International Journal of Scientific Research & Engineering Trends
Volume 8, Issue 4, July-Aug-2022, ISSN (Online): 2395-566X

A Review of Intrusion Detection System

M.Tech. Scholar Megha Tomar, Asst. Prof. Avinash Pal , Trapti Ozha(HOD), Director Durgesh Mishra
Department of Computer Science and Engineering
Sri Aurobindo Institute of Technology, Indore,India
meghatomar1008@gmail.com , avinash.pal@sait.ac.in , Trapti.ozha@sait.ac.in , durgesh.mishra@sait.ac.in

Abstract-Computer networks are susceptible to being attacked in ways that are relevant to cyberspace because of the proliferation of internet usage. As a direct result of this, a number of different researchers have created several intrusion detection systems, sometimes known as IDSs. One of the most significant challenges in the field of network security research is the identification of network intrusions. As a preventive measure to ensure the network's safety, it helps in the identification of unauthorised uses of the network as well as attacks on the network. Methods such as machine learning-based (ML) approaches, Bayesian-based algorithms, nature-inspired meta-heuristic techniques, swarm smart algorithms, and Markov neural networks are some of the examples of approaches that have been proposed to determine the most useful features and, as a result, increase the effectiveness of intrusion detection systems. The many ongoing research, which number in the hundreds, were compared to an extensive range of data sets over the period of several years. This paper presents a comprehensive analysis of various research articles that employed single, hybrid, and ensemble classification techniques. The analysis covers a wide range of topics. We compared and contrasted the outcomes measures, limits, and datasets used by the studied articles in the production of IDS. This was done so that we could draw conclusions about the quality of the research. In addition, a potential course of action for further prospective research is presented below.

Keywords-Intrusion Detection Systems, Performance Measure , Machine Learning, Anomaly-Based.

I. INTRODUCTION

Intrusion detection is the process of recognising activities that seek to compromise the overall integrity and confidentiality of a resource. This process is referred to as the identification of potential threats to the resource. As a consequence of this, the objective of intrusion detection is to recognise individuals who make an attempt to break into a computer system's security restrictions and gain unauthorised access.

Even if some of the components may be redundant and contribute less to the detection process [1,] the current intrusion detection systems (IDS) scan all data characteristics in order to find any intrusion and abuse patterns. This is done in order to discover any intrusion and abuse trends. Current anomaly-based intrusion detection systems, in addition to a number of other technical strategies, have been designed and put into use in order to monitor novel assaults on systems. This has been done in order to ensure system security. When using these tactics, it is possible to achieve detection rates of up to 98 percent while operating at a high alarm rate and 1 percent when operating at a low alarm rate [2]. This research analyses and contrasts the various types of intrusion detection systems now on the market, as well as the criteria that measure their respective levels of performance.

II. THE CATEGORICAL DISTRIBUTION OF IDS

According to V. Jyothsna [3,] there are three basic varieties of intrusion detection systems, which are as follows: signature-based (SBS) intrusion detection systems, anomaly-based intrusion detection systems, and hybridintrusion detection systems that are behavior-based (ABS), as well as network intrusion detection systems (NIDS). Systems that use pattern recognition technologies, such as Snort [3, utilise a database of signatures from several sources. Examples of such systems include in order to match them with newly processed data, which is retained by SBS systems, previously known attacks are searched for and used. An alarm will go off if there is a correlation between two different objects. On the other hand, ABS systems like PAYL [4 develop a statistical model to represent usual network traffic. Using this model, any abnormal behaviour that deviates from the model is found and analysed. On the other hand, systems that are based on anomalies have the advantage of being able to discover zero-day attacks [2, which is a considerable advantage]. [Citation needed]

1. Detection based on a signature-The development of online commerce, e-business services on the web, e-banking, and other high-profile applications necessitates

the necessity for businesses that offer these services to equip themselves to provide the greatest possible security against unauthorised access. Detection based on a signature: 2. Detection based on a signature: The technique of searching through the data stored on a network in search of a known sequence of harmful bytes or packets is known as signature detection. If we are aware of the kind of network activity that we are looking to identify in the first place, one of the most significant advantages of using this tactic is the ease with which signatures may be crafted and understood. The events that are generated by signature-based intrusion detection systems have the potential to be used as an indication of the cause for the alert. A modest amount of processing power is all that is necessary to complete the pattern matching necessary for a rule set. This is because pattern matching can be carried out more efficiently on more recent computer systems. This tactic is vulnerable to being tricked since it relies only on regular expressions and string matching, both of which are easy to circumvent. The scope of these approaches' searches is restricted when it comes to searching for strings included inside packets that are being sent over the wire. In addition, signatures are only effective against attacks that display a predetermined pattern of behaviour; they are worthless against attacks that are started by a human or a worm that exhibits self-modifying behavioural characteristics.

This kind of detection, which is particularly effective against known attacks and is also known as a misuse-based detection system, is known as a signature-based detection system. Although this type of detection is quite successful, it is reliant on collecting regular updates of pattern information [6]. Signature-based detection, on the other hand, does not function as well as one would anticipate it would in situations in which the user makes use of more complex technologies, such as NOP generators, payload encoders, and encrypted data channels. Signature-based systems are much less efficient than other approaches, mainly due to the fact that a new signature has to be generated for each change that is made. The performance of the system engine deteriorates as a direct result of the ongoing growth in the total number of signatures. As a consequence of this, several intrusion detection engines are being placed on computer systems that have multiple central processing units (CPUs) as well as multiple gigabit network cards in order to tackle this danger. Engineers working on the intrusion detection system (IDS) generate new signatures before the adversaries do so that they may stop any new attacks from being conducted against the system. The disparity in the rate at which new signatures are created by developers and attackers [2] is one of the primary factors that determines how well the system works.

2.The recognition of abnormalities by observation It is an intrusion detection system that observes the activity of the system and places it into one of two categories: normal or abnormal. By classifying the behaviour of the system as either normal or abnormal, it has the ability to detect and prevent both computer and network misuse and intrusions. This classification, in contrast to pattern-based or signature-based classification, is based on heuristics or rules, and its goal is to detect any kind of abuse that deviates from the typical functioning of the system. On the other hand, signature-based systems have the disadvantage of being restricted in that they are only able to recognise attacks for which a signature has already been developed [7]. A detection method known as anomaly-based detection is carried out once the behaviour of the network has been described. If the activity on the network does not correspond to the standard behaviour, then it will cause an event to be generated by the anomaly detection system. Approval for the activity is contingent upon its conformance to the standard behaviour. The needs of the network administrators are used in order to either prepare for or comprehend the permitted behaviour that is anticipated on the network.

It is important to keep in mind that one of the essential components in determining how a network behaves is the capability of the IDS engine to navigate through the many protocols present at every level. It is necessary for the Engine to have the capability of digesting the protocols and understanding its goal. The benefits that this protocol analysis generates, such as increasing the rule set, result in fewer false positive alarms. Despite the fact that this study of the protocol is computationally expensive, The complexity in developing the rule set for anomaly detection is the most major drawback of using this method. The degree to which the system can be successfully deployed and assessed across all protocols is a significant factor in determining how effective the system is. The diverse protocols that are used by various providers are also a major factor that has an impact on the process of generating regulations. In addition to this, the process of formulating rules is made more difficult by the use of bespoke protocols. In order for detection to even have a chance of succeeding in the first place, administrators need to have a comprehensive knowledge of the appropriate behaviour for the network. Anomaly detection systems, on the other hand, function brilliantly when the rules have been established and the protocol has been defined.

3. Network Intrusion Detection System, often known as NIDS

In the design of the network, NIDS are positioned in a strategic manner at crucial nodes. Data may be gathered and analysed in order to uncover illegal activities by screening traffic for abnormal behaviour, as well as known attacks, which can be done by matching patterns or signatures in the database. Data can also be gathered and analysed in order to detect known assaults. NIDS are sometimes referred to as "packet-sniffers" due to the fact that they are able to intercept data packets as they pass

across a variety of communication channels. The sensor and the management station are the two primary logical components that make up a network intrusion detection system. A network segment will have the sensor put on it, and it will be responsible for keeping an eye out for any suspicious behaviour on that segment. The management station is the one that receives alarms from the sensor (or sensors), and it is this station that displays them to the operator.

A network's sensors are often highly specialised equipment that were designed specifically for the task of network monitoring. This indicates that they have a network interface that is configured in promiscuous mode, which means that they receive all network traffic, not just the traffic that is directed at their IP address, and that they collect passing network data for analysis. Additionally, this indicates that they do not restrict the network traffic they receive to only that which is directed at their IP address. They are instructed to take anything that seems to be out of the norm back to the analysis station as soon as it is discovered. Alerts may be shown at the analysis station, and further analysis can be performed there as well. Network intrusion detection systems (NIDSs) that passively monitor a network connection have a basic challenge when it comes to the lack of ambiguity in the data stream as it is seen by these systems [8]. An experienced attacker may avoid being identified by the network intrusion detection system by taking advantage of ambiguities in the data stream as it is viewed by the system [8].

III. IDS PERFORMANCE EVALUATION

The vast majority of published articles purporting to analyse In reality, IDSs are comparisons of the systems in issue rather than assessments of such systems. When thinking about evaluation, it is fair to conceive of it as an assessment of the degree to which a particular IDS achieves the performance objectives that have been set [9]. The primary objective of an intrusion detection system is to classify the activity on a computer network as either normal or abnormal while minimising the likelihood that a mistake will be made in the categorization [10]. Intrusion detection systems have a number of problems that need to be resolved before they can be used effectively. These problems include a low capacity for detecting unknown network threats, a high rate of false alarms, and insufficient analytical skills. In a broad sense, one might think of intrusion detection as a classification problem, the purpose of which is to differentiate between normal processes and those that are malicious[11] in their very nature.

According to the book "Intrusion Detection Systems Group Test (2001)" published by National Security Systems, the evaluation of each intrusion detection system involves the examination of two distinct components. One of the first steps is doing an in-depth analysis of the many characteristics and capabilities offered by each product. [12] The comments and evaluations of the many qualities have been thoroughly analysed, and a neutral tone has been maintained throughout them. According to the researchers, a quantitative aspect of the study consisted of four tests on the NIDSs that were carried out within the framework of a laboratory networking system that was under controlled conditions. In particular, these tests looked at important performance indicators including the ability to detect attacks, how well the system performed under load, whether or not it could recognise evasion methods, and whether or not it could pass a test simulating a state loaded with operations.

Among the performance measures that were utilised in these evaluations were attack detection to false positive ratio, ability to detect new and stealthy attacks, comparison of host-based systems to network-based systems for various types of attacks, ability of anomaly detection techniques to detect new attacks, improvements between 1998 and 1999, and accuracy in identifying attacks. The inquiry also aimed to establish why each IDS failed to detect an attack or produced a false positive in each of the cases it was looking at. The IDSs in place at the time of the evaluations in 1998 and 1999 were determined to have a number of weaknesses, which were subsequently fixed.

Since then, solutions have been found for some of these problems, but some of these issues have not been addressed to this day.

During the course of the testing process, the testing method took use of a representative sample of the generated network traffic, audit logs, system logs, and file system information. After that, this information was sent to a number of assessors, all of whom were given the responsibility of delivering the necessary data to the Intrusion Detection Systems. This not only ensured that each system got comparable data, but it also made it possible to correctly configure each computer that was connected to the network.

In the excerpt from Ranum (2001), it was established that it was difficult to develop good benchmarks and tests for IDS, and that in order to accurately measure the complexity of IDS, one needed to expend a significant amount of effort in designing tests and ensuring that the tests were not inherently biassed or inaccurate in their results. This posed a challenge for the IDS, which is especially problematic considering how reliant they are on their respective operational environments. After that, he went on to state that in order to eliminate any possibility of bias, any tests that were carried out were to be predicated on qualitative and comparative measures [36]. In his conclusion, he discussed some of the benchmarking experiences he had gained over the course of his career,

with a specific focus on badly written exams and the repercussions of taking them. In addition, as a result of the progression of technology, the IDS management systems will become more ineffective [13] [14].

Alessandri [14] recommended the use of a systematic description framework, which was subsequently improved upon, in order to maintain control over the descriptions that were used while describing IDS functions. It ought to be feasible to assess IDSs without having to conduct experimental investigations on the devices themselves if one employs a descriptive methodology in the evaluation process. In order for this strategy to be effective, it is vital to give accurate descriptions. It is not possible to put such a way into practise at this time since such a method does not yet exist. It is possible to have a certain degree of optimism in this approach for the future.

IV. PERFORMANCE MEASUREMENT CRITERIA

One of the performance criteria for an NIDS system is the capability to recognise assaults, often known as the capacity to detect intrusions. On the other hand, the concept of what exactly constitutes an invasion is not entirely clear. There is a common tendency among many manufacturers and researchers, in particular, to consider any attempt to deliver malicious communication across a network to be an intrusion [15]. Instead, a more helpful system would capture harmful traffic and only warn the operator if the traffic posed a serious threat to the security of the target host. This would make the system more efficient. As shown by the fact that it utilises alert classes ranging from 1 to 10, Snort is headed in this general direction. There are two distinct categories of security risks: those that simply affect a single point of interest, and those that pose a significant risk to the state of security as a whole [25].

2. Well-known vulnerabilities and attacks that target those vulnerabilities All network intrusion detection systems (NIDS) should be able to recognise well-known vulnerabilities. On the other hand, a number of commercial intrusion detection systems (IDS) don't seem to be able to recognise newly disclosed dangers, as shown by research [16]. Alternately, once a vulnerability or attack has been detected, patches should be applied to all systems or workarounds should be created. This eliminates the need for an NIDS to monitor for these kinds of incidents and eliminates the need for an NIDS. The terrible truth is that many computer systems do not get their vulnerabilities fixed or updated when new vulnerabilities are discovered and exploits are employed [26].

Strong indication of this is the large number of system compromises that take place on a daily basis, as well as the fact that the vast majority of the problems on the SANS top twenty list are mostly old, well-known issues for which patches are easily accessible. Both of these facts point to the fact that there is a serious lack of system security [27].

3. The ability to preserve continuity and equilibrium Important factors to take into account are dependability and safety: Any intrusion detection system worth its salt should be able to function reliably regardless of the environmental factors. An application and operating system that has been thoughtfully developed should be able to continue working normally for a significant amount of time without demonstrating any segmentation issues or memory leaks [28]. The capability of an NIDS to report occurrences that are similar in nature in a manner that is consistent and on a regular basis is an important characteristic. One of the drawbacks of a product that is dependent on signature recognition is that several users have the potential to set off their own individual alarms at the same time, therefore simultaneously communicating a variety of information [29]. This implies that the same amount of traffic on various networks might set off a variety of alarms depending on the kind of system they are on, even though the traffic is the same. A myriad of actions are now being conducted all around the world to solve this problem. Both security focus and CVE provide data bases of exploits targeting known vulnerabilities in addition to the data bases of known vulnerabilities and exploits that target them that are provided by both of these resources. In addition to this, the system has to be able to withstand any attempts made to compromise its reliability. If an attacker is successful in locating an NIDS on a network, they will have added what may turn out to be a very useful weapon to their collection. It is also possible that the attacker will attempt to stop the system by using denial of service or distributed denial of service assaults (DoS or DDoS). Every one of these different kinds of assaults need to be able to get past the defences of the system [17].

4. Convenience vs complexity in configuration: It is an unfortunate fact that the utility of a system is often inversely proportional to the system's flexibility and the degree to which it may be customised. The demands of the system's users, as well as the network environment in which it will operate, as well as the level of functionality that the system is anticipated to deliver for those users, will determine the system's degree of flexibility and the configuration choices that are available to users [30]. Because it is unlikely that a network administrator who is also responsible for conventional network administration would have the time required to optimise and set up the system, the usability of the system is going to be the most significant issue that has to be taken into consideration. On the other hand, if an intrusion analyst is specifically recruited to manage intrusion detection [18], it is possible

that a system that is more sophisticated and has a greater capacity would be necessary.

5. Variables that may be configured according to your preferences: The NIDS need to have the capacity to be adapted to suit the particular requirements of any system that is linked to the network. As was said before, doing HTTP analysis on a network that does not have a web server is a waste of time. If the network that is being investigated does not have a web server, then this study will be useless [31]. The level of thoroughness with which the analysis is carried out will also be affected by the volume of traffic that is moving across the network. It is possible for the sensor and analytical capabilities to be merged into a single unit with a simple system, which is suitable for a single network segment that has limited traffic. If a network has a significant amount of light traffic, it is possible that it will be required to distribute the sensor and analytical functions over a number of different hosts in order to guarantee adequate performance [19].

Scalability is a key consideration since the vast majority of organisations mature and grow over time. The infrastructure that supports them, which includes computer networks, also expands in tandem with the company's growth. Any kind of intrusion detection system worth its salt should have the capacity to expand with the network. It is probable that more NIDS may be needed when new network segments are added, so plan accordingly [32]. If the answer is affirmative, would it be possible to aggregate the reports from many NIDS into one interface that is pleasant to users? The manner in which this data will be kept in the years to come is going to be another significant area of worry. Flat files as a method of data storage could be a workable option for a relatively small network that is carefully supervised. As the amount of data that is being acquired continues to increase, however, it is possible that it may become necessary to move this data storage onto a database [20].

Interoperability is the eighth need that must be met: The correlation of information gleaned from a variety of various sources has been shown in a number of studies to be essential for the most effective type of intrusion detection. This includes data obtained from network intrusion detection systems (NIDS), host intrusion detection systems (HIDS), system logs, firewall logs, and any other information sources that are made available to users [33]. At the time this article was written, the Intrusion Detection Working Group (IDWG) had already published a number of articles that specified standards for communication between different types of intrusion detection systems (IDSs). In accordance with the anticipation, the RFCs will most likely be made public in the not too distant future. Once the standard protocols have been completely established, any intrusion detection system (IDS) that is compatible with them will be able to communicate with and interact with other IDS. This will make it possible for an organisation to install a number of different intrusion detection systems from a number of different suppliers while still preserving the system's interoperability [21].

8. Support from Vendors The amount of assistance from vendors that will be required during an implementation will be determined by the skill levels of the employees who will be installing the system. Nevertheless, due to the high rates of employee turnover that are typical in the information technology industry, it is essential to evaluate the level of help that is offered by the vendor [22].

9. Alterations to signatures The ability of any signature-based intrusion detection system to identify intrusions is dependent on the signatures that make up the system. It has been shown that the capability of these systems to recognise newly discovered breaches, or even breaches that have been updated, is limited [23]. In order for these systems to be effective, newly discovered flaws and vulnerabilities must be exploited, and updated signatures must be made available as soon as newly reported flaws and vulnerabilities are publicised [34]. An important development is that the operator of many signature-based systems may now construct their own signatures using the tools provided by the system [35]. Instead of relying on the vendor to provide updates, the system might be designed in this manner to automatically check for any newly discovered warnings as soon as they are discovered. On the other hand, monitoring vulnerabilities and developing signatures as they appear is a time-consuming procedure [24].

V. CONCLUSION

It's possible that locating and installing a network intrusion detection system (NIDS) may be challenging. There are many aspects to take into account, and the aspects that need to be investigated will change depending on the specifics of the event. An organisation should first do an analysis of its requirements before looking for a solution that meets those prerequisites. Doing so will increase the likelihood that the deployment will be successful.

REFERENCES

[1] Srilatha Chebrolua, Ajith Abrahama, Johnson P.Thomasa, (2005). Feature deduction and ensembledesign of intrusion detection systems. ELSEVIER,Pp. 295–307.
[2] V. Jyothsna, V.V. Rama Prasad, K. MunivaraPrasad. (2011). A Review of Anomaly basedIntrusion Detection Systems. International Journal ofComputer Applications, pp. 26-36.
[3] Shirazi, H. M. (2009).” Anomaly Intrusion DetectionSystem using Information Theory, K-NN and KMCAlgorithms. Australian Journal of Basic and AppliedSciences, pp. 2581-2597.

[4] Wang. K and Stolfo.S.J. (2004). Anomalous PayloadbasedNetwork Intrusion Detection. 7th Symposiumon Recent Advances in Intrusion Detection (pp.pp.203–222). USA: LNCS Springer Verlag.

[5] S. Waskle, L. Parashar and U. Singh, "Intrusion Detection System Using PCA with Random Forest Approach," 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), 2020, pp. 803-808, doi: 10.1109/ICESC48915.2020.9155656.

[6] Asmaa Shaker Ashoor, Prof. Sharad Gore. (2005).Importance of Intrusion Detection System (IDS).International Journal of Scientific Engineering Research, pp. 1-7.

[7] Anomaly-based intrusion detection system. (2016, July 16th). Retrieved December 20th, 2016, from Wikipedia Encyclopedia: https://en.wikipedia.org/ wiki/Anomalybased_intrusion_detection_system

[8] Mark Handley, Vern Paxson and Christian Kreibich. (2001). Network Intrusion Detection: Evasion, Traffic Normalization, and End-to-End Protocol Semantics. Berkeley, CA 94704 USA: International Computer Science Institute.

[9] Wilkison, M. (2002, June 10th). IDFAQ: How to Evaluate Network Intrusion Detection Systems? Retrieved from SANS Technology Institute: https:// www.sans.org/security-resources idfaq/howtoevaluate- network-intrusio -detection systems/8/10

[10] Leila Mohammadpour, Mehdi Hussain, Alihossein Aryanfar, Vahid Maleki Raee and Fahad Sattar. (2015). Evaluating Performance of Intrusion Detection System using Support Vector Machines: Review. International Journal of Security and Its Applications, pp.225-234.

[11] Kuang, F., Xu, W., & Zhang, S. (2014). A novel hybrid KPCA and SVM with GA model for intrusion detection. Applied Soft Computing, pp. 178-184.

[12] The NSS Group. (2001, March 23rd). Intrusion Detection Systems Group Test (edition 2). Retrieved from NSS Group: http://www.nss.co.uk

[13] Ranum, M. J. (2001). Experiences Benchmarking Intrusions Detection Systems. New York City, USA: NFR Security Technical Publications

[14] Alessandri, D. (2001). Using Rule-Based Activity Descriptions to Evaluate Intrusion Detection Systems.: RAID 2001

[15] ICSA. (2000). Intrusion Detection Systems. Japan: Information Technology Promotion Agency.

[16] S. Varshney, Shikha, S. Singhi and B. Sharma, "Intelligent Intrusion Detection System Using Deep Learning Models," 2021 5th International Conference on Trends in Electronics and Informatics (ICOEI), 2021, pp. 787-793.

[17] X. Jin, Y. Xie and Y. Yin, "BotCatcher:A Complementary Advantages and Deep Learning Based Scheme for Intrusion Detection," 2021 13th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC), 2021, pp. 95-98.

[18] S. Jiang and X. Xu, "Network Data Classification Mechanism for Intrusion Detection System," 2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD), 2021, pp. 342-347.

[19] U. S. Musa, S. Chakraborty, M. M. Abdullahi and T. Maini, "A Review on Intrusion Detection System using Machine Learning Techniques," 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), 2021, pp. 541-549.

[20] G. Yedukondalu, G. H. Bindu, J. Pavan, G. Venkatesh and A. SaiTeja, "Intrusion Detection System Framework Using Machine Learning," 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA), 2021, pp. 1224-1230.

[21] S. S. Swarna Sugi and S. R. Ratna, "Investigation of Machine Learning Techniques in Intrusion Detection System for IoT Network," 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), 2020, pp. 1164-1167.

[22] A. Srivastava, A. Agarwal and G. Kaur, "Novel Machine Learning Technique for Intrusion Detection in Recent Network-based Attacks," 2019 4th International Conference on Information Systems and Computer Networks (ISCON), 2019, pp. 524-528.

[23] A. Halimaa A. and K. Sundarakantham, "Machine Learning Based Intrusion Detection System," 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2019, pp. 916-920.

[24] P. Illavarason and B. Kamachi Sundaram, "A Study of Intrusion Detection System using Machine Learning Classification Algorithm based on different feature selection approach," 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2019, pp. 295-299.

[25] R. Yadav, A. Choorasiya, U. Singh, P. Khare, and P. Pahade, "A Recommendation System for E-Commerce Base on Client Profile," in Proceedings of the 2nd International Conference on Trends in Electronics and Informatics, ICOEI 2018, 2018, doi: 10.1109/ICOEI.2018.8553930.

[26] V. Prakaulya, R. Sharma, U. Singh, and R. Itare, "Railway passenger forecasting using time series decomposition model," in Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212725.

[27] D. Bhuriya, G. Kaushal, A. Sharma, and U. Singh, "Stock market predication using a linear regression," in Proceedings of the International Conference on

Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212716.

[28] R. Verma, P. Choure, and U. Singh, "Neural networks through stock market data prediction," in Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212717.

[29] P. Kewat, R. Sharma, U. Singh, and R. Itare, "Support vector machines through financial time series forecasting," in Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212859.

[30] A. Sharma, D. Bhuriya, and U. Singh, "Survey of stock market prediction using machine learning approach," in Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212715.

[31] S. Sable, A. Porwal, and U. Singh, "Stock price prediction using genetic algorithms and evolution strategies," in Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212724.

[32] A. Roshan, A. Vyas, and U. Singh, "Credit Card Fraud Detection Using Choice Tree Technology," in Proceedings of the 2nd International Conference on Electronics, Communication and Aerospace Technology, ICECA 2018, 2018, doi: 10.1109/ICECA.2018.8474734.

[33] H. Soni, A. Vyas, and U. Singh, "Identify Rare Disease Patients from Electronic Health Records through Machine Learning Approach," in Proceedings of the International Conference on Inventive Research in Computing Applications, ICIRCA 2018, 2018, doi: 10.1109/ICIRCA.2018.8597203.

[34] A. Saxena, A. Vyas, L. Parashar and U. Singh, "A Glaucoma Detection using Convolutional Neural Network," 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2020, pp. 815-820, doi: 10.1109/ICESC48915.2020.9155930.

[35] B. Bamne, N. Shrivastava, L. Parashar and U. Singh, "Transfer learning-based Object Detection by using Convolutional Neural Networks," 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2020, pp. 328-332, doi: 10.1109/ICESC48915.2020.9156060.

[36] Gupta, P., Shukla, M., Arya, N., Singh, U., Mishra, K. (2022). Let the Blind See: An AIIoT-Based Device for Real-Time Object Recognition with the Voice Conversion. In: Al-Turjman, F., Nayyar, A. (eds) Machine Learning for Critical Internet of Medical Things. Springer, Cham. https://doi.org/10.1007/978-3-030-80928-7_8