

EFFICIENT DECENTRALIZED ARCHITECTURE USING ABE SCHEME

A.Anitha¹, S.Mohan², S.Sugnaya Devi³, K. Amuthambigayin Sundari⁴, B.Manoharan⁵ and M. Jeganathan⁶

^{1,2,3,4}, Assistant Professor, Department of Electronics and Communication Engineering,
Nehru Institute of Technology, Coimbatore 641 105.

⁵, Professor (Tenure), PMIST, Vallam, Thanjavur.

⁶, Associate Professor, Designed Environment and Research Institute (DEAR Institute) Trichy- 621 213.
smohan2507@gmail.com jegann1978@gmail.com

ABSTRACT

In an open communication environment, such as internet, cloud, distributed systems, sensitive data must be encrypted prior to being transmitted. Encryption schemes are employed to protect confidentiality of sensitive data. However traditional encryption schemes cannot express complex access policy. Also the center must know all the public keys of the receiver. Decentralized attribute-based encryption (ABE) is an efficient encryption scheme and can express complex access structure. This scheme eliminates the heavy communication cost and the need for collaborative computation in the setup stage. Furthermore, every authority can join or leave the system freely without the necessity of re-initializing the system. In the existing system the system requires collaboration among multiple authorities to conduct the system setup and attributes of the user can be easily collected by tracing his GID (Global Identifier). In our system we are proposing a decentralized ABE scheme to protect the user's privacy by tying all his secret keys to his identifier thus resisting the collusion attack. In our system only authorized user can decrypt the data as the system is provided with strong Access Control. The protocol of the system is very flexible to operate and scalable with the growth of data sharers.

INTRODUCTION

In this paper a novel secure data service mechanism, to efficiently achieve both of the secrecy and access control of data has been adopted. Specifically, the dynamic user can securely shift the data computing and distribution overhead to the server while the server has no idea about data content in the whole process. Additionally only authorized users can decrypt the cipher text while unauthorized users would learn nothing about the data. In this project the overhead of communication for the data sharing is reduced to the size of a re-encryption key. This could greatly reduce the cost of the user side which is charged based on the size of communication system. (Manikandan et.al., 2016, Sethuraman et.al., 2016, Senthil Thambi et.al., 2016).

LITERATURE SURVEY

The complexity of encryption is just related the number of attributes associated. The data file, and is independent to the number of users in the system. It achieves high scalability and data confidentiality. It achieves fine grained access control. Not flexible in attribute management. Not

scalable in multiple levels of attributes [1]. Fine-grained access control where User access structure is able to describe sophisticated logics over attributes. Collusion resistance where each user's secret key has a unique secret sharing scheme. Secret keys from different users do not "match" each other. Not possible to assign multiple attributes to a single user, so flexibility is lost CP-ABE schemes that support numerical attributes (i.e., allow numerical comparisons in policies) are limited to assigning only one value to any given numerical attribute within a key [2]. The CP-ASBE scheme can be used by assigning multiple values to the group of attributes but in different sets. Using CP-ASBE, an efficient cipher text policy encryption scheme is obtained for several scenarios where existing CP-ABE scheme are insufficient. Single authority is responsible for all the user processes [3]. (Vasanthi and Jeganathan 2007, Vasanthi et.al., 2008, Raajasubramanian et.al., 2011, Jeganathan et.al., 2012, 2014 Sridhar et.al., 2012, Gunaselvi et.al., 2014, Premalatha et.al., 2015, Seshadri et.al., 2015, Shakila et.al., 2015, Ashok et.al., 2016, Satheesh Kumar et.al., 2016).

EXISTING SYSTEM

A central authority controls a user's access to sensitive data. Users are validated using their unique identities. Sender must know the public keys of the receiver. This scheme requires nonstandard complexity assumptions (eg: q-decisional Diffie-Hellman inversion) and interactions among multiple authorities. The system requires collaboration among multiple authorities to conduct the system setup. Attributes of the user can be collected by tracing his GID (Global Identifier)

Demerits: * Difficult task to manage numerous user identities. * User is totally dependent on the central authority. * Cannot express complex access policy. * Sender must know all the public keys of the receiver. * Multiple authorities must be online and setup the system interactively. * Heavy communication cost and the need for collaborative computation in the setup stage.

PROPOSED SYSTEM

We are proposing a privacy-preserving decentralized ABE scheme to protect the user's privacy using decisional bilinear Diffie-Hellman algorithm. In our scheme, all the user's secret keys are tied to his identifier to resist the collusion attacks while the multiple authorities do not know anything about the user's identifier. Each authority can join or leave the system freely without the need of reinitializing the system and there is no central authority. Any access structure can be expressed in our scheme using the access tree technique. Allow users to be validated by descriptive attributes instead of their unique identities. A user can share his data by specifying an access structure so that all the users whose attributes satisfy it can access the data without knowing their identities. Our scheme relies on the standard complexity assumptions by using privacy preserving extract protocol.

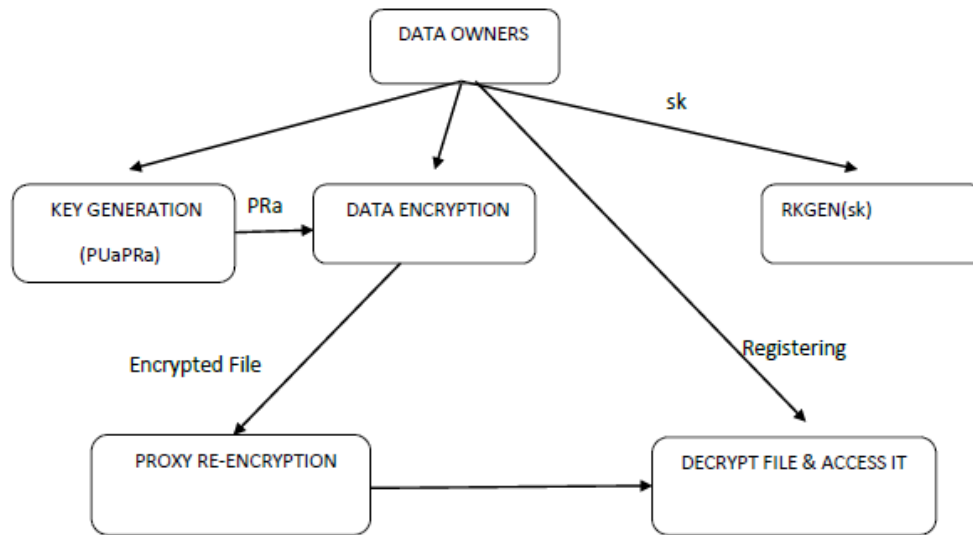


Fig 1: Proposed System

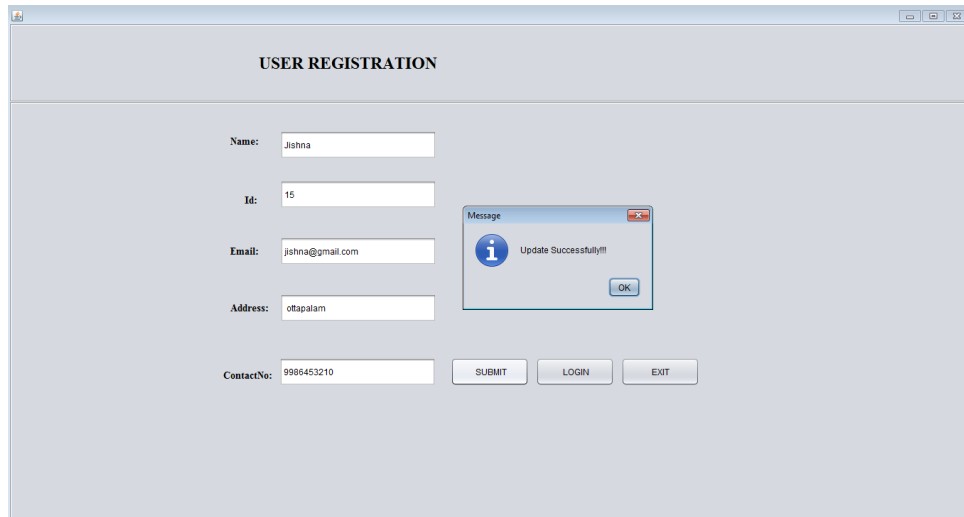
RESULTS AND DISCUSSION

This form is used to create a domain and register the domain in the system. It will get the Domain Name, Password, Email, Address and Contact No. from the user which helps the server to uniquely identify the Domain. While registering the Domain, the form validates whether the domain is already registered to the server or it is a new registration.

The screenshot displays the 'DOMAIN AUTHORITY REGISTRATION' web form. The form fields are filled with the following data: Name: swathy, Password: (masked), ConfirmPassword: (masked), Email: swa@gmail.com, Address: palakkad, and Mobile No: 9876543210. There are 'SUBMIT', 'LOGIN', and 'EXIT' buttons at the bottom. A central graphic shows three 3D figures holding a banner that reads 'WWW.CON.NET.ORG'. A small 'Message' dialog box is open in the bottom right corner, displaying an information icon and the text 'Update Successfully!!!' with an 'OK' button.

Fig 2: Domain Registration

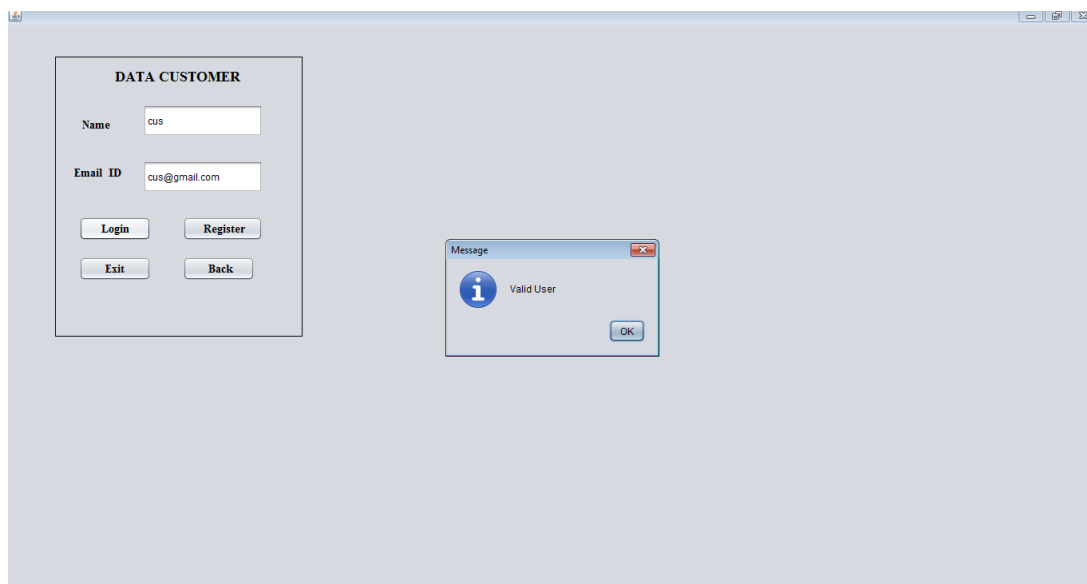
When Domain is accessed, new users are to be registered. For this we create a User registration form. It will get the user's Name, ID, Email, Address and Contact No. for registration. This form also validates while registering.



The screenshot displays a 'USER REGISTRATION' window. It contains five input fields: 'Name' (Jishna), 'Id' (15), 'Email' (jishna@gmail.com), 'Address' (ottapalam), and 'ContactNo' (9986453210). Below these fields are three buttons: 'SUBMIT', 'LOGIN', and 'EXIT'. A 'Message' dialog box is open, showing an information icon and the text 'Update Successfully!!!' with an 'OK' button.

Fig 3: User Registration

This form is used to register a new Data Customer using his Name and Email ID. In this stage a Secret Key is also provided to the customer.



The screenshot shows a 'DATA CUSTOMER' window. It has two input fields: 'Name' (cus) and 'Email ID' (cus@gmail.com). Below these are four buttons: 'Login', 'Register', 'Exit', and 'Back'. A 'Message' dialog box is open, displaying an information icon and the text 'Valid User' with an 'OK' button.

Fig 4: Data Customer Registration

In this form the customer is verified by the server for a valid customer.

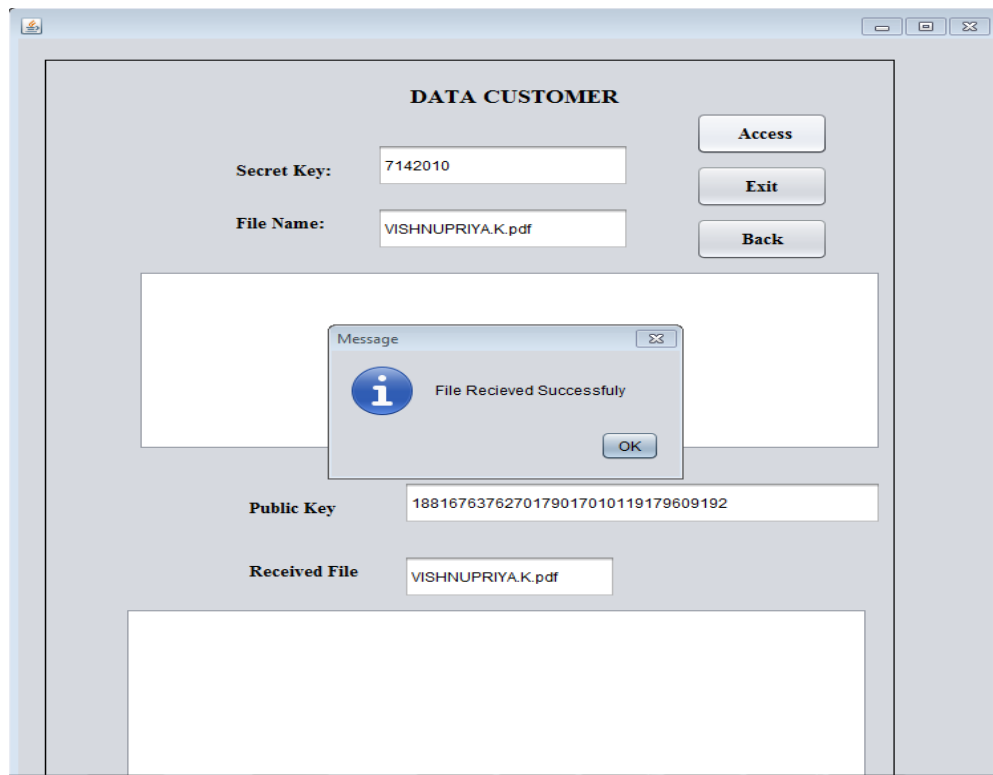


Fig 5: Data Customer Verification

Next the secret key is validated to confirm that the customer is already registered with the local host.

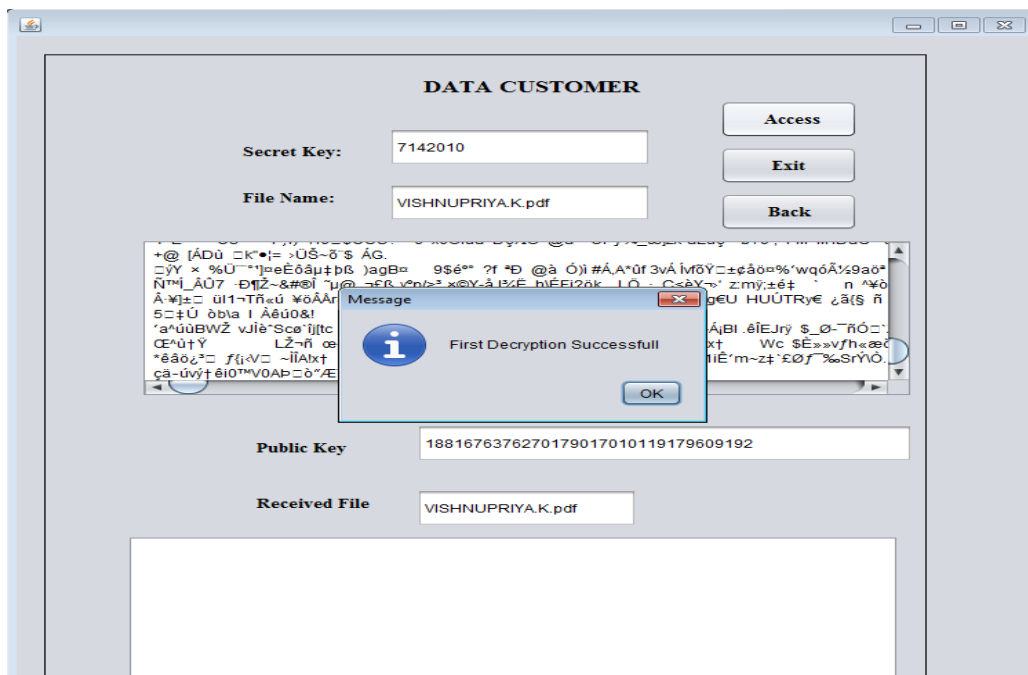


Fig 6: Secret Key Validation

Finally a decrypted file is received at the customer's end which is same as the sent file by the owner. Thus the file is transferred successfully.

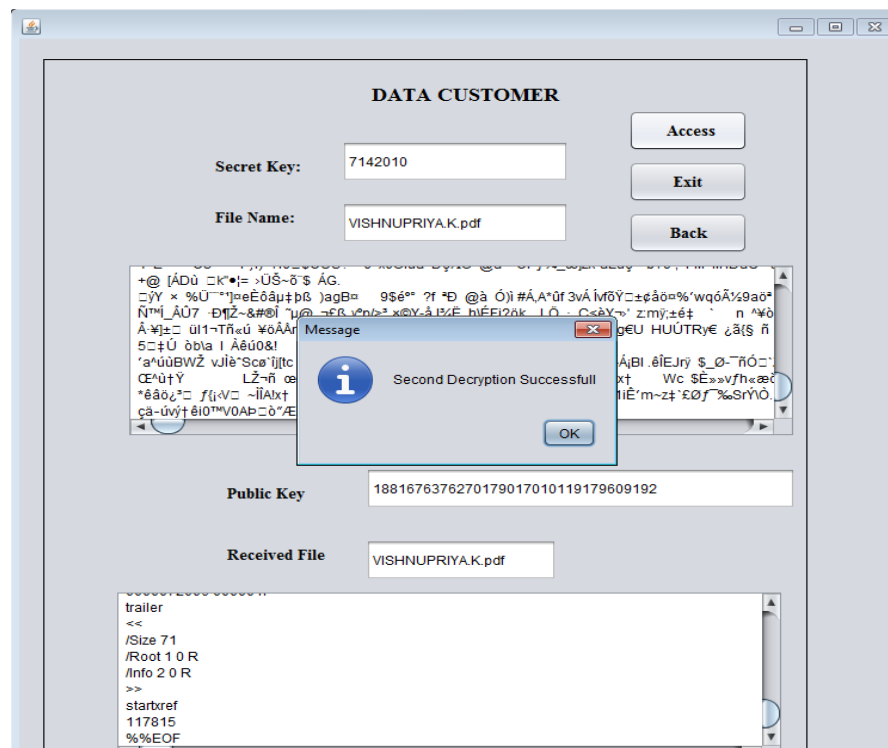


Fig 5: Receiving Decrypted File

CONCLUSION AND FUTURE WORK

The decentralized ABE scheme has attracted a lot of attention, because it can reduce the trust on merely a single centralized authority. In order to resist the collusion attacks in the decentralized ABE schemes, the global identifier GID is used to tie all the user's secret keys from multiple authorities together. However, this will risk the user being traced and impersonated by the corrupted authorities. In this paper, we proposed a privacy-preserving decentralized ABE scheme to protect the user's privacy. In our scheme, all the user's secret keys are tied to his identifier to resist the collusion attacks while the multiple authorities cannot know anything about the user's identifier. Notably, each authority can join or leave the system freely without the need of reinitializing the system and there is no central authority. Furthermore, any access structure can be expressed in our scheme using the access tree technique. Finally, our scheme relies on the standard complexity assumption (e.g., DBDH), rather than the non-standard complexity assumptions (e.g., DDHI). A conjunctively combined scheme between key policy and cipher text

policy attribute based encryption are the previous available types of attribute based encryption. It allows simultaneously to access control mechanism over encrypted data.

Involves policies over objective attributes ascribed to data. Other involves policies our subject attribute ascribed to user credentials. Previous two type of attribute based encryption can only allow either functionality one at a time. This can be implemented more efficiently.

REFERENCES

- [1] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute- based encryption and (hierarchical inner product encryption," in Proceedings: Advances in Cryptology EUROCRYPT'10 (H. Gilbert:, ed.), vol. 6110, Springer, May 30 - June 3 2010.
- [2] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, J. Bethencourt, A. Sahai, and B. Waters, "Cipher text-policy attribute-based encryption," in Proceedings: IEEE Symposium on Security and Privacy (S & P'07), (Oakland, California, USA), pp. 321–34, IEEE, May 20-23 2007.
- [3] D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, Efficient and provably secure realization," in Proceedings:Public Key Cryptography - PKC'11, vol. 6571, March 6-9 2011.
- [4] Jinguang Han, Willy Susilo, Yi Mu and Jun Yan, "Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption", in Proceedings: IEEE Transactions on Parallel and Distributed Systems VOL.23 NO.11 2012.
- [5] J. Camenisch, M. Kohlweiss, A. Rial, and C. Sheedy, "Blind and anonymous identity-based encryption and authorised private searches on public key encrypted data," in Proceedings: Public Key Cryptography - PKC'09 (S. Jarecki and G. Tsudik, eds.), vol. 5443 of March 18-20 2009.
- [6] J. Li, Q. Huang, X. Chen, S. S. M. Chow, D. S. Wong, and D. Xie, "Multi authority cipher text-policy attribute-based encryption with accountability," in Proceedings: ACM Symposium on Information, Computer and Communications Security-ASIACCS'11, pp. 386–390, ACM, 2011.
- [7] Lewko and B. Waters, "Decentralizing attribute - based encryption," in Proceedings: Advances in Cryptology-EUROCRYPT'11.
- [8] M. Green and S. Hohenberger, "Blind identity-based encryption and simulatable oblivious transfer," in Proceedings: Advances in Cryptology ASIACRYPT'07 (K. Kurosawa, ed.), vol. 4833, December 2-6 2007.
- [9] N. Attrapadung and H. Imai, "Dual-policy attribute based encryption," in Proceedings: Applied Cryptography and Network Security-ACNS'09 (M. Abdalla, D. Pointcheval, P.-A. Fouque, and D. Vergnaud, eds.), June 2-5 2009.

- [10] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute- based encryption with non-monotonic access structures," in Proceedings: ACM Conference on Computer and Communications Security-CCS'07, (Alexandria, Virginia, USA), pp. 195–203, ACM, October 28-31 2007.
- [11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings: ACM Conference on Computer and Communications Security-CCS'06, (Alexandria, VA, USA), pp. 89–98, ACM, October 30-November 3 2006.
- [12] Vasanthi M and M. Jeganathan. 2007. Ambient air quality in terms of NO_x in and around Ariyalur, Perambalur DT, Tamil Nadu. Jr. of Industrial pollution Control., 23(1):141-144.
- [13] Vasanthi. M ,A.Geetha, M. Jeganathan,and A.Anitha. 2007. A study on drinking water quality in Ariyalur area. J.Nature Environment and Pollution Technology. 8(1):253-256.
- [14] Ramanathan R ,M. Jeganathan, and T. Jeyakavitha. 2006. Impact of cement dust on azadirachtain dicaleaves – a measure of air pollution in and Around Ariyalur. J. Industrial Pollution Control. 22 (2): 273-276.
- [15] Vasanthi M and M. Jeganathan. 2007. Ambient air quality in terms of NO_x in and around Ariyalur, Perambalur DT, Tamil Nadu. Pollution Research., 27(1):165-167.
- [16] Vasanthi M and M. Jeganathan. 2008. Monitoring of air quality in terms of respirable particulate matter – A case study. Jr. of Industrial pollution Control., 24(1):53 - 55.
- [17] Vasanthi M, A.Geetha, M. Jeganathan, and M. Buvaneswari. 2008. Phytoremediation of aqueous dye solution using blue devil (*Eichhornia crassipes*). J. Current Science. 9 (2): 903-906.
- [18] Raajasubramanian D, P. Sundaramoorthy, L. Baskaran, K. Sankar Ganesh, AL.A. Chidambaram and M. Jeganathan. 2011. Effect of cement dust pollution on germination and growth of groundnut (*Arachis hypogaea* L.). IRMJ-Ecology. International Multidisciplinary Research Journal 2011, 1/1:25-30 : ISSN: 2231-6302: Available Online: <http://irjs.info/>.
- [19] Raajasubramanian D, P. Sundaramoorthy, L. Baskaran, K. Sankar Ganesh, AL.A. Chidambaram and M. Jeganathan. 2011. Cement dust pollution on growth and yield attributes of groundnut. (*Arachis hypogaea* L.). IRMJ-Ecology. International Multidisciplinary Research Journal 2011, 1/1:31-36.ISSN: 2231-6302. Available Online: <http://irjs.info/>
- [20] Jeganathan M, K. Sridhar and J.Abbas Mohaideen. 2012. Analysis of meteorological conditions of Ariyalur and construction of wind roses for the period of 5 years from January 2002. J.Ecotoxicol.Environ.Monit., 22(4): 375-384.
- [21] Sridhar K, J.Abbas Mohaideen M. Jeganathan and P Jayakumar. 2012. Monitoring of air quality in terms of respirable particulate matter at Ariyalur, Tamilnadu. J.Ecotoxicol.Environ.Monit., 22(5): 401-406.

- [22] Jeganathan M, K Maharajan C Sivasubramaniyan and A Manisekar. 2014. Impact of cement dust pollution on floral morphology and chlorophyll of heilianthus annus plant – a case study. J.Ecotoxicol.Environ.Monit., 24(1): 29-34.
- [23] Jeganathan M, C Sivasubramaniyan A Manisekar and M Vasanthy. 2014. Determination of cement kiln exhaust on air quality of ariyalur in terms of suspended particulate matter – a case study. IJPBA. 5(3): 1235-1243. ISSN:0976-3333.
- [24] Jeganathan M, S Gunaselvi K C Pazhani and M Vasanthy. 2014. Impact of cement dust pollution on floral morphology and chlorophyll of heilianthus annus.plant a case study. IJPBA. 5(3): 1231-1234. ISSN:0976-3333.
- [25] Gunaselvi S, K C Pazhani and M. Jeganathan. 2014. Energy conservation and environmental management on uncertainty reduction in pollution by combustion of swirl burners. J. Ecotoxicol. Environ.Monit., 24(1): 1-11.
- [26] Jeganathan M, G Nageswari and M Vasanthy. 2014. A Survey of traditional medicinal plant of Ariyalur District in Tamilnadu. IJPBA. 5(3): 1244-1248. ISSN:0976-3333.
- [27] Premalatha P, C. Sivasubramanian, P Satheeshkumar, M. Jeganathan and M. Balakumari.2015. Effect of cement dust pollution on certain physical and biochemical parameters of castor plant (ricinus communis). IAJMR.1(2): 181-185.ISSN: 2454-1370.
- [28] Premalatha P, C. Sivasubramanian, P Satheeshkumar, M. Jeganathan and M. Balakumari.2015. Estimation of physico-chemical parameters on silver beach marine water of cuddalore district. Life Science Archives. 1(2): 196-199.ISSN: 2454-1354.
- [29] Seshadri V, C. Sivasubramanian P. Satheeshkumar M. Jeganathan and Balakumari.2015. Comparative macronutrient, micronutrient and biochemical constituents analysis of arachis hypogaea. IAJMR.1(2): 186-190.ISSN: 2454-1370.
- [30] Seshadri V, C. Sivasubramanian P. Satheeshkumar M. Jeganathan and Balakumari.2015. A detailed study on the effect of air pollution on certain physical and bio chemical parameters of mangifera indica plant.Life Science Archives. 1(2): 200-203.ISSN: 2454-1354.
- [31] Shakila N, C. Sivasubramanian, P. Satheeshkumar, M. Jeganathan and Balakumari.2015. Effect of municipal sewage water on soil chemical composition- A executive summary. IAJMR.1(2): 191-195.ISSN: 2454-1370.
- [32] Shakila N, C. Sivasubramanian, P. Satheeshkumar, M. Jeganathan and Balakumari.2015. Bacterial enumeration in surface and bottom waters of two different fresh water aquatic eco systems in Ariyalur, Tamillnadu. Life Science Archives. 1(2): 204-207.ISSN: 2454-1354.
- [33] Ashok J, S. Senthamil kumar, P. Satheesh kumar and M. Jeganathan. 2016. Analysis of meteorological conditions of ariyalur district. Life Science Archives. 2(3): 579-585.ISSN: 2454-1354. DOI: 10.21276/lsa.2016.2.3.9.

- [34] Ashok J, S. Senthamil Kumar, P. Satheesh Kumar and M. Jeganathan. 2016. Analysis of meteorological conditions of cuddalore district. IAJMR.2 (3): 603-608.ISSN: 2454-1370. DOI: 10.21276/iajmr.2016.2.3.3.
- [35] Satheesh Kumar P, C. Sivasubramanian, M. Jeganathan and J. Ashok. 2016. South Indian vernacular architecture -A executive summary. IAJMR.2 (4): 655-661.ISSN: 2454-1370. DOI: 10.21276/iajmr.2016.2.3.3.
- [36] Satheesh Kumar P, C. Sivasubramanian, M. Jeganathan and J. Ashok. 2016. Green buildings - A review. Life Science Archives. 2(3): 586-590.ISSN: 2454-1354. DOI: 10.21276/lsa.2016.2.3.9.
- [37] Satheesh Kumar P, C. Sivasubramanian, M. Jeganathan and J. Ashok. 2016. Indoor outdoor green plantation in buildings - A case study. IAJMR.2 (3): 649-654.ISSN: 2454-1370. DOI: 10.21276/iajmr.2016.2.3.3.
- [38] Manikandan R, M. Jeganathan, P. Satheesh Kumar and J. Ashok. 2016. Assessment of ground water quality in Cuddalore district, Tamilnadu, India. Life Science Archives. 2(4): 628-636.ISSN: 2454-1354. DOI: 10.21276/lsa.2016.2.3.9.
- [39] Manikandan R, M. Jeganathan, P. Satheesh Kumar and J. Ashok. 2016. A study on water quality assessment of Ariyalur district, Tamilnadu, India. IAJMR.2 (4): 687-692.ISSN: 2454-1370. DOI: 10.21276/iajmr.2016.2.3.3.
- [40] Sethuraman G, M. Jeganathan, P. Satheesh Kumar and J. Ashok. 2016. Assessment of air quality in Ariyalur, Tamilnadu, India. Life Science Archives. 2(4): 637-640.ISSN: 2454-1354. DOI: 10.21276/lsa.2016.2.3.9.
- [41] Sethuraman G, M. Jeganathan, P. Satheesh Kumar and J. Ashok. 2016. A study on air quality assessment of Neyveli, Tamilnadu, India. IAJMR.2 (4): 693-697.ISSN: 2454-1370. DOI: 10.21276/iajmr.2016.2.3.3.
- [42] Malarvannan J, C. Sivasubramanian, R. Sivasankar, M. Jeganathan and M. Balakumari. 2016. Shading of building as a preventive measure for passive cooling and energy conservation – A case study. Indo – Asian Journal of Multidisciplinary Research (IAJMR): ISSN: 2454-1370. Volume – 2; Issue - 6; Year – 2016; Page: 906 – 910. DOI: 10.21276.iajmr.2016.2.6.10.
- [43] Malarvannan J, C. Sivasubramanian, R. Sivasankar, M. Jeganathan and M. Balakumari. 2016. Assessment of water resource consumption in building construction in tamilnadu, India. Life Science Archives (LSA) ISSN: 2454-1354 Volume – 2; Issue - 6; Year – 2016; Page: 827 – 831 DOI: 10.21276/lsa.2016.2.6.7.
- [44] Sivasankar R, C. Sivasubramanian, J. Malarvannan, M. Jeganathan and M. Balakumari. 2016. A Study on water conservation aspects of green buildings. Life Science Archives (LSA),ISSN: 2454-1354. Volume – 2; Issue - 6; Year – 2016; Page: 832 – 836, DOI: 10.21276/lsa.2016.2.6.8.
- [45] Ashok J , S. Senthamil Kumar , P. Satheesh Kumar and M. Jeganathan. 2016. Analysis and design of heat resistant in building structures. Life Science Archives (LSA), ISSN:

2454-1354. Volume – 2; Issue - 6; Year – 2016; Page: 842 – 847. DOI:
10.21276/lsa.2016.2.6.10.