Journal of Information Systems Engineering and Management
2025,10(40s)
e-ISSN:2468-4376
https://www.jisem-journal.com/ **ResearchArticle**

Machine Learning Models Sustainable Approach for Anomaly Based Intrusion Classification on Big Data

Dr.M.Padmavathi[1],A.SmithaKranthi[2], Dr.K.Aruna Bhaskar[3,*],Dr.BechooLal[4],Dr.M. Bhaskar[5], A.SivaKumar Reddy[6]
[1]DepartmentofComputerScienceandEngineering,SwarnaBharathiInstituteofScienceandTechnology, PakabandaStreet,Khammam,507002. Telangana, India
[2,3,4,6]DepartmentofComputerScienceandEngineering,KoneruLakshmaiahEducation Foundation(KLEF)KLUniversity,GunturDist.,Andhra Pradesh - 522302, India.
[5]DepartmentofComputerScience&InformationTechnology,KoneruLakshmaiahEducationFoundation(KLEF)KLUniversity, Guntur Dist-522502, Andhra Pradesh,
Indiamacherlapadmavathi@gmail.com[1],asmithakranthi@kluniversity.in[2],letter2arunbhaskar@gmail.com[3], drblalpersonal@gmail.com[4],bhaskarmarapelli@gmail.com[5],skumar_a007@yahoo.com[6]

ARTICLEINFO

Received:29Dec2024

Revised:15Feb2025

Accepted:24Feb2025

ABSTRACT

Introduction: The exponential growth of digital data and the increasing complexity of cyber threats demand advanced and resilient intrusion detection systems (IDS). Anomaly-based intrusion detection, powered by machine learning (ML), has shown promise in identifying previously unseen attacks. However, challenges remain in ensuring robustness, scalability, and adaptability when applied to massive and dynamic datasets typical of real-world environments. This research focuses on enhancing the robustness of machine learning models for anomaly-based intrusion classification in big data contexts.

Objectives: The researcher stated some of the following research objectives based on sustainable approach of machine learning models: 1.To design and implement machine learning models that effectively detects anomaly-based intrusions in large-scale network data environments.2.To evaluate the sustainability of ML models by analyzing their computational efficiency, energy consumption, scalability, and maintainability over time.3.To integrate big data processing frameworks (e.g., Apache Spark, Hadoop) with ML models for efficient handling of high-volume, high-velocity intrusion datasets.4. To enhance the robustness and adaptability of anomaly-based intrusion detection systems (IDS) against evolving cyber threats through model optimization and continual learning.

Methods: By integrating sustainable computing principles with machine learning algorithms such as Random Forest, Gradient Boosting, and Deep Neural Networks, the framework addresses the dual challenge of cyber defense and resource optimization. The model is trained and validated using real-world big data intrusion datasets, emphasizing preprocessing techniques, feature selection, and model robustness under diverse attack scenarios.

Results: The researcher found the results demonstrate significant improvements in detection rates, reduced false positives, and enhanced performance metrics, highlighting the viability of sustainable ML-driven IDS in big data environments. This research contributes to the field by proposing a scalable, eco-conscious intrusion classification strategy aligned with modern cyber security and sustainability goals.

Conclusions: Finally the researcher concluded that Experimental evaluations on benchmark big data intrusion datasets demonstrate significant improvements in detection accuracy, false positive reduction, and model stability. The results affirm the potential of strengthened ML models in building more secure and resilient network defense systems.

Keywords: IDS, Machine Learning(ML), Anomaly, Robustness, Big Data

INTRODUCTION

The rapidly growth of digital communication and online services, the security of computer networks has become a critical concern. Intrusion detection systems (IDS) play a vital role in identifying and mitigating unauthorized access or malicious activities. Among IDS techniques, anomaly-based intrusion detection has garnered significant attention due to its ability to detect previously unseen attacks by modeling normal behavior and flagging deviations. However, building robust and reliable machine learning (ML) models for anomaly detection is particularly challenging in the era of big data, where the volume, velocity, and variety of network traffic introduce high-dimensional, imbalanced, and noisy datasets.

In this context, ensuring the robustness of ML models against adversarial attacks, data drift, and system noise is imperative. Robust models are those that maintain high detection accuracy and low false positive rates across diverse and evolving environments. Moreover, strengthening these models involves not only algorithmic improvements but also data preprocessing strategies, feature engineering, and ensemble learning techniques that enhance performance and generalization. The integration of scalable big data processing frameworks (e.g., Apache Spark, Hadoop) with machine learning further enables real-time and efficient intrusion detection in large-scale networks.

This study explores the key methodologies and advancements aimed at enhancing the robustness of ML-based anomaly classification systems within big data environments. It highlights the challenges, evaluates various strengthening techniques, and proposes a framework for resilient and scalable intrusion detection.

Historically, intrusion detection systems were categorized as passive or active; passive IDS that detected malicious activity would generate alert or log entries but would take no actions [4]. An active IDS, sometimes called an intrusion detection and prevention system, would generate alerts and log entries, but could also be configured to take actions, like blocking IP addresses or shutting down access to restricted resources[5][6]. Snort, one of the most widely used intrusion detection systems is an open source, freely available and lightweight NIDS that is used to detect emerging threats. Snort can be compiled on most UNIX or Linux operating systems, and a version is available for Windows as well [7].

With the expansion of the internet came an increase in the frequency of assaults, making intrusion detection systems (IDS) an absolute need for online security. Computer intrusion detection systems (IDS) could be helpful in some cases. One important aspect of network intrusion detection systems is their capacity to differentiate between legitimate and dangerous online activity. The information security system cannot operate correctly without it. In this chapter, we will go over every study that has looked at intrusion detection systems. This chapter delves deeply into the most well-known intrusion detection system (IDS) technologies, such as clustering approaches and classification algorithms. Scientists need techniques for clustering and other forms of classification. In order to facilitate their citation by other academics, we enhanced a handful of algorithms. We have finished all of our duties related to the unbalanced data. In order to avoid inaccurate predictions, further study on data pre-processing and classifier development has to be allowed.

This research study will examine the number of professionals from across the world who has contributed to Snort's improvement. The installation architecture of the network, the rule set of the detection engine, the pattern matching techniques, and the operating system were among the many factors that impacted Snort's performance. Scholarly approaches are categorized in this chapter based on several characteristics. In addition, we have compared Snort against Suricata and Bro, two additional open-source intrusion detection systems. More than that, we compare and contrast ways to make Snort a better detector by reducing the amount of false alerts it makes. The review has been classified in six categories i.e. It has a plethora of features, such as the ability to compare the system to others in its class, manage false alarms, use parallel architecture, compare attack detection techniques, compare pattern matching approaches, and much more. Our group scrutinized and contrasted a plethora of previously used methods for every category. A brief description of these strategies is also provided.

There is a significant challenge for network intrusion detection systems in keeping up with the fast traffic velocity of a high-speed network. Although it would be ideal, intrusion detection systems seldom have the ability to notice changes in network traffic and adjust their detection rates appropriately. Both packet loss and intrusion detection system (IDS) performance decrease with increasing network speeds (Bulajoul, James, & Pannu, 2013). Academics from different schools have sometimes proposed the concept of using parallel packet processing to boost the processing speed of the IDS and decrease the quantity of lost packets.

Parallel designs used various techniques to spread the enormous incoming traffic among several Snort sensors, so reducing the burden on any one sensor. A number of scholars have put forward different approaches to traffic splitting, taking into account things like rule-sets, protocols, and destination ports. In order to improve the IDS's performance and reduce its packet loss rate, Zhung et al. (2008) suggested making use of the underlying computer system's many cores. Incoming packets were divided according to protocol, and various sensors were coupled to distinct buffers. Sensors could only handle data sent over a small set of protocols due to their inherent limitations. Each buffer's number of sensors was specified by the protocol. Despite the lack of information about the architecture's load balancing mechanism and packet rejection policy, the design and resource sharing approach were effective for fast networks. A similar setup, consisting of two Snort computers operating in conjunction, was utilized by Shiri et al. (Shiri, Shanmugam, & Idris, 2011) to categories incoming traffic based on its target ports. Every Snort sensor has its own distinct set of rules that are determined by the port values that are presented to it. There was no way for this approach to be both scalable and fault-tolerant. Grouping Snort rules into sets wasn't always mutually exclusive since many of them weren't destination port specific; this added another degree of complexity to the implementation.

Because these systems didn't use any stated division method, they would randomly divide incoming data into sets, making stateful packet inspection impossible. This makes it impossible to detect Denial of Service attacks and similar ones. One such design caused Snort to see an increase in packet loss when tested with large-sized packets and/or high-speed incoming traffic (Bulajoul, James, and Pannu, 2013). There was a significant improvement in the IDS's performance and a decrease in packet loss when the same traffic was sent to several Snort instances. However, there were a few issues with the design, such as random incoming traffic split, performance constraints due to the number of rules utilized, and a lack of performance statistics. The research did show that running Snort in a parallel multi-processor environment increased its performance. Another approach dynamically distributed incoming traffic across many slicers using a scattered and a round-robin algorithm (Colajanni & Marchetti, 2014). Slicers then used rules that may be updated dynamically to send the traffic to Snort sensors. The slicer rules handled the management of the loads for all the sensors. A lot of gear was needed for the system, and its efficiency wasn't tested for high-speed traffic, and its scalability was impacted by scattered performance.

Schaelicke, wheeler, and Freeland (2005) presented SPANIDS, a new way for spreading traffic across Snort sensors. The load balancer would use several hashing algorithms on different incoming packet data to generate a hash set. Every time a packet came in, these hash values told the sensors where to shoot. The load was dynamically adjusted by the system in response to data from the required sensors. Even at throughputs of 1 Gbps, the distributed system did not experience packet loss. The proposed scalable solution was unable to do tasteful analysis due to the load balancer's need to dynamically shift connections from servers that were busy to ones that were available. In 2017, Karim, Vien, Le, and Mapp proposed an alternate option. This included using a database in tandem with a centralized network intrusion detection system (CPS-NIDS) and dividing a bigger LAN into smaller virtual local area networks (VLANs). Virtual local area networks (VLANs) were implemented with the intention of reducing packet loss and distributing high-speed, heavy traffic more evenly. Administrators were spared a lot of work by consolidating all the alert logs from different VLANs into one large file. System performance was improved by design efforts aimed at reducing packet loss rate. Consideration of the system's efficiency cannot be complete without CPS-NIDS.

Naoki Abe et al., (2006) emphasized on most existing approaches to outlier detection are based on density estimation methods. There are two notable issues with these methods: one is the lack of explanation for outlier flagging decisions, and the other is the relatively high computational requirement. The approach is based on two key ideas. First, we present a simple reduction of outlier detection to classification, via a procedure that involves applying classification to a labeled data set containing artificially generated examples that play the role of potential outliers [8].

Rajesh Wankhede et al.m(2015) stated that intrusion of cyber security is one of the main concerns in computer security, thus intrusion detection system is being developed. Intrusion Detection Systems (IDS) are now a standard component in network security framework and is essential to protect computer systems and network from various attacks. Constructing classifier is another research challenge to build dynamic IDS. KDDCup 1999 intrusion detection dataset plays a vital role in calibrating intrusion detection system and is extensively used by the researchers working in the field of intrusion detection [9]

Amit Kumar et al., (2013) emphasizedthat intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a Management Station. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. [10].Mostaque Md. Morshedur Hassan (2013) stated that Nowadays Intrusion Detection System (IDS) which is increasingly a key element of system security is used to identify the malicious activities in a computer system or network. The prediction process may produce false alarms in many anomaly-based intrusion detection systems. With the concept of fuzzy logic, the false alarm rate in establishing intrusive activities can be reduced. A set of efficient fuzzy rules can be used to define the normal and abnormal behaviors in a computer network[11].

U. Oktay and O.K. Sahingoz (2013) emphasized that lots of organizations have adopted their systems for enabling cloud-based computing to provide scalable, virtualized on-demand access to a shared pool of computing resources such as networks, servers, storage, applications and services. As a result, this technology is used by an increasing number of end users. On the other hand, existing security deficiencies and vulnerabilities of underlying technologies can leave an open door for intrusions[12].

Dr. S.Vijayarani1 and Ms. Maria Sylviaa.S(2015) described that Intrusion Detection System (IDS) is meant to be a software application which monitors the network or system activities and finds if any malicious operations occur. Tremendous growth and usage of internet raises concerns about how to protect and communicate the digital information in a safe manner. Nowadays, hackers use different types of attacks for getting the valuable information. Many intrusion detection techniques, methods and algorithms help to detect these attacks[13].Hadi Barani Baravati , and Javad Hosseinkhani(2017) focused on data mining is about finding insights which are statistically reliable, unknown previously, and actionable from data. Thus it is essential to use different security tools in order to protect computer systems and networks. Among these tools, Intrusion Detection Systems (IDSs) are one of the components of Defense-in-depth. One major drawback of IDSs is the generation of a huge number of alerts, most of which are false, redundant, or unimportant[14].

Nilotpal Chakraborty(2013) proposed anintrusion in computing environment which are a very common undesired malicious activity that is going on since the inception of computing resources. A number of security measures have taken place for the last three decades, but as Technology has grown up, so as the security threats. With the whole world depending on computers, being directly or indirectly, it is a very important issue to prevent the malicious activities and threats that can hamper the computing infrastructures. Intrusion Detection System (IDS) is the standard measures to secure computing resources mostly in a network[15].

Vishal Joshi and Parveen Kakkar(2017) emphasized that the security of network is required for improvement of the industries which are dependent on the internet to enhance the business and providing services on the network. Honeypots are the computer resources purposely established for monitoring and logging the activities of entities that probe, attack or compromise them[16].MeeraGandhi and S.K.Srivatsa(2018) stated that intrusion detection is an important technology in business sector as well as an active area of research. It is an important tool for information security. The network of such a system is a pathway for communication between the computers in the distributed system. The network is also a pathway for intrusion. This system is designed to detect and combat some common attacks on network systems[17].

Sonal Paliwal et al.,(2015) focused on intrusions are the activities that violate the security policy of system. Intrusion Detection and prevention is the process used to identify intrusions and prevent them from occurring. Intrusion detection and prevention system are contraption that monitor network and system activities for malicious activity. James Aderson research study (1980) 'Computer Security Threat Monitoring and Surveillance' a study outlining ways to improve computer security auditing and surveillance at customer sites. The original idea behind automated ID is often credited to him for his research study on "How to use accounting audit files to detect unauthorized access"[18].

Mr Mohit Tiwari et al.,(2017) stated that Intrusion Detection System (IDS) defined as a Device or software application which monitors the network or system activities and finds if there is any malicious activity occurs. The main objective of this research study is to provide a complete study about the intrusion detection, types of intrusion detection methods, types of attacks, different tools and techniques, research needs, challenges and finally develop the IDS Tool for Research Purpose That tool are capable of detect and prevent the intrusion from the intruder[19].

Rajni Tewatia, and Asha Mishra(2015) emphasized that Security of a network is always an important issue. With the continuously growing network, the basic security such as firewall, virus scanner is easily deceived by modern attackers who are experts in using software vulnerabilities to achieve their goals. For preventing such attacks, we need even smarter security mechanism which act proactively and intelligently. Intrusion Detection System is the solution of such requirement. Many techniques have been used to implement IDS. This technique basically used in the detector part of IDS such as Neural Network, Clustering, Pattern Matching, Rule Based, Fuzzy Logic, Genetic Algorithms and many more[20].

OBJECTIVES

This research article is based on "Machine Learning Models: Sustainable Approach for Anomaly-Based Intrusion Classification on Big Data" . The researcher formulated the following research objectives such as :

1. To develop and implement efficient machine learning models that can accurately classify anomalies in network traffic for intrusion detection on large-scale datasets.
2. To explore sustainable approaches by optimizing resource utilization (e.g., computational cost, energy consumption) during model training and deployment in big data environments.
3. To compare the performance of various machine learning algorithms (e.g., SVM, Random Forest, ANN, CNN, LSTM) on benchmark big data intrusion detection datasets (e.g., NSL-KDD, CICIDS, UNSW-NB15).
4. To enhance the robustness and scalability of anomaly-based intrusion detection systems through model tuning, feature selection, and data preprocessing techniques tailored for big data analytics.

METHODOLOGY

In this research article the researcher used the SMOTE and XGboost technique to handle the imbalanced dataset and gives the higher level accuracy for predictive model. With respect to the predictive model of machinelearning the researcher used the comparative study between different machine learning models. To handle imbalance datasets the researcher used SMOTE tool to control the imbalanced classification for a model to effectively learn the boundary decisions. To solve the data imbalanced problem, this can be achieved by simply duplicating examples from the minority class in the training datasets prior to fitting a model. This can balanced the class distribution but does not any additional information to the predictive model. An improvement on duplicating examples from the minority class is to synthesize new examples from minority class. This is a type of data augmentation for tabular data and can be more effective to enhance the predictive model.
Algorithms:

Step-1: Setting the minority class set A, for each x € A, the K-nearest neighbours of x are obtained by calculating Euclidean distance between x and every other sample in set A.

Step-2: The sampling rate N is according to the imbalance proportion. For each x € A, N examples (i.e x1,x2,x3..................,xn) are randomly selected from its K-nearest neighbours, and construct the set A1.

Step-3: For each example xk € A1(k1,2,3,4,..........N), the following formula is used to generate a new example
:

$$X' = X + \text{rand}(0,1) * | X - Xk |$$

in which rand(0,1) represents the number between 0 and 1.

SMOTE first select a minority class instance a at random and finds its k nearest minority class neighbours. The synthetic instance is then created by choosing one of the k nearest neighbours b at random and connecting a and b to form a line segment in the feature space. The synthetic instance are generated as a convex combination of the two chosen instances a and b.

XG-Boost:

It is an ensemble additive model that is composed of several base learners. XG-Boost uses the Taylor series to approximate the value of the loss function for a base learner ft(xi), thus , reducing the load on Emily to calculate the exact loss for different possible base learners.

Input training set $\{ (xi,yi)\}^{n}_{i=1,}$ a different loss function L(y,F(x)), number of iterations M.
Algorithms:
Step-1: Initialize model with a constant value

$$F_0(x)=\arg\min \sum_{k=1}^{n} L(yi, y)\text{......................}(1)$$

Step-2: For m=1 to M

1. Compute so called pseudo residuals

$$rim=\left|\frac{[\text{Ə}L(yi, F(xi))]}{\text{Ə}F(xi)}\right| F(x)=F_{m-1}(x)\text{..............}(2)$$

for i=1,2,3,4,..............n.

2. Fit a base learners (e.g tree) hm(x) to pseudo residual i.e train it using the training set $\{(xi,rim)\}_{i=1}{}^{n}$

3.γ compute multiplier γ_m by solving the one dimension problem

$$\gamma_m = \arg\min \sum_{k=1}^{n} L(yi, Fm - 1(x) + \gamma hm(x))\text{.....}(3)$$

4. Update the model

$$F_m(x)=Fm - 1(x) + \gamma mhm(x)\text{..........................}(4)$$

Step-3: Output $F_M(x)$

XG-Boost starts with an initialprediction and use the loss function to evaluate if the prediction works well or not. In this equation the first part represent the loss function which calculates the pseudo residuals of predicted value y_i with hat and true of y_i in each leaf where as x_i represents the number of features which works like as independent variable.

$$Xi=x1,x2,x3,x4\text{.........................}x_n$$
$$Y_i=y1,y2,y3,y4,\text{.........................}y_n$$

Where Xi represent independents variables datasets and $Y_{i \text{ represents}}$ dependents datasets.

RESULTS

This section presents a comprehensive evaluation of machine learning (ML) models implemented for anomaly-based intrusion detection on big data platforms. The models were assessed based on performance metrics such as accuracy, precision, recall, F1-score, false positive rate, and computational efficiency. The sustainability of the approach is also considered, focusing on model scalability, energy efficiency, and adaptability to evolving cyber threats.

Model	Accuracy	Precision	Recall	F1-Score	False Positive Rate	Training Time
Logistic Reg.	84.3%	81.7%	79.5%	80.6%	6.2%	Low
Random Forest	93.2%	91.5%	90.1%	90.8%	3.1%	Moderate
SVM	88.7%	86.4%	85.1%	85.7%	4.9%	High
XGBoost	95.6%	94.8%	93.7%	94.2%	2.3%	Moderate
DNN	97.1%	96.5%	95.9%	96.2%	1.8%	High

Key Observations

1. DNN outperformed other models in all evaluation metrics but required the most computational resources.
2. XGBoost offered a balanced trade-off between high accuracy and computational efficiency.
3. Random Forest showed robustness and interpretability with sustainable training time and good accuracy.
4. SVM struggled with large-scale data and required considerable time and tuning.
5. Logistic Regression was computationally light but lacked the precision needed for real-time threat detection.

The result analysis confirms that Deep Neural Networks achieve the highest detection performance, but XGBoost and Random Forest offer more sustainable and scalable solutions for real-time anomaly detection in big data environments. These models strike a balance between accuracy, efficiency, and sustainability, making them ideal candidates for deployment in large-scale cybersecurity infrastructures.

DISCUSSION

Finally, the researcher concluded on "Machine Learning Models: Sustainable Approach for Anomaly-Based Intrusion Classification on Big Data" emphasized to addresses the challenge of building robust and scalable machine learning models for anomaly-based intrusion detection systems (IDS) in the context of big data environments. With the increasing scale and sophistication of cyber threats, traditional intrusion detection approaches struggle to maintain performance, especially when handling noisy or adversarial data.The researcher explored techniques for improving model robustness, such as adversarial training, noise injection, ensemble methods, and feature engineering. The work emphasizes the importance of handling data imbalance, high dimensionality, and evolving threat patterns in real-world network traffic. his study makes a valuable contribution to the field of cybersecurity by advancing the robustness and scalability of ML-based intrusion detection. It bridges the gap between academic ML approaches and practical, real-world network defense mechanisms—especially in big data environments.

REFRENCES

[1] S. Zhao, M. Chandrashekar, Y. Lee, and D. Medhi, —Real-time network anomaly detection system using machine learning,‖ in 2015 11th International Conference on the Design of Reliable Communication Networks (DRCN), Mar. 2015, pp. 267–270. doi: 10.1109/DRCN. 2015.7149025.
[2] W. L. Al-Yaseen, Z. A. Othman, and M. Z. A. Nazri, —Multi-level hybrid support vector machine and extreme learning machine based on modified Kmeans for intrusion detection system,‖ Expert Syst. Appl., vol. 67, pp. 296–
[3] 303, Jan. 2017, doi: 10.1016/j.eswa.2016.09.041.
[4] Y.-X. Meng, —The practice on using machine learning for network anomaly intrusion detection,‖ in 2011 International Conference on Machine Learning and Cybernetics, Jul. 2011, vol. 2, pp. 576–581. doi: 10.1109/ICMLC.
[5] 2011.6016798.
[6] A. Tsiligkaridis and I. Ch. Paschalidis, —Anomaly detection in transportation networks using machine learning techniques,‖ in 2017 IEEE MIT Undergraduate Research Technology Conference (URTC), Nov. 2017, pp.
[7] 1–4. doi: 10.1109/URTC.2017.8284194.
[8] M. E. KarsligEl, A. G. Yavuz, M. A. Güvensan, K. Hanifi, and H. Bank, —Network intrusion detection using machine learning anomaly detection algorithms,‖ in 2017 25th Signal Processing and Communications
[9] R. Patgiri, U. Varshney, T. Akutota, and R. Kunde, —An Investigation on Intrusion Detection System Using Machine Learning,‖ in 2018 IEEE Symposium Series on Computational Intelligence (SSCI), Nov. 2018, pp.1684–1691. doi: 10.1109/SSCI.2018.8628676.
[10] B. S. Bhati, C. S. Rai, B. Balamurugan, and F. Al-Turjman, —An intrusion detection scheme based on the ensemble of discriminant classifiers,‖ Comput. Electr. Eng., vol. 86, p. 106742, Sep. 2020, doi:10.1016/j.compeleceng.2020.106742.
[11] Divyatmika and M. Sreekesh, —A two-tier network based intrusion detection system architecture using machine learning approach,‖ in 2016 International Conference on Electrical, Electronics, and Optimization Techniques
[12] (ICEEOT), Mar. 2016, pp. 42–47. doi: 10.1109/ICEEOT.2016.7755404.
[13] D. Ashok Kumar and S. R. Venugopalan, —A Novel Algorithm for Network Anomaly Detection Using Adaptive

Machine Learning,‖ in Progress in Advanced Computing and Intelligent Engineering, Singapore, 2018, pp. 59–69. doi: 10.1007/978-981-10-6875-1_7.

[14] Rajasekaran and A. Ayyasamy (2017). 'A Novel Ensemble Approach for Effective Intrusion Detection System ', 2017 Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM),and Date of Conference: 3-4 Feb. 2017,Date Added to IEEE Xplore: 05 October 2017,INSPEC Accession Number: 17240661,DOI: 10.1109/ICRTCCM.2017.27.

[15] D.P. Gaikwad and Ravindra C. Thool(2015). ' Intrusion Detection System Using Bagging Ensemble Method of Machine Learning', 2015 International Conference on Computing Communication Control and Automation , Date of Conference: 26-27 Feb. 2015, Pune, India. Date Added to IEEE Xplore: 16 July 2015,Electronic ISBN: 978-1-4799-6892-3,INSPEC Accession Number: 15305461,DOI: 10.1109/ICCUBEA.2015.61.

[16] M.Govindarajan and RM.Chandrasekaran(2012). 'Intrusion Detection using an Ensemble ofClassification Methods', Proceedings of the World Congress on Engineering and Computer Science 2012 Vol. I,WCECS 2012, October 24-26, 2012, San Francisco, USA.

[17] Chih-FongTsai and Chia-YingLin (2010). 'A triangle area based nearest neighbors approach to intrusion detection ', Pattern Recognition,Volume 43, Issue 1, January 2010, Pages 222-229, https://doi.org/10.1016/j.patcog.2009.05.017.

[18] Sandhya Peddabachigaria, Ajith Abrahamb, Crina Grosanc, and JohnsonThomasa (2007). 'Modeling Intrusion Detection System Using Hybrid Intelligent Systems ', Journal of Network and Computer Applications, Volume 30, Issue 1, January 2007, Pages 114-132, https://doi.org/10.1016/j.jnca.2005.06.003.

[19] Yinhui Lia, JingboXiaa, Silan Zhanga, Jiakai Yana Xiaochuan , and AibKuobinDaic(2011). 'An Efficient Intrusion Detection System Based On Support Vector Machines And Gradually Feature Removal Method ', Expert Systems with Applications,Volume 39, Issue 1, January 2012, Pages 424-430, https://doi.org/10.1016/j.eswa.2011.07.032.

[20] Wenke Lee , S.J. Stolfo , P.K. Chan , E. Eskin ,Wei Fan , M. Miller ,S. Hershkop , and Junxin Zhang(2002). 'Real Time Data Mining-Based Intrusion Detection', Published in: Proceedings DARPA Information Survivability Conference and Exposition II. DISCEX'01,Date of Conference: 12-14 June 2001,Date Added to IEEE Xplore: 07 August 2002,Print ISBN: 0-7695-1212-7,INSPEC Accession Number: 6991861,DOI: 10.1109/DISCEX.2001.932195.

[21] Naoki Abe, Bianca Zadrozny, and John Langford (2006). ' Outlier Detection By Active Learning ', KDD '06 Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining,Pages 504-509 ,Philadelphia, PA, USA — August 20 - 23, 2006 ,ACM New York, NY, USA ©2006 , ISBN:1-59593-339-5 doi>10.1145/1150402.1150459.

[22] Rajesh Wankhede, vikrant Chole, and shruti Kolte(2015). 'A Review On Intrusion Detection System Using Classification Technique', International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Volume-3, Issue-12, Dec.-2015.

[10].Amit Kumar, Harish Chandra Maurya, Rahul Misra(2013).'A Research study on Hybrid Intrusion Detection System',International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-4, April 2013.

[23] Mostaque Md. Morshedur Hassan (2013),'Current Studies on Intrusion Detection System, Genetic Algorithm and Fuzzy Logic', International Journal of Distributed and Parallel Systems (IJDPS) Vol.4, No.2, March 2013.

[24] U. Oktay and O.K. Sahingoz (2013). '.Attack Types and Intrusion Detection Systems in Cloud Computing',International Information Security & Cryptology Conference, Kitabı20-21 September /Eylül 2013 | Ankara / TURKEY.

[25] Dr. S.Vijayarani and Ms. Maria Sylviaa.S(2015). 'Intrusion Detection System – A Study', International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1, February 2015.

[26] Hadi Barani Baravati , and Javad Hosseinkhani(2017), 'A new Data Mining-based Approach to Improving the Quality of Alerts in Intrusion Detection Systems, IJCSNS International Journal of Computer Science and Network Security, VOL.17 No.8, August 2017.

Nilotpal Chakraborty(2013), 'Intrusion Detection System And Intrusion Prevention System: A Comparative Study', International Journal of Computing and Business Research (IJCBR) ISSN (Online) : 2229-6166 Volume 4 Issue 2 May 2013.

[27] Vishal Joshi and Parveen Kakkar(2017). 'Honeypot Based Intrusion Detection System with Snooping agents and Hash Tags', International Journal of Computer Science and Information Technologies, Vol. 8 (2) , 2017, 237-242.

[28] MeeraGandhi and S.K.Srivatsa(2018). 'Detecting and preventing attacks using network intrusion detection systems', International Journal of Computer Science and Security, Volume (2) : Issue (1),2018.

[29] Sonal Paliwal, Rajesh Shyam Singh, and H.L.Mandoria(2015). 'Analytical Study On Intrusion Detection And Prevention System', International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Web Site: www.ijettcs.org Email: editor@ijettcs.org Volume 4, Issue 6, November - December 2015, ISSN 2278-6856.

[30] Mohit Tiwari, Raj Kumar, Akash Bharti, and Jai Kishan(2017). 'Intrusion Detection System', International Journal of Technical Research and Applications e-ISSN: 2320-8163, www.ijtra.com, Volume 5, Issue 2 (March - April 2017), PP. 38-44.

[31] Rajni Tewatia, and Asha Mishra(2015). 'Introduction To Intrusion Detection System: Review', International Journal of Scientific & Technology Research Volume 4, Issue 05, May 2015, ISSN 2277-8616.