A CLASSIFIER MECHANISM FOR HOST-BASED INTRUSION DETECTION AND PREVENTION SYSTEM IN CLOUD COMPUTING ENVIRONMENT

AWS NASER JABER AL-ZARQAWEE

DOCTOR OF PHILOSOPHY

UNIVERSITI MALAYSIA PAHANG

SUPERVISOR'S DECLARATION

We hereby declare that we have checked this thesis, and, in our opinion, this thesis is adequate in terms of scope and quality for the award of the degree of Doctor of Philosophy

_____

(Supervisor's Signature)

Full Name : T.S DR. MOHAMAD FADLI ZOLKIPLI

Position : SENIOR LECTURER

Date : / /2018

_____

(Co-supervisor's Signature)

Full Name : DR. MAZLINA BINTI ABDUL MAJID

Position : ASSOC. PROFESSOR

Date : / /2018

STUDENT'S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Universiti Malaysia Pahang or any other institutions.

_____

(Student's Signature)

Full Name : AWS NASER JABER AL-ZARQAWEE

ID Number : PCC13011

Date : / /2018

A CLASSIFIER MECHANISM FOR HOST BASED INTRUSION DETECTION AND PREVENTION SYSTEM IN CLOUD COMPUTING ENVIRONMENT

AWS NASER AL-ZARQAWEE

Thesis submitted in fulfilment of the requirements
for the award of the degree of
Doctor of Philosophy

Faculty of Computer Systems and Software Engineering

UNIVERSITI MALAYSIA PAHANG

SEPTEMBER 2018

DEDICATION

Dedicated to my parents.

For their endless love, support and encouragement.

ACKNOWLEDGEMENTS

Alhamdulillah with the will of Allah, I have successfully completed this research. Without the strength applied to me, I would not be able to finish this subject field on time devoted. This thesis is prepared to fulfil the requirements for Doctor of Philosophy from Faculty of Computer Systems & Software Engineering, Universiti Malaysia Pahang

I would like to take this opportunity to convey my sincere thanks and deepest gratitude to Dr. Mohamad Fadli Zolkipli and Associate Professor Dr. Mazlina Abdul Majid for all their help and valuable guidance provided to me during the preparation of this thesis.

I consider myself privileged to have had the opportunity to work under his guidance. Moreover, I would like to dedicate this thesis to the dearest ones, my wife Zena for her patience and the encouragement he provided me with during the entire period of the study, and my mother who shared the stress in my life, encouraged me in times of dismay, cheered me up in times of distress, and renewed my hope in times of despair

ABSTRAK

Serangan Distributed Denial-of-Service (DDoS) adalah insiden yang sering berlaku dalam persekitaran pengkomputeran awam yang menyebabkan gangguan utama prestasi. Sistem pengesanan dan pencegahan pencerobohan (IDP) adalah merupakan alat untuk melindungi daripada sebarang insiden tersebut, dan penempatan sistem ID/IP yang tepat pada rangkaian adalah sangat penting untuk pemantauan yang optimum dan mencapai keberkesanan yang maksimum dalam melindungi sistem. Walaupun dengan adanya sistem tersebut, tahap keselamatan pengkomputeran awam mesti dipertingkatkan. Semakin banyak serangan yang lebih kuat cuba untuk mengawal persekitaran pengkomputeran awam tersebut; serangan tersebut adalah termasuk hyperjacking mesin-maya (VM) dan juga ancaman keselamatan rangkaian tradisional seperti pengintipan trafik (memintas trafik rangkaian), pengintipan alamat dan pemalsuan VM atau alamat IP. Menguruskan IDPS berasaskan hos (H-IDPS) adalah sangat sukar kerana maklumat perlu dikongfigurasikan dan diuruskan oleh setiap hos, ianya penting untuk memastikan penganalisis keselamatan dapat memahami struktur rangkaian sepenuhnya bagi membezakan antara positif palsu dan masalah sebenar. Untuk tujuan tersebut, adalah sangat penting untuk memahami pengelas paling utama dalam pembelajaran mesin, kerana ianya menawarkan perlindungan terhadap penggera positif palsu dalam serangan DDoS. Bagi merancang lebih banyak pengelasan yang berkesan, sistem bagi menilai pengelas perlu dibangunkan. Dalam thesis ini, mekanisma reka bentuk untuk pengelas H-IDPS dalam persekitaran pengkomputeran awam telah dibangunkan. Reka bentuk mekanisme ini berdasarkan Optimasi Antlion hibrid Algoritma (ALO) dengan Multilayer Perceptron (MLP) untuk berlindung dari serangan DDoS. Untuk melaksanakan mekanisme yang dicadangkan, kami menunjukkan kekuatan pengelas menggunakan satu dataset yang dikurangkan dimensi menggunakan NSL-KDD. Selain itu, kami memberi tumpuan terperinci kepada kajian dataset NSL-KDD yang mengandungi hanya rekod terpilih. Dataset yang dipilih ini menyediakan analisis yang baik terhadap pelbagai teknik pembelajaran mesin untuk H-IDPS. Penilaian terhadap Sistem H-IDPS ini menunjukkan peningkatan ketepatan pengesanan pencerobohan dan mengurangkan penggera positif palsu berbanding hasil kajian lain yang berkaitan. Ini dapat digambarkan dengan menggunakan teknik matriks kekeliruan untuk mengatur pengelas, menggambarkan prestasi dan menilai tingkah laku secara keseluruhan.

ABSTRACT

Distributed denial-of-service (DDoS) attacks are incidents in a cloud computing environment that cause major performance disturbances. Intrusion-detection and prevention system (IDPS) are tools to protect against such incidents, and the correct placement of ID/IP systems on networks is of great importance for optimal monitoring and for achieving maximum effectiveness in protecting a system. Even with such systems in place, however, the security level of general cloud computing must be enhanced. More potent attacks attempt to take control of the cloud environment itself; such attacks include malicious virtual-machine (VM) hyperjacking as well as traditional network-security threats such as traffic snooping (which intercepts network traffic), address spoofing and the forging of VMs or IP addresses. It is difficult to manage a host-based IDPS (H-IDPS) because information must be configured and managed for every host, so it is vital to ensure that security analysts fully understand the network and its context in order to distinguish between false positives and real problems. For this, it is necessary to know the current most important classifiers in machine learning, as these offer feasible protection against false-positive alarms in DDoS attacks. In order to design a more efficient classifier, it is necessary to develop a system for evaluating the classifier. In this thesis, a new mechanism for an H-IDPS classifier in a cloud environment has desigend. The mechanism's design is based on the hybrid Antlion Optimization Algorithm (ALO) with Multilayer Perceptron (MLP) to protect against DDoS attacks. To implement the proposed mechanism, we demonstrate the strength of the classifier using a dimensionally reduced dataset using NSL-KDD. Furthermore, we focus on a detailed study of the NSL-KDD dataset that contains only selected records. This selected dataset provides a good analysis of various machine-learning techniques for H-IDPS. The evaluation process H-IDPS system shows the increases of intrusion detection accuracy and decreases the false positive alarms when compared to other related works. This is epitomized by the skilful use of the confusion matrix technique for organizing classifiers, visualizing their performance, and assessing their overall behaviour.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ALAD	Application Layer Anomaly Detection
ALO	Antlion Optimization Algorithm
ANN	Artificial Neural Network
BPNN	Backpropagation Neural Network
CPU	Central Processing Unit
DARPPA	Defence Advanced Research Projects Agency
DDoS	Denial-Of-Service Attack
DNS	Domain Name System
EV	Evolutionary Computation
FDR	Fisher's Discriminant Ratio
FL	Fuzzy Logic
FN	False Negative
FP	False Positive
GA	Genetic Algorithm
GAR-forest	Greedy randomized adaptive search procedure with annealed randomness
GRASP	Greedy Randomized Adaptive Search Procedure
H-IDPS	Host-Based Intrusion Detection and Prevention System
HTTP	Hypertext Transfer Protocol
IASS	Infrastructure as A Service
ICMP	Internet Control Message Protocol
IDPS	Intrusion Detection System and Prevention System
IDS	Intrusion Detection System
IP	Internet Protocol Address
IPS	Intrusion Prevention Systems
IT	Information Technology
KNN	K-Nearest Neighbours
KVM	Kernel-Based Virtual Machine
LAN	Local Area Network
LDA	Linear Discriminant Analysis
LERAD	Learning Rules for Anomaly Detection

MLF	Multi-Level Fuzzy Min-Max Neural Network
MLP	Multilayer Perceptron
NN	Neural Network
NTP	Network Time Protocol
OTN	Option List
PASS	Platform as A Service
PCA	Principal Component Analysis
PCAP	Packet Capture
PHAD	Packet Header Anomaly Detection
QoS	Quality of Service
R2L	Remote to Local Attack
RQs	Research Questions
SAAS	Software as A Service
SU	Symmetrical Uncertainty
SVM	Support Vector Machine
SYN	Synchronize
TN	True Negatives
TP	True Positive
TTL	Time to Live
U2R	User to Root Attack
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
VLAN	Virtual LAN
VMs	Virtual Machines
XML	Extensible Markup Language

REFERENCES

Aburomman, A. A., & Reaz, M. B. I. (2016). *Ensemble of Binary SVM Classifiers Based on PCA and LDA Feature Extraction for Intrusion detection*. Advanced Information Management, Communicates, Electronic and Automation Control Conference , pp. 636-640.IEEE.

Agrawal, N., & Tapaswi, S. (2017). Defense Schemes for Variants of Distributed Denial-Of-Service (DDoS) attacks in cloud computing: A survey. *Information Security Journal: A Global Perspective, 26*(2), pp. 61-73.

Ahmad, T., Haque, M. A., Al-Nafjan, K., & Ansari, A. A. (2013). Development of Cloud Computing and Security Issues. *Information and Knowledge Management*. Vol. 3, No. 1.

Badis, H., Doyen, G., & Khatoun, R. (2014). *Toward a Source Detection of Botclouds: a PCA-Based Approach.* International Conference on Autonomous Infrastructure, Management and Security, pp. 105-117. Springer, Berlin, Heidelberg.

Behal, S., & Kumar, K. (2016). Trends in Validation of DDoS Research. *Procedia Computer Science*, 85, pp.7-15.

Bhardwaj, A., Subrahmanyam, G. V. B., Avasthi, V., Sastry, H., & Goundar, S. (2016). *DDoS attacks, New DDoS Taxonomy and Mitigation Solutions—A survey*. International Conference on Signal Processing, Communication, Power and Embedded System, pp.793-798. IEEE.

Bharot, N., Verma, P., Sharma, S., & Suraparaju, V. (2017). Distributed Denial-Of-Service Attack Detection and Mitigation Using Feature Selection and Intensive Care Request Processing Unit. *Arabian Journal for Science and Engineering*, 43(2), pp.959-967.

Bhat, A. H., Patra, S., & Jena, D. (2013). Machine Learning Approach For Intrusion Detection on Cloud Virtual Machines. *International Journal of Application or Innovation in Engineering & Management (IJAIEM), 2*(6), pp.56-66.

Birje, M. N., Challagidad, P. S., Goudar, R., & Tapale, M. T. (2017). Cloud computing Review: Concepts, Technology, Challenges and Security. *International Journal of Cloud Computing, 6*(1), pp.32-57.

Boughorbel, S., Jarray, F., & El-Anbari, M. (2017). Optimal Classifier for Imbalanced Data Using Matthews Correlation Coefficient metric. *PLoS ONE,* 12(6), pp.1-17.

Chatterjee, T., & Bhattacharya, A. (2014). VHDL Modeling of Intrusion Detection & Prevention System (IDPS) A Neural Network Approach. *International Journal of Computer Trends and Technology (IJCTT)*. 8(1), pp.52-56.

Chen, Chia-Mei, D. J. Guan, Yu-Zhi Huang, and Ya-Hui Ou. *Attack Sequence Detection in Cloud Using Hidden Markov Model*. 7th Asia Joint Conference on Information Security, pp. 100-103. IEEE.

Chiba, Z., Abghour, N., Moussaid, K., & Rida, M. (2016). A Cooperative and Hybrid Network Intrusion Detection Framework in Cloud Computing Based on Snort And Optimized Back Propagation Neural Network. *Procedia Computer Science, 83*, pp. 1200-1206.

Cunningham, J. P., & Ghahramani, Z. (2015). Linear Dimensionality Reduction: Survey, Insights, and Generalizations. *The Journal of Machine Learning Research, 16*(1), pp. 2859-2900.

Da Silva Filho, H. C., de Figueiredo Carneiro, G., Costa, E. S. M., & Monteiro, M. (2018). Tools to Support SMEs to Migrate to the Cloud: Opportunities and Challenges. In *Information Technology-New Generations*, pp. 159-165. Springer, Cham.

Daryabar, F., Dehghantanha, A., Eterovic-Soric, B., & Choo, K.-K. R. (2016). Forensic Investigation of OneDrive, Box, GoogleDrive and Dropbox Applications on Android and iOS devices. *Australian Journal of Forensic Sciences, 48*(6), pp. 615-642.

De la Hoz, E., de la Hoz, E., Ortiz, A., Ortega, J., & Martínez-Álvarez, A. (2014). Feature Selection by Multi-Objective Optimisation: Application to Network Anomaly Detection by Hierarchical Self-Organising Maps. *Knowledge-Based Systems, 71*, pp. 322-338.

De la Hoz, E., De La Hoz, E., Ortiz, A., Ortega, J., & Prieto, B. (2015). PCA Filtering and Probabilistic SOM for Network Intrusion Detection. *Neurocomputing, 164*, pp. 71-81.

Denning, T., Kohno, T., & Shostack, A. (2013). Control-Alt-Hack: *A card game for computer security outreach and education*.Technical Symposium on Computer Science Education, pp. 729-729. ACM.

Deshpande, P., Sharma, S. C., Peddoju, S. K., & Junaid, S. (2014). HIDS: A Host Based Intrusion Detection System for Cloud Computing Environment. *International Journal of System Assurance Engineering and Management*, 9(3), pp. 567-576.

Drago, I., Mellia, M., M Munafo, M., Sperotto, A., Sadre, R., & Pras, A. (2012). *Inside Dropbox: Understanding Personal Cloud Storage Services*. Internet Measurement Conference, pp. 481-494. ACM.

Eid, H. F., Darwish, A., Hassanien, A. E., & Kim, T.-h. (2011). Intelligent Hybrid Anomaly Network Intrusion Detection System. In *Communication and Networking*, pp. 209-218. Springer.

Elkhadir, Z., Chougdali, K., & Benattou, M. (2017, April). *A Median Nearest Neighbors LDA for Anomaly Network Detection*. International Conference on Codes, Cryptology, and Information Security, pp. 128-141. Springer, Cham.

Enache, A. C., & Patriciu, V. V. (2014, May). *Intrusions Detection Based On Support Vector Machine Optimized with Swarm Intelligence.* IEEE International Symposium on Applied Computational Intelligence and Informatics, pp. 153-158. IEEE.

Everett, C. (2009). Cloud computing – A Question of Trust. *Computer Fraud & Security, 2009*(6), pp. 5-7.

Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges. *Computers & Security, 28*(1), pp.18-28.

Garg, A., & Maheshwari, P. (2016, January). *PHAD: Packet Header Anomaly Detection*. International Conference on Intelligent Systems and Control (ISCO), pp. 1-5. IEEE.

Ghamisi, P., & Benediktsson, J. A. (2015). Feature Selection Based on Hybridization Of Genetic Algorithm and Particle Swarm Optimization. *IEEE Geoscience and Remote Sensing Letters, 12*(2), pp. 309-313.

Ghosh, P., & Mitra, R. (2015, February). *Proposed GA-BFSS and Logistic Regression Based Intrusion Detection System*. Conference on Computer, Communication, Control and Information Technology, pp. 1-6. IEEE.

Gillman, D., Lin, Y., Maggs, B., & Sitaraman, R. K. (2015). Protecting Websites from Attack with Secure Delivery Networks. *Computer, 48*(4), pp. 26-34.

Grossman, R. L., Gu, Y., Sabala, M., & Zhang, W. (2009). Compute and Storage Clouds Using Wide Area High Performance Networks. *Future Generation Computer Systems, 25*(2), pp.179-183.

Hassanien, A. E., Kim, T.-H., Kacprzyk, J., & Awad, A. I. (2014). *Bio-inspiring Cyber Security and Cloud Services: Trends and Innovations, v*ol. 70. Springer.

Hatef, M. A., Shaker, V., Jabbarpour, M. R., Jung, J., & Zarrabi, H. (2018). HIDCC: A Hybrid Intrusion Detection Approach in Cloud Computing. *Concurrency and Computation: Practice and Experience, 30*(3).

Himmel, M. A., & Grossman, F. (2014). Security on Distributed Systems: Cloud Security Versus Traditional IT. *IBM Journal of Research and Development*, 58(1), pp. 3-1.

Hota, H., & Shrivas, A. K. (2014). *Data Mining Approach for Developing Various Models Based on Types of Attack and Feature Selection as Intrusion Detection Systems (IDS)*. International Conference on Advanced Computing, Networking, and Informatics, vol 243, pp. 845-851. Springer.

Ingre, B., & Yadav, A. (2015*). Performance Analysis of NSL-KDD Dataset using ANN*. International Conference on Signal Processing and Communication Engineering Systems, pp. 92-96. IEEE.

Iyengar, N. C. S., Banerjee, A., & Ganapathy, G. (2014). A Fuzzy Logic Based Defense Mechanism Against Distributed Denial of Services Attack in Cloud Environment. *International Journal of Communication Networks and Information Security*, 6(3).

Jaber, A. N., Zolkipli, M. F., Shakir, H. A., & Jassim, M. R. (2017). *Host Based Intrusion Detection and Prevention Model Against DDoS Attack in Cloud Computing.* International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, pp. 241-252. Springer, Cham.

Jiao, J., Ye, B., Zhao, Y., Stones, R. J., Wang, G., Liu, X.& Xie, G. (2017). *Detecting TCP-Based DDoS Attacks in Baidu Cloud Computing Data Centers*. 2017 IEEE Symposium on Reliable Distributed Systems, pp. 256-258. IEEE.

Kamatchi, R., Ambekar, K., & Parikh, Y. (2017). Security Mapping of a Usage Based Cloud System. *Network Protocols and Algorithms, 8*(4), pp. 56-71.

Kanakarajan, N. K., & Muniasamy, K. (2016). *Improving the Accuracy of Intrusion Detection Using GAR-Forest with Feature Selection*. International Conference on Frontiers in Intelligent Computing: Theory and Applications, pp. 539-547. Springer, New Delhi.

Karimi, A. M., Niyaz, Q., Sun, W., Javaid, A. Y., & Devabhaktuni, V. K. (2016). *Distributed Network Traffic Feature Extraction for A Real-Time IDS*. International Conference on Electro Information Technology, pp. 0522-0526. IEEE.

Kaul, S., Sood, K., & Jain, A. (2017). Cloud Computing and its Emerging Need: Advantages and Issues. *International Journal of Advanced Research in Computer Science, 8*(3).

Kazemi, S., Aghazarian, V., & Hedayati, A. (2015). Improving False Negative Rate in Hypervisor-Based Intrusion Detection in IaaS Cloud. *International Journal of Computing and Technology.2*(9).

Keerthi Vasan, K., & Surendiran, B. (2016). Dimensionality reduction using Principal Component Analysis for network intrusion detection. *Perspectives in Science, 8,* pp. 510-512.

Khan, M. T., Hyun, M., Kanich, C., & Ur, B. (2018). Forgotten But Not Gone: *Identifying the Need for Longitudinal Data Management in Cloud Storage*. Conference on Human Factors in Computing Systems (p. 543). ACM.

Kim, H., Kim, J., Kim, Y., Kim, I., & Kim, K. J. (2018). Design of Network Threat Detection and Classification Based on Machine Learning on Cloud Computing. *Cluster Computing*, 1-10.

Kizza, J. M. (2017). System Intrusion Detection and Prevention. In *Guide to computer network security*, pp. 275-301. Springer.

Kritikos, K., Kirkham, T., Kryza, B., & Massonet, P. (2017). Towards a Security-Enhanced PaaS Platform for Multi-Cloud Applications. *Future Generation Computer Systems, 67*, pp.206-226.

Kumar, P. A. R., & Selvakumar, S. (2013). Detection Of Distributed Denial of Service Attacks using an Ensemble Of Adaptive and Hybrid Neuro-Fuzzy Systems. *Computer Communications, 36*(3), pp.303-319.

Latha, S., & Prakash, S. J. (2017). *A Survey on Network Attacks and Intrusion detection Systems*. International Conference on Advanced Computing and Communication Systems, pp.1-7. IEEE

Lee, Y.-J., Yeh, Y.-R., & Wang, Y.-C. F. (2013). Anomaly Detection via Online Oversampling Principal Component Analysis. *IEEE Transactions on Knowledge and Data Engineering, 25*(7), pp.1460-1470.

Li, H., Liu, B., Mukherjee, A., & Shao, J. (2014). Spotting Fake Reviews Using Positive-Unlabeled Learning. *Computación y Sistemas, 18*(3), pp.467-475.

Lin, Y., & Li, B. (2018). WebAD^2: *A Cascading Model Based on Machine Learning for Web Attacks Detection*. International Conference on Security and Privacy in Communication Systems, pp. 145-165. Springer International Publishing.

Lonea, A. M., Popescu, D. E., & Tianfield, H. (2013). Detecting DDoS Attacks In Cloud Computing Environment. *International Journal of Computers Communications & Control, 8*(1), pp.70-78.

Maher, M., Smith, A., & Margiotta, J. (2014). *A Synopsis of the Defense Advanced Research Projects Agency (DARPA) Investment in Additive Manufacture and What Challenges Remain*. International Society for Optics and Photonics,vol. 8970, pp. 897002.

Mani, M., Bozorg-Haddad, O., & Chu, X. (2018). Ant Lion Optimizer (ALO) Algorithm. In *Advanced Optimization by Nature-Inspired Algorithms*, pp. 105-116. Springer.

Manickam, M., & Rajagopalan, S. P. (2018). A hybrid multi-Layer Intrusion Detection System in Cloud. *Cluster Computing*, pp.1-9.

Mirjalili, S. (2015). The Ant Lion Optimizer. *Advances in Engineering Software, 83*, pp. 80-98.

Mkuzangwe, N. N. P., & Nelwamondo, F. V. (2017). *A Fuzzy Logic Based Network Intrusion Detection System for Predicting the TCP SYN Flooding Attack*. Asian Conference on Intelligent Information and Database Systems, pp. 14-22. Springer, Cham.

Modi, C. N., & Acha, K. (2017). Virtualization layer security challenges and intrusion detection/prevention systems in cloud computing: a comprehensive review. *the Journal of Supercomputing*, *73*(3), 1192-1234.

Mohamed, E. M., Abdelkader, H. S., & El-Etriby, S. (2012). Enhanced data security model for cloud computing. International Conference on Informatics and Systems (pp. CC-12). IEEE.

More, S., & Chaudhari, S. (2016). Third Party Public Auditing Scheme for Cloud Storage. *Procedia Computer Science*, 79, pp. 69-76.

Mukhopadhyay, I., Chakraborty, M., Chakrabarti, S., & Chatterjee, T. (2011). Back Propagation Neural Network Approach to Intrusion Detection System. International Conference on Recent Trends in Information Systems, pp. 303-308. IEEE.

Nazer, G. M., & Selvakumar, A. A. L. (2011). Current Intrusion Detection Techniques in Information Technology-A Detailed Analysis. *European Journal of Scientific Research, 65*(4), pp. 611-624.

Ndibwile, J. D., Govardhan, A., Okada, K., & Kadobayashi, Y. (2015). *Web Server Protection Against Application Layer DDoS Attacks Using Machine Learning and Traffic Authentication*. Annual Computer Software and Applications Conference, vol. 3, pp. 261-267. IEEE.

Osanaiye, O., Cai, H., Choo, K.-K. R., Dehghantanha, A., Xu, Z., & Dlodlo, M. (2016). Ensemble-Based Multi-Filter Feature Selection Method for DDoS Detection in Cloud Computing. *EURASIP Journal on Wireless Communications and Networking, 2016*(1), pp.130.

Pajouh, H. H., Dastghaibyfard, G., & Hashemi, S. (2017). Two-Tier Network Anomaly Detection Model: A Machine Learning Approach. *Journal of Intelligent Information Systems, 48*(1), pp. 61-74.

Patel, A., Taghavi, M., Bakhtiyari, K., & JúNior, J. C. (2013). An intrusion detection and prevention system in cloud computing: A systematic review. *Journal of Network and Computer Applications, 36*(1), 25-41.

Perez-Botero, D., Szefer, J., & Lee, R. B. (2013). *Characterizing Hypervisor Vulnerabilities in Cloud Computing Servers*. International workshop on Security in cloud computing, pp. 3-10. ACM.

Pervez, M. S., & Farid, D. M. (2014). *Feature Selection and Intrusion Classification in NSL-KDD Cup 99 Dataset Employing SVMs*. 8th International Conference on Software, Knowledge, Information Management and Applications, pp. 1-6. IEEE.

Purwanto, Y., & Rahardjo, B. (2014). *Traffic Anomaly Detection in DDos Flooding Attack*. International Conference on Telecommunication Systems Services and Applications, pp. 1-6. IEEE.

Raja, S., & Ramaiah, S. (2016). Performance Comparison of Neuro-Fuzzy Cloud Intrusion Detection Systems. *Int. Arab J. Inf. Technol., 13*(1A), pp.142-149.

Rastegari, S., Hingston, P., & Lam, C.-P. (2015). Evolving statistical Rulesets For Network Intrusion Detection. *Applied Soft Computing, 33*, pp. 348-359.

Rathore, M. M., Ahmad, A., & Paul, A. (2016). Real Time Intrusion Detection System for Ultra-High-Speed Big Data Environments. *The Journal of Supercomputing, 72*(9), pp. 3489-3510.

Reddy, N. C. S., Vemuri, P. C. R., & Govardhan, A. (2017). Evaluation of PCA and K-means Algorithm for Efficient Intrusion Detection. *International Journal of Applied Engineering Research, 12*(12), pp. 3370-3376.

Saad, A. A., Khalid, C., & Mohamed, J. (2015). *Network Intrusion Detection System Based on Direct LDA*. 2015 Third World Conference on Complex Systems, pp. 1-6. IEEE.

Sahani, R., Rout, C., Badajena, J. C., Jena, A. K., & Das, H. (2018). Classification of Intrusion Detection Using Data Mining Techniques. *In Progress in Computing, Analytics and Networking*, pp. 753-764. Springer, Singapore.

Saied, A., Overill, R. E., & Radzik, T. (2016). Detection Of Known and Unknown DDoS Attacks Using Artificial Neural Networks. *Neurocomputing, 172*, pp. 385-393.

Salman, T., Bhamare, D., Erbad, A., Jain, R., & Samaka, M. (2017). Machine Learning for Anomaly Detection and Categorization in Multi-Cloud Environments. International Conference on Cyber Security and Cloud Computing, pp. 97-103. IEEE.

Sanchez, M. A., Castillo, O., & Castro, J. R. (2017). An Overview of Granular Computing Using Fuzzy Logic Systems. *In Nature-Inspired Design of Hybrid Intelligent Systems*, pp. 19-38. Springer, Cham.

Shah, B., & Trivedi, B. H. (2015). *Reducing Features of KDD CUP 1999 Dataset for Anomaly Detection using Back Propagation Neural Network*. International Conference on Advanced Computing & Communication Technologies. pp. 247-251. IEEE.

Singh, J., Kumar, K., Sachdeva, M., & Sidhu, N. (2012). DDoS Attack's Simulation using Legitimate and Attack Real Data Sets. *International Journal of Scientific & engineering research, 3*(6), pp.1-5.

Singh, K., Singh, P., & Kumar, K. (2017). Application Layer HTTP-GET Flood DDoS Attacks: Research landscape and challenges. *Computers & Security, 65*, pp. 344-372.

Su, B., Ding, X., Wang, H., & Wu, Y. (2017). Discriminative Dimensionality Reduction For Multi-Dimensional Sequences. *IEEE Transactions on Pattern Analysis and Machine Intelligence, PP*(99), pp.1-1.

Subashini, S., & Kavitha, V. (2011). A Survey on Security Issues in Service Delivery Models of Cloud Computing. *Journal of Network and Computer Applications, 34*(1), pp.1-11.

Sudharsan, N. S., & Latha, K. (2013). *Improvising Seeker Satisfaction in Cloud Community Portal: Dropbox*. 2013 International Conference on Communication and Signal Processing, pp. 321-325. IEEE.

Tang, J., Deng, C., & Huang, G.-B. (2016). Extreme Learning Machine for Multilayer Perceptron. *IEEE transactions on neural networks and learning systems, 27*(4), pp 809-821.

Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009, July). *A Detailed Analysis of the KDD CUP 99 Data Set.* Symposium on Computational Intelligence for Security and Defense Applications, pp. 1-6. IEEE.

Thaseen, I. S., & Kumar, C. A. (2014). *Intrusion Detection Model using Fusion of PCA and Optimized SVM*. International Conference on Contemporary Computing and Informatics, pp. 879-884. IEEE.

Usmani, S., Rehman, F., Umair, S., & Khan, S. A. (2018). A Review of Security Challenges in Cloud Storage of Big Data. *Handbook of Research on Big Data Storage and Visualization Techniques*, pp. 175-195. IGI Global.

Zlomislić, V., Fertalj, K., & Sruk, V. (2017). Denial of Service Attacks, Defences and Research Challenges. *Cluster Computing*, 20(1), pp. 661-671.