation operator attempts to share the private key to all the m key servers with the threshold.

(2) Data Storage: consider the message is created by the user A and is divided into k blocks such as $m1, m2, \dots, mk$. These message blocks are stored in the cloud storage system with the identifier ID. The user A calculates the identity token $\tau = h^{f(a_3, ID)}$ and encrypts the messages block with the identity token and receives the cipher texts of the message blocks as $C1, C2, \dots, Ck$. The encrypted message blocks are sent to the randomly chosen v storage message servers. All the encrypted message blocks are gathered in a single storage server along with the same identity token which is used for the representing the missing cipher texts [13]. Once the set of original cipher texts are gathered in a single server, the server does the encoding operation on the k cipher texts. The result of this encoding process is the code word symbol.

The encryption process of the set k original message blocks are as follows:

$$C_i = Enc\ (PK_A, \tau, m1, m2, \dots, mk) = \left(0, g^{r_i}, \tau, m_i e(g^{a1}, \tau^{r_i})\right) \quad (3)$$

for $1 \le i \le k$, where 0 represents the leading bit that represent the original cipher text.

The encoding process of the original cipher text C_i is as follows:

Choose the coefficient g_i randomly for each original cipher text C_i. If any cipher text is missing, then the identity token is used to represent the missing one and the coefficients for such missing cipher texts are taken as "0". The result of the encoded cipher text is termed as code word symbol C' which is calculated by using

$$C' = \left(0, \prod_{i=1}^{k}(\propto_i^{g_i}), \beta, \prod_{i=1}^{k}(\gamma_i^{g_i})\right) = (0, g^{r'}, \tau, We(g, \tau)^{a1 r'}) \quad (4)$$

Homomorphic encryption: the data stored in the storage server after the encryption and encoding process. Traditionally the data once encrypted, cannot be updated with any changes. If suppose the modification to the data is necessary, then the data have to be decrypted, modification is performed and again encrypted and stored in the server. But the homomorphic encryption modeled along with the threshold proxy re-encryption performs the changes in the encrypted message without decrypting it [14]. Therefore the system becomes more secure and the data owner alone knows the private key.

(3) Data Forwarding: once the data is message is encrypted, encoded and stored in the storage server, there may have the chance of either forwarding the data or retrieving the data [15]. Consider the user A, who stores the data on the cloud, forwards the message to user B. like the original message, the secret key also divided into components such as $SK = a1, a2, a3$ and stored in the different key servers. If the user A does not have the components of the corresponding secret key, then it asks all the key servers.

(i) The user A can get the key component of the message secret key SK_A using the algorithm called $KeyRecover(.)$. The $keyRecover(SK_{A,i_1}, SK_{A,i_2}, \dots, SK_{A,i_t})$. The algorithm utilizes the Lagrange interpolation in order to get the secret key component a_1 as follows:

$$a_1 = \sum_{s \in T}\left(f_{A,1}(s) \prod_{s' \in T/\{s\}} \frac{-s'}{s - s'}\right) mod\ p \quad (5)$$

(ii) The re-encryption key $RK_{A \to B}^{ID}$ is computed with the message identifier ID using the $ReKeyGen(.)$ algorithm as $ReKeyGen(PK_A, SK_A, ID, PK_B)$.

$$RK_{A \to B}^{ID} = \left((h^{b_2})^{a1(f(a3, ID)+e)}, h^{a_1 e}\right) \quad (6)$$

(iii) Then the algorithm $ReEnc(.)$ is used to re-encrypts the original code word symbol C''. This code word symbol has the leading bit $b = 1$. Let the C' computed in the data storage stage is represented as $C' = (0, \propto, \beta, \gamma)$ and the computed Re-encryption key is taken and the re-encrypted code word symbol is computed as follows:

$$C'' = \left(1, g^{r'}, h^{b_2 a1(f(a3, ID)+e)}, We(g, h)^{a1 r'(f(a_3, ID)+e)}\right) \quad (7)$$

(4) Data Retrieval: the data retrieval is possible during two situations either the user A wants to retrieve his own message stored in the storage server system or the user B wants to retrieve the message sent to it [16].

In the first case while the user A is in need of retrieving the message owned by him, the user A apprise the entire key servers along with the identity token. Then the original code word symbols are retrieved by a single key server from the randomly selected storage servers.

(i) The partially decryption operation $ShareDec(.)$ is performed on the retrieved original code word symbol and provides the partially decrypted code word symbol as follows:

$$C_{i,j} = (b, \propto, \beta, \beta^{sk_b}, \gamma) \quad (8)$$

Where $X_i = (b, \propto, \beta, \gamma)$ and is the code word symbol, the share key is SK_j and the partial decryption is termed as $ShareDec(SK_j, X_i)$.

(ii) Once the key servers send the partially decrypted code word symbols to the user A, then the $Combine(.)$ algorithm is performed on the partially decrypted code word in order to get/retrieve the original message blocks $m1, m2, \dots, mk$ as $Combine(C_{i1,j1}, C_{i2,j2}, \dots, C_{it,jt})$. Once the partially decrypted code words are combined, the identity token is computed through the Lagrange interpolation as:

$$\tau^{a_1} = \prod_{(i,j) \in S}\left(\left(\beta_{i,j}'\right)^{\prod_{r \in S, r \ne j} \frac{-j}{r-j}}\right) = \tau^{f_{A,1}(0)} \quad (9)$$

Using the identity token and the combined partially decrypted code word, the algorithm calculates the encoded block as follows:

$$\omega_i = \frac{\gamma_{i,j}}{\hat{e}\left(\alpha_{i,j}, \tau^{f_{A,1}(0)}\right)} \quad (10)$$

The obtained encoded block is $\omega_i = K$, in order to retrieve the original message (i.e.) the K^{-1} have to be computed, then output the blocks $m1, m2, \dots, mk$.

In the second case, if the message is send from user A to user B, then the user B wants to retrieve the message from the storage server. The encoded message will be:

$$\omega_i = \frac{\gamma_{i,j}}{\hat{e}\left(\alpha_{i,j}, h^{(f(a_3, ID)+e)a_1}\right)} \quad (11)$$

$$where, h^{(f(a_3,ID)+e)a_1} = \prod_{(i,j)\in S}\left(\left(\beta'_{i,j}\right)^{\prod_{r\in S_j, r\neq j}\frac{-j}{r-j}}\right) = h^{(f(a_3,ID)+e)a_1 b_2 f_{B,2}(0)} \quad (12)$$

The other steps in the second case are as same as in the first case.

Thus the message is decomposed into the cloud environment, stored over different cloud storage server and the successful retrieval process is performed with proper authentication using the Threshold Proxy Re-Encryption Scheme where the Improved Delegation mechanism and the homomorphic encryption is achieved through the efficiently implemented four step process.

5. Result Analysis

The proposed system consists of Threshold Proxy Re-Encryption Scheme incorporated with the Delegation and homomorphic encryption property. The data to be stored in the cloud platform is decomposed into different block and encrypted and stored in different servers in the cloud. During the data retrieval process, the data blocks from different servers are combined in a single server.

The figure 1 shows that the response time of the servers always maintains the moderate rate when the servers are increased.

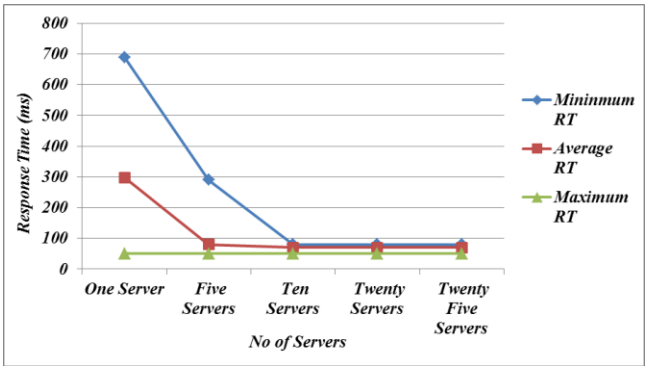

Fig 1 Servers' Response Time

The figure 2 shows that the data decomposed, and encrypted in different independent servers. This shows how much amount of data stored in the each server. For instances, two servers and four data are taken here.

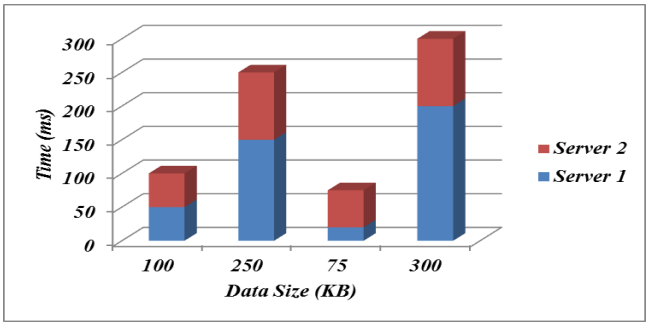

Fig 2 Data Decomposition Rate

Figure 3 shows the overall processing time required for the decomposing the data, storing in different servers, re-encryption process and finally retrieving. This figure shows that the processing time is considerably moderate even when the number of data stored in the cloud increases.

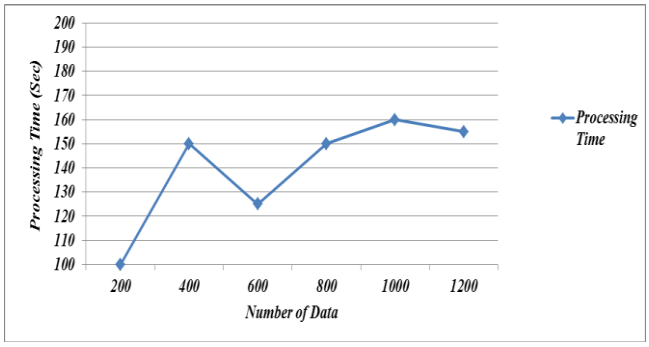

Fig 3 Overall Processing Time

6. Conclusion

In this paper the Threshold Proxy Re-Encryption Scheme is proposed with Improved Delegation mechanism and the homomorphic encryption as property that improves the storage and retrieval process of data over the cloud much easier and more efficient. The system model is emerged with two types of server namely key server and storage server. The Threshold Proxy Re-Encryption Scheme encodes the message, decompose it and store in the different independent servers. Then the second encryption process is performed while storing in the storage server and the corresponding secret/private keys are stored in the key servers. The dynamic changes in the stored encrypted data are done using the homomorphic property included in the encryption scheme where the arbitrary operations are performed on the encrypted data. The overall system is processed with the secured storage and retrieval of data in the decentralized cloud platform and the delegation mechanism is achieved by providing proper access rights to the users in the cloud.

References

[1] W. Sharon Inbarani, G. ShenbagaMoorthy, C. Kumar Charlie Paul, "An Approach for Storage Security in Cloud Computing- A Survey", International Journal of Advanced Research in Computer Engineering & Technology, Volume 2, Issue 1, ISSN: 2278 – 1323, pp. 174-179, January 2013.

[2] S.Amritha1, S.Saravana Kumar, "Secure Data Forwarding In Distributed Environment Using Cloud Storage System", International Journal Of Computational Engineering Research (ijceronline.com) Vol. 3 Issue. 3, ISSN: 2250-3005, pp. 267-271, March 2013.

[3] Chang-Ji Wang and Jian-FaLuo, "A Key-policy Attribute-based Encryption Scheme with Constant Size Ciphertext", Eighth International Conference on Computational Intelligence and Security, IEEE, pp.447-451, ISBN: 4673-4725, November 2012.

[4] Zhibin Zhou, Dijiang Huang and Zhijie Wang, "Efficient Privacy-Preserving Ciphertext-Policy Attribute Based-Encryption and Broadcast Encryption", IEEE

Transactions on Computers, Volume 64, Issue 1, ISSN: 0018-9340, pp. 126-138, December 2014.

[5] S.SeenuIropia and R.Vijayalakshmi, "Decentralized Access Control of Data Stored in Cloud Using Key Policy Attribute Based Encryption", International Journal of Inventions in Computer Science and Engineering, Volume 1 Issue 2, ISSN: 2348 – 3539, 2014.

[6] VeerrajuGampala, SrilakshmiInuganti, SatishMuppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography", International Journal of Soft Computing and Engineering (IJSCE) Volume-2, Issue-3, ISSN: 2231-2307, pp. 138-141, July 2012.

[7] Smith Jones, "Effective Algorithmic Approach for Cloud Security Based on Hash Cryptography", International Journal of Enterprise Computing and Business Systems, Volume 4, Issue 1, ISSN: 2230-8849, July 2014.

[8] M.Saranya and R.Vasuki, "Improving Data Security in KP-ABE With Third Party Auditing", International Journal of Inventions in Computer Science and Engineering, Volume 2, Issue 2, ISSN: 2348-3539, Feb 2015.

[9] LaurențiuBurduşel, "New Cryptographic Challenges in Cloud Computing Era", Proceedings of the Romanian Academy, Series A, Volume 14, Issue 1, pp. 72-77, 2013.

[10] Omer K. Jasim, Safia Abbas, El-Sayed M. El-Horbaty and Abdel-Badeeh M. Salem, "Efficiency of Modern Encryption Algorithms in Cloud Computing", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2, Issue 6, ISSN: 2278-6856, Dec 2013.

[11] Muhammad M. Monowarand Ebtesam A. Alomari, "A Survey of Security Issues for Data Sharing over Untrusted Cloud Providers", Journal of Emerging Trends in Computing and Information Sciences, Volume 5, Issue 8, ISSN: 2079-8407, pp. 609-619, August 2014.

[12] Priyadharshini. B, Carmel Mary Belinda and M. Ramesh Kumar, "A Secure Code Based Cloud Storage System Using Proxy Re-Encryption Scheme in Cloud Computing", Journal of Computer Engineering (IOSR-JCE), Volume 9, Issue 2, ISSN: 2278-8727, pp. 22-27, Feb 2013.

[13] S.Poonkodi, V.Kavitha and K.Suresh, "Providing a Secure Data Forwarding in Cloud Storage System Using Threshold Proxy Re-Encryption Scheme", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Special Issue 1, ISSN: 2250-2459, Jan 2013.

[14] R. Kanagavalli and Vagdevi S, "A Survey of Homomorphic Encryption Schemes in Cloud Data Storage", International Journal of Recent Development in Engineering and Technology, Volume 3, Issue 1, ISSN: 2347-6435, July 2014.

[15] SonaliA.Wanjari and Bharat Tidke, "Securely Data Forwarding and Maintaining Reliability of Data in Cloud Computing", Journal of Engineering Research and Applications, Volume 5, Issue 2, ISSN: 2248-9622, pp. 72-78, Feb 2015.

[16] J.Shyamala, D.Femila, and B.VinishaCathrineAntonus, "Automated Auditing and Logging Mechanism for Secure Data Storage in Cloud Using Proxy Re-encryption", International Journal of Advanced Research in Computer Engineering & Technology, Volume 2, Issue 3, ISSN: 2278 – 1323, March 2013.

[17] Kalaivany.S and Dr.T.Nalini ,"An Investigation on the Issues in Cloud Data Storage System with Secure Data Forwarding", International Journal of Computing, Communication and Information Security, Volume 6, Issue :3, ISSN:0976-1349, pp.106-117, July-Sep 2014.

Author Profile

Mrs. S.kalaivany Working as Assistant Professor in Mailam Engineering College, Mailam, Tamilnadu. She has 2 years of experience in Industry and 8 years of experience in academic fields. She completed her Bachelor of Technology (IT) in Pondicherry University and Master of Engineering (CSE) in Anna University Now, doing as Research Scholar in Vels University, Pallavaram, Chennai in the field of Computer Science. Her area of Interest includes Cloud Security. She has also life member for several association and society.

Dr.T.Nalini Working as a professor in Bharath University. She did her M.Tech (computer Science and Engineering) and PhD in Bharath University. She has received Master degree in Computer applications (MCA) in Madras University and also she has received M.Sc degree in Information Technology in Karnataka University. She has presented more than 75 papers in various national and international conferences. And she also published 70 papers in Scopus index and referred index journals.She is having Life member of many professional bodies like ISTE, CSI and IEEE, IAENG. She is also Technical advisor and Technical committee member for various international conferences.And she is also reviewer in WASET (World Applied Science in Engineering Technology) WASJ (World Applied Science Journal).