NOVEL INTRUSION DETECTION SYSTEM BASED ON PARTICLE SWARM OPTIMIZATION ALGORITHM WITH EXTREME LEARNING MACHINE

Devendra Singh, GGV, Bilaspur (C.G.), INDIA (devendra.singh170@gmail.com)
Manish Shrivastava**,** GGV, Bilaspur (C.G.), INDIA (manbsp@gmail.com)

ABSTRACT

As the complexity of the network is increasing day by day along with the benefits we are getting there are also a lot of complexities involved with it, so there is a need for the study of Intrusion Detection System. The present category of Intrusion Detection Systems are however good but there are problems regarding performance and time. So we study the Intrusion Detection System Based on Particle Swarm Optimization algorithm and extreme learning machine which effectively reduces the total cost of time and gives efficient output. Lots of worked done in the field of the intrusion detection system. The main focus of our paper develops the hybrid model of PSO-ELM with feature selection. Result of our model is 99.7% accurate.

KEYWORDS: Intrusion Detection System, Particle Swarm Optimization, Features optimization, Extreme Learning Machine.

INTRODUCTION

In the past few years due to the increased complexities of the networks there raised many security issues. By the reports of Computer Emergency Response Team (CERT) the amount of intrusions has excessively increased year by year. If any dangerous intrusion or attack on the network vulnerabilities, computers or information systems may lead to serious disasters, and violate the computer security policies, i.e., Confidentiality, Integrity and Availability (CIA)Ms. Parag K. Shelke et. al. 2012;Hassen Mohammed Alsafi et. al. 2012;Kazi Zunnurhain and Susan V. Vrbsky 2013. As of now, the threats to information security are still significant research issues. Though there are a number of existing literatures to survey IDS (Denning,1987; Lunt, 1993; Mukherjee et al. 1994; Debar et al., 1999; Axelsson., 2000; Mishra et al., 2004; Krugeland Toth,2000; Jones and Sielken, 2000; Debar et al., 2000; Mukkamala and Sung, 2003; Estevez-Tapiador et al., 2004; Delgado et al., 2004; Kabir and –Ghorbani., 2005; Anantvalee and Wu., 2007; Patcha and Park, 2007; Tucker et al., 2007; Mandala et al., 2008; Garcia Teodoro et al., 2009; Amer and Hamilton,2010; Xie et al.,2011;We try to give more understanding about IDS and Particle Swarm OptimizationMs. Parag et. al. 2012; S. Gajek et. al. 2007;C. Yue and H. Wang 2010;. First of all, we want to differentiate between the intrusion detection, intrusion detection system (IDS) and intrusion prevention system(IPS)Y. del Valle et. al. 2008;Yonghe Lu et. al. 2015; T.Sousa et. al. 2004;I. De Falco et. al. 2007; Qi Shen et. al. 2007;Qi Shen et. al. 2008; Li-Yeh Chuang et. al. 2008.

Initially, National Institute Of Standards and Technology (NIST) described that intrusion is an attempt to compromise CIA Ms. Parag K. Shelke et. al. 2012;Hassen Mohammed Alsafi et. al. 2012;Kazi Zunnurhain and Susan V. Vrbsky 2013.The intrusion detection is a process of monitoring the harm-full events that are occurring in our computer system or network, and analyzing the signature of the intruder or harmful users, As the wireless networks are growing too high and gaining widespread deployment, everyone is adopting wireless network which is not very much secured so this one is easier one to attack than any other wired network.

Denial Of Service(DOS) Attacks analyzed and IDS can be categorized as wireless-based Intrusion Detection System. The intrusion detection system, Intrusion Detection System(IDS) is the software or hardware system to perform the intrusion detection process (Bace and Mell, 2001; Stavroulakis and Stamp, 2010). Intrusion Prevention System is a system, which tries to stop the attacks from the attackers and it will remember the intruder’s details for recognizing the further attacks. Y. Leu et. al. 2008;Bharat Rathi and Dattaray V.Jadhav 2014;Mehdi maukhafi et. al. 2017; Mohammad Sazzadul Hoque et. al. 2012. In some articles, Intrusion Detection and Prevention system(IDPs) and Intrusion Prevention System(IPS) are treated as synonyms.

Where the IDPs is used in the security community, here we focus on the classification of IDS based on the work that it is going to perform, the other hand cloud computing leverages existing technologies, such as virtualization and distributed computing, and has recently became popular as a new paradigm for hosting and delivering services over the internet. Chen et. al. 2013;Amjad Hussain Bhat et. al. 2013;Mehdi maukhafi et. al. 2017; Mohammad Sazzadul Hoque et. al. 2012;Han C. et. al.2011.

It has recently emerged as a new paradigm for hosting and delivering services over the Internet. Virtualization is a technology that abstracts away the details of physical hardware and provides the capability of pooling computing resources from clusters of servers, storages, and networks for high-level applications Dr. V. Venkatesa Kumar and M. Nithya 2014. Cloud platforms leverage virtualization technology to achieve the goal of providing computing resources as a utility. Therefore, we also study security issues on Virtual Machines (VMs). The remainder of this paper as follows. We describe IDS methodologies, and the classification of IDS approaches then introduces four classes of IDS technologiesQ. Chen et. al. 2013.We study Intrusion Detection System(IDS) issues on VMs Subsequently, two software-oriented solutions, Snort and Clam AV, are mentioned, as they are well known and widely used open-source tools. And then draws our conclusion, and gives future challenges.

EXTREME LEARNING MACHINE (ELM)

This algorithm is a feature optimization algorithm. ELM worked for filling the gap in between Frank Rosenblatt's Dream and John von Neumann's puzzle. This is a feature optimization and classification technique. This will be worked on a single hidden layer withthe feed-forward-neural network. The hidden layer will generate random basis G.B. Hung et. al. 2006; G. B. Hung and L. Chen 2007;G. B. Huang et. al.2012;G.B. Huang 2014;J. Tang et. al. 2015;G.B. Huang et. al. 2015; L. L. C. Kasun et. al. 2013. ELM provides the best features for training and testing. We can find the best result by using this algorithm G.B. Hung et. al. 2006; G.B. Hung and L. Chen 2007; G. B. Huang et. al. 2012; G.B. Huang 2014; J. Tang et. al. 2015; G.B. Huang et. al. 2015; L. L. C. Kasun et. al. 2013.

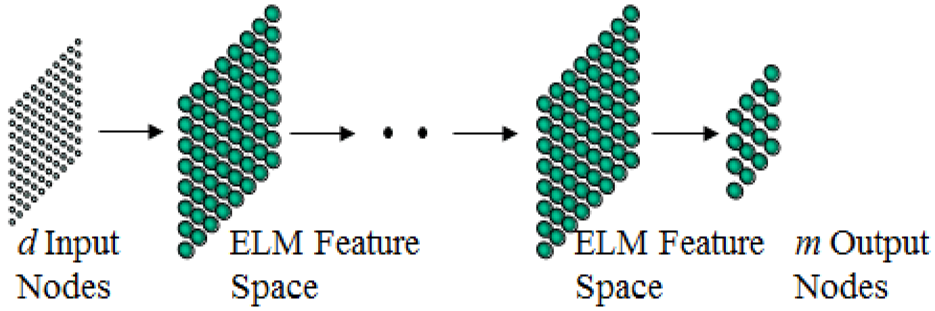

Figure1: Working model of ELM.

PARTICLE SWARM OPTIMIZATION ALGORITHM

PSO is a simple algorithm based on swarm intelligence which is used for solving many issues. It is mainly used to optimize the output using mathematical formulas. PSO used in various domains to solve their problems like load balancing, workflow scheduling, searching, enhancing performance and so on. This algorithm can also be implemented in the cloud and for this, some changes are going to make in the steps of an algorithm without changing the core concepts. Parag et. al. 2012. The algorithm has made a successful run using different languages and tools like Java, .NET, MATLAB, C++. We have worked on MATLAB trial version.

PSO algorithm is adopted in the field of task mapping, resource allocation, and scheduling. For example, PSO could be able to find a near-optimal solution for mapping all tasks in the workflow for the given set of resources Hassen Mohammed Alsafi et. al. 2012; Abdulhamit Subasi 2013;Bing Xue et. al. 2014;H. Hannah Inbarani et. al. 2014; Subhajit Kar et. al. 2015. Tasgetiren et al. proposed a PSO based algorithm for resource allocation by keeping the track of position value and fitness value calculated from a fitness function. Xue et al., S. Gajek et. al. 2007 developed an algorithm for time-cost optimization on scheduling workflow applicationsper Unler and Alper Murat 2010;Alper Unler et. al. 2011; Pei-Chann Chang et. al. 2012;Abdulhamit Subasi 2013; Bing Xue et. al. 2014;H. Hannah Inbarani et. al. 2014; Subhajit Kar et. al. 2015.

Many meta-heuristic algorithms have been proposed such as PSO algorithm that is appropriate for dynamic task scheduling include. On the other hand, Particle Swarm Optimization (PSO) has become popular because of its simplicity and its effectiveness in a broad range of application. Some of the applications that have used PSO to solve NP-Hard problems like Scheduling problem C. Yue and H. Wang 2010 and the task allocation problem Dr. V. Venkatesa Kumar and M. Nithya 2014. Many meta-heuristic algorithms have been proposed such as PSO algorithm that is appropriate for dynamic task schedulingBehnam amir et. al. 201;Abdulhamit Subasi 2013;Bing Xue et. al. 2014;H. Hannah Inbarani et. al. 2014; Subhajit Kar et. al. 2015.

DETECTION METHODOLOGIES

Intrusion Detection Methodologies can be classified into three major categories: Signature-based Detection (SD), Anomaly-based Detection(AD) and State-full Protocol Analysis (SPA).

Signature-based Detection(SD):- A Signature is a pattern or string which is used to detect the known attacks. SD(signature-based detection) is a process of comparing patterns against events that are occurring to detect the possible intrusion. These systems work by matching user activity with stored signatures of known attacks. Such detection systems use a predefined knowledge base to check whether the new network connection is in that knowledge database. If yes, the IDS consider this connection as a possible attack and then block it.

Anomaly-Based Detection:- It is a process of comparing normal profiles with events recognized to detect the possible attacks. e.g. attempted break-in, masquerading, penetration by a legitimate user, Denial of Service (DOS), Trojan horse, etc. It detects the intrusion by comparing the behavior of the individual with normal behavior. If it is abnormal, then he is marked as unauthenticated and he is stopped from entering into the network Mianyang Sichuan (2014),Bharat Rathi and Dattaray V. Jadhav 2014. It is used for finding out the unknown attacks, which is its advantage. But the main disadvantage behind this is that it is having a high false rate.

State-full Protocol Analysis (SPA):- The network protocol models in SPA are based originally on protocol standards from international standard organizations, e.g., IETF. SPA is also defined as Specification-based Detection. Hybrid IDS use more different methodologies to give more extensive and accurate results. Because of different methodologies focuses on known attacks/threats and the latter focuses on unknown attacks.One author Stavroulakis and StampS. Gajek et. al. 2007proposed classification to subdivide these Approaches into three subcategories including computation, Depended on approach, and biological concepts. We present a classification of five subclasses with an in-depth perspective on their characteristics: Statistics-based, Pattern-based, Rule-based, State-based and Heuristic-basedAli Al-maamari and Fatma A. Omara 2015.

TECHNOLOGY TYPES

Nowadays, there exist many types of IDS technologies. We can divide the technologies into four classes according to where they are deployed to inspect suspicious activities, and what the events they are capable of recognizing, The four classes are as follows: Host-based Intrusion Detection System (HIDS), Network-based Intrusion Detection System (NIDS), Wireless-based Intrusion Detection System (WIDS), Network Behavior Analysis (NBA) and Mixed Intrusion Detection System (MIDS). The HIDS collects and monitors the host with sensitive information and host running public servers. A NIDS captures the network traffic at the particular segment of the network and analyzes the activities of the application to detect the possible intrusions. WIDS is same as NIDS, but it captures wireless network traffic, such as ad-hoc networks, wireless sensor network, and wireless mesh networks. Besides, an NBA system inspects network traffic to recognize attacks with unexpected traffic flows. Adopting multiple technologies like MIDS gives a more accurate resultMohammad Sazzadul Hoque et. al.2012;Bharat Rathi and Dattaray V. Jadhav 2014; JamesKennedy and Russell Eberhart 1995.

The components in IDS include sensor and agent, where the first one is typically used for NIDS, WIDS and NBA systems to monitor the systems on the networks, and HIDS uses the other to monitor and analyze activities. Both the agent and sensor are capable of delivering data to the Management Server(MS) and Database Server(DS), where the MS is core device for storing information of the events occurred and the DS is just a repository storing event information. Moreover, there are two types of network architectures. The former one is the Managed Network (MN), an isolated network deployed to hide or protect the secret information from intruders

Detection methodologies in most of the computer need good tuning to get deployed, As to the prevention issue, we suggest the reader to refer the paperAli Al-maamari and Fatma A. Omara 2015for better expositions. A common drawback of IDS is they cannot give accurate detection. False-positive (FP) and false-negative (FN) are the indicators to assess the extent of accuracyBharat Rathi and dattaray v.jadhav 2014;Mehdi maukhafi et. al. 2017;James Kennedy and Russell Eberhart 1995;Mohammad Sazzadul Hoque et. al. 2012.

Further, we summarize and refine the previous surveys to give a new perspective for IDSs. In the part of System deployment, the centralized network architecture collects data from single monitored System, ‘‘distributed" network architecture that collects data from multiple monitored systems so as to detect the entire network, distributed and cooperative attacks or ‘‘hybrid" of both. The distributed configuration must be cloud-based or grid-based, at last, the view of Detection Strategy directs that the Detection Discipline would be ‘‘state-based" (secure or insecure) or ‘‘transition-based"(from secure to insecure and vice versa), and both may be stimulating or non-obtrusive evaluation. Besides, Processing Strategy is logically ‘‘centralized" or ‘‘distributed". For the Detection Methodology, one of ‘‘Anomaly-based", ‘‘signature-based" and‘‘specification-based" is adopted and explained in the part. Y. Leu et. al. 2008;Bharat Rathi and Dattaray V.Jadhav 2014;Mehdi maukhafi et. al. 2017;Mohammad Sazzadul Hoque et. al. 2012.

RESULT OF HYBRID MODEL PSO-ELM

We have applied the dataset of KDD'99 intrusion detection dataset. That dataset is available for research purpose. On this dataset, there are 41 features of IDS dataset. We have worked on features. We have a reduced number of features and get the result of our model.We have found five best features. That dataset downloaded from UCI repository for training the hybrid model of PSO-ELM and we have found the result of our model. We get the result of our hybrid model is 99.7% accuracy for detection of IDSG.B. Hung et. al. 2006;G.B. Hung and L. Chen 2007;G.B. Huang et. al.2012; J. Tang et. al. 2015;G.B. Huang et. al. 2015;L. L. C. Kasun et. al. 2013.

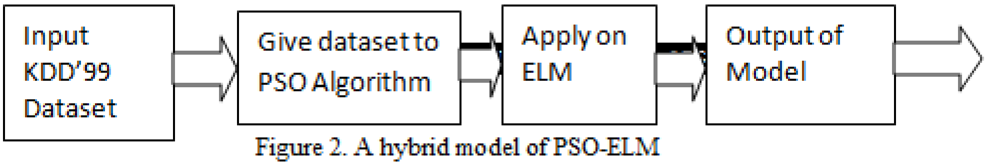

Figure 2. A hybrid model of PSO-ELM

CONCLUSIONS

We have introduced an overview of detection methodologies, approaches, and technologies for IDSs. Each technique has its own advantages and disadvantages, so that we should be careful while selecting the methodologies, let's see the pattern-based IDS for a while, although it is simple to implement and very effective to inspect known attacks, it is very difficult for this approach to identify the unknown attacks concealed by evasion techniques and many types of known attacks. And several rule-based techniques proposed to detect the unknown attacks, such techniques may lead to the problem of creating and updating the knowledge for given attacks. Currently, we got the result by using with single objective PSO-ELM model and accuracy of that ids model is 99.7% with a minimum of time by using KDD'99 dataset of 25129 datasets from UCI repository. Performance of the ELM based PSO model is the best one compare to the other algorithms is with time requirements.

REFERENCES

Shelke, Ms. Sneha Sontakke, Dr. A. D. Gawande (2012). Intrusion Detection System for Cloud Computing,
nal Journal Of Scientific & Technology Research Volume1.

Mohammed Alsafi, Wafaa Mustafa Abdullah and Al-Sakib Khan Pathan(2012). IDPS: An Integrated Intrusion Handling
Cloud Computing Environment, Department of Computer Science Faculty of Information and Communication
gy International Islamic University Malaysia (IIUM), Malaysia abosafi87@gmail.com, heevy9@yahoo.com, and
m.edu.my

ngh, Binay Kumar Pandey, Ratnesh Srivastava, Neha Rawat, Poonamrawat, Awantika. Cloud Computing Attacks: A
n With Solutions, College of Technology, GBPUAT, Pantnagar, Uttarakhand-263145, India

nurhain and Susan V. Vrbsky (2013). FAPA: Flooding Attack Protection Architecture in a Cloud System,Department of
Science The University Of Alabama Tuscaloosa, kzunnurhain@crimson.ua.edu, vrbsky@cs.ua.edu

enkatesa Kumar, M. Nithya (2014). International journal of advanced research in computer and communication engg,vol3,

Chouhan, Rajendra Singh. International Journal of Advanced Research in Computer Science and Software Engineering.

, Sichuan (2014). International Journal of Grid and Distributed Computing Vol.7, 2014.7.1.04.

amari, Fatma A. Omara, (2015). Department of Computer Science, Cairo University, Egypt International Journal of Grid
on ComputingVol. 8, 2015.8.5.24

, K. Shelke, Ms. Sneha Sontakke, Dr. A. D. Gawande (2012). Intrusion Detection System for Cloud Computing,
nal Journal Of Scientific & Technology Research Volume1.

A. Sadeghi, C. Stuble, and M. Winandy (2007): Compartmented security for browsers—Or how to thwart a phisher with
mputing, in Proc. IEEE Int. Conf. Avail., Rel. Security, Vienna, Austria, 120–127.

I. Wang, (2010): BogusBiter: A transparent protection against phishing attacks, ACM Trans. Int. Technol., vol. 10, no. 2,

S. Abdelwahed, and A. Erradi (2013). A model-based approach to self-protection in the computing system, in Proc. ACM
tonomic Comput. Conf., Miami, FL, USA, 1–10.

, M. C. Li, J. C. Lin, and C. T. Yang (2008). Detection workload in a dynamic grid-based intrusion detection environment, J.
istrib. Comput., vol. 68, no. 4, 427–442.

Zhao, X. Wang, and J. Su (2013). DiffSig: Resource differentiation based malware behavioral concise signature generation, nun. Technol., vol. 7804, 271–284.

X. Wang, T. Chiueh, and X. Meng (2011). Safe side effects commitment for OS-level virtualization, inProc. ACM Int. Conf. ic Comput., Karlsruhe, Germany, 111–120.

gers and K. Seigfried (2004). The future of computer forensics: A needs analysis survey, Computer. Security, vol. 23, no. 1,

C. Choi, B. Ko, D. Choi, and P. Kim (2013): Detecting web-based DDoS attack using Map Reduce operations in a cloud g environment, J. Internet Serv. Inf. Security, vol. 3, no. 3/4, 28–37.

L. Vu, K. Nahrstedt, and H. Khurana (2010): MIS: Malicious nodes identification scheme in network-coding-based peer-to-ming, in Proc. IEEE INFOCOM, San Diego, CA, USA, 1–5.

T. Giffin, Somesh Jha, and Barton P. Miller (2006). Automated Discovery of Mimicry Attacks..

i Lv, Yang D., Hao Y. (2011). An Intrusion Detection System Based on Neural Network, 2011 International Conference on nic Science, Electric Engineering and Computer IEEE Publication.

do(2002). Optimal power flow using particle swarm optimization using particle swarm optimization electrical power and stem, 24, 563-571.

Amiri, mahboubeh mirzabaghari and Yong Shi (2015). A new intrusion detection approach using PSO based multiple criteria ogramming, Procedia Computer Science 55, 231-237

thi,dattaray v.jadhav (2014): Network intrusion detection using PSO based on Adaptive and Genetic Algorithm. International science and research volume 5, issue 8.

aukhafi, Khalid yel hasini and seddik bri (2017). A Novel Anomaly intrusion detection based on SMO .journal of mobile ia vol 13, no 3 &4, 197-209.

nnedy and Russell Eberthart (1995). Particle swarm optimization, IEEE international conference, pp (1942-1948).

mar, Khaled Al-Shalfan. Neural network-based feature selection from KDD intrusion detection dataset, Al-Imam Mohammad Islamic University, New development in computational intelligence and computer science. ISBN: 978-1-6-6, 232-236.

ad Sazzadul Hoque, Md abdul Mukit, Md abu naser bikas (2012). An implementation of intrusion detection system using a gorithm.international journal of network security and its application (ijnsa) Vol 4, No.2, March 2012.

G., Dr. Genapathy Sannasi (2017). A review on intelligent data mining and soft computing technique for effective intrusion . International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2017
ussain Bhat1 , Sabyasachi Patra, Dr. Debasish Jena (2013). Machine learning approach for intrusion detection on cloud virtual nternational journal of application and innovation in engineering and management (IJAIEM), Volume 2, Issue 6,

lle, Salman Mohagheghi, Ganesh K. Venayagamoorthy, Jean Carlos Hernandez Mejia (2008). Particle Swarm Optimization: ncepts, Variants, and Applications in Power Systems, Article inIEEE Transactions on Evolutionary Computation · 3, DOI: 10.1109/TEVC.2007.896686 · Source: IEEE Xplore.

u, Minghui Liang, Zeyuan Ye, Lichao Cao (2015). Improved particle swarm optimization algorithm and its application in text lection, Applied Soft Computing 35, 629–636.

A.Silva, A.Neves, (2004). Particle swarm-based data mining algorithms for classification tasks, Parallel Comput. 30(5), 767–

o, A. Della Cioppa, E. Tarantino (2007). Facing classification problems with Particle Swarm Optimization, Applied Soft ng, 7, 652–658.

Wei-Min Shi, Wei Kong, Bao-Xian Ye (2007). A combination of modified particle swarm optimization algorithm and support chine for gene selection and tumor classification, Talanta, 71, 1679–1683.

Wei-Min Shi, Wei Kong (2008). Hybrid particle swarm optimization and tabu search approach for selecting genes for tumor tion using gene expression data, Computational Biology and Chemistry, 32, 53–60.

huang, Hsueh-Wei Chang, Chung-Jui Tu, Cheng-Hong Yang, (2008). Improved binary PSO for feature selection using gene n data, Computational Biology and Chemistry, 32, 29–38.

ler, Alper Murat (2010). A discrete particle swarm optimization method for feature selection in binary Classification problems, ournal of Operational Research, 206, 528–539.

ler , Alper Murat , Ratna Babu Chinnam (2011). mr2PSO: A maximum relevance minimum redundancy feature selection ased on swarm intelligence for support vector machine classification, Information Sciences, 181, 4625–4641.

n Chang, Jyun-Jie Lin, Chen-Hao Liu (2012): An attribute weight assignment and particle swarm Optimization algorithm for latabase classifications, computer methods, and programs in biomedicine, 107, 382-392.

nit Subasi, (2013). Classification of EMG signals using PSO optimized SVM for diagnosis of neuromuscular disorders, rs in Biology and Medicine, 43, 576–586.

, Mengjie Zhang, Will N. Browne, (2014). Particle swarm optimisation for feature selection in classification: Novel ion and updating mechanisms, Applied Soft Computing, 18, 261–276.

h Inbarani, Ahmad Taher Azar, G. Jothi (2014). Supervised hybrid feature selection based on PSO and rough sets for medical , computer methods and programs in biomedicine, 113, 175–185.

Kar, Kaushik Das Sharma, Madhubanti Maitra (2015). Gene selection from microarray gene expression data for classification subgroups employing PSO and adaptive K-nearest neighborhood technique, Expert Systems with Applications, 42,

ing, Dunwei Gong, Ying Hu, Wanquiu Zhang (2015). Feature selection algorithm based on bare-bones particle swarm ion, Neurocomputing, 146, 150-157.

g, L. Chen and C. L. Siew (2006). Universal Approximation Using Incremental Constructive Feed-Forward Networks with Hidden Nodes, IEEE Transactions on Neural Networks, vol. 17, no. 4, 879-892.

g, L. Chen (2007). Convex Incremental Extreme Learning Machine, Neurocomputing, vol. 70,3056-3062.

ng, H. Zhou, X. Ding, and R. Zhang (2012). Extreme Learning Machine for Regression and Multiclass Classification, IEEE ons on Systems, Man, and Cybernetics-Part B: Cybernetics, vol. 42, no. 2, 513-529.

ng (2014). An Insight into Extreme Learning Machines: Random Neurons, Random Features, and Kernels, Cognitive tion, vol. 6, 376-390.

. Deng, and G.-B. Huang (2015). Extreme Learning Machine for Multilayer Perceptron, IEEE Transactions on Neural and Learning Systems.

ng, Z. Bai, L. L. C. Kasun, and C. M. Vong (2015). Local Receptive Fields Based Extreme Learning Machine, IEEE tional Intelligence Magazine, vol. 10, no. 2, 18-29.

L. L. C. Kasun, H. Zhou, G.-B. Huang, and C. M. Vong (2013). Representational Learning with Extreme Learning Machine for Big Data, IEEE Intelligent Systems, vol. 28, no. 6, 31-34.

1999 Data - UCI KDD Archive http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html