www.ijirtm.com
editor@ijirtm.com
International Journal of Innovative Research in Technology and Management
Volume-1, Issue-1, 2017

A Comparative Performance Analysis Using Hybrid Model for Malware Detection Techniques

Mr. Sumit Gupta
Research Scholar, PHD
Dept of CSE, MANIT, Bhopal (M.P.)
sumitgupta888@gmail.com

ABSTRACT
The growth of internet technology spread a large amount of data communication. The communication of data compromised network threats and security issues. The network threats and security issues raised a problem of data integrity and loss of data. In this paper we proposed a hybrid model for feature selection and Malware Classification. Feature selection is important issue in Malware Classification. The selection of feature in attack attributes and normal traffic attribute is challenging task. The selection of known and unknown attack is also faced a problem of classification.

Keywords:- Malware detection, Virus, Worms, Artificial Intelligence (AI), Machine Learning, Dos, Probe.

INTRODUCTION
Malware is defined as computer software that has been explicitly designed to harm computers or networks. In the past, malware creators were motivated mainly by fame or glory [8]. Most current malware, however, is economically motivated. Commercial anti-malware solutions rely on a signature database for detection. An example of a signature is a sequence of bytes that is always present within a malicious executable and within the files already infected by that malware [10]. In order to determine a file signature for a new malicious executable and to devise a suitable solution for it, specialists must wait until the new malicious executable has damaged several computers or networks. In this way, suspect files can be analyzed by comparing bytes with the list of signatures. If a match is found, the file under test will be identified as a malicious executable [16].

Some study has shown that security metrics are more suitable for human representation and abstraction of features. This is because features are mainly collected through statistical analysis while metrics are mapped by analyst. Offering protection from unknown malware is an important challenge in malware detection due to the increasing growth of malware. Data mining approaches usually rely on machine-learning algorithms that use both malicious executables and benign software to detect malware in the wild [7].

The rest of this paper is organized as follows in section II we discuss about the about comparative performance evaluation of various malware detection and categorization techniques. In section IV we conclude the about our paper which is based on the rich literature survey journey and comparative experimental result analysis.

II COMPARASION OF EXPERIMENTAL RESULT ANALYSIS
In this section show the selection of variable no. of attribute for the process of the classification algorithm and Modified method. The variable no. of attribute differs the classification rate and classification time. The evaluation parameter corresponding to attribute shown in given below table.

Method Name	Value	TYPES OF ATTACK	TPR	TNR
		NORMAL	4.273	0.703

ISMCS	0.1	DOS	4.373	0.296
		PROBE	4.483	1.703
		U2R	5.273	0.407
		R2L	3.473	1.592

Table 1: Shows that the performance evaluation of TPR and TNR, for ICMCS method, and the input value is 0.1.

Method Name	Value	TYPES OF ATTACK	FPR	FNR
CIMDS	0.1	NORMAL	1.708	0.701
		DOS	1.706	0.631
		PROBE	0.608	0.131
		U2R	0.848	1.731
		R2L	0.408	1.851

Table 2: Shows that the performance evaluation of FPR and FNR for CIMDS method, and the input value is 0.1.

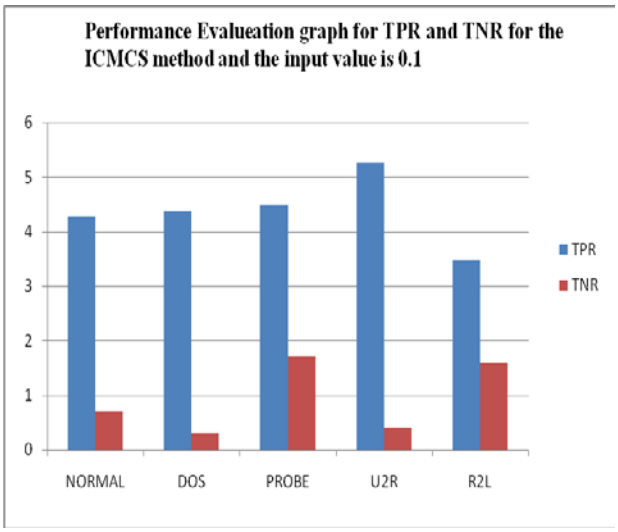

Fig 1: Shows that the performance evalueation of TPR and TNR for the ICMCS method and the input value is 0.1.

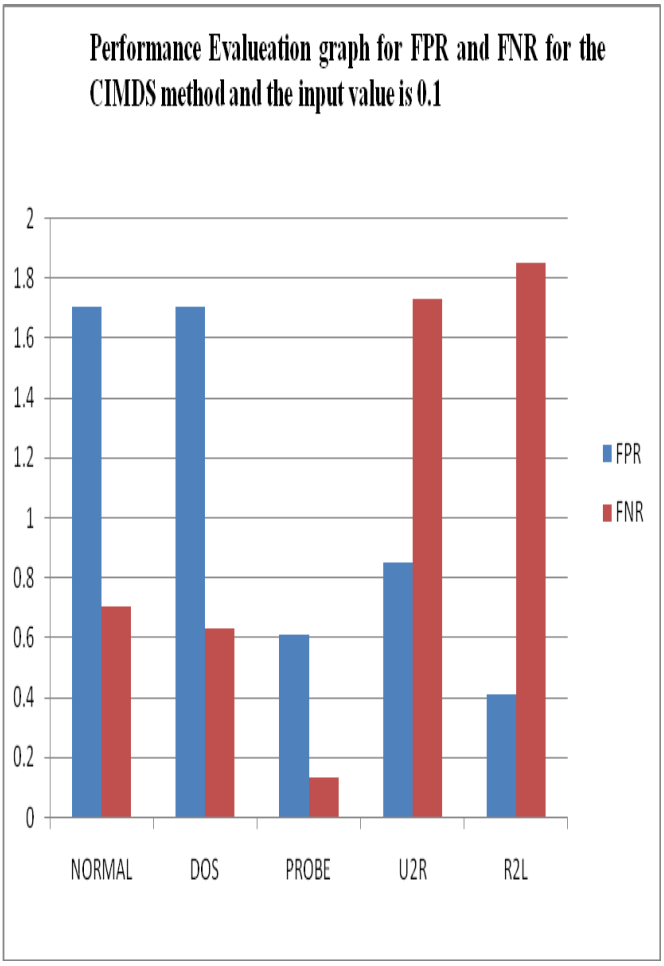

Fig 2: Shows that the performance evalueation of FPR and FNR for the CIMDS method and the input value is 0.1.

IV CONCLUSION

In this paper, we have proposed a novel hybrid method, based on DAG and Gaussian Support Vector Machines, for malware classification. Experiments with the KDD Cup 1999 Data show that SVM-DAG can provide good generalization ability and effectively classified malware data. Moreover, the modified algorithms proposed in this paper outperform conventional CIMDS and ISMCS in terms of precision and recall.

REFERENCES:-

[1] Tawfeeq S. Barhoom, Hanaa A. Qeshta "Adaptive Worm Detection Model Based on Multi classifiers" 2013 Palestinian International Conference on Information and Communication Technology, IEEE 2013. Pp 58-67.

[2] Ibrahim Aljarah, Simone A. Ludwig "Map Reduce Intrusion Detection System based on a Particle Swarm Optimization Clustering Algorithm" IEEE Congress on Evolutionary Computation, 2013. Pp 955-963.

[3] Kai Huang, Yanfang Ye, Qinshan Jiang "ISMCS: An Intelligent Instruction Sequence based Malware Categorization System" IEEE 2010. Pp 658-662.

[4] Jonghoon Kwon, Heejo Lee "Bin Graph: Discovering Mutant Malware using Hierarchical Semantic Signatures" IEEE, 2012. Pp 104-112.

[5] P.R.Lakshmi Eswari, N.Sarat Chandra Babu "A Practical Business Security Framework to Combat Malware Threat" World Congress on Internet Security, IEEE 2012. Pp 77-81.

[6] Ahmed F.Shosha, Chen-Ching Liu, Pavel Gladyshev, Marcus Matten "Evasion-Resistant Malware Signature Based on Profiling Kernel Data Structure Objects" 7th International Conference on Risks and Security of Internet and Systems, 2012. Pp 451-459.

[7] Hira Agrawal, Lisa Bahler, Josephine Micallef, Shane Snyder, Alexandr Virodov "Detection of Global, Metamorphic Malware Variants Using Control and Data Flow Analysis" IEEE, 2013. Pp 1-6.

[8] Vinod P., V.Laxmi, M.S.Gaur, Grijesh Chauhan "MOMENTUM: MetamOrphic Malware Exploration Techniques Using MSA signatures" International Conference on Innovations in Information Technology, IEEE 2012. Pp 232-238.

[9] Robiah Y, Siti Rahayu S., Mohd Zaki M, Shahrin S., Faizal M. A., Marliza R. "A New Generic Taxonomy on Hybrid Malware Detection Technique" International Journal of Computer Science and Information Security, Vol-5, 2009. Pp 56-61.

[10] anfang Ye, Tao Li, Qingshan Jiang, Youyu Wang "CIMDS: Adapting Postprocessing Techniques of Associative Classification for Malware Detection" IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS, IEEE Vol-40, 2010. Pp 298-307.

[11] Raman Singh, Harish Kumar, R.K. Singla "Review of Soft Computing in Malware Detection" IJCA, 2013. Pp 55-60.

[12] Mihai Christodorescu, Somesh Jha, Sanjit A. Seshia, Dawn Song, Randal E. Bryant "Semantics-Aware Malware Detection"

[13] Sarnsuwan N.; Wattanapongsakorn N.; and Charnsripinyo Ch."A New Approach for Internet Worm Detection and Classification" etworked Computing (INC), 6th International Conference, 2010. Pp 546-552.

[14] Wang X.; Yu W.; Champion A.; Fu X.; and Xuan D "Detecting Worms via Mining Dynamic Program Execution" Authorized licensed use limited to: The Ohio State University, 2008. Pp 696-702.

[15] Z. Gao, T. Li, J. Zhang, C. Zhao, and Z. Wang "A parallel method for unpacking original high speed rail data based on map reduce" Springer Berlin Heidelberg, vol. 124, 2012. Pp 59–68.

[16] W. Zhu, N. Zeng, and N. Wang "Sensitivity, specificity, accuracy associated confidence interval and roc analysis with practical SAS implementations" in In Proceedings of the NorthEast SAS Users Group Conference NESUG10, 2010.

[17] I. Aljarah and S. A. Ludwig "Parallel particle swarm optimization clustering algorithm based on map reduce methodology" in Proceedings of the Fourth World Congress on Nature and Biologically Inspired Computing (NaBIC'12), Mexico City, Mexico, November 2012, Pp 104–111.

[18] J. Mazel, P. Casas, Y. Labit, and P. Owezarski "Subspace clustering, inter-clustering results association & anomaly correlation for unsupervised network anomaly detection" in Proceedings of the 7th International Conference on Network and Services Management, Paris, France, 2011, Pp 73–80.

[19] Z. Li, Y. Li, and L. Xu "Anomaly intrusion detection method based on k-means clustering algorithm with particle swarm optimization" in Proceedings of the 2011 International Conference of Information Technology, Computer Engineering and Management Sciences. Washington, DC, USA: IEEE Computer Society, 2011, Pp 157–161.

[20] Y. Ye, D.Wang, T. Li, and D. Ye "IMDS: Intelligent malware detection system" In Proccedings of ACM International conference on Knowledge Discovery and Data Mining, 2007, Pp 1043-1047.

[21] Y. Ye, D.Wang, T. Li, D. Ye and Q. Jiang "An intelligent PE malware detection system based on association mining" Journal in Computer Viorology, 2008. Pp323-334.

[22] L.Jing, M.K.Ng, J.Z.Huang "An Entropy Weighting k-Means Algorithm for Subspace Clustering

of High-Dimensional Sparse Data ” IEEE Transactions on Knowledge and Data Engineering, 2007, Pp 1-16.