HYBRID INTELLIGENT APPROACH FOR NETWORK INTRUSION DETECTION

WAEL HASAN ALI AL-MOHAMMED

MASTER OF SCIENCE (INFORMATION TECHNOLOGY)

SCHOOL OF COMPUTING

COLLEGE OF ARTS AND SCIENCES

UNIVERSITY UTARA MALAYSIA

2015

PERMISSION OF USE

In presenting this thesis in fulfilment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the Universiti Library may make it freely available for inspection. I further agree that permission for the copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor(s) or, in their absence, by the Dean of Awang Had Salleh Graduate School of Arts and Sciences. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to:

Dean of Awang Had Salleh Graduate School of Arts and Sciences
UUM College of Arts and Sciences
Universiti Utara Malaysia
06010 UUM Sintok

ABSTRAK

Sejak kebelakangan ini, rangkaian komputer telah meluas dan sangat rumit. Banyak informasi sensitif disalurkan kepada pelbagai jenis peranti komputer, dari komputer mini ke pelayan dan juga dari komputer mini ke peranti mudah alih. Perubahan ini menyebabkan serangan ke atas maklumat penting ke atas sistem rangkaian semakin bertambah setiap tahun. Pencerobohan adalah ancaman utama terhadap rangkaian. Ia ditakrifkan sebagai satu siri aktiviti yang bertujuan untuk menjejaskan keselamatan sistem rangkaian dari segi kerahsiaan, integriti dan ketersediaan. Oleh itu, pengesanan pencerobohan adalah sangat penting sebagai sebahagian daripada pertahanan. Oleh itu, ia perlu meningkatkan teknik pengesanan pencerobohan rangkaian dan sistem. Disebabkan pendekatan pengesanan pencerobohan sebelum ini terlalu terhad, kami mencadangkan pendekatan hibrid pintar untuk mengesan pencerobohan rangkaian berdasarkan pengelompokan k-means algoritma dan mesin sokongan vektor algoritma. Tujuan penyelidikan adalah untuk mengurangkan kadar penggera palsu dan juga untuk meningkatkan kadar pengesanan untuk dibandingkan dengan pendekatan pengesanan pencerobohan yang sedia ada. Pencerobohan dataset NSL-KDD telah digunakan untuk latihan dan menguji pendekatan yang dicadangkan. Beberapa langkah telah dilakukan sebelum tujuan pengelasan untuk meningkatkan prestasi pengelasan. Pertama, menyatukan jenis dan menapis dataset melalui data transformasi. Kemudian, pemilihan ciri algoritma telah digunakan untuk membuang ciri yang tidak relevan dalam tujuan pencerobohan. Ciri-ciri yang terpilih telah mengurangkan 41 ciri kepada 21 ciri untuk mengesan pencerobohan dan kemudian kaedah-kaedah yang biasa digunakan untuk dilaksanakan serta mengurangkan perbezaan di antara maklumat. Pengelompokan adalah langkah terakhir pemprosesan sebelum pengelasan dijalankan menggunakan k-means algoritma. Klasifikasi telah dilakukan dengan menggunakan mesin sokongan vektor. Selepas latihan dan menguji pendekatan pintar hibrid yang telah dicadangkan, keputusan penilaian prestasi telah menunjukkan bahawa ia mencapai ketepatan yang tinggi dan kadar pengesanan palsu yang rendah. Ketepatannya ialah 96.025% dan penggera palsu adalah 3.715%.

Kata Kunci: Rangkaian Pengesanan Pencerobohan, Pendekatan Pintar Hibrid, Rangkaian Serangan, Pengelompokan , Klasifikasi, Pencerobohan dataset NSL-KDD, K-Means algoritma, Mesin Sokongan Vektor algoritma.

ABSTRACT

In recent years, computer networks are broadly used, and they have become very complicated. A lot of sensitive information passes through various kinds of computer devices, ranging from minicomputers to servers and mobile devices. These occurring changes have led to draw the conclusion that the number of attacks on important information over the network systems is increasing with every year. Intrusion is the main threat to the network. It is defined as a series of activities aimed for exposing the security of network systems in terms of confidentiality, integrity and availability, as a result; intrusion detection is extremely important as a part of the defense. Hence, there must be substantial improvement in network intrusion detection techniques and systems. Due to the prevailing limitations of finding novel attacks, high false detection, and accuracy in previous intrusion detection approaches, this study has proposed a hybrid intelligent approach for network intrusion detection based on k-means clustering algorithm and support vector machine classification algorithm. The aim of this study is to reduce the rate of false alarm and also to improve the detection rate, comparing with the existing intrusion detection approaches. In the present study, NSL-KDD intrusion dataset has been used for training and testing the proposed approach. In order to improve classification performance, some steps have been taken beforehand. The first one is about unifying the types and filtering the dataset by data transformation. Then, a features selection algorithm is applied to remove irrelevant and noisy features for the purpose of intrusion. Feature selection has decreased the features from 41 to 21 features for intrusion detection and later normalization method is employed to perform and reduce the differences among the data. Clustering is the last step of processing before classification has been performed, using k-means algorithm. Under the purpose of classification, support vector machine have been used. After training and testing the proposed hybrid intelligent approach, the results of performance evaluation have shown that the proposed network intrusion detection has achieved high accuracy and low false detection rate. The accuracy is 96.025 percent and the false alarm is 3.715 percent.

Keywords: Network Intrusion Detection, Hybrid Intelligent Approach, Network Attacks, Clustering, Classification, NSL-KDD intrusion dataset, K-Means algorithm, Support Vector Machine algorithm.

DEDICATION

Every challenging work needs self-efforts as well as guidance and support of others, especially those who are very close to our heart.

Therefore, I dedicate this humble work

To my sweet and beloved

FAMILY

Whose love, support, and pray of day and night for making me able to reach such success.

To my lovely homeland

IRAQ

Which opening my eyes to this world. I hope it will get the peace soon.

To the marvelous land

MALAYSIA

Which granted me the opportunity to complete my study.

ACKNOWLEDGEMENT

In the Name of Allah, the Most Merciful, the Most Compassionate all praise be to Allah, the Lord of the worlds; and prayers and peace is being upon Mohamed His servant and messenger.

First and foremost, I acknowledge my unlimited thanks to Allah Almighty, the Ever-Magnificent and the Ever-Thankful for his help and blessings for which this thesis would not have been possible to achievement without his help. I would like to thank and appreciate our first teacher, prophet Mohammed, and his family who taught us the struggling, and patience to achieve the success.

To finally accomplish this journey which began in February, 6, 2013 (06:00 AM BGD it is the time when I left my home, heading to Malaysia), I have to thank many persons who deserve my gratitude. I was guided, supported and encouraged by them.

I convey a profound appreciation to my supervisor, Associate Professor Dr. Hatim Mohammad Tahir, for his guidance, advice, assistance, and oversight. I have been very fortunate to have been able to work with him since undertaking my master degree. I thank the kind dissertation's examiners Dr. Mohd Nizam Omer and Dr. Nur Haryani Zakaria for their comments and suggestions. I extend my appreciation to the head of department, coordinators and all staff of the school of computing.

My deepest and heartfelt gratitude, loves, thanks and appreciation for my dearest parents and my beloved siblings who are a part of my happiness, success, and the inspiration that led me for the quest for knowledge and self-empowerment through night and day. I hope I can put a smile on their faces for giving back their tremendous support and encouragement, patience, unconditional love, and prayers for me. Thank you for giving me the strength to chase and reach my dreams.

I owe a huge debt of gratitude and thanks to my close friend Dr. Hayder Mohammed Ali, The person who had a main role in my master's candidature. I am forever grateful for him. I wish all the best for him and I am praying to Allah Almighty to ease his life, especially his PhD journey.

I would like to express my wholehearted appreciation to my soulmates, closest and best friends (Hussein Abdulkhaliq – Mohammed Zuhair – Ahmed Shakir – Tammar Hayder – Hayder Kurdi – Rasoul Faik) for their gorgeous support and encouragement along the way in countless ways. I want to exploit this opportunity to thank them for our pure and wonderful friendship over twelve years.

I extend my appreciation to Iraqi friends who met them in UUM (especially Abbass, Maitham, Mohammed, Samer, Wadhah, and Zaid), all my friends in my country and UUM, bachelor's lecturers, bachelor's colleagues, master's lecturers, master's colleagues, UUM staff, the people who are praying, supported, helped, guided and wished the best for me, Malaysian people who are very gentle with me.

Thank You All.

"This Thesis is only the beginning of my journey."

WAEL HASAN ALI AL-ZUWAINY

Northern University of Malaysia, Kedah, Malaysia

Monday, October 20, 2014

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

A	Accuracy
AI	Artificial Intelligent
ANN	Artificial Neural Network
DoS	Daniel of Services Attack
DR	Detection Rate
FAR	False Alarm Rate
FN	False Negative
FP	False Positive
HIDS	Host-based Intrusion Detection System
IDS	Intrusion Detection System
NID	Network Intrusion Detection
NIDS	Network-based Intrusion Detection System
R2L	Remote to Local Attack
SVM	Support Vector Machine
TN	True Negative
TP	True Positive
U2R	User to Root Attack

CHAPTER ONE

INTRODUCTION

1.1 Introduction

This chapter has discussed briefly the background of network security impacts, network intrusion problems and its solutions. On the other hand, it presents amply the statement of the problem in this study. This chapter defines the research questions, objectives of this study, the scope of research, research's significance and contributions of the study as well.

1.2 Background of study

In recent years, computer networks are broadly omnipresent and have become very complicated. Almost everybody with a computer or mobile device, is linked with the Internet in order to have access to data or send messages. A lot of sensitive information passes through various kinds of computer devices, ranging from minicomputers to servers and mobile devices (Elbasiony et al., 2013; Upadhyaya & Jain, 2013). In a wide scale, all governments, higher education organizations and different organizations depend on the network computer systems for the daily processes to perform, and network computer system play an essential role for the processes (Shanmugam & Idris, 2011).

The contents of the thesis is for internal user only

References:

Ahmad, A., Bharanidharan Shanmugam, Norbik Bashah Idris, Ganthan Nayarana Samy, & AlBakri, S. H. (2013). Danger Theory Based Hybrid Intrusion Detection Systems for Cloud Computing. *International Journal of Computer and Communication Engineering, Vol. 2*(No. 6), (pp. 650-654).

Akbar, S., Rao, K. N., & Chandulal, J. (2011). Implementing rule based genetic algorithm as a solution for intrusion detection system. *Int. J. Comput. Sci. Netw. Secur, 11*(8), 138.

Al-Jarrah, O., & Arafat, A. (2014). *Network Intrusion Detection System using attack behavior classification.* Paper presented at the Information and Communication Systems (ICICS), 2014 5th International Conference on (pp. 1-6). IEEE.

Babatunde, R., Adewole, K., Abdulsalam, S., & Isiaka, R. (2014). Development of an intrusion detection system in a computer network. *International Journal of Computers & Technology, 12*(5), 3479-3485.

Bahrololum, M., & Khaleghi, M. (2008). Anomaly Intrusion Detection System Using Hierarchical Gaussian Mixture Model. *International journal of computer science and network security, 8*(8), 264-271.

Baili, N. (2013). *Unsupervised and semi-supervised fuzzy clustering with multiple kernels.* (Doctor o f Philosophy), University of Louisville.

Bansal, D. R., Gupta, V., & Malhotra, R. (2010). Performance analysis of wired and wireless LAN using soft computing techniques-A review. *Global Journal of Computer Science and Technology, 10*(8), 67-71.

Bhavsar, Y. B., & Waghmare, K. C. (2013). Intrusion Detection System Using Data Mining Technique: Support Vector Machine. *International Journal of Emerging Technology and Advanced Engineering, 3*(3), 581-586.

Bhuyan, M., Bhattacharyya, D., & Kalita, J. (2013). Network Anomaly Detection: Methods, Systems and Tools. *Communications Surveys & Tutorials, IEEE, 16*(1), 303 - 336.

Chae, H.-s., Jo, B.-o., Choi, S.-H., & Park, T.-k. (2013). Feature Selection for Intrusion Detection using NSL-KDD. *Recent Advances in Computer Science*, 184-187.

Chang, C.-C., & Lin, C.-J. (2011). LIBSVM: a library for support vector machines. *ACM Transactions on Intelligent Systems and Technology (TIST), 2*(3), 27.

Chapke Prajkta, P., & Raut, A. (2012). Hybrid Model For Intrusion Detection System. *International Journal Of Engineering And Computer Science, 1*(3), 151-155.

Chen, J., Wang, X., & He, L. (2008). *An architecture for differentiated security service.* Paper presented at the Electronic Commerce and Security, 2008 International Symposium on (pp. 301-304). IEEE.

Chimphlee, W. H., Abdul; Sap, Mohd Noor Md; Chimphlee, Siriporn; Srinoy, Surat. (2007). A Rough-Fuzzy Hybrid Algorithm for computer intrusion detection. *The International Arab Journal of Information technology*, *4*(3), 247-254.

Chitrakar, R., & Chuanhe, H. (2012). *Anomaly detection using Support Vector Machine classification with k-Medoids clustering.* Paper presented at the Internet (AH-ICI), 2012 Third Asian Himalayas International Conference on (pp. 1-5). IEEE.

Chitrakar, R., & Huang, C. (2012). *Anomaly based Intrusion Detection using Hybrid Learning Approach of combining k-Medoids Clustering and Naïve Bayes Classification.* Paper presented at the Wireless Communications, Networking and Mobile Computing (WiCOM), 2012 8th International Conference on (pp. 1-5). IEEE.

Chowdhary, M., Suri, S., & Bhutani, M. (2014). Comparative Study of Intrusion Detection System. *International Journal of Computer Sciences and Engineering, 2*(4), 197-200.

Daniel, J. V., Joshna, S., & Manjula, P. (2013). A Survey of Various Intrusion Detection Techniques in Wireless Sensor Networks.

Danziger, M., & de Lima Neto, F. B. (2010). *A hybrid approach for IEEE 802.11 intrusion detection based on AIS, MAS and naïve Bayes.* Paper presented at the Hybrid Intelligent Systems (HIS), 2010 10th International Conference on (pp. 201-204). IEEE.

Davis, J. J., & Clark, A. J. (2011). Data preprocessing for anomaly based network intrusion detection: A review. *Computers & Security*, *30*(6), 353-375.

Dhawan, A. (2013). Data mining with Improved and efficient mechanism to detect the Vulnerabilities using intrusion detection system. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 2*(2), pp: 787-791.

Elbasiony, R. M., Sallam, E. A., Eltobely, T. E., & Fahmy, M. M. (2013). A hybrid network intrusion detection framework based on random forests and weighted k-means. *Ain Shams Engineering Journal*, *4*(4), 753-762.

Engen, V., Vincent, J., & Phalp, K. (2011). Exploring discrepancies in findings obtained with the KDD Cup'99 data set. *Intelligent Data Analysis, 15*(2), 251-276.

Eric, K. (2009). *Simulation on Network Security Design Architecture for Server Room in Rwanda Information Technology Agency*. Universiti Utara Malaysia.

Esh Narayan, P. S. a. G. K. T. (2012). Intrusion Detection System Using Fuzzy C_ Means Clustering with Unsupervised Learning via EM Algorithms. *VSRD-IJCSIT, Vol. 2*(6), 502-510.

Gan, G., Ma, C., & Wu, J. (2007). *Data clustering: theory, algorithms, and applications* (Vol. 20): Siam.

Gao, M., & Wang, N. (2014). A Network Intrusion Detection Method Based on Improved K-means Algorithm. *Advanced Science and Technology Letters, 53*, 429-433.

Garzia, F., Tirocchi, N., Scarpiniti, M., & Cusani, R. (2012). Optimization of Security Communication Wired Network by Means of Genetic Algorithms. *Communications & Network, 4*(3), 196-204.

Ghadiri, A., & Ghadiri, N. (2011). *An adaptive hybrid architecture for intrusion detection based on fuzzy clustering and RBF neural networks.* Paper presented at the Communication Networks and Services Research Conference (CNSR), 2011 Ninth Annual. (pp. 123-129). IEEE.

Govindarajan, M. (2014). A Hybrid RBF-SVM Ensemble Approach for Data Mining Applications. *International Journal of Intelligent Systems and Applications (IJISA), 6*(3), 84 - 95.

Govindarajan, M., & Chandrasekaran, R. (2012). *Intrusion Detection using an Ensemble of Classification Methods.* Paper presented at the Proceedings of the world congress on engineering and computer science (Vol. 1).

Hameed, S. M., Saad, S., & AlAni, M. F. (2013). An Extended Modified Fuzzy Possibilistic C-Means Clustering Algorithm for Intrusion Detection. *Lecture Notes on Software Engineering, 1*(3), 273-278.

Hameed, S. M., & Sulaiman, S. S. (2012). Intrusion Detection Using a Mixed Features Fuzzy Clustering Algorithm. *Iraq Journal of Science (IJS), 53*(2), 427-434.

Husagic, A., Koker, R., & Selman, S. (2013). *Intrusion detection using neural network committee machine.* Paper presented at the Information, Communication and Automation Technologies (ICAT), 2013 XXIV International Symposium on (pp. 1-6). IEEE.

Ibrahim. (2010). Artificial Neural Network for Misuse Detection. *Journal of Communication and Computer, 7*(6), 38-48.

Ibrahim, Basheer, D. T., & Mahmod, M. S. (2013). A Comparison Study For Intrusion Database (Kdd99, Nsl-Kdd) Based On Self Organization Map (SOM) Artificial Neural Network. *Journal of Engineering Science and Technology, 8*(1), 107-119.

Idika, N. C., Marshall, B. H., & Bhargava, B. K. (2009). *Maximizing network security given a limited budget.* Paper presented at the the Fifth Richard Tapia Celebration of Diversity in Computing Conference: intellect, initiatives, insight, and innovations (pp. 12-17). ACM.

Ishida, M., Takakura, H., & Okabe, Y. (2011). *High-performance intrusion detection using optigrid clustering and grid-based labelling.* Paper presented at the Applications and the Internet (SAINT), 2011 IEEE/IPSJ 11th International Symposium on (pp. 11-19). IEEE.

Jain, Sharma, S., & Sisodia, M. S. (2011). Network Intrusion Detection by using Supervised and Unsupervised Machine Learning Technique-A Survey. *International Journal of Computer Technology and Electronics Engineering, 1*(3), 14 - 20.

Jain, Singh, T., & Sinhal, A. (2013). A Survey on Network Attacks, Classification and Models for Anomaly-based network intrusion detection systems. *International Journal of Engineering Research and Science & Technology, 4*(2), 64 - 73.

Jaisankar, N., & Kannan, A. (2011). A Hybrid Intelligent Agent Based Intrusion Detection System. *Journal of Computational Information Systems, 7*(8), 2608-2615.

Jawhar, M. M. T., & Mehrotra, M. (2010). Design network intrusion detection system using hybrid fuzzy-neural network. *International Journal of Computer Science and Security, 4*(3), 285.

Jiang, S. (2012). Internet Development Versus Networking Modes *Future Wireless and Optical Networks* (pp. 17-35): Springer.

Joshi, S., & Varsha, S. P. (2013). Network Intrusion Detection System (NIDS) based on Data Mining. *International Journal of Engineering Science and Innovative Technology (IJESIT), 2*(1), 95 - 98.

Jyothsna, V., & Prasad, K. M. (2011). A Review of Anomaly based Intrusion Detection Systems. *International Journal of Computer Applications, 28*(7), 26 - 35.

Kong, Y.-H., & Xiao, H.-M. (2009). *A new approach for intrusion detection based on Local Linear Embedding algorithm.* Paper presented at the Wavelet Analysis and Pattern Recognition, 2009. ICWAPR 2009. International Conference on (pp. 107-111). IEEE.

Kshirsagar, V., & Patil, D. R. (2010). Application of Variant of AdaBoost based Machine Learning Algorithm in Network Intrusion Detection. *International Journal of Computer Science and Security (IJCSS), 4*(2), 1-6.

Kulhare, R., & Singh, D. (2013). Survey paper on intrusion detection techniques. *International Journal of Computers & Technology, 6*(2), 329-335.

Kumar, Gulshan, K., & Krishan. (2012). The use of artificial-intelligence-based ensembles for intrusion detection: a review. *Applied Computational Intelligence and Soft Computing, 2012,* 1 - 20.

Li, L., & Yuan, Y. (2010). Data Preprocessing for Network Intrusion Detection. *Applied Mechanics and Materials, 20,* 867-871.

Liao, H.-J., Richard Lin, C.-H., Lin, Y.-C., & Tung, K.-Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications, 36*(1), 16-24.

Liu, Wan, P., Wang, Y., & Liu, S. (2014). Clustering and Hybrid Genetic Algorithm based Intrusion Detection Strategy. *TELKOMNIKA Indonesian Journal of Electrical Engineering, 12*(1), 762-770.

Liu Li , Wan Pengyuan Wang , Y., & Songtao, L. (2014). Clustering and Hybrid Genetic Algorithm based Intrusion Detection Strategy. *TELKOMNIKA Indonesian Journal of Electrical Engineering, 12*(1), 762-770.

Liu, Z. (2011). A method of svm with normalization in intrusion detection. *Procedia Environmental Sciences, 11*, 256-262.

Maldonado, S., Weber, R., & Basak, J. (2011). Simultaneous feature selection and classification using kernel-penalized support vector machines. *Information Sciences, 181*(1), 115-128.

Mohammad, M. N., Sulaiman, N., & Khalaf, E. T. (2011). A Novel Local Network Intrusion Detection System Based on Support Vector Machine. *Journal of Computer Science, 7*(10), 1560-1564.

Muniyandi, A. P., Rajeswari, R., & Rajaram, R. (2012). Network anomaly detection by cascading k-Means clustering and C4. 5 decision tree algorithm. *Procedia Engineering, 30*, 174-182.

Neethu, B. (2013). Adaptive Intrusion Detection Using Machine Learning. *IJCSNS, 13*(3), 118.

NSL-KDD intrusion dataset , (2014, June 1). Retrieved from http://www.nsl.cs.unb.ca/NSL-KDD/.

Omit, I.-V. (2008). *A fuzzy feature evaluation framework for network intrusion detection.* (Doctor of Philosophy), The university of New Brunswick.

Panda, M., Abraham, A., & Patra, M. R. (2010). *Discriminative multinomial naive bayes for network intrusion detection.* Paper presented at the Information Assurance and Security (IAS), 2010 Sixth International Conference on (pp. 5-10). IEEE.

Panda, M., Abraham, A., & Patra, M. R. (2012). A hybrid intelligent approach for network intrusion detection. *Procedia Engineering, 30*, 1-9.

Panda, M., & Patra, M. R. (2008). Some clustering algorithms to enhance the performance of the network intrusion detection system. *Journal of Theoretical and Applied Information Technology*, 710-716.

Panwar, S. S., Sharma, R., Kumar, V., & Maheshwari, V. (2014). A Comprehensive Study of Clustering Techniques to Analyze NSL-KDD Dataset and Research Challenges. *International Journal of Enhanced Research in Science Technology & Engineering, 3*(1), 557-564.

Patra, M. R., & Panigrahi, A. (2013). *Enhancing Performance of Intrusion Detection through Soft Computing Techniques.* Paper presented at the Computational and Business Intelligence (ISCBI), 2013 International Symposium on (pp. 44-48).

Pei, L., Li, C., Hou, R., Zhang, Y., & Ou, H. (2013). *Computer Simulation of Denial of Service attack in Military Information Network using OPNET*. Paper presented at the 3rd International Conference on Multimedia Technology (ICMT-13).

Pillai, M. B., Singh, M. U. P., & Lnct, A. P. C. (2011). NIDS For Unsupervised Authentication Records of KDD Dataset in MATLAB. *IJACSA) International Journal of Advanced Computer Science and Applications, Special Issue on Wireless & Mobile Networks*, 57-61.

Powers, S. T., & He, J. (2012). A hybrid artificial immune system and Self Organising Map for network intrusion detection. *arXiv preprint arXiv:1208.0541*.

Prabha, K., & Sukumaran, S. (2013). Single-Keyword Pattern Matching Algorithms for Network Intrusion Detection System. *International Journal of Computer and Internet Security, 5*(1), 11-18.

Raghuveer, K. (2012). Performance evaluation of data clustering techniques using KDD Cup-99 Intrusion detection data set. *International Journal of Information and Network Security (IJINS), 1*(4), 294-305.

Rangadurai, K., R, Hattiwale, V. P., & Ravindran, B. (2012). *Adaptive network intrusion detection system using a hybrid approach.* Paper presented at the Communication Systems and Networks (COMSNETS), 2012 Fourth International Conference on (pp. 1-7). IEEE.

RavinderReddy, R., Kavya, B., & Ramadevi, Y. (2014). A Survey on SVM Classifiers for Intrusion Detection. *International Journal of Computer Applications, 98*(19), 34-44.

Revathi, S., & Malathi, A. (2014). Network Intrusion Detection Using Hybrid Simplified Swarm Optimization and Random Forest Algorithm on Nsl-Kdd Dataset. *International Journal Of Engineering And Computer Science, 3*(2), 3873-3876.

Sanyal, S., & Thakur, M. R. (2012). A Hybrid Approach towards Intrusion Detection Based on Artificial Immune System and Soft Computing. *arXiv preprint arXiv:1205.4457*.

Satpute, K., Agrawal, S., Agrawal, J., & Sharma, S. (2013). *A survey on anomaly detection in network intrusion detection system using particle swarm optimization based machine learning techniques.* Paper presented at the Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA).

Selman, A. H. (2013). Intrusion Detection System using Fuzzy Logic. *SouthEast Europe Journal of Soft Computing, 2*(1), 14 - 20.

Shanmugam, B., & Idris, N. B. (2011). Hybrid Intrusion Detection Systems (HIDS) using Fuzzy Logic. *Intrusion Detection Systems, Dr. Pawel Skrobanek, Ed. Croatia, Europe: InTech*, 135-155.

Shiravi, A., Shiravi, H., Tavallaee, M., & Ghorbani, A. A. (2012). Toward developing a systematic approach to generate benchmark datasets for intrusion detection. *Computers & Security*, *31*(3), 357-374.

Shivakumar, M., Subalakshmi, R., Shanthakumari, S., & Joseph, S. J. (2013). Architecture for Network-Intrusion Detection and Response in open Networks using Analyzer Mobile Agents. *International Journal of Scientific Research in Network Security and Communication, 1*, 1-7.

Siddiqui, M. (2004). *High performance data mining techniques for intrusion detection.* University of Central Florida Orlando, Florida.

Song, G., Guo, J., & Nie, Y. (2011). *An Intrusion Detection Method based on Multiple Kernel Support Vector Machine.* Paper presented at the Network Computing and Information Security (NCIS), 2011 International Conference on (Vol. 2, pp. 119-123). IEEE.

Stein, G., Chen, B., Wu, A. S., & Hua, K. A. (2005). *Decision tree classifier for network intrusion detection with GA-based feature selection.* Paper presented at the Proceedings of the 43rd annual Southeast regional conference-Volume 2.

Sung, A. H., & Mukkamala, S. (2003). *Identifying important features for intrusion detection using support vector machines and neural networks.* Paper presented at the Applications and the Internet, 2003. Proceedings. 2003 Symposium on on (pp. 209-216). IEEE.

Tavallaee, M. (2011). *An Adaptive Hybrid Intrusion Detection System.* University of New Brunswick.

Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A.-A. (2009). *A detailed analysis of the KDD CUP 99 data set.* Paper presented at the Proceedings of the Second IEEE Symposium on Computational Intelligence for Security and Defence Applications 2009.

Teng, S., Du, H., Wu, N., Zhang, W., & Su, J. (2010). A cooperative network intrusion detection based on fuzzy SVMs. *Journal of Networks, 5*(4), 475-483.

Upadhyaya, D., & Jain, S. (2013). Hybrid Approach for Network Intrusion Detection System Using K-Medoid Clustering and Naïve Bayes Classification. *International Journal of Computer Science Issues (IJCSI), 10*(3), 231 - 236.

Wang, Hao, J., Ma, J., & Huang, L. (2010). A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering. *Expert Systems with Applications, 37*(9), 6225-6232.

Wang, Zhang, X., Gombault, S., & Knapskog, S. J. (2009). *Attribute normalization in network intrusion detection.* Paper presented at the Pervasive Systems, Algorithms, and Networks (ISPAN), 2009 10th International Symposium on (pp. 448-453). IEEE.

Wang, Y. (2004). *A comparitive study of classification alforithms for network intrusion detection.* (Degree of Master), Florida Atlantic University.

Wankhade, K., Patka, S., & Thool, R. (2013). *An Overview of Intrusion Detection Based on Data Mining Techniques.* Paper presented at the Communication Systems and Network Technologies (CSNT), 2013 International Conference on (pp. 626-629). IEEE.

Xiang, C., Xiao, Y., Qu, P., & Qu, X. (2014). Network Intrusion Detection Based on PSO-SVM. *TELKOMNIKA Indonesian Journal of Electrical Engineering, 12*(2), 1502-1508.

Yang, J., & Ning, Y. (2010). *Research on feature weights of fuzzy c-means algorithm and its application to intrusion detection.* Paper presented at the Environmental Science and Information Application Technology (ESIAT), 2010 International Conference on (Vol. 3, pp. 164-166). IEEE.

Yassin, W., Udzir, N. I., Muda, Z., & Sulaiman, M. N. (2013). *Anomaly-based intrusion detection through K-Mean clustering and Naives bayes classification.* Paper presented at the 4th International Conference on Computing and Informatics, ICOCI, Sarawak, Malaysia.

Zhou, M. (2005). *Network Intrusion Detection: Monitoring, Simulation and Visualization.* University of Central Florida Orlando, Florida.