IMPROVED INTRUSION DETECTION MODEL USING DECISION SUPPORT SYSTEM IN DATA ENGINEERING

K.Arunpatrick[1], R.Amutha[2], R.Gowrishankar[3], Shreedharan M.D[4] and Jeganathan M[5]

Assistant Professor, Department of Computer Science and Engineering, Nehru Institute of Technology, Coimbatore.

[4]Associate Professor, Excel College of Architecture & Planning, Komarapalayam, Tamil Nadu.

[5]Assistant Professor, Department of Environment and Herbal Sciences, Tamil University, Thanjavur, Tamil Nadu.

jegann1978@gmail.com

Abstract

   The fundamental goal of this paper is to build up a verified logging as an administration in cloud design. So in the proposed strategy, protection and safeguarding techniques are upgraded. The verified logging contains six noteworthy functionalities to guarantee more securities: Correctness, Confidentiality, information logs, Privacy and Preservation. The rightness manages accuracy information of the genuine history. Classification manages delicate data not showing amid inquiry. Information logs manages the information history for recognizing fitting clients. Security plot manages document connecting and information get to history. Conservation manages upgraded shading code. Lastly VPS manages the intermediary server for virtual information get to. The usage of the above given techniques are appeared any condition, which manages enormous number of information with numerous clients. There are very little contrast among programmers and interlopers in the cloud engineering. Programmers are from different systems mean while interlopers are from same systems. Programmers can be maintained a strategic distance from and interlopers are can't be stayed away from. This is on the grounds that interlopers may know about the system where they will interfere. So that verified logging as an administration is much essential for all sort of cloud server condition so as to give appropriate login to approved client and triggers out the unapproved clients.

Keywords: Secured Logging, Decision support system, security, Information logs, intruder, hacker.

Introduction:

                  Cloud security architecture is effective only if the correct defensive implementations are in place. Efficient cloud security architecture should recognize the issues that will arise with security management. The security management addresses these issues with security controls. These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. While there are many types of controls behind cloud security architecture, they can usually be found in one of the following categories:

A) **Deterrent Controls:** These controls are set in place to prevent any purposeful attack on a cloud system. Much like a warning sign on a fence or a property, these controls do not reduce the actual vulnerability of a system.

B) **Preventative Log Control :** These controls upgrade the strength of the system by managing the vulnerabilities. The preventative control will safeguard vulnerabilities of the system. If an attack were to occur, the preventative log controls are in place to cover the attack and reduce the damage and violation to the system's security.

C) Corrective log Controls : Corrective log controls are used to reduce the effect of an attack. Unlike the preventative controls, the corrective controls take action as an attack is occurring.

D) Detective log Controls : Detective log controls are used to detect any attacks that may be occurring to the system. In the event of an attack, the detective control will signal the preventative or corrective log controls to address the issue.

Related Works:

We define the forward integrity security property, motivate its appropriateness as a systems security requirement, and demonstrate designs that achieve this property. Applications include secure audit logs (e.g., syslogd data) for intrusion detection or accountability, communications security, and authenticating partial results of computation for mobile agents [1]. The need for secure logging is well-understood by the security professionals, including both researchers and practitioners [1]. The ability to efficiently verify all (or some) log entries is important to any application employing secure logging techniques. In this paper, we begin by examining state-of-the-art in secure logging and identify some problems inherent to systems based on trusted third-party servers [2]. Unix systems in many cases record personal data in log files. We present tools that help in practice to retrofit privacy protection into existing Unix audit systems [3]. This paper gives a short overview on the currently existing technical solutions for anonymous communication. The problem of anonymous communication is defined, and its basic solution is described [4]. Many security systems, whether they protect privacy, secure electronic-commerce transactions, or use cryptography for something else, do not directly prevent fraud [5]. The popular application Tripwire keeps cryptographic fingerprints of all files on a computer, allowing administrators to detect when attackers compromise the system and modify important system files [6]. (Vasanthy and Jeganathan 2007, Vasanthy 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).

Methodology

Properties of Secure Logging as A Service

Secure log the board administration dependent on the distributed computing worldview. We will thusly investigate our system against these properties.

A)Rightness: Log information is helpful just on the off chance that it reflects genuine history of the framework at the season of log age. The put away log information ought to be right, that is, it ought to be actually equivalent to the one that was created. B)Undeniable nature: It must be conceivable to watch that all sections in the log are available and have not been modified. Every passage must contain enough data to check its realness autonomous of others. On the off chance that a few passages are modified or erased, the capacity to independently confirm the rest of the sections (or squares of sections) makes it conceivable to recuperate some valuable data from the harmed log. In addition, the individual sections must be connected together such that makes it conceivable to decide if any passages are absent. C)Privacy: Log records ought not be calmly perused capable or accessible to assemble delicate data. Genuine inquiry access to clients, for example, reviewers or framework chairmen ought to be permitted. Moreover, since nobody can keep an assailant who has com-

guaranteed the logging framework from getting to delicate data that the framework will put in future log passages, the objective is to shield the pre bargained log records from privacy breaks. D)Security: Log records ought not be calmly discernible or linkable to their sources amid travel and away. (Manikandan et.al., 2016, Sethuraman et.al., 2016, Senthil Thambi et.al., 2016, Ashok et.al., 2018, Senthilkumar et.al., 2018).

Gaussian Mixture and Keystroke

Distributed computing security is a developing sub-space of PC security, arrange security, and, all the more comprehensively, data security. It alludes to a wide arrangement of strategies, advances, and controls conveyed to ensure information, applications, and the related foundation of distributed computing.

The strategy utilized here for security is keystroke logging. This permits just the correct client to login at the ideal time. It is the activity of following the keys struck on a console, with the goal that the individual utilizing the console is unconscious that their activities are being observed. At whatever point a client is made, the keystroke time of composing his/her secret word ought to be noted. At the point when a client logins to sends subtleties, the keystroke time for composing his/her secret phrase should matches with the time that is produced in the client creation. So this will gives a well security to the client's id and secret phrase from programmers.

Working with Gaussian Mixture and Keystroke:

The working of Gaussian Mixture and Keystroke dependent on the console input given by the client

These qualities are determined into 3 esteems, specifically

• Mean Value

• Actual Value

• Median Value

In the event of the key stroke esteem said to be 3.76: Mean esteem will be lesser than the genuine esteem, the esteem will be 3.75 or 3.76. The genuine qualities will a similar esteem. The middle will be expanded from the genuine esteem; the esteem will be 3.76 or 3.77. Empowering high security should be possible by the real esteem as it were.

Proposed Design

According to the Output Design most of the functions are based on the input design. The output design is mainly focused in the proper output calculation and process done in the backend and the data's stored in the database which can be notified by the screen.

Output Warnings:

- Invalid username and Password

- Invalid IP address

- Invalid file name

- Invalid date

- Invalid colour code

- Invalid keystroke

Most of the output has been shown in the data grid format. This is because, grid shows all the output at a same time. For the admin side, to show the output, graphs and charts are used. Through the chart admin can easily identify the output. In case of unauthorized user trying to login, a warning message will appear on the admin's home page screen. Admin can unblock the warning through the output design. According to the colour code totally 12 to 16 colours are displayed. Each colour is designed using colour patterns. And Selecting a colours will generate an equivalent sequential code value. The code is the identity of the selected colour value. For Gaussian mixture and keystroke an internal timer has been generated. The timer enables when the text box gets focused. And the timer stops when the text box lost the focus. The interval time has been taken in seconds. That is the keystroke value of the user. The properly formatted grids are generated wherever it is needed and in the screens where ever it is needed the report grid are prompted on the screens.

Last accessed Login Date	Last Uploaded data	Last accessed system IP	Accessing person	Percentage
✓	✓	✓	Intruder	80% Intruder
✕	✕	✕	Hacker	80% Hacker
✕	✓	✓	Intruder	60% Intruder
✕	✓	✕	Intruder	40% Intruder
✕	✕	✓	Intruder	40% Intruder

			Hacker	60% Hacker

Algorithm Used – Secured Login Service

- Initiating function f(x,y),
- $x = (x_1, ..., x_d)^T$
- Generating values for stroke x_i (i = 1, 2, ..., n)
- Values for disorder I_i at x_i is determined by $f(x_i)$
- Define light absorption coefficient γ
- while (t <max generation),
- for i=1: n all n keystroke
- for j =1 : i all n c1,c2,c3
- if<I_j >I_i),
- Move stroke i towards j in d-dimension; end if
- Attractiveness varies with distance r via exp[−γr]
- Evaluate new solutions and update light intensity
- end for j
- end for i
- Rank the login and find the current best
- end while
- Post process results and visualization

Result and Discussion
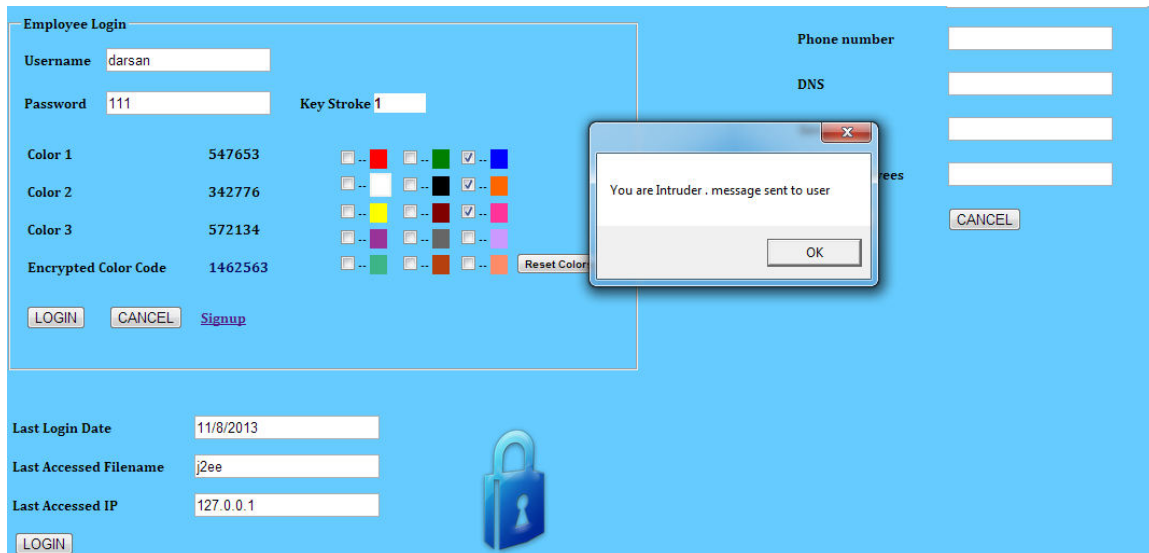
The above mention screen shot is the security screen; here the application is tested with various data input.

Accessed Filename	Accessed ip	Member
aaa	12	Hacker
applets	127.0.0.1	Intruder
applets	127.0.0.1	Intruder
qqq	13221	Hacker
c#.net	127.0.0.1	Intruder

The Above mention table shows the various types of users

Conclusion

Thus we are concluding that all the result obtained according to the committed abstract. In this paper, we consider a cloud storage system consists of storage servers and key servers. We integrate a newly proposed threshold encryption scheme and codes over exponents. The encryption scheme supports encoding, forwarding, and partial decryption operations in a distributed way. To decrypt a message of k blocks that are encrypted and encoded ton code word symbols, each key server only has to partially decrypt two codeword symbols in our system. By using the threshold proxy re-encryption scheme, we present a secure cloud storage system that provides secure data storage and secure data forwarding functionality in a decentralized structure. Moreover, each storage server independently performs encoding and re-encryption and each key server independently perform partial decryption. Our storage system and some newly proposed content addressable file systems and storage systems are highly compatible. Our storage servers act as storage nodes in a content addressable storage system for storing content addressable blocks. Our key servers act as access nodes for providing a front-end layer such as a traditional file system interface. Further study on detailed cooperation is required.

Reference

[1]   U. Flegel, "Pseudonymizing unix log file," inProc. Int. Conf. Infrastru-ture Security, LNCS 2437. Oct. 2002, pp. 162–179.

[2]   C. Eckert and A. Pircher, "Internet anonymity: Problems and solutions," in Proc. 16th IFIP TC-11 Int. Conf. Inform. Security, 2001, pp. 35–50 .

[3]   M. Rose, The Blocks Extensible Exchange Protocol Core, Request for Comment RFC 3080, Internet Engineering Task Force, Network Working Group, Mar. 2001.

[4]   B. Schneier and J. Kelsey, "Security audit logs to support computer forensics," ACM Trans. Inform. Syst. Security, vol. 2, no. 2, pp. 159– 176, May 1999.

[5]   J. E. Holt, "Logcrypt: Forward security and public verification for secure audit logs," inProc. 4th Australasian Inform. Security Workshop, 2006, pp. 203–211.

[6]   R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," inProc. 12th Ann. USENIX Security Symp., Aug. 2004, pp. 21–21.

[7]   The Tor Project, Inc. (2011, Sep.) Tor: Anonymity Online [Online]. Available: http://www.torproject.org

[8]   D. Dolev and A. Yao, "On the security of public key protocols," IEEE Trans. Inform. Theory, vol. 29, no. 2, pp. 198–208, Mar. 1983.

[9]   A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[10]   G. R. Blakley, "Safeguarding cryptographic keys," inProc. Nat. Comput. Conf., Jun. 1979, p. 313.

[11]   Vasanthy M and M. Jeganathan. 2007. Ambient air quality in terms of NOx in and around Ariyalur, Perambalur DT, Tamil Nadu. Jr. of Industrial pollution Control., 23(1):141-144.

[12]   Vasanthy. 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.

[13]   Ramanathan R ,M. Jeganathan, and T. Jeyakavitha. 2006. Impact of cement dust on azadirachtain dicaleaves – ameasure of air pollution in and Around Ariyalur. J. Industrial Pollution Control. 22 (2): 273-276.

[14] Vasanthy M and M. Jeganathan. 2007. Ambient air quality in terms of NOx in and around Ariyalur, Perambalur DT, Tamil Nadu. Pollution Research., 27(1):165-167.

[15] Vasanthy 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.

[16] Vasanthy 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.

[17] 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/.

[18] 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/

[19] Jeganathan M, K. Sridhar and J.Abbas Mohaideen. 2012. Analysis of meterological 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.

[20] 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.

[21] Jeganathan M, K Maharajan C Sivasubramaniyan and A Manisekar. 2014. Impact of cement dust pollution on floral morphology and chlorophyll of *healianthus annus* plant – a case study. J.Ecotoxicol.Environ.Monit., 24(1): 29-34.

[22] 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.

[23] Jeganathan M, S Gunaselvi K C Pazhani and M Vasanthy. 2014. Impact of cement dust pollution on floral morphology and chlorophyll of *healianthus annus*.plant a case study. IJPBA. 5(3): 1231-1234. ISSN:0976-3333.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] 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.

[38] 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.

[39] 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.

[40] 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.

[41] Senthil Thambi J, C. Sivasubramanian and M. Jeganathan. 2018. Ambient Air quality monitoring in terms of (Nitrogen di oxide in and around Ariyalur District, Tamilnadu, India. IAJMR.4 (3): 1414-1417.ISSN: 2454-1370. DOI: 10.22192/iajmr.2018.4.3.2.

[42] Senthil Thambi J, C. Sivasubramanian and M. Jeganathan. 2018. Study of Air pollution due to vehicle emission in Ariyalur District, Tamilnadu, India. Life Science Archives. 4(4): 1409-1416.ISSN: 2454-1354. DOI: 10.22192/lsa.2018.4.4.3.

[43]   Ashok J, S.Senthamil kumar, P.Satheesh kumar and M.Jeganathan. 2018. Estimation of Cement kiln exhaust on Air quality of Ariyalur in terms of suspended particulate matter - A Case Study. International Journal Of Civil Engineering And Technology. 9 (12): Scopus Indexed Journal ISSN: 0976 – 6316.

[44]   Ashok J, S.Senthamil kumar, P.Satheesh kumar and M.Jeganathan.2018. Air quality assessment of Neyveli in Cuddalore District, Tamilnadu, India. International Journal Of Civil Engineering And Technology. 9 (12): Scopus Indexed Journal ISSN: 0976 – 6316.

[45]   Senthilkumar M, N. Nagarajan, M. Jeganathan and M. Santhiya. 2018. Survey of Medicinal Plants diversity on Bodha Hills in Salem District, Tamil Nadu, India. Indo – Asian Journal Of Multidisciplinary Research (IAJMR) ISSN: 2454-1370.

[46]   Senthilkumar M, N. Nagarajan, M. Jeganathan and M. Santhiya. 2018. Survey of Traditional Medicinal Plants in and around Ariyalur in TamilNadu, India. Life Science Archives (LSA) ISSN: 2454-1354. DOI: 10.22192/lsa.2018.4.6.5.

[47]   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.

[48]   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.

[49]   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.

[50]   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.