IJCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

A Survey of various machine learning techniques used in Intrusion Detection System

Anil Lamba

Dept. C.S.E., Himalayan institute of Engineering & Technology, Kala-amb, H.P., India

Corresponding Author: anil.lambain@gmail.com, Tel.: 7015118805

DOI: https://doi.org/10.26438/ijcse/v7i5.557563 | Available online at: www.ijcseonline.org

Accepted: 19/May/2019, Published: 31/May/2019

Abstract— The Intrusion Detection System helps people and organization to detect the attacks, hackers, their logging information and report these information to the owner of the computer system. The Intrusion Detection System not only identifies the attack on the computer system, it also determines problems with current security policies.

The popular conventional security mechanisms are – authentication and firewall security. The authentication protects the computer integrity and security from unauthorized person but it cannot prevent authorized (legitimate) users from performing harmful operations on a computer system. On the other hand firewall only security from some internal attacks to the computer peripherals and information, it cannot provide complete security from outside attacks on the internet. The intrusion detection system is a powerful technology that provides security from both the inside as well as outside attacks. In the world of communication, we exchange our data with another users using internet. Also in the age of cloud computing our data is stored on the remote computer which can be accessed using Internet.

Therefore, security of data is big concern for different users. We need not only to protect the data, which exchanged through internet but also to protect the stored data from different types of attacks. An Intrusion Detection System does all the above activities for us. Successful Intrusion Detection Systems protect computer systems from various types of computer system attacks. We can construct Intrusion Detection Systems on various platforms. One such platform is data mining.

***Keywords*—**Intrusion Detection System, Classifications of IDS.

I. INTRODUCTION

Intrusion detection system

Intrusion Detection term was first introduced by James Anderson in 1980s. Now it is an important part network and firewall security. The primary goal of Intrusion Detection Systems (IDS) is to identify (detect) attacks from insecure networks such as internet to our computer system. With Intrusion Detection Systems, we can obtain all the intrusion related information that occurs during the monitoring of system. We then analyze these information to determine whether our computer system is intrusive against any attack or security breach or not. When Intrusion Detection System detects something disturbing then it gives signal to the network administrator and performs some types of acts already defined to protect the system. In the field of Information and data Security, intrusion detection systems determine the security breaches that compromise the three important security terms – confidentiality, integrity and availability. The intrusion detection system provides system logs regarding security breach, on the basis of these logs the administrator can determine the person that misuses the system and then he/she minimize their rights for future.

Intrusion detection system (ids) performs many functions which are vital for the system. These are as follows:

A. The Intrusion detection system can monitoring different system and users activities. On the basis of this monitoring it analyse the risk for current types of attacks

B. Intrusion detection system can analyse the system Vulnerabilities and it also analyse the configuration of computer system.

C. With intrusion detection system, we can access and maintain the integrity of computer file and system.

D. With intrusion detection system, we can identify pattern of different types of attacks. We can analyse activity patterns, which are not normal.

E. With intrusion detection system, we can determine the violation of user's policy.

Intrusion detection system (ids) classifications

The Intrusion Detection Systems can be divided into following two categories:

A. According to Based on Data Sources : According to data sources used for IDS, the intrusion detection system can be categorized as host-based IDS, network-based IDS, Distributed IDS, Mobile agent based IDS, Cluster based IDS, Cryptography based IDS, Neighhood watch IDS, Cross-feature analysis IDS, Collaborative IDS.

1) Host-based Intrusion Detection Systems: The data for host based Intrusion Detection Systems collected from host records of various activities such as operation system's audit record, classification logs, application programs information, etc. For example, the event logs mechanism of Windows NT operation system finds and gathers following three system events patterns – "Operation system event, safety event and application event".

2) Network-based Intrusion Detection Systems : The intrusion detection of this type collect its data network stream with the help of different segments of data for example Internet packets. This method removes the burden from the hosts because it uses network traffic for checking the data source. Thereby hosts perform their normal operation of computing. It detect different types of network attacks such as signature based, anomaly based etc. Its main limitation is that there are large numbers of false alerts.

3) Distributed Intrusion Detection Systems: The distributed intrusion detection system collects the data for auditing from various hosts. It also obtains the audit data from the network connecting different hosts. It generally detects attacks, which involve multiple hosts.

4) Mobile Agent Based Intrusion Detection Systems: In this type of intrusion detection technique mobile nodes examine the different activities of nodes & gives report for intrusion.Based on intrusion report, the intrusion detection process starts. The limitation of this approach is that it involve large communication overhead. Its main advantage is that it reduces the energy consumption rate of various sensor nodes because in this method mobile agents take the burden of data or information collection about intrusion.

5) Cluster based Intrusion Detection Systems: As the name suggests in this method we divide nodes into multiple clusters. Each cluster group has one cluster head & the cluster head monitors the nodes. The information collected by one cluster head is transferred to all the clusters through gateway. There are number of factors that help to construct the cluster head such as – average load, faithfulness etc.

6) Cryptography based Intrusion Detection Systems: Another method for intrusion detection is cryptography based Intrusion Detection Systems. It detect false route using route discovery technique. The network control traffic is need not to validate the route.

7) Neighbourhood Watch Intrusion Detection Systems: In this method of Intrusion Detection Systems, we check the number of nodes received from neighbours and number packets forwarded by it. If number mismatches then intrusion is detected and reports send to neighbour nodes.

8) Collaborative Intrusion Detection Systems: In this method of Intrusion Detection Systems, the decision for an intruder node is collaboratively taken. But in this method there is vast amount of communication overhead.

B. According to based on Different Analysis Methods:

According to analysis method, intrusion detection system can be classified as "Misuse Detection and Anomaly Detection".

1) Misuse Detection : The misuse detection scheme of intruder detection is also termed as signature- based detection. It stores attack related information in the signature database. Now when an attack occurs then it is first compared with database of attacks signature. After confirmation from signature database the attack related data is termed as actual attack.

In misuse detection approach, "it defines abnormal system behaviour at first, and then defines any other behaviour, as normal behaviour. It assumes that abnormal behaviour and activity has a simple to define model. It advances in the rapid of detection and low percentage of false alarm. It fails in discovering the non-pre-elected attacks in the feature library, so it cannot detect the abundant new attacks".

The framework of system model consists of following components

a) Data Collection Module
b) Pre processing Modules
c) Associative rule mining modules
d) Detection & analysis Modules

2) Anomaly Detection : This method of intrusion detection predicts in advance the expected behavior of the network. If in future expected behavior is not reported then there must be some attacks on the network.

"The main advantage of this approach is that it can examine unknown and more complicated intrusions. The shortcoming of this approach is its low detection rate and high false alarm rate".

II. LITERATURE SURVEY

Suthaharan, S. (2012) [1] Intrusion detection datasets play a major role in evaluating machine learning techniques for Intrusion Detection Systems. The Intrusion detection datasets are generally very large and contain many noncontributing features and redundant data. These drawbacks lead to inaccurate intrusion detection and increased computational cost when machine learning techniques are evaluated. Several data cleaning techniques have been proposed to eliminate redundant records and noncontributing features. These techniques reduce the size of the datasets significantly and make the characteristics of the data closer to the characteristics of intrusions in a real network. This paper identifies anomaly problems in normal and intrusion attacks data, and proposes an ellipsoid-based technique to detect anomalies and clean the intrusion detection datasets further. Publically available KDD'99 and NSL-KDD datasets are used to demonstrate its performance. It reveals an interesting property, i.e. monotonically decreasing behavior, of the NSL-KDD dataset.

Ng, J., Joshi, D., & Banik, S. M. (2015) [2] In our current society, the threat of cyber intrusion is increasingly high and harmful. With the rise of usage in computers, criminal activity has also shifted from physical intrusion into cyber intrusion. Intrusion detection systems provide the ability to identify security breaches in a system. A security breach will be any action the owner of the system deems unauthorized. Current methods used for these systems include using anomaly detection or a signature database. In this research we use both anomaly detection and a signature database using data mining techniques. Our solution provides a tool that would run data mining tools against a log file to detect patterns that may be considered an unauthorized activity. The tool gains additional patterns as time goes by and grows more effective. It allowed us to detect brute force password cracking and Denial-of-Service (DoS) attacks on a system in the Ubuntu platform.

Zhou, Z., Liu, L., & Han, G. (2015) [3] In order to solve the problem that existing wireless sensor network intrusion detection evaluation system are usually lack of consideration in terms of node survival duration, this paper presents a novel intrusion detection evaluation system for the wireless sensor networks. We add low-power resistance and survival continuity to the intrusion detection algorithm which is utilized in traditional network. Experiment results show that the continuity of quality is not only determined by the algorithm itself, it mainly depends on the attack strength and density of nodes.

Mehmood, T., & Rais, H. B. M. (2016) [4] Design of efficient, accurate, and low complexity intrusion detection system is a challenging task. Intrusion detection method is a core of intrusion detection system and it can be either signature based or anomaly based. Although, signature based has high detection rate but it cannot detect novel attacks. Asymmetrically, anomaly based detection method can detect novel attacks but it has high false positive rate. Many machine learning techniques have been developed to cope with this problem. These machine learning algorithms develop a detection model in a training phase. This paper compares different supervised algorithms for the anomaly-based detection technique. The algorithms have been applied on the KDD99 dataset, which is the benchmark dataset used for anomaly-based detection technique. The result shows that not a single algorithm has a high detection rate for each class of KDD99 dataset. The performance measures used in this comparison are true positive rate, false positive rate, and precision.

Jaiswal, A., Manjunatha, A. S., Madhu, B. R., & Murthy, P. C. (2016) [5] Intrusion is one of the most serious problems with network Security, as new types of intrusions are getting much more challenging to detect. Large amount of network traffic has been generated due to the use of internet; most of the generated traffic is in the format which cannot be used directly to arrive at meaningful information. The cleansing and labeling of data each time needs a considerable amount of human effort, and is time consuming. In this paper we show how, Semi supervised machine learning technique can be used in intrusion detection, for both labeled and unlabeled data. In the proposed technique we take a small amount of labeled data to create model and using this model we show how to predict the unlabeled traffic. Machine Learning tool is used for this purpose which uses semi-supervised classifier to build the model. The created model is then integrated in Pentaho which with the help of Weka Scoring provides the expected output. The proposed technique helps the network administrator to take quick decision by classifying the incoming traffic as either malicious or normal and hence efficient detection of intrusion.

Borkar, A., Donode, A., & Kumari, A. (2017) [6] Around the world, billions of people access the internet today. Intrusion detection technology is a new generation of security technology that monitor system to avoid malicious activities. The paper consists of the literature survey of Internal Intrusion Detection System (IIDS) and Intrusion Detection System (IDS) that uses various data mining and forensic techniques algorithms for the system to work in real time. Data mining methods are proposed for cyber analytics in support of intrusion detection.

Samrin, R., & Vasumathi, D. (2017) [7] In computer system and network, Intrusion detection is an important research area. A lot of mechanisms are available for detect the network intrusion, but that is not able to identify the new kind of attacks. Various techniques have already been implemented for finding and categorizing intrusions. The

Intrusion Detection system (IDS) is two types, namely Network based IDS and Host IDS (HIDS). The manual classification of network data inspection is time consuming task, expensive as well as repetitive job. IDS mechanism is very helpful to find the network attacks and anomalies. In IDS, data mining methods is broadly used for extracting useful information from the massive amount dataset. This paper presents the investigation of different techniques and intrusion classification on KDD Cup 99 dataset. So, by classifying the different network issues a new and effective technique is implemented which can categorize and identify intrusions in the KDD Cup 99 dataset.

Zhang, Q., Qu, Y., & Deng, A. (2018) [8] The purpose of the intrusion detection systems is to detect attacks on computer systems and networks. Many technologies can be used for intrusion detection, and one of the most effective technologies is data mining. The rapid development of network technology and internet of things makes network intrusion detection become one of the hot topics for research. Various classifiers have been applied in the field of network intrusion detection, but the performance of such approaches highly depends on the features used. Therefore, feature selection approaches have been usually used along with classifiers for network intrusion detection, including the fuzzy rough feature selection. The fuzzy-rough sets is an extension of the classical rough sets, which can deal with the imprecision and uncertainty of discrete, real value or noise data. It can be seen from the practical applications that there are some shortcomings. Therefore, researchers combine fuzzy-rough sets with kernel methods in order to solve these problems. In this paper, the kernel-based fuzzy-rough feature selection method is used to select the feature subset for the intrusion detection. The proposed approach is validated and evaluated using the KDD 99 dataset with the support of different common classifiers. The experimental outcomes obtained by applying the kernel based fuzzy-rough feature selection method on KDD data set demonstrate that it performs well in terms of reduction effect and accuracy.

Gupta, D., Singhal, S., Malik, S., & Singh, A. (2016) [9] There are many risk of network attacks in the Internet environment. Nowdays, Security on the internet is a vital issue and therefore, the intrusion detection is one of the major research problem for business and personal networks which resist external attacks. A Network Intrusion Detection System (NIDS) is a software application that monitors the network or system activities for malicious activities and unauthorized access to devices. The goal of designing NIDS is to protect the data’s confidentiality and integrity. Our project focuses on these issues with the help of Data Mining. This research paper includes the implementation of different data mining algorithms including Linear regression and K-Means Clustering to automatically generate the rules for classify network activities. A comparative analysis of these techniques to detect intrusions has also been made. To learn the patterns of the attacks, NSL-KDD dataset has been used.

Wankhade, K., Patka, S., & Thool, R. (2013) [10] Intrusion Detection System (IDS) is becoming a vital component of any network in today’s world of Internet. IDS are an effective way to detect different kinds of attacks in an interconnected network thereby securing the network. An effective Intrusion Detection System requires high accuracy and detection rate as well as low false alarm rate. This paper focuses on a hybrid approach for intrusion detection system (IDS) based on data mining techniques. The main research method is clustering analysis with the aim to improve the detection rate and decrease the false alarm rate. Most of the previously proposed methods suffer from the drawback of k-means method with low detection rate and high false alarm rate. This paper presents a hybrid data mining approach encompassing feature selection, filtering, clustering, divide and merge and clustering ensemble. A method for calculating the number of the cluster centroid and choosing the appropriate initial cluster centroid is proposed in this paper. The IDS with clustering ensemble is introduced for the effective identification of attacks to achieve high accuracy and detection rate as well as low false alarm rate.

Sultana, A., & Jabbar, M. A. (2016)[11] With the tremendous growth of usage of internet and development in web applications running on various platforms are becoming the major targets of attack. New threats are create everyday by individuals and organizations that attack network systems. Intrusion is a malicious, externally induced operational fault. Intrusion is used as a key to compromise the integrity, availability and confidentiality of a computer resource. Hence intrusion detection systems (IDS) are becoming a key part of system defense, to detect anomalies and attacks in the network. Data mining based IDS can effectively identify intrusions. Average one dependence estimators (AODE) is one of the recent enhancements of naIve bayes algorithm. AODE solves the problem of independence by averaging all models generated by traditional one dependence estimator and is well suited for incremental learning. In this paper, we propose intelligent network intrusion detection system using AODE algorithm for the detection of different types of attacks. In order to evaluate the performance of our proposed system, we conducted experiments on NSL-KDD data set. Empirical results show that proposed model based on AODE is efficient with low FAR and high DR.

Sharma, B., & Gupta, H. (2014)[12] The role of the intrusion detection system is to enforce the pattern matching policies decided for the network. Basically Proposed IDS executes on the KDD’99 Data set; this data set is used in international level for evaluating/calculating the performance of various intrusion detection systems (IDS). First step is association phase in which frequent item set are produced by apriori algorithm. The second step is clustering phase in which clusters are created by k- Means. Proposed technique uses the standard KDD99 (knowledge Discovery and Data Mining) intrusion detection contest data set. Proposed system can detect the attacks/intrusions and classifies them into different categories: U2R (User to Root), probe, R2L (Remote to Local), and Denial of Service (DoS). The prime task of the proposed IDS is to improve effectiveness with efficiency. An experiment is carried out to evaluate/calculate the performance of the proposed approach using KDD 99’ dataset. Here the result shows that the proposed IDS technique performs better in term of efficiency(Execution Speed) & effectiveness.

El Moussaid, N., & Toumanari, A. (2014)[13] Most of traditional intrusion detection systems, Anomaly-Based detection and Signature-based detection, suffer from many drawbacks. This paper exposes the limits and drawback of traditional Intrusion detection systems. Consequently the main goal of this paper is to expose data mining techniques and approaches to improve the performance of the traditional intrusion detection system to identify known and unknown attack's patterns.

Deepa, V. K., & Geetha, J. R. R. (2013)[14] The development of Information

Technology has generated large amount of databases and huge data in various areas. Loose coupling is adapted in Data Mining System, since it can fetch any portion of data stored in database by more flexibility and in efficient manner. Therefore the Data mining system can be classified according to the kinds of databases mined, the kinds of knowledge mined, the techniques used or the application adapted. The traditional method is used to analyse data manually for patterns for the extraction of knowledge. In Banking, Health care, marketing, Science there will be a data analyst to work with data and scrutinizing the final role of decisions. This work is done by Data Mining. Data mining application can be generic or domain specific. It allows reusability in a feasible way and finally it makes possible to build large and scalable system. Applications of Data mining in computer security are designed to meet the needs of a professional audience composed of researchers and practitioners in various fields. This paper gives the overview of Data mining system and few of its applications. Data mining is becoming a technology in activities as diverse as using historical data to predict the success of marketing.

Bjerkestrand, T., Tsaptsinos, D., & Pfluegel, E. (2015)[15] Intrusion detection is concerned with monitoring and analysing events occurring in a computer system in order to discover potential malicious activity. Data mining, which is part of the procedure of knowledge discovery in databases, is the process of analysing the collected data to find patterns or correlations. As the amount of data collected, store and processed only increases, so does the significance and importance of intrusion detection and data mining. A dataset that has been particularly exposed to research is the dataset used for the Third International Knowledge Discovery and Data Mining Tools competition, KDD99. The KDD99 dataset has been used to identify what data mining techniques relate to certain attack and employed to demonstrate that decision trees are more efficient than the Naïve Bayes model when it comes to detecting new attacks. When it comes to detecting network intrusions, the C4.5 algorithm performs better than SVM. The aim of our research is to evaluate and compare the usage of various feature selection and reduction algorithms against publicly available datasets. In this contribution, the focus is on feature selection and reduction algorithms. Three feature selection algorithms, consisting of an attribute evaluator and a test method, have been used. Initial results indicate that the performance of the classifier is unaffected by reducing the number of attributes.

China Appala Naidu, R., & Avadhani, P. S. (2012)[16] The Expositional increase in the traffic across networks has necessitated the need to detect unauthorized access. In this sense Intrusion Detection has become one of the major research areas In this paper three data mining techniques namely CS.O Decision Tree, Ripper Rule and Support Vector Machines are studied and compared for the efficiency in detecting the Intrusion, It is found that the CS.O Decision Tree is efficient than the other two. The data mining tool Clementine is used for evaluating this on the KDD99 dataset.

Ariafar, E., & Kiani, R. (2017)[17] Nowadays, detection of various attacks constitutes a significant aspect of network security. The task of an intrusion detection system (IDS) is to identify and detect any unauthorized use, exploitation or damage to network resources and systems. In this paper, an optimized framework for network attack detection is presented using data mining techniques. The framework is based on the K-means clustering and decision tree (DT) classification techniques in which a genetic algorithm (GA) is used to optimize such parameters as number of clusters (K), max_runs, and confidence. Simulation results on the NSL-KDD 2009 dataset have revealed that the suggested method achieved a 99.1% of detection rate (DR) and 1.8% of false alarm rate (FAR), demonstrating an improvement compared with the new ensemble clustering (NEC) method.

Elekar, K. S. (2015)[18] As Internet continues to influence our day to day activities like eCommerce, eGoverence, eEducation etc. the threat from hackers has also increased. Due to which many researcher thinking intrusion detection systems as fundamental line of defense. However, many commercially available intrusion detection systems are predominantly signature-based that are designed to detect known attacks. These systems require frequent updates of signature or rules and they are not capable of detecting unknown attacks. One of the solution is use of anomaly base intrusion detection systems which are extremely effective in detecting known as well as unknown attacks. One of the major problem with anomaly base intrusion detection systems is detection of high false alarm rate. In this paper, we provide solution to increase attack detection rate while minimizing high false alarm rate by combining various data mining techniques.

Das, A., & Sathya, S. S. (2012)[19] Analyzing the KDD CUP 99 provides useful information in the development of intrusion detection systems to be used in networks. The classification of records in the KDD dataset into normal and attack records involves mining rules involving the features present in the dataset. Since the KDD dataset contains a huge number of features, mining rules becomes a difficult task. Hence several algorithms have been developed to extract the most relevant set of features that contribute to the accurate classification of records. The selected features should result in the least misclassification rate. This paper presents a fuzzy approach to feature reduction and analyzes the evolved features using classification algorithms in Tanagra. It is found that the algorithm yields a very low misclassification rate when compared to other algorithms.

Prachi Tembhare1, Neeraj Shukla (2017)[20] Cloud computing environments are easy targeted by intruders and pose new risks and threats to an organization because of its service and operational models, the underlying technologies, and their distributed nature that relies on the network for its working. However, IDSs are among the efficient security mechanisms that can handle most of the threats of cloud computing. In spite this, several deficiencies of current IDSs technologies and solutions hinder their adoption in a cloud. The proposed work focuses on developing improved IDS that provides an integrated approach of both techniques i.e. anomaly based as well as knowledge based whether implement on network or host based IDS for cloud computing to detect masquerade, host, and network attacks and provides efficient deployments to detect DDoS attacks. The work comprises of integration of two powerful open source tool Suricata and Snort together with the proposed DDoS detection rule make the working of IDS more effective and high alarm rate generating Hybrid IDS.

P**. Rutravigneshwaran (2017)[21]** IDS is a software consequence monitors the humiliation or behavior plus investigate any immoral operation suggest itself. Fantastic increase and tradition of internet raises concerns in relation to how to defend and communicate the digital in order in a safe approach. Nowadays, hackers use different types of attacks for getting the valuable information. In the proposed Fast Hierarchical Relevance Vector Machine (FHRVM), Analytical Hierarchy Process Method (AHP) issued to select the input weight sand hidden biases. Simulation has been carried out using Math works MATLAB R2012a. KDD Cup 1999 dataset is taken for testing the performance of the proposed work and the results indicate that FHRVM has achieved higher detection rate and low false alarm rate than that of existing SVM algorithm. This research evaluate the efficiency of machine learning methods in intrusion detection system, together with classification tree and support vector machine, with the expect of given that reference for establishing intrusion detection system in future. Compared with further interrelated works in data mining based intrusion detectors accuracy, detection rate, false alarm rate. It moreover show improved act than KDD Winner, particularly used for two types of attacks namely, U2R type and R2L type. Comparison results of C4.5, SVM. we finds that C4.5 is superior to SVM in accuracy and detection; in accuracy for Probe, Dos and U2R attacks, C4.5 is also better than SVM and FHRVM; but in false alarm rate FHRVM is better. In this paper enhance that FHRVM is better than c4.5 and SVM for U2R attack & R2L attack.

III. Conclusion

In this paper, we have study the various machine learning algorithms like SVM, naive Bayes, J.48, and decision table for anomaly detection. The performance of the algorithms is tested on KDD99. For each class, each algorithm has different result and no single algorithm has high TPR for all 5 different classes. But the overall accuracy of J.48 decision tree is high among all other algorithms and low misclassification rate. The reason can be that decision tree yields good result in the presence of the redundant features. Therefore, the future work would be using the above algorithm with some feature selection algorithms.

References

[1] Suthaharan, S. (2012). An iterative ellipsoid-based anomaly detection technique for intrusion detection systems. 2012 Proceedings of IEEE Southeastcon.

[2] Ng, J., Joshi, D., & Banik, S. M. (2015). Applying Data Mining Techniques to Intrusion Detection. 2015 12th International Conference on Information Technology - New Generations.

[3] Zhou, Z., Liu, L., & Han, G. (2015). Survival Continuity on Intrusion Detection System of Wireless Sensor Networks. 2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC).

[4] Mehmood, T., & Rais, H. B. M. (2016). Machine learning algorithms in context of intrusion detection. 2016 3rd International Conference on Computer and Information Sciences (ICCOINS).

[5] Jaiswal, A., Manjunatha, A. S., Madhu, B. R., & Murthy, P. C. (2016). Predicting unlabeled traffic for intrusion detection using semi-supervised machine learning. 2016 International Conference on Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT).

[6] Borkar, A., Donode, A., & Kumari, A. (2017). A survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and protection system (IIDPS). 2017 International Conference on Inventive Computing and Informatics (ICICI).

[7] Samrin, R., & Vasumathi, D. (2017). Review on anomaly based network intrusion detection system. 2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT).

[8] Zhang, Q., Qu, Y., & Deng, A. (2018). Network Intrusion Detection Using Kernel-based Fuzzy-rough Feature Selection. 2018 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE).

[9] Gupta, D., Singhal, S., Malik, S., & Singh, A. (2016). Network intrusion detection system using various data mining techniques. 2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS).

[10] Wankhade, K., Patka, S., & Thool, R. (2013). An efficient approach for Intrusion Detection using data mining methods. 2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI).

[11] Sultana, A., & Jabbar, M. A. (2016). Intelligent network intrusion detection system using data mining techniques. 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT).

[12] Sharma, B., & Gupta, H. (2014). A Design and Implementation of Intrusion Detection System by Using Data Mining. 2014 Fourth International Conference on Communication Systems and Network Technologies.

[13] El Moussaid, N., & Toumanari, A. (2014). Overview of intrusion detection using data-mining and the features selection. 2014 International Conference on Multimedia Computing and Systems (ICMCS).

[14] Deepa, V. K., & Geetha, J. R. R. (2013). Rapid development of applications in data mining. 2013 International Conference on Green High Performance Computing (ICGHPC).

[15] Bjerkestrand, T., Tsaptsinos, D., & Pfluegel, E. (2015). An evaluation of feature selection and reduction algorithms for network IDS data. 2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA).

[16] China Appala Naidu, R., & Avadhani, P. S. (2012). A comparison of data mining techniques for intrusion detection. 2012 IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT).

[17] Ariafar, E., & Kiani, R. (2017). Intrusion detection system using an optimized framework based on datamining techniques. 2017 IEEE 4th International Conference on Knowledge-Based Engineering and Innovation (KBEI).

[18] Elekar, K. S. (2015). Combination of data mining techniques for intrusion detection system. 2015 International Conference on Computer, Communication and Control (IC4).

[19] Das, A., & Sathya, S. S. (2012). A fuzzy approach to feature reduction in KDD intrusion detection dataset. 2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12).

[20] Prachi Tembhare1, Neeraj Shukla (2017)[20] An Integrated and Improved Scheme for Efficient Intrusion Detection in Cloud.

[21] P. Rutravigneshwaran (2017) A Study of Intrusion Detection System using Efficient Data Mining Techniques.

Authors Profile

Ikshita Banasal is pursuing Master of Technology (Computer Science & Engineering) from Himalayan institute of Engineering & Technology, Kala-amb, H.P., India. She has completed her Bachelor of Technology (Computer Science & Engineering) from Eternal University, Baru Sahib, H.P. , India in 2012.

Dr. Anil Lamba, PhD, is a H.O.D. at Himalayan Institute of Engineering & Technology Kala-amb, H.P., India. He is Associate Professor in Computer Science & Technology Department in Himalayan Institute. He is a dynamic person having good research background.Dr. Anil Lamba has published number of research paper in various International and National journals.