IMPROVED HYBRID TEACHING LEARNING BASED OPTIMIZATION-JAYA AND SUPPORT VECTOR MACHINE FOR INTRUSION DETECTION SYSTEMS

MOHAMMAD KHAMEES KHALEEL
ALSAJRI

DOCTOR OF PHILOSOPHY

UNIVERSITI MALAYSIA PAHANG

Universiti Malaysia PAHANG
Engineering • Technology • Creativity

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 : TS. DR. MOHD ARFIAN BIN ISMAIL
Position : SENIOR LECTURER
Date : 1 March 2022

____
(Co-supervisor's Signature)

Full Name : DR. JUNAIDA BINTI SULAIMAN
Position : SENIOR LECTURER
Date : 1 March 2022

Universiti
Malaysia
PAHANG
Engineering • Technology • Creativity

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 : MOHAMMAD KHAMEES KHALEEL ALSAJRI

ID Number : PCC17021

Date : 1 March 2022

IMPROVED HYBRID TEACHING LEARNING BASED OPTIMIZATION-JAYA AND SUPPORT VECTOR MACHINE FOR INTRUSION DETECTION SYSTEMS

MOHAMMAD KHAMEES KHALEEL ALSAJRI

Thesis submitted in fulfillment of the requirements
for the award of the
Doctor of Philosophy

Faculty of Computing
UNIVERSITI MALAYSIA PAHANG

March 2022

ACKNOWLEDGEMENTS

First and foremost, praises and thanks to the God, the Almighty, for His blessings throughout this study and for the grace to successfully complete the research.

I acknowledge the invaluable guidance of my supervisor, Dr Mohd Arfian Bin Ismail throughout this study. His motivation, vision, dynamism, and sincerity deeply inspired me throughout the study period. I consider it a great privilege to work under his guidance.

I am extremely grateful to my parents for their love, prayers, care, and sacrifices towards my education for a better future. I am much thankful to my wife and my daughters for their love, understanding, prayers and continuing support to complete this research work. Also, I express my thanks to my sisters, brothers, sister-in-law and brothers-in law for their support and valuable prayers. My special thanks go to my brother, Dr Ahmed Khamees Aljanabi, for the keen interest he showed towards a successful completion of this study. This study was supported by Fundamental Research Grant Scheme (FRGS) with Vote No. FRGS/1/2018/ICT02/UMP/02/2: RDU190113 from The Ministry of Higher Education (MOHE), Malaysia and managed by the University Malaysia Pahang (UMP)

Mohammad Khamees Khaleel Alsajri

March 2022 .

ABSTRAK

Sistem pengesanan pencerobohan (IDS) pada masa kini mempunyai beberapa kelemahan seperti kadar tanda palsu positif yang tinggi, kadar pengesanan yang rendah terhadap serangan yang jarang tetapi berbahaya, dan keperluan campur tangan manusia dan penalaan yang berterusan. Setiap hari, terdapat laporan mengenai insiden seperti penggodaman data untuk tujuan mencuri identiti, nombor kredit kad dan harta intelektual, serta untuk mengawal sumber rangkaian. Pendekatan pembelajaran mesin telah digunakan secara meluas untuk meningkatkan keberkesanan platform pengesanan pencerobohan. Walaupun beberapa teknik pembelajaran mesin adalah berkesan untuk mengesan jenis serangan tertentu, tidak ada kaedah yang diketahui digunakan secara universal dan mencapai hasil yang konsisten untuk pelbagai jenis serangan. Situasi ini menjadikan pengesanan serangan berasaskan siber pada rangkaian komputer adalah bidang penyelidikan yang relevan dan mencabar. Mesin vektor sokongan (SVM) adalah salah satu algoritma pembelajaran mesin yang paling berkesan, dan dengan ciri prestasi pembelajaran yang sangat baik. Walau bagaimanapun, SVM mengalami banyak masalah yang mempengaruhi prestasinya iaitu pemilihan ciri dan pengoptimuman parameter. Proses pemilihan ciri dan pengoptimuman parameter adalah operasi penting perlu dilakukan untuk meningkatkan prestasi SVM. Tujuan kajian ini adalah untuk membina satu kaedah pengoptimuman yang lebih baik bagi ISA yang cekap dan berkesan di dalam pemilihan ciri subset dan pengoptimuman parameter. Untuk mencapai tujuan kajian, satu algoritma pengoptimuman berasaskan pembelajaran pengajaran yang lebih baik telah dicadangkan dalam berurusan dengan pemilihan ciri subset. Sementara itu, satu algoritma Jaya selari yang lebih baik telah dicadangkan untuk pengoptimuman parameter. Kajian ini mencadangkan satu algoritma pengoptimuman berasaskan pembelajaran pengajaran yang lebih baik (ITLBO), algoritma yang dicadangkan digunakan untuk pemilihan ciri subset di dalam SVM, sementara itu algoritma Jaya selari yang lebih baik (IPJAYA) dicadangkan untuk mencari nilai parameter SVM (C, Gama) yang terbaik. Oleh itu, satu kaedah pengelasan berasaskan SVM tercipta yang di beri nama ITLBO-IPJAYA-SVM,di mana dapat meninggkatkan keberkesanan gangguan rangkaian pada set data yang mengandungi pelbagai kelas serangan. Kaedah-kaedah ini telah diuji dengan menggunakan set data pengesanan pencerobohan NSL-KDD dan CICIDS, dan hasilnya menunjukkan bahawa pendekatan yang dicadangkan yang digunakan dalam sistem berfungsi dengan baik dalam pemprosesan set data yang besar. Beberapa eksperimen telah dilakukan, hasil keputusan menunjukkan bahawa kaedah yang dicadangkan mencapai ketepatan 0.9823 untuk set data NSL-KDD dan 0.9817 untuk set data CICIDS, di mana ketepatan yang dihasilkan dalam kajian ini lebih tinggi berbanding kajian yang lain. Kesimpulannya, kajian ini telah mencadangkan satu kaedah pengoptimuman yang lebih baik bagi IDS di mana kaedah ini berupaya untuk menigkatkan ketepatan IDS dengan mencadangkan satu kaedah penambahbaikan dalam di dalam pemilihan pemilihan ciri subset dan pengoptimuman parameter.

ABSTRACT

Most of the currently existing intrusion detection systems (IDS) use machine learning algorithms to detect network intrusion. Machine learning algorithms have widely been adopted recently to enhance the performance of IDSs. While the effectiveness of some machine learning algorithms in detecting certain types of network intrusion has been ascertained, the situation remains that no single method currently exists that can achieve consistent results when employed for the detection of multiple attack types. Hence, the detection of network attacks on computer systems has remain a relevant field of research for some time. The support vector machine (SVM) is one of the most powerful machine learning algorithms with excellent learning performance characteristics. However, SVM suffers from many problems, such as high rates of false positive alerts, as well as low detection rates of rare but dangerous attacks that affects its performance; feature selection and parameters optimization are important operations needed to increase the performance of SVM. The aim of this work is to develop an improved optimization method for IDS that can be efficient and effective in subset feature selection and parameters optimization. To achieve this goal, an improved Teaching Learning-Based Optimization (ITLBO) algorithm was proposed in dealing with subset feature selection. Meanwhile, an improved parallel Jaya (IPJAYA) algorithm was proposed for searching the best parameters (C, Gama) values of SVM. Hence, a hybrid classifier called ITLBO-IPJAYA-SVM was developed in this work for the improvement of the efficiency of network intrusion on data sets that contain multiple types of attacks. The performance of the proposed approach was evaluated on NSL-KDD and CICIDS intrusion detection datasets and from the results, the proposed approaches exhibited excellent performance in the processing of large datasets. The results also showed that SVM optimization algorithm achieved accuracy values of 0.9823 for NSL-KDD dataset and 0.9817 for CICIDS dataset, which were higher than the accuracy of most of the existing paradigms for classifying network intrusion detection datasets. In conclusion, this work has presented an improved optimization algorithm that can improve the accuracy of IDSs in the detection of various types of network attack.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

IDS	Intrusion detection system
IPS	Intrusion prevention system
SSO	Simplified swarm optimization
ACO	Ant Colony Optimization
SVM	Support vector machine
TLBO	Teaching learning-based optimisation algorithm
ITLBO	Improved Teaching learning-based optimisation algorithm
IPJAYA	Improved parallel JAYA
HIDS	Host-based Intrusion Detection System
NIDS	Network Intrusion Detection Systems
ADAM	Audit Data Analysis and Mining
MADAMID	Mining Audit Data for Automated Models for Intrusion Detection
IoT	Internet of Things
ALAC	Adaptive Learner for Alert Classification
ML	Machine Learning
K-NN	k-Nearest Neighbour
SADE	self-adaptive differential evolution
ANN	Artificial Neural Networks
DNN	Deep Neural Networks
RNN	Recurrent Neural Network
RBM	restricted Boltzmann machines
CNN	convolutional neural network
DT	Decision Trees
GA	Genetic Algorithm
PCA	principle component analysis
DR	Detection Rate
BN	Bayesian network
MCLP	multiple criteria linear programming

PSO	Particle swarm optimization algorithm
MCX	multi-cut crossover
FSS	Feature subset selection
RBF	radial basis function
HS	Hybrid Swarm
HSO	Hybrid Swarm Optimization
TP	True Positive
FP	False Positive
TN	True Negative
FN	False Negative
FPR	False Positive Rate
FNR	False Negative Rate
ACC	Accuracy
F-M	F-Measure
ER	Error Rate
DOS	Denial of service attack
R2L	Remote to User attack
R2U	User to Root Attack
IDDM	Intrusion Detection Using Data Mining Techniques
NN	Neural networks
BMA	Bayesian Model Averaging
CPD	conditional probability distribution
LS-SVM	Least Square Support Vector Machine
KPCA	kernel principal component analysis
MU	Mobile Unit
NEP	Nash Equilibrium Point
NFV	Network Functions Virtualization
NP-hard	Non-Deterministic Polynomial-Time hard
TVCPSO	time varying chaos particle swarm optimization
HG-GA	Hypergraph based Genetic Algorithm

REFERENCES

Abdulhammed, R., Musafer, H., Alessa, A., Faezipour, M., & Abuzneid, A. (2019). Features Dimensionality Reduction Approaches for Machine Learning Based Network Intrusion Detection. *Electronics,Vol. 8* No.3, 322.

Abraham, T. (2001). IDDM: Intrusion detection using data mining techniques. *defence science and technology organisation salisbury (australia) electronics and surveillance research.*

Aburomman, A. A., & Reaz, M. B. I. (2017). A survey of intrusion detection systems based on ensemble and hybrid classifiers. *Computers & Security, Vol.65,*pp. 135-152.

Alaidaros, H., Mahmuddin, M., & Al Mazari, A. (2011, November). An overview of flow-based and packet-based intrusion detection performance in high speed networks. *In Proceedings of the International Arab Conference on Information Technology* (pp. 1-9).

Alhakami, W., ALharbi, A., Bourouis, S., Alroobaea, R., & Bouguila, N. (2019). Network Anomaly Intrusion Detection Using a Nonparametric Bayesian Approach and Feature Selection. *IEEE Access, Vol.7,*pp. 52181-52190.

Aljarah, I., & Ludwig, S. A. (2013, June). MapReduce intrusion detection system based on a particle swarm optimization clustering algorithm. In *2013 IEEE congress on evolutionary computation* (pp. 955-962). IEEE.

Aljarah, I., & Ludwig, S. A. (2013, June). Mapreduce intrusion detection system based on a particle swarm optimization clustering algorithm. *In 2013 IEEE congress on evolutionary computation* (pp. 955-962). IEEE.

Al-Qatf, M., Lasheng, Y., Al-Habib, M., & Al-Sabahi, K. (2018). Deep Learning Approach Combining Sparse Autoencoder With SVM for Network Intrusion Detection. *IEEE Access,Vol. 6,*pp. 52843-52856.

Alsajri, M., Ismail, M. A., & Abdul-Baqi, S. (2018). A review on the recent application of Jaya optimization algorithm. Paper presented at the 2018 *1st Annual International Conference on Information and Sciences* (AiCIS) (pp. 129-132). IEEE.

Altwaijry, H. (2013). Bayesian based intrusion detection system. In *IAENG Transactions on Engineering Technologies* (pp. 29-44): Springer.

Amor, N. B., Benferhat, S., & Elouedi, Z. (2004, March). Naive bayes vs decision trees in intrusion detection systems. *In Proceedings of the 2004 ACM symposium on Applied computing* (pp. 420-424).

Anderson, D., Frivold, T., Tamaru, A., & Valdes, A. (1994). Next-generation intrusion detection expert system (NIDES), *software users manual, beta-update release. Computer Science Laboratory,* SRI International, Menlo Park, CA, USA, Technical Report SRI-CSL-95-0 (May 1994).

Aslahi-Shahri, B., Rahmani, R., Chizari, M., Maralani, A., Eslami, M., Golkar, M. J., & Ebrahimi, A. (2016). A hybrid method consisting of GA and SVM for intrusion detection system. *Neural computing and applications, vol. 27* issue 6,pp. 1669-1676.

Axelsson, S. (2000). Intrusion detection systems: A survey and taxonomy, *Technical repor*t (Vol. 99, pp. 1-15).

Azwar, H., Murtaz, M., Siddique, M., & Rehman, S. (2018, November). Intrusion Detection in secure network for Cybersecurity systems using Machine Learning and Data Mining. In *2018 IEEE 5th international conference on engineering technologies and applied sciences (ICETAS)* (pp. 1-9). IEEE.

Bamakan, S. M. H., Wang, H., Yingjie, T., & Shi, Y. (2016). An effective intrusion detection framework based on MCLP/SVM optimized by time-varying chaos particle swarm optimization. *Neurocomputing, Vol.199*,pp. 90-102.

Barbará, D., & Jajodia, S. (2002). Applications of data mining in computer security (Vol. 6): *Springer Science & Business Media.*

Bivens, A., Palagiri, C., Smith, R., Szymanski, B., & Embrechts, M. (2002). Network-based intrusion detection using neural networks. *Intelligent Engineering Systems through Artificial Neural Networks, Vol.12* No.1,pp. 579-584.

Bridges, S. M., & Vaughn, R. B. (2000, October). Fuzzy data mining and genetic algorithms applied to intrusion detection. *In Proceedings of 12th Annual Canadian Information Technology Security Symposium* (pp. 109-122).

Caplan, N. (2013). Cyber War: The Challenge to National Security. *Global Security Studies,* Vol. 4 Issue 1, p93-115. 23p.

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM computing surveys (CSUR), Vol.41* No.3,p. 15.

Chung, Y. Y., & Wahid, N. (2012). A hybrid network intrusion detection system using simplified swarm optimization (SSO). *Applied Soft Computing, Vol.12* No.9,pp. 3014-3022.

Council, N. R. (2009). Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities. Washington, DC: *The National Academies Press.*

Das, S. P., & Padhy, S. (2018). A novel hybrid model using teaching–learning-based optimization and a support vector machine for commodity futures index forecasting. *International Journal of Machine Learning and Cybernetics, Vol.9* No.1,pp. 97-111.

Das, S. P., Achary, N. S., & Padhy, S. (2016). Novel hybrid SVM-TLBO forecasting model incorporating dimensionality reduction techniques. *Applied Intelligence, Vol.45* No.4,pp. 1148-1165.

Dash, M., & Liu, H. (1997). Feature selection for classification. *Intelligent data analysis, 1*(1-4), 131-156.

Debar, H., Dacier, M., & Wespi, A. (2000, July). A revised taxonomy for intrusion-detection systems. *In Annales des télécommunications* (Vol. 55, No. 7, pp. 361-378). Springer-Verlag.

Denning, D. E. (1987). An intrusion-detection model. *IEEE Transactions on software engineering*, Volume: SE-13, Issue: 2, pp. 222-232.

Dorigo, M., Maniezzo, V., & Colorni, A. (1996). Ant system: optimization by a colony of cooperating agents. *IEEE Transactions on Systems, man, and cybernetics, Part B: Cybernetics, vol.26* No.1,pp. 29-41.

Dumais, S., Platt, J., Heckerman, D., & Sahami, M. (1998, November). Inductive learning algorithms and representations for text categorization. *In Proceedings of the seventh international conference on Information and knowledge management* (pp. 148-155).

Elhag, S., Fernández, A., Bawakid, A., Alshomrani, S., & Herrera, F. (2015). On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on intrusion detection systems. *Expert Systems with Applications, vol.42* No.1,pp. 193-202.

Fadlullah, Z. M., Nishiyama, H., Kato, N., & Fouda, M. M. (2013). Intrusion detection system (IDS) for combating attacks against cognitive radio networks. *IEEE network, Vol.27* No.3,pp. 51-56.

Farid, D. M., & Rahman, M. Z. (2010). Anomaly Network Intrusion Detection Based on Improved Self Adaptive Bayesian Algorithm. *J. Comput, vol.5* No.1,pp. 23-31.

Feng, W., Zhang, Q., Hu, G., & Huang, J. X. (2014). Mining network data for intrusion detection through combining SVMs with ant colony networks. *Future Generation Computer Systems,vol. 37*,pp. 127-140.

Fossaceca, J. M., Mazzuchi, T. A., & Sarkani, S. (2015). MARK-ELM: Application of a novel multiple kernel learning framework for improving the robustness of network intrusion detection. *Expert Systems with Applications, Vol.42* No.8,pp. 4062-4080.

Gatzlaff, K. M. (2012). Implications of privacy breaches for insurers. *Journal of Insurance Regulation*,vol 31issue 1, pp.190-197.

Gong, C. (2017). An Enhanced Jaya Algorithm with a Two Group Adaption. *International Journal of Computational Intelligence Systems, Vol.10* No.1,pp. 1102-1115.

Hausken, K., & Levitin, G. (2012). Review of systems defense and attack models. *International Journal of Performability Engineering, Vol.8* No.4,pp. 355-366.

Holland, J. H. (1992). Genetic algorithms. *Scientific american, Vol.267* No.1,pp. 66-73.

Hovav, A., & D'Arcy, J. (2004, June). The impact of virus attack announcements on the market value of firms. In *WOSIS* vol. 13 issue 3, pp. 146-156.

Huang, M.-Y., Jasper, R. J., & Wicks, T. M. (1999). A large scale distributed intrusion detection framework based on attack strategy analysis. *Computer Networks, vol. 31* issue 23,pp. 2465-2475.

Jabbar, M. A., Aluvalu, R., & Reddy, S. S. S. (2017, February). Cluster based ensemble classification for intrusion detection system. *In Proceedings of the 9th International Conference on Machine Learning and Computing* (pp. 253-257).

Jahan, A., Mustapha, F., Ismail, M. Y., Sapuan, S., & Bahraminasab, M. (2011). A comprehensive VIKOR method for material selection. *Materials & Design,Vol. 32* No.3,pp. 1215-1221.

Jajodia, D. B. J. C. S., & Wu, L. P. N. (2001). Adam: Detecting intrusions by data mining. In *Workshop on Information Assurance and Security* (Vol. 1, p. 1100).

Jan, S. U., Ahmed, S., Shakhov, V., & Koo, I. (2019). Toward a Lightweight Intrusion Detection System for the Internet of Things. *IEEE Access, Vol.7,*pp. 42450-42471.

Kabir, E., Hu, J., Wang, H., & Zhuo, G. (2018). A novel statistical technique for intrusion detection systems. *Future Generation Computer Systems, vol 79,*pp. 303-318.

Kannan, A., Maguire Jr, G. Q., Sharma, A., & Schoo, P. (2012, December). Genetic algorithm based feature selection algorithm for effective intrusion detection in cloud networks. *In 2012 IEEE 12th International Conference on Data Mining Workshops* (pp. 416-423). IEEE.

Kennedy, J., & Eberhart, R. (1995, November). Particle swarm optimization. *In Proceedings of ICNN'95-international conference on neural networks* (Vol. 4, pp. 1942-1948). IEEE..

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity, Vol.2* No.1,pp. 20-31.

Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications, vol.41* No.4,pp. 1690-1700.

Kiziloz, H. E., Deniz, A., Dokeroglu, T., & Cosar, A. (2018). Novel multiobjective TLBO algorithms for the feature subset selection problem. *Neurocomputing, vol. 306,* pp. 94-107.

Kuang, F., Xu, W., & Zhang, S. (2014). A novel hybrid KPCA and SVM with GA model for intrusion detection. *Applied Soft Computing, vol. 18,*pp. 178-184.

Kuang, F., Zhang, S., Jin, Z., & Xu, W. (2015). A novel SVM by combining kernel principal component analysis and improved chaotic particle swarm optimization for intrusion detection. *Soft Computing, vol.19* No.5,pp. 1187-1199.

Lee, W., & Stolfo, S. (1998). Data mining approaches for intrusion detection. Proceedings of the 7th USENIX Security Symposium, January 26-29, 1998, San Antonio, Texas

Lee, W., & Stolfo, S. J. (2000). A framework for constructing features and models for intrusion detection systems. *ACM transactions on Information and system security (TiSSEC), vol.3* No.4,pp. 227-261.

Levitin, K. H. G. (2012). Review of systems defense and attack models. *International Journal of Performability Engineering,* vol. *8* issue 4, pp. 348- 355.

Li, C., Wang, J., & Ye, X. (2018). Using a recurrent neural network and restricted Boltzmann machines for malicious traffic detection. *NeuroQuantology, vol.16* No.5,pp. 823-831.

Li, L., Yu, Y., Bai, S., Hou, Y., & Chen, X. (2017). An Effective Two-Step Intrusion Detection Approach Based on Binary Classification and k-NN. *IEEE Access, vol. 6,*pp. 12060-12073.

Li, L., Zhang, H., Peng, H., & Yang, Y. (2018). Nearest neighbors based density peaks approach to intrusion detection. *Chaos, Solitons & Fractals, vol.110,*pp. 33-40.

Liao, H.-J., Lin, C.-H. R., Lin, Y.-C., & Tung, K.-Y. (2013). Intrusion detection system: A comprehensive review. *Journal of network and computer applications, Vol.36* No.1,pp. 16-24.

Lin, W.-C., Ke, S.-W., & Tsai, C.-F. (2015). CANN: An intrusion detection system based on combining cluster centers and nearest neighbors. *Knowledge-Based Systems, vol.78*,pp. 13-21.

Ludwig, S. A. (2019). Applying a Neural Network Ensemble to Intrusion Detection. *Journal of Artificial Intelligence and Soft Computing Research, vol.9* No.3,pp. 177-188.

Luo, J., & Bridges, S. M. (2000). Mining fuzzy association rules and fuzzy frequency episodes for intrusion detection. *International Journal of Intelligent Systems, vol.15* No.8,pp. 687-703.

Ma, J., Liu, X., & Liu, S. (2008, October). A new intrusion detection method based on bpso-svm. *In 2008 International Symposium on Computational Intelligence and Design* (Vol. 1, pp. 473-477). IEEE.

Manzoor, I., & Kumar, N. (2017). A feature reduced intrusion detection system using ANN classifier. *Expert Systems with Applications, Vol.88*,pp. 249-257.

Migallón, H., Jimeno-Morenilla, A., & Sanchez-Romero, J.-L. (2018). Parallel improvements of the Jaya optimization algorithm. *Applied Sciences, Vol.8* No.5, 819.

Moradi, M., & Zulkernine, M. (2004, November). A neural network based system for intrusion detection and classification of attacks. *In Proceedings of the IEEE international conference on advances in intelligent systems-theory and applications* (pp. 15-18). IEEE Lux-embourg-Kirchberg, Luxembourg.

National Research Council. (2009). Technology, policy, law, and ethics regarding US acquisition and use of cyberattack capabilities. *National Academies Press (*pp. 55-80*)*.

Papamartzivanos, D., Mármol, F. G., & Kambourakis, G. (2018). Dendron: Genetic trees driven rule induction for network intrusion detection systems. *Future Generation Computer Systems,Vol. 79*,pp. 558-574.

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, vol.36* issue 1, pp. 25-41.

Peng, K., Leung, V., Zheng, L., Wang, S., Huang, C., & Lin, T. (2018). Intrusion detection system based on decision tree over big data in fog environment. *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 4680867, 10 pages.

Peterson, L. E. (2009). K-nearest neighbor. *Scholarpedia, Vol.4* No.2, pp. 1875-1883.

Phoungphol, P., Zhang, Y., & Zhao, Y. (2012). Robust multiclass classification for learning from imbalanced biomedical data. *Tsinghua Science and technology, Vol.17* No.6,pp. 619-628.

Pietraszek, T. (2004, September). Using adaptive alert classification to reduce false positives in intrusion detection. *In International workshop on recent advances in intrusion detection* (pp. 102-124). Springer, Berlin, Heidelberg.

Raghav, I., Chhikara, S., & Hasteer, N. (2013). Intrusion detection and prevention in cloud environment: a systematic review. *International Journal of Computer Applications,Vol. 68* No.24.

Rajasegarar, S., Leckie, C., Bezdek, J. C., & Palaniswami, M. (2010). Centered hyperspherical and hyperellipsoidal one-class support vector machines for anomaly detection in sensor networks. *IEEE Transactions on Information Forensics and Security, Vol.5* No.3, 518-533.

Raman, M. G., Somu, N., Kirthivasan, K., Liscano, R., & Sriram, V. S. (2017). An efficient intrusion detection system based on hypergraph-Genetic algorithm for parameter optimization and feature selection in support vector machine. *Knowledge-Based Systems, Vol.134*,pp. 1-12.

Rao, R. (2016). Jaya: A simple and new optimization algorithm for solving constrained and unconstrained optimization problems. *International Journal of Industrial Engineering Computations, Vol.7* No.1,pp. 19-34.

Rao, R. V., & Patel, V. (2013). An improved teaching-learning-based optimization algorithm for solving unconstrained optimization problems. *Scientia Iranica, Vol.20* No.3, 710-720.

Rao, R. V., & Patel, V. (2013). An improved teaching-learning-based optimization algorithm for solving unconstrained optimization problems. *Scientia Iranica, Vol.20* No.3,pp. 710-720.

Rao, R. V., Savsani, V. J., & Vakharia, D. (2011). Teaching–learning-based optimization: a novel method for constrained mechanical design optimization problems. *Computer-Aided Design, Vol.43* No.3, 303-315.

Rao, R. V., Savsani, V., & Balic, J. (2012). Teaching–learning-based optimization algorithm for unconstrained and constrained real-parameter optimization problems. *Engineering Optimization, Vol.44* No.12, 1447-1462.

Rodriguez, J. D., Perez, A., & Lozano, J. A. (2009). Sensitivity analysis of k-fold cross validation in prediction error estimation. *IEEE transactions on pattern analysis and machine intelligence,Vol. 32* No.3,pp. 569-575.

Salo, F., Injadat, M., Nassif, A. B., Shami, A., & Essex, A. (2018). Data Mining Techniques in Intrusion Detection Systems: A Systematic Literature Review. *IEEE Access,vol. 6,* pp. 56046-56058.

Samuel, A. L. (1967). Some studies in machine learning using the game of checkers. II—Recent progress. *IBM Journal of research and development, Vol. 11* No. 6, 601-617.

Samuel, O., Javaid, N., Aslam, S., & Rahim, M. H. (2018, March). JAYA optimization based energy management controller for smart grid: *In 2018 International Conference on Computing, Mathematics and Engineering Technologies* (iCoMET) (pp. 1-8). IEEE.

Schultz, E., Mellander, J., & Endorf, C. F. (2003). Intrusion Detection And Prevention *McGraw-Hill Osborne Media. December, Vol.18,* 221-254.

Senthilnayaki, B., Venkatalakshmi, K., & Kannan, A. (2015, March). Intrusion detection using optimal genetic feature selection and SVM based classifier. *In 2015 3rd international conference on signal processing, communication and networking* (ICSCN) (pp. 1-4). IEEE.

Shah, S. A. R., & Issac, B. (2018). Performance comparison of intrusion detection systems and application of machine learning to Snort system. *Future Generation Computer Systems, Vol. 80,* 157-170.

Shams, E. A., & Rizaner, A. (2018). A novel support vector machine based intrusion detection system for mobile ad hoc networks. *Wireless Networks, Vol. 24* no.5, pp. 1821-1829.

Shon, T., & Moon, J. (2007). A hybrid machine learning approach to network anomaly detection. *Information Sciences, Vol.177* No.18, 3799-3821.

Sinclair, C., Pierce, L., & Matzner, S. (1999, December). An application of machine learning to network intrusion detection. *In Proceedings 15th Annual Computer Security Applications Conference (ACSAC'99)* (pp. 371-377). IEEE.

Singh, R., Kumar, H., & Singla, R. (2015). An intrusion detection system using network traffic profiling and online sequential extreme learning machine. *Expert Systems with Applications,Vol. 42* No.22, 8609-8624.

Sokolova, M., & Lapalme, G. (2009). A systematic analysis of performance measures for classification tasks. *Information processing & management, Vol.45* No.4,pp. 427-437.

Sommer, R., & Paxson, V. (2010, May). Outside the closed world: On using machine learning for network intrusion detection. *In 2010 IEEE symposium on security and privacy* (pp. 305-316). IEEE.

Sultana, A., & Jabbar, M. A. (2016, July). Intelligent network intrusion detection system using data mining techniques. *In 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology* (iCATccT) (pp. 329-333). IEEE.

Tang, H., & Cao, Z. (2009). Machine learning-based intrusion detection algorithms. *Journal of Computational Information Systems, Vol.5* No.6, 1825-1831.

Tao, P., Sun, Z., & Sun, Z. (2018). An improved intrusion detection algorithm based on GA and SVM. *IEEE Access, vol. 6*, pp. 13624-13631.

Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009, July). A detailed analysis of the KDD CUP 99 data set. *In 2009 IEEE symposium on computational intelligence for security and defense applications* (pp. 1-6). IEEE.

Thangavel, M., Thangaraj, P., & Saravanan, K. (2010). Defend against Anomaly Intrusion Detection using SWT Mechanism. *International Journal of Innovation, Management and Technology,vol. 1* issue 2,pp. 201- 209.

Thaseen, I. S., & Kumar, C. A. (2017). Intrusion detection model using fusion of chi-square feature selection and multi class SVM. *Journal of King Saud University-Computer and Information Sciences, Vol.29* No.4,pp. 462-472.

Thottan, M., Liu, G., & Ji, C. (2010). Anomaly detection approaches for communication networks. In *Algorithms for Next Generation Networks* (pp. 239-261): Springer.

Tianfield, H. (2017). Data mining based cyber-attack detection. *System Simulation Technology, Vol.13* No.2, 3.

Tombini, E., Debar, H., Mé, L., & Ducassé, M. (2004, December). A serial combination of anomaly and misuse IDSes applied to HTTP traffic. *In 20th annual computer security applications conference* (pp. 428-437). IEEE.

Vapnik, V. The nature of statistical learning theory.[Sl]: *Springer science & business media*, 2013. *Citado na*, 27.

Vijayanand, R., Devaraj, D., & Kannapiran, B. (2018). Intrusion detection system for wireless mesh network using multiple support vector machine classifiers with genetic-algorithm-based feature selection. *Computers & Security, Vol.77,*pp. 304-314.

Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep Learning Approach for Intelligent Intrusion Detection System. *IEEE Access, Vol.7,*pp. 41525-41550.

Wahl, R. S. (2016). Latency in intrusion detection systems (IDS) and cyber-attacks: A quantitative comparative study (*Doctoral dissertation, Capella University*).

Wang, G., Chen, S., & Liu, J. (2015). Anomaly-based intrusion detection using multiclass-SVM with parameters optimized by PSO. *International Journal of Security and Its Applications, Vol.9* No.6, 227-242.

Wang, H., Xiao, Y., & Long, Y. (2017). Research of intrusion detection algorithm based on parallel SVM on spark. Paper presented at the *Electronics Information and Emergency Communication (ICEIEC), 2017 7th IEEE International Conference on,* (pp. 153-156). IEEE.

Wang, J., Hong, X., Ren, R. R., & Li, T. H. (2009). A real-time intrusion detection system based on PSO-SVM. In Proceedings. *The 2009 International Workshop on Information Security and Application* (IWISA 2009) (p. 319). Academy Publisher.

Wang, S.-H., Muhammad, K., Lv, Y., Sui, Y., Han, L., & Zhang, Y.-D. (2018). Identification of Alcoholism based on wavelet Renyi entropy and three-segment encoded Jaya algorithm. *Complexity,* vol. 2018, Article ID 3198184, 13 pages.

Wattanapongsakorn, N., Srakaew, S., Wonghirunsombat, E., Sribavonmongkol, C., Junhom, T., Jongsubsook, P., & Charnsripinyo, C. (2012, June). A practical network-based intrusion detection and prevention system. *In 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications* (pp. 209-214). IEEE.

Xiao, L., Chen, Y., & Chang, C. K. (2014, July). Bayesian model averaging of Bayesian network classifiers for intrusion detection. *In 2014 IEEE 38th International Computer Software and Applications Conference Workshops* (pp. 128-133). IEEE.

Xingzhu, W. (2015). ACO and SVM selection feature weighting of network intrusion detection method. *International Journal of Security and Its Applications, Vol.9* No.4, 129-270.

Xue, Y., Jia, W., Zhao, X., & Pang, W. (2018). An evolutionary computation based feature selection method for intrusion detection. *Security and Communication Networks,* vol. 2018, Article ID 2492956, 10 pages,.

Yayla, A. A., & Hu, Q. (2011). The impact of information security events on the stock value of firms: The effect of contingency factors. *Journal of Information Technology, vol. 26* issue 1,pp. 60-77.

Yi, Y., Wu, J., & Xu, W. (2011). Incremental SVM based on reserved set for network intrusion detection. *Expert Systems with Applications,Vol. 38* No.6,pp. 7698-7707.

Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access,Vol. 5*,pp. 21954-21961.

Yu, K., Liang, J., Qu, B., Chen, X., & Wang, H. (2017). Parameters identification of photovoltaic models using an improved JAYA optimization algorithm. *Energy Conversion and Management, Vol.150*,pp. 742-753.

Yu, Z., Tsai, J. J., & Weigert, T. (2007). An automatically tuning intrusion detection system. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), Vol.37* No.2,pp. 373-384.

Zamli, K. Z., Din, F., Baharom, S., & Ahmed, B. S. (2017). Fuzzy adaptive teaching learning-based optimization strategy for the problem of generating mixed strength t-way test suites. *Engineering Applications of Artificial Intelligence, Vol.59,*pp. 35-50.

Zhang, Y., Chen, X., Jin, L., Wang, X., & Guo, D. (2019). Network Intrusion Detection: Based on Deep Hierarchical Network and Original Flow Data. *IEEE Access, Vol.7,* pp.37004-37016.