International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 8 Issue 6, June-2019, Impact Factor: 3.578

Machine Learning Technique in System Security

Ch. Vinay Santosh[1], Y. Srinivasa Rao[2], K. Bangaru Lakshmi[3]

[1,2,3]K.B.N. College (Autonomous), Vijayawada-520001, Andhra Pradesh, India

ABSTRACT

Cyber security specialists face a significant problem in protecting information systems from compromises in their confidentiality, integrity, and availability. The goal of this research is to keep information systems secure and maintained in a secure state during their usage (lifetime). Intrusion detection using Naive Bayes, KNN, and Decision Tree Models were created using a consistency features selection reduced training dataset, and the models were tested using the work's testing dataset. The results of our evaluation on the UNSW-NB15 dataset show that Decision has the highest overall model classification accuracy of 86.77 percent, Worms attack has the highest attackcategories classification accuracy with the three models, Generic attack categories has the highest classification precision of 0.9765 Naive Bayes, 0.91706 KNN, and 0.9726 Decision Tree, Analysis attacks has the lowest false alarm rate of 0.0001 on both NB and KNN models and precision of 0.00 on both NB and KNN models,

Keywords: Information System, Intrusion Detection System, Confidentiality, Integrity, Availability.

INTRODUCTION

Due to the ever-increasing nefarious actions of cyber attacks and network hackers, information system security has become a very difficult undertaking., that work To violate the confidentiality throughout the clock, before an information system to be adjudged secure, these three components of information system protection must be enforced consistently. Attackers are continually attempting to enter computer networks in order to steal valuable information or impair computer resources, and they are constantly breaking security rules. Each attack type has its own sophisticated style and poses major hazards to computer networking. An attack is an information security threat that attempts to acquire, change, obliterate, delete, confiscate, deny access to, or disclose information without approved right or permission..

According to [1,] attacks can be divided into two categories: active and passive. When an attack attempts to change system resources or interrupt their operation, it is characterized as active. This compromises the network's Integrity or Availability. A passive attack tries to learn or use information from the system without affecting system resources, putting Confidentiality at risk. Unauthorized access and or modification of an information system are intrusions; they are activities that violate the system's security policy; network attacks are the vehicles used by intruders to perpetrate intrusion into an information system; preventing these attacks will enforce the security of the information system. Any intrusion detection system's main goal is to detect and prevent attacks. The method of detecting invasions is known as intrusion detection.

It is assumed and believed that the profile or An attacker's behavior will undoubtedly differ from that of legitimate and authorized users; the difference in behavior between authorized and unauthorized users makes unauthorized actions detectable; an intrusion detection system is software or hardware that continuously monitors an information system to detect intrusive actively(unauthorized activities) and curb it. Because of the variety of protocols and services involved, network packets have various attributes. Attributes are properties of a network packet. Some of these attributes are redundant or irrelevant (i.e., their values have no bearing on or effect over the value of the class label).

The existence of redundant characteristics is one of the primary causes of an increase in the False Alarm Rate (FAR) and a decrease in the detection rate. Before being provided to the machine- learning algorithm used as a classifier, feature selection is an efficient approach to remove redundant and irrelevant information from the network packet or incursion dataset. Feature selection is a preprocessing procedure in the data mining area that involves finding and

deleting as many unnecessary and redundant characteristics as feasible while maintaining the dataset's informative richness [2]. This minimizes the dataset's dimensionality, allowing data mining and machine learning algorithms to function more quickly and effectively. It also increases the accuracy of categorization models. The goal of feature selection is to select the smallest amount of feature subsets from a problem domain while still accurately expressing the original features (Richard and Qiang, 2008).

This study used three (3) filtered based feature selection methods to reduce the number of attributes subsets in the UNSW-NB15 dataset. The reduced attributes subset was then used to train a machine learning algorithm to build intrusion detection models for detecting attack categories of an instance in the testing dataset.

LITERATURE REVIEW

Attacks on networks have been discovered to be as diverse as the systems they attempt to breach. Technically skilled intruders have been interested in attacking the protocols used for secure communication between networking devices, and attacks have been known to be either purposeful or unintentional. [3]. [4] suggested a Monitoring Stubs (MSs) system for detecting cyber assaults on protocols; the MSs detect the attack and alert the victim server, as well as tracing the attacker's origin using DTRAB (Detection and Trace Back). [5] developed a mathematical model for identifying DDoS assaults based on the entropy and determinism of specified packet properties.

They used live network traffic traces for performance checks and anomaly detection, and several mathematical model characteristics such as laminarity entropy and determinism were used to determine the dataset's uncertainty or unpredictability.

Intrusion detection (IDS) is a critical issue in safeguarding the security of information systems, especially in light of the worldwide rise in cyber-attacks. Because the major concern of IDS is its capacity to accurately identify a wide range of intrusions in real time, it is critical to establish the set of characteristics attributes capable and sufficient for determining these intrusions (attacks). The goal of feature selection is to pick the smallest number of feature subsets from a problem domain while still accurately expressing the original features set [6]. According to [7], feature selection improves the accuracy of learning algorithms, which is important in cyber threat detection. [8] The feature selection approaches were divided into three categories: filter, wrapper, and hybrid (embedded). Our research focuses on the filter approach, which is independent of the learning prediction algorithm used to evaluate the performance of the selected features subset [2]. [9] used the Rough Set (RS) technique to choose relevant characteristics from the KDDcup dataset, and the six features that were chosen were analyzed using rough set and two other machine learning algorithms.

Classification

In the normal category, RS is ranked second, while in the attack category, it performs similarly to Multivariate Adaptive Regression Spines (MARS) and Support Vector Decision Function (SVDF). For feature selection in intrusion detection, [10] used three approaches: Support Vector Decision Function Ranking (SVDF), Linear Genetic Programming (LGP), and Multivariate Regression Splines (MARS). These approaches' performance is measured in terms of classification accuracy on test data. [11] suggested a decision-dependent correlation-based feature selection approach (DDC).Mutual information of each feature and decision is calculated and top 20 important features {feature no.: 3, 5, 40, 24, 2, 10, 41, 36, 8, 13, 27, 28, 22, 11, 14, 17, 18, 7, 9 and 15} are selected and evaluated by SVM classifier. Theclassified result is 93.46% detection accuracy

UNSW-NB15 Dataset

The UNSW_NB 15 (University of New South Wales –NB 2015) is the latest published dataset which was created in 2015 to develop a combination of realistic modern normal activities and synthetic contemporary attack behaviors from network traffics for research purposes in intrusion detection utilizing the IXIA Perfect Storm tool in the Cyber Range Laboratory of the Australian Centre for Cyber Security (ACCS). There are 82,332 and 175,341 records in the training and testing sets, respectively.

Analysis, Dos, Exploits, Fizzers, Generic, Reconnaissance, Shellcode, Worms, and Backdrop are among the nine attacks in the dataset; a description of each attack can be found in Table 2. There are 44 feature attributes in the Training and Testing dataset (4 - Categorical, 28 Integer, 10 Float and 3 binary). As indicated in Table 3 and Figure 1, the nine assault types can be grouped into three groups: seizure attacks, penetration attacks, and scanning attacks. The UNSW-NB15 dataset has several advantages over the NSLKDD data set, including similarity between the training and testing datasets and the capacity to effectively and reliably evaluate existing and future threats [12].

Table 1: Description of the attacks types in the UNSW-NB15 dataset

Type	No of Records	Description
Fuzzers	24,246	This attack scan to discover flaws and security loopholes in a program, operatingsystem, or network by feeding it with the massive inputting ofrandom data to make it crash.
Analysis	2,677	A port based intrusion attack against web applications
Backdoors	2,329	This is a remote attack to gain unauthorized access to a system
DoS	16,353	This attack exhaust the destinations resources so that resources required by the isnot made available and normal traffic becomes denied
Exploits	44,525	a sequence of instructions that takes advantage of a glitch, bug, or vulnerability tobe caused by an unintentional or unsuspected behavior on a host or network.
Generic	58,871	A techniques works against all block-ciphers (with a given block and keysize),without consideration about the structure of the block-cipher
Reconnaissance	13,987	This is a probe attack that that gathers information about a computer network to
		evade its security controls
Shell code	1,511	Small program with instructions from a shell to compromised thevictim's computer
Worms	174	A Self replicating malicious code attack that that spread itself to other computers, mostly over a computer network, without attaching itself to a program like a virus

Table 2: UNSW-NB15 Dataset attacks classification

Attacks Type	Attacks Classification
Fuzzers	Scanning
Analysis	Penetration
Backdoors	Penetration
DoS	Seizure
Generic	Penetration
Exploits	Penetration
Reconnaissance	Scanning
Shell code	Penetration
Worms	Scanning

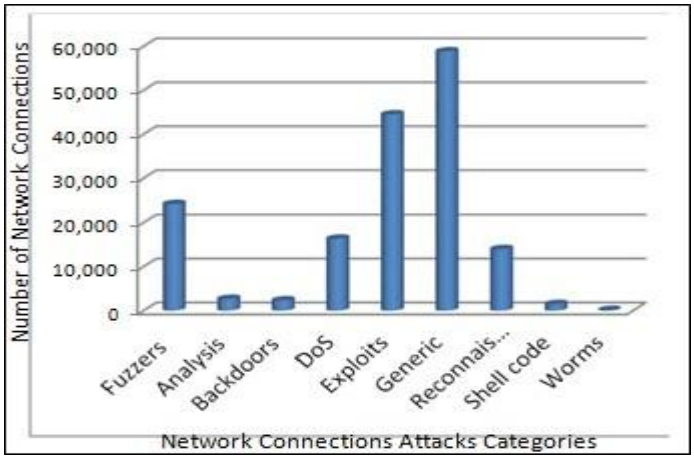

Figure 1: Description of the attacks types in theUNSW-NB15 dataset

Scanning Attacks

Scanning attacks are information gathering network attacks in quest of the status and vulnerabilities of hosts and the network, it sends a port scan (probe) to ascertain the strength/ weakness of the host , the responds of the host system will be scrutinized to uncover the characteristics of the target system and it weakness, scanning attacks is generally used to detect a potential victim, scanning is more than an type of attack it's also the first phase of in seizure and penetration attacks

Seizures Attacks

Seizure attacks are Claim-and-hold attacks; it legitimately grasp a system resources and declines to release it for other users that needs it, which result to a seizure of the computer resources and denying service to legitimate users. Denial of service (DoS) attacks is a good example of a seizure attacks,

Penetration attacks

Penetration attacks exploit imperfection in the software design and development and use it to modify and alter the state of the system, it installed malware and viruses on compromised system in ordergain an unauthorized control of the system. Secure Shell (SSH), are penetration attacks used to gain an unauthorized access to an host without having to ask permission or assistance from the system administrator [13]. SSH employs public/private key technology for authenticating and encrypting sessions between user accounts on distributed hosts on the Internet.

Experimental Setup

Unsw-nb15 dataset has two attributes that can serve as class label; label and the attack_cat attributes, the label attribute is a binary label attribute has value of 0 for normal connection and value of 1 for attack connection, the attack_cat attribute has 10 values, each for the nine attacks categories connections and the normal connection. Selection of relevant attributes that determine each of the nine attacks were carried out using the consistency filter based features selection method, the obtained reduced dataset were used to train and build classification models using. Naive bayes, KNN and C4.5 Decision Tree machine learning algorithms, the built models were evaluated using the test dataset.

Performance Metrics

The performance of intrusion detection models was carried out by evaluating the measures from the values in the coincidence matrix also known as the confusion matrix The confusion matrix shows the distribution of instances that are either correctly classified or wrongly classified.

Results and Discussion

The performance of the Naive bayes base model on the consistency reduced dataset shows an overall model classification accuracy of 70.20% with 123,081 correctly classified instances out of 175,341 are shown in Table 4. and Table 5. worm attack has the highest classification accuracy of 98.92% while Exploits attacks recorded the least classification accuracy of 84.15% with Naive bayes classification model

Table 3: Confusion Matrix of Naive Bayes Model on Consistency Reduced TestingDataset

classified as	1	2	3	4	5	6	7	8	9	10
1 = analysis	1251	213	17	236	68	0	91	111	11	2
2 = backdoor	114	1056	16	23	100	2	18	200	197	20
3 = dos	861	196	7199	952	694	17	343	1241	562	199
4 = exploits	1352	5132	339	16743	1544	78	758	4644	1952	851
5 = fuzzers	174	1246	147	222	12026	244	209	1614	2212	90
6 = generic	7	208	18	159	78	38902	109	328	135	56
7= normal	294	1788	501	4904	2565	495	38824	2234	4349	46
8 = reconnaissance	166	498	44	26	226	83	80	6002	3359	7
9 = shellcode	4	30	1	0	26	9	7	32	1023	1
10 = worms	0	0	0	6	6	9	3	41	10	55

Table 4: Network Connection Accuracy of Naive Bayes Model on the Consistency Reduced Dataset

Network Connections Category (NCC)	TP	FP	TN	FN	Accuracy	Precision FP/(FP+TP)	TP Rate Sensitivity/Recall TP/(TP+FN)	False Alarm Rate FP/(TN+FP)	TN Rate specificity
Analysis	1251	2972	121830	749	97.07%	0.2962	0.6255	0.0238	0.9762
Backdoor	1056	9311	122025	690	92.49%	0.1019	0.6048	0.0709	0.9291
Dos	7199	1083	115882	5065	95.24%	0.8692	0.5870	0.0093	0.9907
Exploits	16743	6528	106338	16650	84.15%	0.7195	0.5014	0.0578	0.9422
Fuzzers	12026	5307	111055	6158	91.48%	0.6938	0.6614	0.0456	0.9544
Generic	38902	937	84179	1098	98.37%	0.9765	0.9726	0.0110	0.9890
Normal	38824	1618	84257	17176	86.75%	0.9600	0.6933	0.0188	0.9812
Reconnaissance	6002	10445	117079	4489	89.18%	0.3649	0.5721	0.0819	0.9181
Shellcode	1023	12787	122058	110	90.52%	0.0741	0.9029	0.0948	0.9052
Worms	55	1272	123026	75	98.92%	0.0414	0.4231	0.0102	0.9898

The performance of the K Nearest Neighbor basemodel on the consistency reduced dataset shows an overall model classification accuracy of 82.05% with 143,868 correctly classified instances out of 175,341 testing dataset instances, the confusion matrix and the detailed attack categories classification accuracy are shown in Table 6 and Table 7. worm attack has the highest classification accuracy of 99.88% while Exploits attacks recorded the least classification accuracy of 89.69% with KNNclassification model

Table 5: Confusion Matrix of KNN Model on the Consistency Reduced Testing Dataset

classified as	1	2	3	4	5	6	7	8	9	10
1 = analysis	0	1	1113	191	5	136	549	4	1	0
2 = backdoor	0	849	306	267	23	94	144	51	11	1
3 = dos	1	28	8929	961	229	1005	897	152	59	3
4 = exploits	2	51	7602	21017	352	1732	1463	964	142	68
5 = fuzzers	0	8	1165	898	13046	234	1884	860	79	10
6 = generic	0	4	266	255	19	39320	100	26	7	3
7 = normal	11	0	215	474	1190	150	53806	122	27	5
8 = reconnaissance	0	9	1340	939	199	187	1534	6184	87	12
9 = shellcode	0	4	52	129	33	15	121	119	659	1
10 = worms	0	0	8	39	2	3	6	12	2	58

Table 6: Network Connection Accuracy of KNN Model on Consistency Reduced Dataset

Network Connections Category (NCC)	TP	FP	TN	FN	Accuracy	Precision FP/(FP+TP)	TP Rate Sensitivity/Recall TP/(TP+FN)	False Alarm Rate FP/(TN+FP)	TN Rate specificity
Analysis	0	14	143868	2000	98.62%	0.00000	0.0000	0.0001	0.9999
Backdoor	849	105	143019	897	99.31%	0.88994	0.4863	0.0007	0.9993
Dos	8929	12067	134939	3335	90.33%	0.42527	0.7281	0.0821	0.9179
Exploits	21017	4153	122851	12376	89.69%	0.83500	0.6294	0.0327	0.9673
Fuzzers	13046	2052	130822	5138	95.24%	0.86409	0.7174	0.0154	0.9846
Generic	39320	3556	104548	680	97.14%	0.91706	0.9830	0.0329	0.9671
Normal	53806	6698	90062	2194	94.18%	0.88930	0.9608	0.0692	0.9308
Reconnaissance	6184	2310	137684	4307	95.60%	0.72804	0.5895	0.0165	0.9835
Shellcode	659	415	143209	474	99.39%	0.61359	0.5816	0.0029	0.9971
Worms	58	103	143810	72	99.88%	0.36025	0.4462	0.0007	0.9993

The performance of the Decision Tree base model on the consistency reduced dataset shows an overall model classification accuracy of 86.77% with 152,135 correctly classified instances out of 175,341 testing dataset instances, the confusion matrix and the detailed Connection categories classification are shown in Table 8 and Table 9. worm attack has the highest classification accuracy of 99.94% while Exploits attacks recorded the least classification accuracy of 91.24% with the Decision Tree classification model

Table 7 Confusion Matrix of Decision Tree Model on the Consistency Reduced Testing Dataset

classified as	1	2	3	4	5	6	7	8	9	10
1 = analysis	454	0	1115	277	0	27	127	0	0	0
2 = backdoor	0	1125	121	401	22	37	20	20	0	0
3 = dos	0	10	10063	1580	121	281	95	50	64	0
4 = exploits	1	22	7588	23876	348	571	650	189	106	42
5 = fuzzers	0	1	1688	892	14282	102	870	273	74	2
6 = generic	0	3	284	225	26	39396	55	6	5	0
7= normal	0	1	107	469	998	13	54336	61	15	0
8 = reconnaissance	0	1	1336	1195	41	43	138	7723	11	3
9 = shell code	0	2	76	37	40	24	109	49	796	0
10 = worms	0	0	6	20	4	10	4	1	1	84

Table 8: Network Connection Accuracy of Decision Tree Model on the Consistency Reduced Dataset

Network Connections Category (NCC)	TP	FP	TN	FN	Accuracy	Precision FP/(FP+TP)	TP Rate Sensitivity/Recall TP/(TP+FN)	False Alarm Rate FP/(TN+FP)	TN Rate specificity
Analysis	454	1	151681	1546	98.99%	0.9978	0.2270	0.00001	1.0000
Backdoor	112	540	151010	621	99.57%	0.9657	0.6443	0.00026	0.9997
Dos	10063	12321	142072	2201	91.29%	0.4496	0.8205	0.07980	0.9202
Exploits	23876	5096	128259	9517	91.24%	0.8241	0.7150	0.03821	0.9618
Fuzzers	14282	1600	137853	3902	96.51%	0.8993	0.7854	0.01147	0.9885
Generic	39396	1108	112739	604	98.89%	0.9726	0.9849	0.00973	0.9903
Normal	54336	2068	97799	1664	97.61%	0.9633	0.9703	0.02071	0.9793
Reconnaissance	7723	649	144412	2768	97.80%	0.9225	0.7362	0.00447	0.9955
Shellcode	796	276	151339	337	99.60%	0.7425	0.7026	0.00182	0.9982
Worms	84	47	152051	46	99.94%	0.6412	0.6462	0.00031	0.9997

Table 10 shows the performances of the classification models on each of the network connection types in terms of accuracy, false alarm rate and precision, Naive Bayes, KNN and Decision Tree models has highest accuracy of 98.2%, 99.88% and 99.94% with worms network connection respectively, figure 2 show the line graphs that indicates the performance of each models on each network connection types. KNN and Decision Tree returns lowest false alarm rate of 0.0001 each respectively on analysis network connection and 0.0093 on DOS Network Connection with Naive Bayes, Figure 3 show the line graph showing the performance of each models on the network connection categories. the three models recorded their highest precision on Generic attacks; Naive bayes recorded 0.9765, KNN, 0.9765 and 0,9726 with Decision Tree as indicated in figure 4.

Table 9: Models Performances on Network Connection Types

Network Connection Types	Accuracy			False Alarm Rate			Precision		
	NB	KNN	DT	NB	KNN	DT	NB	KNN	DT
Analysis	97.07%	98.62%	98.99%	0.0238	0.0001	0.00001	0.2962	0.00000	0.9978
Backdoor	92.49%	99.31%	99.57%	0.0709	0.0007	0.00026	0.1019	0.88994	0.9657
Dos	95.24%	90.33%	91.29%	0.0093	0.0821	0.07980	0.8692	0.42527	0.4496
Exploits	84.15%	89.69%	91.24%	0.0578	0.0327	0.03821	0.7195	0.83500	0.8241
Fuzzers	91.48%	95.24%	96.51%	0.0456	0.0154	0.01147	0.6938	0.86409	0.8993
Generic	98.37%	97.14%	98.89%	0.0110	0.0329	0.00973	0.9765	0.91706	0.9726
Normal	86.75%	94.18%	97.61%	0.0188	0.0692	0.02071	0.9600	0.88930	0.9633
Reconnaissance	89.18%	95.60%	97.80%	0.0819	0.0165	0.00447	0.3649	0.72804	0.9225
Shellcode	90.52%	99.39%	99.60%	0.0948	0.0029	0.00182	0.0741	0.61359	0.7425
Worms	98.92%	99.88%	99.94%	0.0102	0.0007	0.00031	0.0414	0.36025	0.6412

CONCLUSION

In this paper, we proposed a Machine Learning, Network Intrusion Detection system for the protection of information system based on theUNSW-NB15 dataset, Naive Bayes, KNN and Decision Models were built with a consistency features selection reduced training dataset, the models were evaluated using the testing dataset, from the work, the following conclusions can be made: Decision tree model recorded highest models classification accuracy of 86.77%, closely followed by KNN and Naive Bayes with classification accuracy of 82.05% and 70.20% respectively, Worms attack categories detection has the highest classification accuracy of 70.20% with Naive Bayes, model, followed by 82.05% KNN and 86.77% for DT Models. Generic attacks categories has the highest precision of 0.9765 with Naive Bayes model, followed by 0.91706 with KNN and 0.9726 with Decision Tree. Analysis attacks detection has the lowest FAR of 0.0001 with both Naive Bayes and KNN models and FARof 0.0093 with Dos attack on Decision tree model

REFERENCES

[1] Nikhil S. M., Arvind R. B.P. and Abhijit S.P. (2014) Network Attacks and Their Detection Mechanisms, International Journal of Computer Applications (0975 – 8887) 9(9).

[2] Liu, H. & Yu, L. (2005). Towards integrating feature selection algorithms for classification and clustering.IEEE Transactions on Knowledge and Data Engineering, 17(4), 491-502

[3] Reed D., 2003. Network Model to Information Security. Retrieved: . Available at: http://www.sans.org/reading_room/whitepap ers/protocols/applying-osilayer-network- model-information-security_1309

[4] Fadlullah Z. M., Taleb A. V., Guizani M.and Kato N., (2010) "DTRAB: Combating Against Attacks on Encrypted Protocols through Traffic-Feature Analysis",IEEE/ACM Trnsaction on Networking, 18(4).

[5] Jeyanthi N, Vinithra J, Sneha, and Thandeeswaran R , (2011) “A Recurrence Quantification Analytical approach to DetectDDoS Attacks”, International Conference onComputational Intelligence and Communication Systems

[6] Richard Jensen, Qiang Shen, 2008 Computational intelligence and featureselection, IEEE press series on computational intelligence, A John Wiley & Sons, Inc., Publication.

[7] Quiet G., Hariri S. and Yousif M. (2005), "A New Dependency and Correlation Analysis for Features", IEEE Transactions on Knowledge and Data Engineering, 17(9), 1199-1207.

[8] Blum, Avrim L. & Pat Langley (1997). Selection of relevant features and examples in machine learning Artificial Intelligence, 97(1-2), 245–271

[9] Zainal, A.,. Maarof M.A, and Shamsuddin S.M., (2006). Feature Selection Using Rough Set in Intrusion Detection. TENCON2006. 2006 IEEE Region 10 Conference, pp:1-4

[10] Mukkamala, S. & Sung, A. H. (2003). Feature Selection for Intrusion Detection Using Neural Networksand Support Vector Machines. Journal of the Transportation Research Board of the National Academics, Transportation Research Record No 1822,33-39

[11] Fadaeieslam, M. J. (2007). Comparison of two feature selection methods in Intrusion Detection Systems. Seventh International Conference on Computer and Information Technology, pp: 83-86

[12] Moustafa N. and Slay J. (2015) A hybrid feature selection for network intrusion detection systems: Central points, Australian Information Warfare and Security Conference, 2015

[13] Alex Lam (2005), "New IPS to Boost Security, Reliability and Performance of the Campus Network," Newsletter of Computing Services Center.