International Journal of Future Generation Communication and Networking
Vol. 13, No. 3, (2020), pp. 2107–2116

Single Attack to Multi-attack Intrusion Detection System- A Survey

S. R. Khonde[1,2*], V. Ulagamuthalvi[1]
[1]*Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, India*
[2]*Department of Computer Engineering, M.E.S. College of Engineering, Pune, S.P.Pune University, Maharashtra, India*
**E-mail-khonde.shraddha@gmail.com*

Abstract

In new era due to huge use of internet most of the networks are getting compromised. Main reason behind it is an intelligent system which generates some mischief data which easily breaks security of network and become vulnerable. Such systems or a mankind is called as intruder. Most of the intruders break security of network and compromise network such that it will enter in an unstable or unsecure state. Intruders make system vulnerable such that easily all activities from network can be controlled and managed. Any vulnerable system is open for any type of malicious activity as no security breach is available. These types of systems mostly targeted by attack a type of malicious activity. Attacks once happened on the network or a system mostly captures all the important information about the network to conduct deceitful activities. Once the intrusion happen in system it is difficult to stop and rectify it. To avoid such type of attacks an intelligent device is used called intrusion detection system (IDS). IDS mostly helps administrator to avoid malicious activities to happen or enter in the network. Most of the IDS nowadays are using various machine learning techniques to detect and stop such type of malicious activities. Most of the IDS use to detect single type of attack using various algorithms. Now a day's intruders are trying to enter into the network by changing the behaviour of attack from single to multi. At a time if system is compromised with multi attack then it is not possible for any IDS to detect it and stop it. Multi-attack can be defined as a multiple attacks attacking on the system at same time or combination of various attacks attacking on system. To handle such type of attack IDS systems need to improve so that they can detect multi-attack with single attack. Standard dataset used by IDS also provides signature of single attack. None of the standard dataset provides or handles signatures of multi-attack. In real work most of the attack happening now a days are not basic attacks neither single attack. To provide better security need to IDS is to detect multi-attack. In this paper, we discuss various types of attacks and approaches to implement intelligent IDS. This paper also focuses on various machine learning algorithms which can be used for attack detection. Paper also provides survey of various datasets used for attack detection by IDS.

Keywords: *Intrusion detection system, multi-attack, machine learning, classifiers, dataset, network security*

1. Introduction

Security has become an important area for researchers now a day due to growing number of intrusion and intruders. To maintain security of data and information our system should have good firewall or IDS to maintain confidentiality and security of network. Most of the malicious activities happen now days in network are because of poor security available at the gate or entry point of the network. In such cases intruders can get easily access to all the data and network. Firewall or IDS are the security tools which are used to provide security to the network but most of the intruders use more powerful tool to get entry into the network. Once the network or system got vulnerable intruder has overall control of network. In this case all activities of the network can be suspended or aborted. In case if intruders did not get chance to enter into a system then mostly intruder make use of various attacks to target system such that security

ISSN: 2233-7857 IJFGCN

can be break easily. Attacks are the threat coming from information security that mostly attempts to destroy or remove or alter the confidential data inside the network. Mostly this type of threat is used to reveal confidential information to unauthorised use without access permission of owner of data. Any type of information either an individual or organizational it can be manipulated with these threats. There are two main types of attacks as passive and active attack. Passive attacks are a type of attack which will work as observer for the system. This type of attack does not interfere into the system resources as well will not interrupt in between communication. Main motto behind this type of attack is to only obtain information from system. Active attacks are the type of attack which tries to change system resources and change all operations. This attack has full control over system so any resource connected to the system can be targeted by this of attack. This attack also attempts to modify confidential data and can generate false data harmful for the system. To handle such types of attacks an intelligence system is used by many organizations called Intrusion Detection System (IDS). Various types of IDS are available to avoid attacks to happen in network.

An IDS is a software or device which helps us to monitor network for malicious activities like attacks happening and generate alert to the administrator to avoid such activities. IDS come in various flavours as network IDS (NIDS) and host IDS (HIDS). NIDS basically used to detect intrusions or attack happening on the network. It avoids malicious data to enter into the system. HIDS is usually used to protect data at system level. It mostly works for a single system. Detection of attacks is done using two main methods by IDS.

1.1 Signature based IDS

This IDS uses signature of various attacks stores previously in the dataset to analyse each packet entering in the network. All the attacks have some specific behaviour or pattern that can be stored as a part of signature. All attacks happen in a network are analysed and administrators try to pattern of attack. Each intrusion mostly leaves its foot print behind, footprint is nothing but some specific activities that happen or occur suddenly in system as automatic shutdown, not able to open application, not able to open folders or specific files. All these foot prints are stored in a dataset as a signature. Signature based IDS makes use of these signature to detect attack happening in the network. This type of IDS provides better detection accuracy if all the attacks penetrating on network have a signature stored in dataset. If a signature of attack is not stored in dataset then such type of attacks cannot be detected using this type of IDS. Limitation of signature based IDS is it will not able to detect novel attacks coming in the network. In such case new or novel attacks harm network for the time it is detected.

1.2 Anomaly based IDS

These IDS mostly check the behaviour or activities of the attack or packet entering into the network. If activities are not normal them it is consider or detected as malicious. As this type of IDS is used to detect attack which are not known it is called as anomaly based IDS. Every IDS has the baseline or behavioural pattern which can be considered as a normal. If any packet entering in the network change its pattern and does not matches with normal pattern it will be considered as a malicious ot novel attack pattern, Anomaly based IDS mostly used baseline patterns to check normal behaviour if it deviates somewhat by the packet entering in the network assumes to be detected as an attack. Limitation of this type of IDS is slight change in the behaviour can be considered as attack which is not correct every time. Most of the time slight behaviour change occurs due to bandwidth changes or network properties. In such cases also as change in pattern is observed by the IDS it generates alarm for attack. When the attack is detected correctly it is consider as true positive and when attack detected by mistake by the IDS it will be consider as false alarm rate. IDS provide better performance when true positive is more and false alarm is less.

ISSN: 2233-7857 IJFGCN

Most of the researchers consider true positive and false alarm rate as one of the parameter to evaluate performance of the IDS.

IDS mostly make use of various data mining, machine learning algorithms for attack detection. As the era of artificial intelligence and neural network is going on most of the IDS are improved using these area. As per research most of the IDS used to detect single attack at a time penetrated on the network. As security has become sensitive area it is not sufficient for IDS to detect only single attack at a time. A switch from single attack to multi-attack is essential for all IDS to improve security and maintain confidentiality and integrity of data. Multi-attack can be a considered as multiple attacks of same type penetrated on network by intruder or it can be considered as multiple attacks of different types penetrated into system at the same time. Multi-attack can also be consider as a combination of different types of attacks such that they can create another type of new attack whose behaviour is different from the base ones. These any type of multi-attack can happen on the network so the IDS need to be more improved and intelligent to deal with such sort of attacks. All these multi-attacks are novel and cannot be detected by IDS trained for detection of single IDS.

2. Related Work

Most of the researchers now a days work in area of information security to find new ways to improve security of data as well as increasing detection accuracy for all types of known as well as unknown attack. To improve performance of IDS various data mining and machine learning algorithms are used. Various supervised, unsupervised and semi-supervised algorithms are used to improve detection accuracy of the IDS. Hasan, et al. [1] make use of two data mining algorithm Random forest and SVM to implement IDS. For both algorithms computational time was compared to find better one. Random forest gives better results as compared to SVM. In SVM radial kernel basis method is used to check the detection accuracy which turns to 92.99% whereas random forest provides 91.41% accuracy with faster processing time. Authors also focused on precision time of both algorithms, random forest provides 10% more precision and less processing time than SVM.

Farnaaz and Jabbar [2] train and test classifiers j48 and random forest using NSL-KDD dataset. Pre-processing is done on dataset to cluster it according to various types of attacks. To reduce number of features for training classifiers symmetrical uncertainty measure feature selection technique is used. Performance parameters used by authors are detection rate, and false alarm rate. Both the classifiers are trained and tested on clustered dataset for evaluation of performance parameters. Random forest with 100 trees shows better accuracy of 99.67% than j48 with 99.83% detection rate and 0.00527% false alarm rate. Lv, et al. [3] use extreme learning method for improving accuracy of attack detection. Combination of gravitational search and differential evolution algorithm is used for testing detection accuracy. Kernel hybrid functions are used to improve prediction accuracy of classifier. Dimensionality reduction is done using kernel principal component analysis for feature extraction. This approach is train and tested on KDD99 and UNSW-NB15 dataset. Results discussed by authors shows improved high accuracy and less processing time.

Standard dataset is mostly use by authors for implementation of IDS. KDD-99 standard dataset is elaborated by Aggarwala and Sharma [4]. KDD-99 dataset is partitioned into four types of attacks basic, content, traffic and host. Detection rate and false alarm rate are the main evaluation metrics used by authors. Classifiers were trained on 15 subsets created after clustering dataset into four types. Clustering dataset into clusters improves the detection rate and reduce false alarm rate. Jha and Ragha [5] make use of SVM classifier whereas feature selection is done by combining k means and information gain. Importance of each feature can be measure using information gain. Authors tested accuracy with top 30

ISSN: 2233-7857 IJFGCN

and 23 features which shows difference of 0.05%. Top 30 or 23 features are selected using information gain values of features. This selection is done by k-means according to ascending order.

Researchers some time use single classifier or algorithm for detection and sometime they opt ensemble of these classifiers. Giorgio, et al. [6] explains approach using modular ensemble. As its ensemble more than one classifier is use where each classifier takes care of certain service as web service, mail service and so on. Each service classifier is tested using density based solutions. K means clustering with v-svc algorithm is used for testing and is ensemble together using simple rules like maximum, mean, product rule and minimum. Dataset used is KDD99 and it is proved that ensemble classifier gives better result as compare to single classifier. A chance of wrong prediction is more in single classifier as compare to ensemble. Another approach for detection is explained by Mahoney and Chan [7, 8] where packet headers are analysed to get the prediction. In this paper authors explain method to extract normal values from header at data link, network and transport layer. As the packet moves from one layer to another header is attached to it. This header can be analysed and used for detection. It mostly focuses on detection of attack in ARPA dataset which mostly exploits at transport layer or in below layers. Ensemble framework is mostly used by researchers to improve efficiency of IDS. Random forest is the most used data mining algorithm. Most of the researchers used it in IDS for improving its accuracy. Khonde and Ulagamuthalvi [9] used Random Forest supervised algorithm for intrusion detection. KDD dataset is used for training and testing. For feature selection probability score is used for calculating score of each feature. Depending on probability and Gini index features having high score are selected for testing. Reduced features are passed to random forest classifier. Random forest works in distributed manner. Random forest algorithm gives 96% of accuracy as per authors. Authors used 50 random forest trees for increasing accuracy and reducing false alarm rate. A novel framework using ensemble method with feature selection is explained by Zhou, et al. [10]. In this correlation between features is used for dimensionality reduction with CFS-BA heuristic algorithm. Classifier C4.5, random forest and a version of random forest (forest PA) is ensemble together for prediction. Voting algorithm is used to generate final prediction of ensemble. This ensemble approach is tested on various dataset like NSL-KDD, CIC-IDS2017 and AWID. Results proved that ensemble classifier approach provides better results as compare to single classifier.

Internet is full of much type of attacks like ransomware, phishing, DoS, DDoS, wormhole, Trojan horse and many more. All the attacks can be handled by IDS but single at a time. Most of the researchers coming with collaborative approach like Gamer [11] for detecting attack in internet. Approach presented in this paper uses collaborative approach to combine prediction from neighbour network without any trust relationship. This approach provides good detection rate but able to detect only single attack at a time. None of the IDS able to handle multi-attacks now days. As the intrusion is growing fast new area for research is coming up in face of multi-attack or collaborative attack detection. An IDS framework using unsupervised machine learning algorithm random forest is explained by Zhang, et al. [12]. KDD99 dataset is used for detection. All types of attack are detected present in this dataset. Algorithm used is random forest which uses bootstrapping for generating sample subsets. Authors also did feature selection to reduce time in training trees for random forest. Pre-processing is done to select important features. Random forest itself works in ensemble as number of trees is used for detection. This algorithm makes use of voting algorithm for finding final prediction from prediction received from number of trees. While detection if the value of packet goes beyond threshold value it is consider as outlier. Results shows improved detection rate with less false alarm rate. Folino, et al. [13] emphasize on ensemble approach for attack detection. It is better to use ensemble rather than using single classifier. Authors elaborate on various data mining algorithms which can be used in ensemble to improve performance of IDS. Approaches like centralised and distributed are also explained in detail by authors. Various supervised and unsupervised algorithms are the once which can use in IDS. All this approaches work for single attack detection not for multi-attack. Authors also mentioned some open issues to help researcher for improving efficiency of NIDS.

ISSN: 2233-7857 IJFGCN

More unsupervised approaches were used by many researchers, as explained by Song, et al. [14] architecture consist of three stages for IDS. Three stages are filtering, clustering and modelling. Filtering is the first stage in this architecture. In this step feature selection and filtering of data from dataset is done. Next step is clustering where clusters of the filtered data is created to maintain the accuracy of detection. The number of clusters to be formed is depending on the parameters used for calculating accuracy. Last step is modelling gin which the each cluster data is used to train SVM classifier. This is use to detect attacks form the normal traffic. Authors use homogeneous ensembling for detection of normal traffic. Another unsupervised approach is presented by Song, et al. [15].This approach use same methods for analysing normal traffic as used in previous paper. The difference is parameter used for analysing detection accuracy does not have any user intervention. Clusters are formed according to samples created in filtering data. If both approaches are compared second approach is more feasible and efficient. Second approach also provides better accuracy as compared to first.

A novel framework is proposed by Nguyen, et al. [16] where operating system audits, system logs and network packets collected in real time environment. Using this methods dataset is generated by authors. This dataset is labelled by domain experts using knowledge of domain. After labelling dataset it is divided into training dataset and validation dataset. Training dataset is used to train classifier k-means, which is used for detection of normal behaviour of packets. KDD'99 dataset is used by authors to compare with capture dataset. All the classifiers are ensemble together using weighted majority voting algorithm to get the final prediction. Experiments were conducted using bagging and boosting methods of ensemble and it is prove that it helps in improving detection accuracy. Collaborative framework with coordinated attacks is elaborated by Zhou, et al. [17]. Author mostly highlight on the coordinated attacks which is the one happen in multiple networks at a time. Such type of attacks cannot be handle by single IDS which is trained for detection of single type of attack. Collaborative IDS is proposed by authors to handle such type of attacks and challenges behind it. Though lots of research is going on in this field we are still not able to address multi-attack scenario if it happens in the network. Khonde and Ulagamuthalvi [18] proposed novel hybrid architecture for intrusion detection system. Authors used feature selection techniques for reducing number of features. Feature selection used is based on average probability score of each feature. The features having less AP score are removed from the set used for training and testing classifiers. Performance parameters used by authors are true positive, true negative and accuracy. Authors make use of various semi-supervised classifiers for intrusion detection. All classifiers used NSL KDD dataset for intrusion detection. With experimental results authors proved that accuracy of hybrid system increased by 10% more than any single classifier. Same authors proposed another approach in [19]. In this paper they used combination of supervised and unsupervised classifiers for intrusion detection system. Authors used various feature selection techniques to improve performance and accuracy of intrusion detection. Authors reduced features up to 7 from 42 of KDD dataset to improve system performance. The architecture proposed by authors is based on hybrid pipeline structure of classifiers. In total seven numbers of classifiers are used for testing system performance. In this paper authors proved that system performance increases and reduce false alarm rate. Dataset used is NSL KDD. Horng, et al. [20] uses clustering algorithm BIRCH on KDD'99 dataset. The dataset is divided according to classes as probe, dos, U2R, R2L and normal. Feature trees are built for each class as a part of BIRCH algorithm to represent each class in compact format. Classifiers used are SVM, decision tree, k-means in ensemble with BIRCH clustering algorithm. Results show comparison of all algorithms individually and after ensemble where SVM shows better performance. Li and Kwok [21] proposed collaborative approach for implementing IDS. In this approach authors allows nodes in IDS to communicate with each other to share information about attack and normal traffic. Main challenge in this approach is communication messages between two nodes. If any node is compromised then attack can happen. Authors focuses on handling massive message finger print attack which mostly occurs while communication inside network. This type of attack is mostly penetrated into network by the insider intruder. Approaches are not limited to collaborative it can be distributed as well. Only the challenge in both approaches is communication, if different types of networks are communicating with each other. Method for robust communication is explained by Perez, et al. [22].

ISSN: 2233-7857 IJFGCN

Authors concentrated on the quality of message delivered between networks. Most of the time we face changing diversity problem that issue authors try to address with the concept of trust diversity. The data coming from sensors of other IDS or from proxy need to be secure first. As it can also be hacked and changed by intruder. Using methods proposed in paper quality and security of the message while communication in distributed or collaborative approach has increased. Chen and Hwang [23] try to detect shrew distributed denial of service attack using collaborative approach. Filtering technique is required to filter unwanted packets from traffic. Analysis of traffic is done using spectral analysis. All TCP/IP packets are analyzed to classify normal traffic against shrew DdoS traffic. Experiments are performed on NS2 simulator to analyze traffic. Result shows 95% detection rate and 10% false alarm rate. Summary of literature survey is provided in table 1.

Table 1. Summary related work

Reference number	Methodology	Classifiers	Standard Dataset	Type of attack detected
[1]	Ensemble	Random Forest, SVM	NSL-KDD	Single
[2]	Clustering	Random Forest	NSL-KDD	Single
[3]	Ensemble	GA , DE	KDD'99, UNSW-NB15	Single
[5]	Ensemble	SVM, K-means	KDD'99	Single
[6]	Ensemble	k-means, v-SVC	KDD'99	Single
[7]	Ensemble	Packet Analysis	ARPA	Single
[9]	Single	Random Forest	NSL-KDD	Single
[10]	Ensemble	CFS-BA heuristic algorithm, C4.5, Random Forest	NSL-KDD, CIC-IDS2017 and AWID	Single
[12]	Single	Random Forest	KDD'99	Single
[14]	Clustering	SVM	NSL-KDD	Single
[16]	Single	K-means	KDD	Single
[18]	Ensemble	Random forest, SVM, decision tree	NSL-KDD	Single
[19]	Ensemble	SVM, Random forest, Decision tree, k-means	NSL-KDD	Single
[20]	Ensemble	BIRCH,SVM	KDD	Single
[21]	Collaborative	PMFA	Self	Single
[23]	Distributed	Packet analysis	Self	Single

As per observations from table 1 we can conclude that most of the approaches used with many algorithms are able to detect only single attack at a time. It gives pen area to researchers to work in direction of multi-attack detection.

3. Challenges / Open Issues

As per mentioned in literature survey many of the data mining and machine learning algorithms are used to build intrusion detection system. Most of them use different approaches like distributed and collaborative to improve the efficiency and performance of IDS. It is very important to improve IDS as security has become a bottleneck of network now days. If by any chance security mechanism is poor network or system will be vulnerable and enter of thief will be easier. Most of the research is going on in this field is shifting towards deep learning and neural network approaches. Most of the researchers are trying to make use of these are to improve IDS for handles various types of attacks. As the intrusions are

ISSN: 2233-7857 IJFGCN

changing faces time to time there is a need in shift of implementation of IDS. IDS should able to handle all types of attacks including novel ones with more detection rate and less false alarm rate. Aldweesh, et al. [24] expressed views about using deep learning to implement advance IDS system. Authors present a survey for analyses of input data, detection, framework, deployment of IDS in deep learning. Authors also present some of the evaluation strategies which can be used. According to analysis presented in paper deep learning can be a new are of research in the field of security provided through IDS. A new IDS system which makes use of semantic re-encoding is elaborated by Wu, et al. [25]. To improve performance deep learning is used with encoding to analyze the network traffic. Deep earning algorithm is use to generalize the classification of network traffic efficiently such that algorithm efficiency and strength can be increased. Dataset used is NSL-KDD for experiment. Author focuses on single attack that is web character injection network attack. Comparison shows that traditional IDS show less accuracy by 8% than IDS implemented using deep learning approach. Performance of IDS is also depends on dataset. We need a strong dataset which covers mostly all types of attacks so that detection rate can be increased. Detail study of various datasets available in cyber security is presented by Ferrag, et al. [26]. Authors describes 35 well-known datasets and divided it into seven categories depend on the features provided in that. Out of these datasets authors tested two datasets using IDS with deep learning approach. Various deep learning models where analyzed by authors to choose accurate model for IDS. Evaluation parameters used are accuracy, false alarm rate and detection rate. Using deep learning approach authors try to reduce false alarm rate and improve performance of IDS. Most of the dataset used by IDS are not compatible with the current attacks. Comparison of various datasets which can be used by IDS in IOT environments is explained by Hadhrami and Hussain [27]. Author describes all the datasets which can be used for communication in IOT environment by IDS. Most of the dataset which are a standard dataset for IDS is not compatible with new emerging technologies like IOT. Author proposed a new framework for collection of real time data which can be used by IDS. Limitation of this dataset is it can be used only for the protocol use for communication in between IOT devices not for other devices.

According to the recent advances in this area as describe in survey we can clearly analyze that none of the IDS is compatible to detect collaborative attack. The biggest challenge researchers are facing now a days is how to deal with multi-attack. Multi-attack can be defined as an attack which itself is a combination of multiple attacks. As the number of novel attacks are emerging now a days there is quite a possibility to have a multi-attack penetrated into network. To elaborate more consider any two types of attacks which are having their own behavior and their own signatures. In other words we can say each attack has its own symptoms also called as foot prints or behavior. By making use of these behaviors IDS makes prediction about that attacks. But what if we combine behavior of multiple attacks together? Yes definitely it will create a new novel attack created with the combination of these two attacks. When IDS tries to detect such attack as the behavior is not matching with any of the single attack it fails to predict it. So a big challenge is how to handle multi-attack or collaborative attack is in front of researchers now a days.

4. Multi-attack Detection

Survey says that now it's a time to shift research from single attack to multi-attack detection. Here we are presenting some possible solutions to deal with the challenge. Most of the IDS are based on signature type of attack detection. For this we need a strong dataset which can be used to detect multi-attack same as a single attack. Datasets used now days are KDD99, DARPA, NSL-KDD, UNSW-NB15, CICIDS2017 and many more. None of these standard datasets are compatible with multi-attack detection. For this type of detection new dataset need to be created, this will consist of signature for behavior of various combination or collaborative attacks. To move a step further in multi-attack detection one can generate an attack with the combination of multiple single attacks. As that attack is penetrated into the system real time dataset can be generated. Packets entering into network can be captured for dataset creation. Each packet can be stored into a pcap file to create final dataset. There can be multiple combinations for

ISSN: 2233-7857 IJFGCN

creating multi-attack. Researchers can stick with only one type of attack and can try to create a real time dataset. Features for this dataset need to be decided according to the behavior of attack. Another challenge in this can be selecting or finalizing features of dataset. As the features of the dataset will depend on combination, every type of multi-attack can have different dataset. Validation of dataset can be another challenge. Dataset can be validated only after testing it in real time environment. Dataset creation for multi-attack can be an important milestone in area of multi-attack detection. As next generation networks are handling multiple types of data like text, audio and video as explained by Manan et al. [28]. There is a need of advanced IDS to provide security to this data. Almogren [29] highlights a technical shift from cloud to edge-of-things [29] including smartphones, routers, sensors for storing our data we need to improve security of each data passing through the network are stored in any device of network .Any framework we use distributed , centralized or collaborative data integrity, confidentiality and security is utmost important. All these issues can be address easily if IDS will able to detect all types of attacks including multi-attack or collaborative attacks.

5. Conclusion

According to survey presented most of the intrusion detection systems are providing good accuracy, detection rate and less false alarm rate. Many frameworks and approaches are used to implement IDS so that all types of attacks can be detected and IDS performance can be improved. Collaborative and distributed approaches are mostly used for attack detection. Most of the researchers make use of standard dataset. Machine learning, data mining, deep learning, neural network algorithms are used to improve efficiency and performance of IDS. The only limitation observed is all IDS are able to detect single attack at a time. Single attack detection accuracy is reached up to 99% in most of the algorithms and architectures presented in survey. Not a single standard dataset is compatible for multi-attack detection. Now it's time to focus on new challenge in emerging world of network that is collaborative or multi-attack detection. If IDS are improved for detecting such type of attack none of the intruder can break security of network. This will help in improving security and providing protection to network. This can be possible by generating new dataset consisting signatures of multiple attacks together and validating it. This dataset can be used to train and test any algorithm used by IDS.

References

1. M. Hasan, M. Naseer, B. Pal, S. Ahmad," Support Vector Machine and Random Forest Modeling for Intrusion Detection System Forman", Journal of Intelligent Learning Systems and Applications, vol. 6, (**2014**), pp. 45-52. http://dx.doi.org/10.4236/jilsa.2014.61005
2. N. Farnaaz and M. Jabbar, "Random Forest Modeling for Intrusion Detection System", Procedia Computer Science, vol. 89, (**2016**), pp. 213-217. https://doi.org/10.1016/j.procs.2016.06.047
3. L. Lv, W. Wang, Z. Zhang, X. Liu, "A novel intrusion detection system based on an optimal hybrid kernel extreme learning machine", Knowledge based systems, vol. 195, (**2020**). https://doi.org/10.1016/j.knosys.2020.105648
4. P.Aggarwala and S. Sharma, "Analysis of KDD Dataset Attributes-Class wise for Intrusion Detection", Procedia Computer Science, vol. 57, (**2015**), pp.842-851. https://doi.org/10.1016/j.procs.2015.07.490
5. J. Jha and L. Ragha," Intrusion Detection System using Support Vector Machine", International Journal of Applied Information Systems, (**2013**), pp. 25-30. DOI: 10.5120/icwac1342
6. G. Giorgio, P. Roberto, D. Mauro, R. Fabio," Intrusion detection in computer networks by a modular ensemble of one-class classifiers", Information Fusion, vol. 9, no. 1, (**2008**), pp. 69-82. https://doi.org/10.1016/j.inffus.2006.10.002

ISSN: 2233-7857 IJFGCN

7. M. Mahoney and P. Chan, "PHAD: Packet header anomaly detection for identifying hostile network traffic", Technical report, Florida Tech., technical report CS-2001-4, (**2001**).
8. M. Mahoney and P. Chan, "Learning models of network traffic for detecting novel attacks", Technical report, Florida Tech (**2002**).
9. S. Khonde and V. Ulagamuthalvi, "Fusion of feature selection and Random Forest for an Anomaly based intrusion detection system", Journal of Computational and Theoretical Nanoscience, vol. 16, (**2019**), pp. 3603-3607. DOI: 10.1166/jctn.2019.8332
10. Y. Zhou, G. Cheng, S. Jiang, M Dia," Building an efficient intrusion detection system based on feature selection and ensemble classifier", Computer Networks, vol. 174, (**2020**). https://doi.org/10.1016/j.comnet.2020.107247
11. T. Gamer," Collaborative anomaly-based detection of large-scale internet attacks", Computer Networks, vol. 56, no. 1, (**2012**), pp. 169-185. https://doi.org/10.1016/j.comnet.2011.08.015
12. J. Zhang, M. Zulkernine, A. Haque "Random-forests based network intrusion detection systems" IEEE Transaction of System, Man Cybernetics. Part C: Applications and Reviews, vol. 38, no. 5, (**2008**), pp. 649–59. DOI: 10.1109/TSMCC.2008.923876
13. G. Folino, P. Sabatino," Ensemble based collaborative and distributed intrusion detection systems: A survey", Journal of Network and Computer Applications, vol. 66, (**2016**), pp. 1-16. https://doi.org/10.1016/j.jnca.2016.03.011
14. J. Song, T. Hiroki, O. Yasuo, Y. Kwon. "Unsupervised anomaly detection based on clustering and multiple one-class SVM" IEICE Transaction of Communication, vol. 92, no. 6, (**2009**), pp.1981–90. DOI: 10.1587/transcom.E92.B.1981 ·
15. J. Song, H. Takakura, Y. Okabe, K. Nakao,"Toward a more practical unsupervised anomaly detection system", Information Sciences, vol. 231, (**2013**), pp. 4-14. https://doi.org/10.1016/j.ins.2011.08.011
16. H. Nguyen, N, Harbi, J. Darmont, "An efficient local region and clustering-based ensemble system for intrusion detection". In: Proceedings of the15th Symposium on International Database Engineering & Applications, IDEAS '11, ACM ,NewYork, NY, USA, (**2011**), pp. 185–191. https://doi.org/10.1145/2076623.2076647
17. C. Zhou, C. Leckie, S. Karunasekera, "A survey of coordinated attacks and collaborative intrusion detection", Computers and Security, vol. 29, no. 1, (**2010**), pp. 124-140. https://doi.org/10.1016/j.cose.2009.06.008
18. S. Khonde and V. Ulagamuthalvi, "Ensemble-based semi-supervised learning approach for a distributed intrusion detection system", Taylor and Francis. Journal of Cyber Security Technology, vol. 3, no. 1, (**2019**), pp. 163-188. https://doi.org/10.1080/23742917.2019.1623475
19. S. Khonde and V. Ulagamuthalvi, "Hybrid Architecture for Intrusion detection system", Ingenierie des Systemes d'Information, vol. 24, no. 1, (**2019**), pp. 19-28. https://doi.org/10.18280/isi.240102
20. S. Horng, M. Su, Y. Chen, T. Kao, R. Chen, J. Lai, C. Perkasa, "A novel intrusion detection system based on hierarchical clustering and support vector machines", Expert Systems and Applications, vol. 38, no. 1, (**2011**), pp. 306–13. https://doi.org/10.1016/j.eswa.2010.06.066
21. W. Li, L. Kwok, "Challenge-based collaborative intrusion detection networks under passive message fingerprint attack: A further analysis", Journal of Information Security and Applications, vol. 47, (**2019**), pp. 1-7. https://doi.org/10.1016/j.jisa.2019.03.019
22. M. Perez, J. Tapiador, J. Clark, G. Perez, A. Gomez," Trustworthy placements: Improving quality and resilience in collaborative attack detection", Computer Networks, vol. 58, (**2014**), pp. 70-86. https://doi.org/10.1016/j.comnet.2013.08.026
23. Y. Chen, K. Hwang," Collaborative detection and filtering of shrew DDoS attacks using spectral analysis", Journal of Parallel and Distributed Computing, vol. 66, no. 9, (**2006**), pp. 1137-1151. https://doi.org/10.1016/j.jpdc.2006.04.007

ISSN: 2233-7857 IJFGCN

24. A. Aldweesh, A. Derhab, A. Emam, "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues", Knowledge-based systems, vol. 189, (**2020**), pp. 105-124. https://doi.org/10.1016/j.knosys.2019.105124
25. Z. Wu, J. Wang, L. Hu, Z. Zhang, H. Wu," A network intrusion detection method based on semantic Re-encoding and deep learning", Journal of Network and Computer Applications, vol. 164, (**2020**). https://doi.org/10.1016/j.jnca.2020.102688
26. M .Ferrag, L. Maglaras, S. Moschoyiannis, H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study", Journal of Information Security and Applications", vol. 50, (**2020**). https://doi.org/10.1016/j.jisa.2019.102419
27. Y. Hadhrami, F. Hussain, "Real time dataset generation framework for intrusion detection systems in IoT", Future Generation Computer Systems, vol. 108, (**2020**), pp. 414-423. https://doi.org/10.1016/j.future.2020.02.051
28. J. Manan, A. Ahmed, I. Ullah, L. Boulahia, D. Gaiti, "Distributed intrusion detection scheme for next generation networks" , Journal of Network and Computer Applications, vol. 147, (**2019**). https://doi.org/10.1016/j.jnca.2019.102422
29. A. Almogren, "Intrusion Detection in Edge-of-Things computing", Journal of Parallel and Distributed Computing, vol. 137, (**2020**), pp. 259-265. https://doi.org/10.1016/j.jpdc.2019.12.008

ISSN: 2233-7857 IJFGCN