ISSN: 2581-3404 (Online) IF: 5.445 (SJIF)

IJIRTM, Volume-7, Issue-4, July-2023.

Performance Analysis of Intrusion Detection System using Supervised Classification Approach

Saleha Khan[1], **Prof. Tanveer Fatima**[2]

[1]M. Tech. Scholar, Department of CSE, ASCT, Bhopal, M.P. (India)

[2]Assistant Professor, Department of CSE, ASCT, Bhopal, M.P. (India)

Abstract: *Electronic information is an asset for any organization, and even in the case of an individual, their data can be quite significant to them, which they cannot afford to lose. Information security has become very important in today's computing world, and it demands potential counters to ever-evolving threats. An IDS is a security mechanism that examines the traffic of all users and applications in the system and detects instant attacks. IDS aim to detect attacks on the system from inside or outside. A typical IDS system examines and analyzes network traffic to detect and analyze attacks, and also to prevent any security violations by generating alarms for network administrator. In this dissertation paper we analyze the different mechanism as used previously by researchers and in currently using for identify the intrusion detection in a network. The proposed mechanism is based on the machine learning based classification model to improve the accuracy rate and performance parameters using the random forest and gradient boost decision trees. The results are compared here in performance parameters based evaluation to identify normal and abnormal attack.*

Keywords: Machine learning, Classification, Intrusion detection system, Malware, Confusion matrix.

Introduction

Advances and widespread use of interconnectivity and interoperability of information and communication technologies (ICT) have become necessary to reshape our relations to daily activities. The vibe of reliance on ICT has enhanced individuals and organizations' posture allowing real-time global business continuity that continuously evolves to offer convenience-related interoperability frontier solutions. The exchange of digital information across networks has opened a path to exploitable vulnerabilities that may have detrimental effects on both individuals and organizations, thus deeming an effective network security solution crucial to maintaining confidentiality, integrity, and availability. Among the layered defensive mechanisms that address different attack vectors, network security controls are recognized as the first defense line [8]. Nowadays we are witnessing rapidly escalating Internet threats, which have become increasingly mature as the Internet and its applications evolve. Today's Internet provides ubiquitous connectivity to a wide range of devices, with different operating systems, which indeed expands the available attack surface including several different attack vectors. An intrusion detection system (IDS) scans network traffic to identify and report a violation based on the preconfigured customized detection levels. Early detection will deter an intrusion and eject it from the system before any damage to the data. IDS assumes that intrusions behavioral features differ from legitimate users' behavior; therefore, IDS quantifies intrusion behavior in terms of its features. However, an exact distinction cannot be deciphered, creating an overlap between normal and abnormal behavior that can be more obvious by deploying an intelligent intrusion detection system [1].

The Intrusion Detection System (IDS) is a critical component of network and data protection. Because of the rapid evolution of network technology, identification of attacks based on contextual knowledge processing can be unique to particular apps and networks. Such a challenge can be solved with the aid of a hybrid intrusion detection system (IDS) [13]. DoS attacks are typically focused on packet flooding with the aim of overburdening the victim's infrastructure. These attacks are now capable of disrupting networks of almost any scale. One of the major testing obstacles for developing high-performance hybrid IDS is dealing with huge volumes of records with a large number of features [5]. A large number of features can make it difficult to identify malicious patterns, resulting in a long training and testing process, increased resource demand, and a low detection rate. Computer security is characterized as the defense of computing systems from threats in order to preserve resource confidentiality, integrity, and availability. An intrusion is described as any series of acts that attempt to compromise network resources and the victim server. The Intrusion Detection System (IDS) is primarily used for tracking incidents that occur in computer systems/networks, analyzing data, identifying, preventing, or reporting to the system administrator so that appropriate action can be taken. The increase in the number of attacks launched by attackers has increased users' skepticism about the Internet. Denial of Service is an effective security assault (DoS). An intrusion detection system (IDS) is a monitoring system that tracks computer networks and network traffic and analyzes it for potential aggressive attacks from outside the organization as well as system abuse or attacks from inside the organization. In layman's words, an intrusion detection device is similar to a burglar detector. A car's lock system, for example, prevents it from burglary. However, if anyone cracks the lock mechanism and attempts to rob the vehicle, the burglar detector senses the broken lock and alarms the owner by raising an alarm sound. Similarly, IDS will function as an alert in a system/network to detect incidents and notify if any malicious behavior occurs. Attackers [15] continue to devise new ways to hack the host/network and conduct illegal operations. The Internet's scale and sophistication, as well as the operating systems on end hosts, make it more vulnerable to vulnerabilities. Because of these problems, existing Internet best practices depend on evidence of detecting attacking trends, monitoring security vulnerabilities, and closing them as soon as possible. Existing intrusion detection systems are seeing an increase in false alarms. Computational Intelligence (CI) components in IDS can be streamlined to minimize these. Many CI strategies were implemented by the researchers, and their accuracy was also measured using benchmark datasets. The Intrusion Detection System (IDS) is a multi colored technique that inspects both inbound and outbound network traffic, detects unusual patterns, and discards them. IDS are made up of three major components: a data base, an analysis engine, and a response manager [16]. The primary component of any IDS, also known as an event driver, is the data base. Host-based monitors, network-based monitors, application-based monitors, and target-based monitors are the four types of data sources.

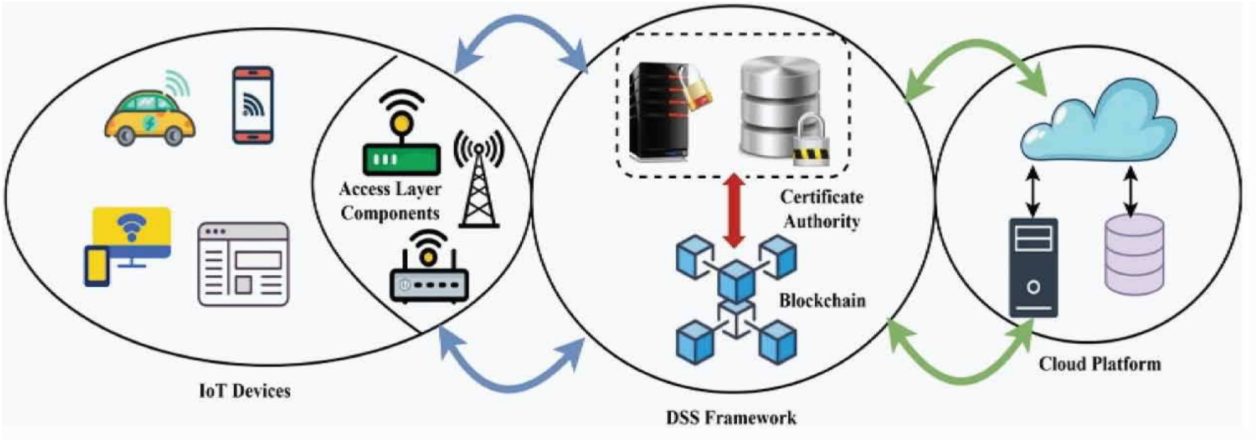


Figure 1: IDS monitoring [12].

II IDS Working

A typical IDS system examines and analyzes network traffic to detect and analyze attacks, and also to prevent any security violations by generating alarms for network administrator. There are two major types of IDS: Host-based IDS and Network-based IDS. IDS can be further classified into Anomaly-based and Signature-based IDS systems. Anomaly-based IDS detects attacks using previously recorded normal real-time traffic image and by comparing it with current traffic. Though, it is widely used in various IDS, it registers a large number of false-positive alarms. The Signature-based IDS uses pattern matching with predefined signatures taken from the already detected malware's stored in a database. Thus, creating a low number of false positive alarms but at the same time, it lets new attacks to pass-through unnoticed. Therefore, a system needs to be developed that can increase detection rate for new attacks and reduce false alarms rate in previously defined signatures.

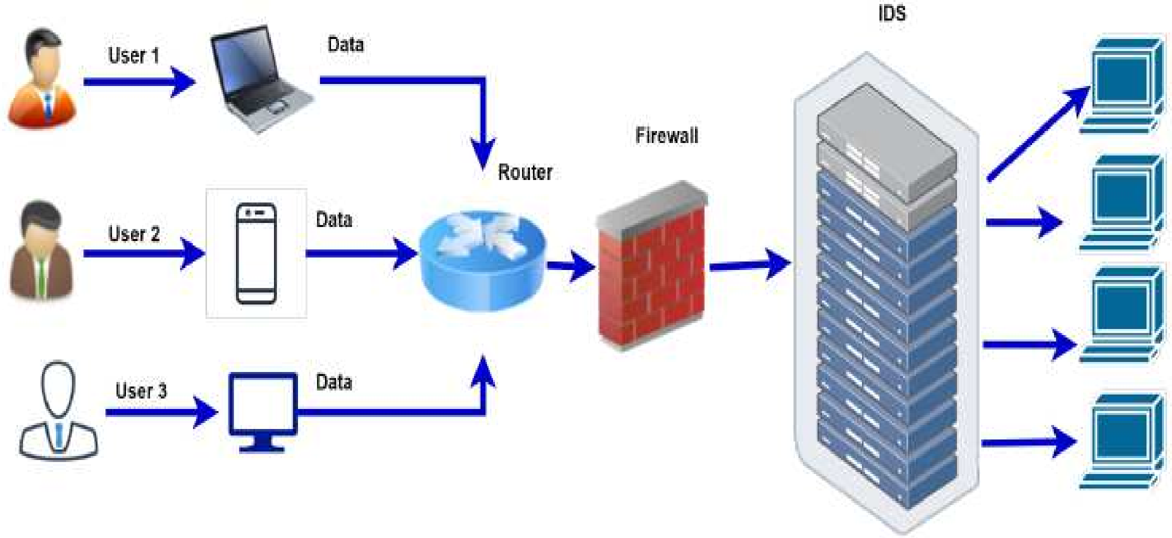


Figure 2: Intrusion detection system working [10].

III Experimental Work

In this chapter presents the proposed model for intrusion detection using some classification techniques such as the random forest, decision tree etc. Intrusion detection systems are used many techniques like machine learning based classification techniques, optimization approach and evolutionary approach for the classification of normal and abnormal data.

The traditional detection methods are not efficient for detecting intrusions on huge data. Machine learning (ML) algorithms can improve intrusion detection efficiency. ML can be classified into supervised, unsupervised, and semi-supervised types [24]. In a supervised method, the labelled input is given to the system for training. With the help of the label, it will separate the different classes available in the dataset. In an unsupervised method, the unlabeled input is given to the system, which will figure out the structure of similarity presented in the input data. A semi-supervised approach uses a few labelled data with many unlabeled data. This method drops between the supervised and unsupervised methods. The accuracy of semi-supervised learning can be improved by using both labelled and unlabeled data [17].

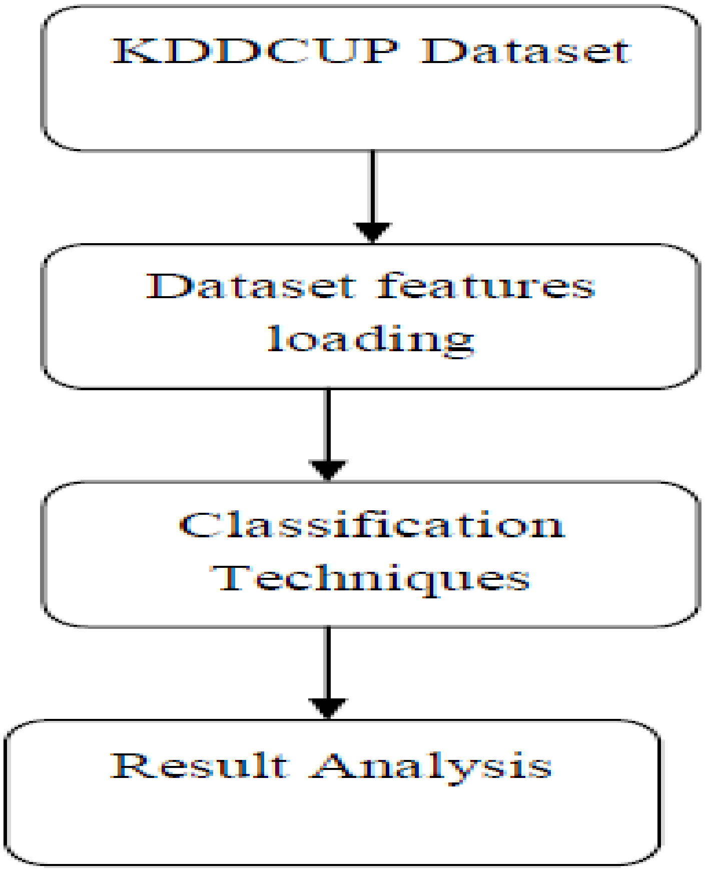
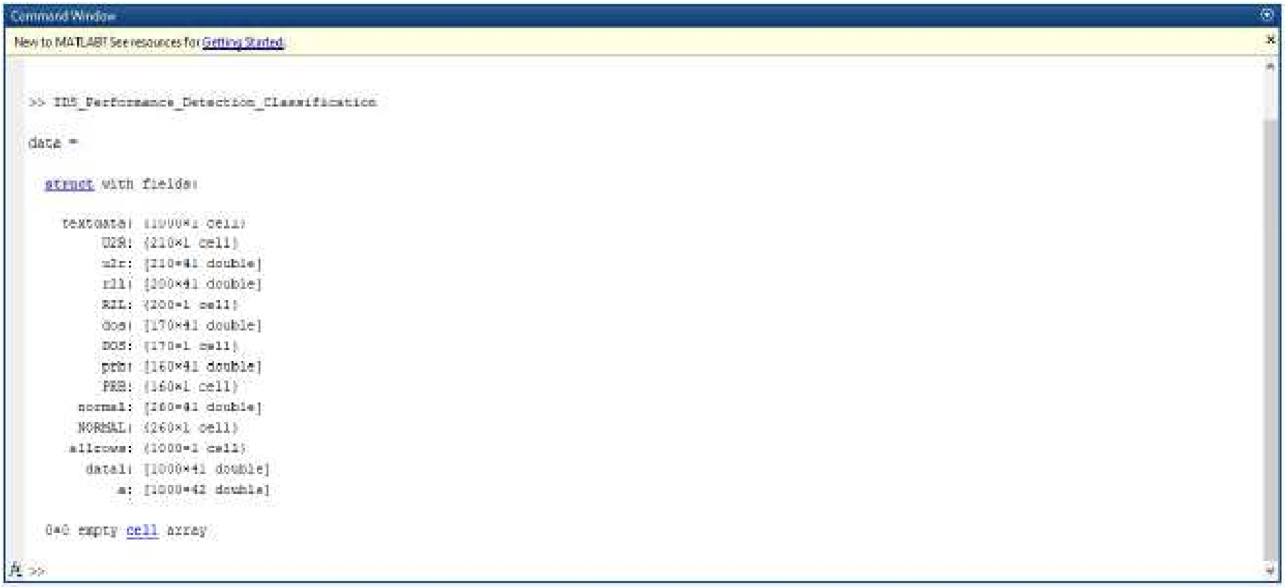


Figure 3: The processing steps for result extraction.



```
>> IDS_Performance_Detection_Classification

data =

  struct with fields:

    textdata: {1000×1 cell}
         U2R: {210×1 cell}
         u2r: [210×41 double]
         r2l: [200×41 double]
         R2L: {200×1 cell}
         dos: [170×41 double]
         DOS: {170×1 cell}
         prb: [160×41 double]
         PRB: {160×1 cell}
      normal: [260×41 double]
      NORMAL: {260×1 cell}
     allrows: {1000×1 cell}
       data1: [1000×41 double]
           a: [1000×42 double]

  0×0 empty cell array

>>
```

Figure 4: This picture uploading the dataset features with normal and abnormal categories for experimental work.

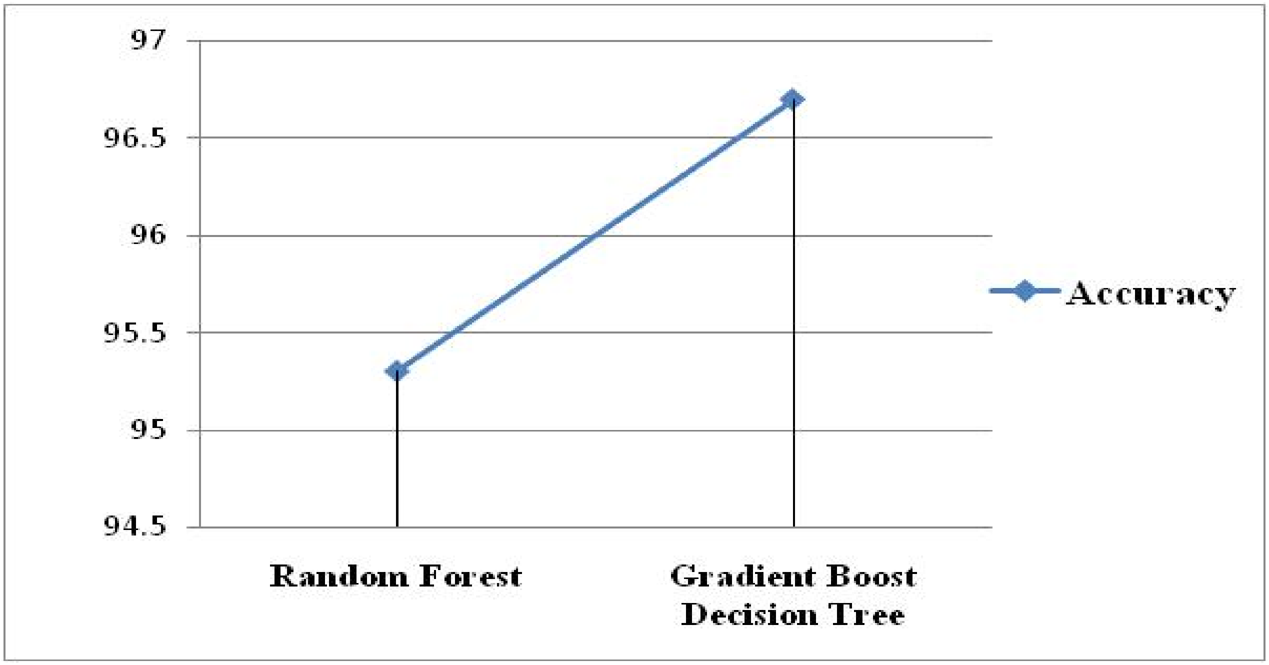


Figure 5: The above figure present the comparative experimental study for classification approach using random forest and gradient boost decision tree with performance parameters i.e. accuracy; here the input value of data range is 0.3.

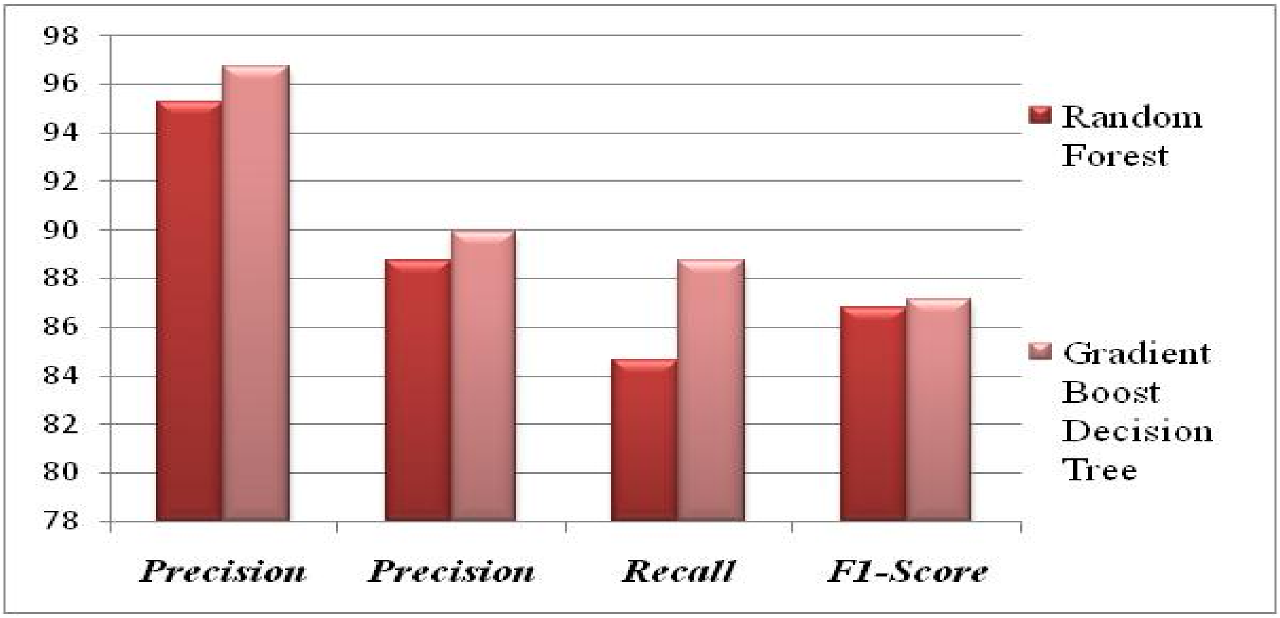


Figure 6: The above figure present the comparative experimental study for classification approach using random forest and gradient boost decision tree with performance parameters i.e. accuracy, precision, recall and F1-score; here the input value of data range is 0.3.

IV Conclusion

The domain of Machine learning (ML) is dedicated to developing systems that can automatically learn from the data and identify hidden patterns without being explicitly programmed to do so. ML algorithms are categorized by the learning style they employ and by the functional similarity of how they work. Machine learning techniques are regarded as efficient methods to improve detection rate, reduce false alarm rate, and in the meantime, decrease computation and communication cost. In this dissertation work we analyze the different mechanism as used previously by researchers and in currently using for identify the intrusion detection in a network. The proposed mechanism is based on the machine learning based classification model to improve the accuracy rate and performance parameters using the random forest and gradient boost decision trees.

References

[1] Abdulhamit Subasi, Khloud Al-Marwani, Reem Alghamdi, Aisha Kwairanga, Saeed M. Qaisar, Malak Al-Nory, Khulood A. Rambo, “Intrusion Detection in Smart Grid Using Data Mining Techniques”, IEEE 2018, pp. 1-6.

[2] Zakaria El Mrabet, Hassan El Ghazi, Naima Kaabouch, “A Performance Comparison of Data Mining Algorithms Based Intrusion Detection System for Smart Grid”, 2018, pp 1-6.

[3] R. Vijayanand, D. Devaraj, B. Kannapiran, “Support Vector Machine Based Intrusion Detection System with Reduced Input Features for Advanced Metering Infrastructure of Smart Grid”, International Conference on Advanced Computing and Communication Systems, 2017, pp. 2-7.

[4] Vimalkumar K, Radhika N, “A Big Data Framework for Intrusion Detection in Smart Grids Using Apache Spark”, IEEE, 2017, pp. 198-205.

[5] P. K. Gupta, N. K. Singh, V. Mahajan, “Intrusion Detection in Cyber-physical Layer of Smart Grid using Intelligent Loop Based Artificial Neural Network Technique”, International Journal of Engineering, 2021, pp. 1250-1256.

[6] Imtiaz Ullah, Qusay H. Mahmoud, “An Intrusion Detection Framework for the Smart Grid”, 30th Canadian Conference on Electrical and Computer, IEEE 2017, pp. 1-6.

[7] Fadi Salo, Mohammadnoor Injadat, Ali Bou Nassif, Abdallah Shami, Aleksander Essex, “Data Mining Techniques in Intrusion Detection Systems: A Systematic Literature Review”, IEEE 2018, pp. 56046-56058.

[8] Anzar Iqbal, Mohammad ummer chopan, Pooja, “Intrusion Detection in Smart Grid”, International Journal of Innovative Science and Research Technology, 2019, pp. 54-57.

[9] Lida Haghnegahdar, Yong Wang, “A whale optimization algorithm-trained artificial neural network for smart grid cyber intrusion detection”, Neural Computing and Applications, Springer 2020, pp. 1-16.

[10] Panagiotis I. Radoglou-Grammatikis, Panagiotis G. Sarigiannidis, “Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems”, IEEE Access, 2019, pp. 46595-46620.

[11] Deepak Kumar Rathore, Dr. Praveen Kumar Mannepalli, “A Review of Machine Learning Techniques and Applications for Health Care “, International Conference on Advances in Technology, Management & Education, 2021, IEEE proceeding, 978-1-7281-8586-6/21.

[12] Muhammad AzmiUmer, KhurumNazirJunejo, “Machine Learning for Intrusion Detection in Industrial Control Systems: Applications, Challenges, and Recommendations”, IEEE, 2022, pp. 1-25.

[13] HananHindy, Ethan Bayne, “Machine Learning Based IoT Intrusion Detection System: An MQTT Case Study”, 2020, pp. 1-14.

[14] Deepak Kumar Rathore, Praveen Kumar Mannepalli, “Diseases Prediction and Classification Using Machine Learning Techniques”, AIP Conference Proceedings 2424, 070001 (2022); https://doi.org/10.1063/5.0076768.

[15] MamataRath, Sushruta Mishra, “Advanced-Level Security in Network and Real-Time Applications Using Machine Learning Approaches”, IGI Global, 2019, pp. 1-22.

[16] Deena BabuMandru, Dr.M.ArunaSafali, “Assessing Deep Neural Network and Shallow for Network Intrusion Detection Systems in Cyber Security”, 2021, pp. 1-13.

[17] Shraddha Mane, DattarajRao, "Explaining Network Intrusion Detection System Using Explainable AI Framework", 2021, pp. 1-10.

[18] R Dubey, D Rathore, D Kushwaha, JP Maurya, "An empirical study of intrusion detection system using feature reduction based on evolutionary algorithms and swarm intelligence methods", International Journal of Applied Engineering Research 12 (19), 2017. pp. 8884-8889.

[19] Md. AlaminTalukder, KhondokarFidaHasan, Manowarul Islam, "A Dependable Hybrid Machine Learning Model for Network Intrusion Detection", IEEE, 2022, pp. 1-44.

[20] GhadaAbdelmoumin, Jessica Whitaker, "A Survey on Data-Driven Learning for Intelligent Network Intrusion Detection Systems", Electronics 2022, pp. 1-22.

[21] GeorgiosKaropoulos, GeorgiosKambourakis, "Demystifying In-Vehicle Intrusion Detection Systems: A Survey of Surveys and a Meta-Taxonomy", Electronics 2022, pp. 1-34.

[22] TourajSattariNaseri, FarhadSoleimanianGharehchopogh, "A Feature Selection Based on the Farmland Fertility Algorithm for Improved Intrusion Detection Systems", Journal of Network and Systems Management, 2022, pp. 1-28.

[23] Deepak Kumar Rathore, Dr. Praveen Kumar Mannepalli, "Recent Trends in Machine Learning for Health Care Sector ", International Journal of Innovative Research in Technology and Management, Vol-5, Issue-2, 2021.

[24] Ahmet Ali Süzen, "Developing a multi-level intrusion detection system using hybrid-DBN", Journal of Ambient Intelligence and Humanized Computing, 2021, pp. 1913-1923.