REG NO : **16MIS0011**

NAME : **V.GOPIKA**

COURSE CODE : **SWE3002**

COURSE TITLE : **INFORMATION AND SYSTEM SECURITY**

SLOT : **C21+C22+TC23**

FACULTY NAME : **Prof. SUMAIYA THASEEN I**

PURPOSE : **J COMPONENT REVIEW - I**

DATE : **18-06-2019**

J COMPONENT REVIEW - I

INTRUSION DETECTION USING MACHINE LEARNING

I. LITERATUE SUMMARY TABLE WITH ADVANTAGES AND DISADVANTAGES

S. NO	PAPER TITLE	TECHNIQUES USED	ADVANTAGES	DISADVANTAGES
1	**Network Intrusion Detection System (NIDS) using Machine Learning Perspective**	1. Support Vector Machine (SVM) 2. Decision Tree 3. Naïve Bayes	• Provides more attack detection accuracy. • It increases the attack detection performance in short span of time.	• Long Training time is required for large datasets to get good accuracy. • High Algorithmic Complexity and extensive memory required.
2	**Network Intrusion Detection Using Machine Learning**	1. Support Vector Machine (SVM) 2. Proposed Method(Modified SVM)	• It provides high accuracy and lower false positive rate and false negative rate.	• Feature Selection is one of the most important parts, whereas the detection accuracy depends on feature selection.

3	**Machine Learning Methods for Network Intrusion Detection**	1. J48 Tree 2. Multilayer Perceptron (MLP) 3. Bayes Network	• Easy To Use and approximate any kind of input or output.	• The training is very slow and the training samples required is three times larger than normal training data set.
4	**Network Intrusion Detection System Using Machine Learning**	1. Decision Tree Classifier	• Processes both numerical and categorical data. • It handles high dimensional data.	• The output created may be more complex than expected. • Chances of detecting abnormal behavior as normal and normal as abnormal.
5	**Intrusion Detection Using Machine Learning: A Comparison Study**	1. Naïve Bayes 2. Support Vector Machine 3. Decision Tree 4. Neural Network 5. K Nearest Neighbor (KNN)	• High accuracy and speed is more. • Simple in implementation and easy to understand the flow.	• Lack of available probability of data. • The probability of the outcome is unstable.
6	**A Review of Intrusion Detection System using**	1. Decision Tree 2. Naïve Bayes	• Both Accuracy and Performance	• The complexity is little higher.

	Machine Learning Approach	3. K Nearest Neighbor 4. K Means 5. Support Vector Machine 6. Principle Component Analysis	are high. • Runs efficiently on large data sets with many features.	• Maintaining and updating the system may be difficult.
7	**Evaluation of Machine Learning Algorithms for Intrusion Detection System**	1. J48 2. Random Forest 3. Random Tree 4. Decision Table 5. Multi Layer Perceptron (MLP) 6. Naïve Bayes 7. Bayes Network	• The results obtained are more acceptable and the performance of the system was also good along with the pattern recognition.	• The time taken to detect the intrusion was higher than the regular time along with huge memory is required for computation
8	**Intrusion Detection System using AI and Machine Learning Algorithm**	1. K Means Clustering 2. Support Vector Machine 3. K Nearest Neighbors	• The results obtained from both evaluation and real life time was good.	• Selecting the appropriate data set determines the rest of the result.
9	**Intrusion detection model using machine learning**	1. Support Vector Machine (SVM) 2. Spark Chi-SVM Proposed Model	• Process, and analyze data with high speed.	• The high dimensionality makes the classification process more

	algorithm on Big Data environment			complex and takes long time.
10	**Application of Machine Learning Approaches in Intrusion Detection System: A Survey**	1. Support Vector Machine (SVM) 2. Decision Tree 3. Naïve Bayes 4. Logistic Regression 5. K Nearest Neighbor	• Very efficient to train and easy to implement as well as easy to measure the performance of complex algorithms.	• Removal of redundant and irrelevant features for data training is a key factor which determines system performance.

II. LITERATURE SUMMARY TABLE WITH DATASETS USED AND ACCURACY OBTAINED

S. NO	PAPER TITLE	TECHNIQUES USED	ACCURACY OBTAINED	DATASETS USED
1	**Network Intrusion Detection System (NIDS) using Machine Learning Perspective**	1. Support Vector Machine (SVM) 2. Decision Tree 3. Naïve Bayes	**91%** **89%** **82%**	KDDCup Dataset
2	**Network Intrusion Detection**	1. Support Vector Machine (SVM)	**88.03%**	ACCS (Australian

	Using Machine Learning	2. Proposed Method(Modified SVM)	**98.76%**	Centre for Cyber Security)
3	**Machine Learning Methods for Network Intrusion Detection**	1. J48 Tree 2. Multilayer Perceptron (MLP) 3. Bayes Network	**93.10%** **91.90%** **90.73%**	KDD Dataset (Knowledge Discovery And Data Mining)
4	**Network Intrusion Detection System Using Machine Learning**	1. Decision Tree Classifier	**90%**	CICIDS 2017
5	**Intrusion Detection Using Machine Learning: A Comparison Study**	1. Naïve Bayes 2. Support Vector Machine 3. Decision Tree 4. Neural Network 5. K Nearest Neighbor (KNN)	**82.66%** **76.61%** **90.88%**	NSL-KDD
6	**A Review of Intrusion Detection System using Machine Learning Approach**	1. Decision Tree 2. Naïve Bayes 3. K Nearest Neighbor 4. K Means	**92%** **94%** **95%** **96%**	CIDDS-001 KDDCup99 NSL-KDD

		5. Support Vector Machine 6. Principle Component Analysis	**92%** **93%**	
7	**Evaluation of Machine Learning Algorithms for Intrusion Detection System**	1. J48 2. Random Forest 3. Random Tree 4. Decision Table 5. Multi Layer Perceptron (MLP) 6. Naïve Bayes 7. Bayes Network	**93%** **93%** **90%** **92%** **91%** **91%** **90%**	KDD Intrusion Dataset
8	**Intrusion Detection System using AI and Machine Learning Algorithm**	1. K Means Clustering 2. Support Vector Machine 3. K Nearest Neighbors	**89%** **90%** **91%**	CTU Dataset
9	**Intrusion detection model using machine learning algorithm on Big Data environment**	1. Support Vector Machine (SVM) 2. Spark Chi-SVM Proposed Model	**94%** **96%**	KDD99 Dataset Resilient Distributed Dataset (RDD)

10	**Application of Machine Learning Approaches in Intrusion Detection System: A Survey**	1. Support Vector Machine (SVM)	**82%**	
		2. Decision Tree	**89%**	KDD Dataset
		3. Naïve Bayes	**94%**	NSL-KDD Dataset
		4. Logistic Regression	**85%**	KDD Cup 1999
		5. K Nearest Neighbor	**93%**	

III. REFERENCES

[1]. Dhende, S., & Ingle, R. (2018). Network Intrusion Detection System (NIDS) using Machine Learning Perspective. *International Journal of Innovative Research in Science and Technology*, 7(1), 7644-7649.

[2]. Chowdhury, M. N., Ferens, K., & Ferens, M. (2016). Network intrusion detection using machine learning. In *Proceedings of the International Conference on Security and Management (SAM)* (p. 30). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

[3]. Alkasassebeh, M., & Almseidin, M. (2018). Machine Learning Methods for Intrusion Detection.

[4] Jamadar, R. (2018). Network Intrusion Detection System Using Machine Learning. *Indian Journal of Science and Technlogy*, 11(48).

[5]. Biswas, S. K. (2018). Intrusion Detection Using Machine Learning: A Comparison Study. *International Journal of Pure and Applied Mathematics*, *118*(19), 101-114.

[6] Kok, S., Abdullah, A., Jhanjhi, N., & Supramaniam, M. (2019). A Review of Intrusion Detection System using Machine Learning Approach. *International Journal of Engineering and Technology*, 12(1), 8-15.

[7]. Almseidin, M., Alzubi, M., Kovacs, S., & Alkasassbeh, M. (2017, September). Evaluation of machine learning algorithms for intrusion detection system. In *2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY)* (pp. 000277-000282). IEEE.

[8]. Repalle, A., & Ratnam, V. (2017). Intrusion Detection System using AI and Machine Learning Algorithm. *International Journal of Engineering and Technology*, 4(12), 1709-1715.

[9]. Othman, S. M., Ba-Alwi, F. M., Alsohybe, N. T., & Al-Hashida, A. Y. (2018). Intrusion detection model using machine learning algorithm on Big Data environment. *Journal of Big Data*, *5*(1), 34.

[10]. Haq, N. F., Onik, A. R., Hridoy, M. A. K., Rafni, M., Shah, F. M., & Farid, D. M. (2015). Application of machine learning approaches in intrusion detection system: a survey. *IJARAI-International Journal of Advanced Research in Artificial Intelligence*, *4*(3), 9-18.