Review Of Network Intrusion Detection Systems

Manjeet Kumar Soni, Ashish Kumar Jain, Chandra Prakash Patidar, Mukul Shukla, Upendra Singh

Abstract: Intrusion detection system performs a vital role in the security of the computer systems from cyber attacks. Among the IDS, the network intrusion detection system is another type, which is used to protect computer networks from unauthorised access and data theft from intruders. However, current approaches are not feasible and sustainable when used in modern networks because human interaction is increasing its level and detection accuracy is going down by its level. In this paper we have reviewed some of the existing approaches used in NIDS, machine learning methods, Genetic Programming, Fuzzy Inference System and honeypot technology. These methods have achieved accuracy between 62.89% to 88.35%. Existing systems have few flaws like processing delays in large scale networks, high cost for data collection. In the future we will propose better approach to counter these flaws.

Keyword : Deep learning, IDS, auto-encoders, KDD, network security.

1 INTRODUCTION

New technology brings new challenges with it. With increasing popularity of Social media, Internet of things, cloud based services the data is increasing and we must ensure that data on a network must not be accessed by any unauthorised person and data transfer or communication over network remains safe and un-interrupted. A strong & efficient Network Intrusion Detection System is the essential part of network security. Even after so many improvements in the IDS, the majority of IDS uses less-capable approach such as 'signature-based techniques' and not the anomaly detection techniques. This dependence on such old, less capable and outdated techniques gives inefficient and less accurate detection. Therefore to overcome these we need an anomaly detection method which can be accepted widely to work properly with the ongoing changes occurring in the modern networks [1]. The 3 main noteworthy points which are of concern in modern network for providing security are 1.) Rapid increase in the quantity of network data. 2.) Another thing is to improve effectivity and accuracy, we need the in-depth monitoring and granularity. 3.) Final point is various protocols & variety of the data that is traversing by modern networks. In the past few years, researchers have been working on the application of machine learning methods, which include Naive Bayes, Support Vector Machines and Decision Trees within NIDS [2]. These techniques provided an increase in detection accuracy of NIDS but there are certain boundations also, like expert interaction are highly required as compared to others(Skilled humans) which makes it a process that is intensive and expensive.

- *Manjeet Kumar Soni, Assistant Professor, Department of Information Technology, SGSITS Indore, India. manjeet.mksoni.soni@gmail.com*
- *Ashish Kumar Jain, Associate Professor, Department of Computer Engineering, IET, DAVV Indore, India. ajain@ietdavv.edu.in*
- *Chandra Prakash Patidar, Assistant Professor, Department of Information Technology, IET, DAVV Indore, India. cpatidar@ietdavv.edu.in*
- *Mukul Shukla, Associate Professor, Department of Information Technology, SGSITS Indore, India. mukulrshukla@gmail.com.*
- *Upendra Singh, Assistant Professor, Department of Information Technology, SGSITS Indore, India. upendrssingh49@gmail.com*

Similarly, the quantity of data that is required for operations to perform is very huge which brings challenge of handling it in an environment that is dynamic [3]. To overcome the described limitations, deep learning methods are attracting researchers as deep learning is advanced branch of machine learning. The research done in this area till now has shown that deep learning techniques are capable of doing better revision of network data and can identify any type of anomalies quickly.

1.1 Intrusion Detection System: This system is one that monitors network data for malicious activity or any threats & issue alerts when such activity happens. A software system that scans a device or system for unwanted activities is called as intrusion detection system. Organizations should verify and properly install their IDS products otherwise sometimes intrusion detection systems can give false alarms[1]. It means one needs to set up the IDS system properly to identify the malicious activity otherwise it may happen that it issue alert even if activity is normal. The Intrusion Detection Systems fall in two classes: Network Intrusion Detection System and Host Intrusion Detection System.

A. Network Intrusion Detection System: This is set up within the network to examine data transfer operations from all devices on the network. Its job is to observe traffic on the entire network and match it to the collection of known attacks. If any attack is verified or any abnormal characteristic is observed, the administrator is alerted .

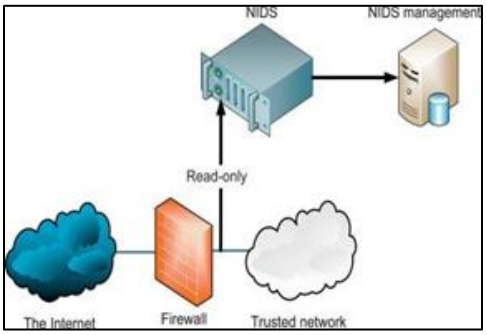

***Figure 1.1**:Network Intrusion Detection System [1]*

B. Host Intrusion Detection System: HIDS are installed for independent machine on the network. It examines the incoming & outgoing data packets from the device only and will warn the administrator if suspicious activity or threat is detected.

1.2 Deep Learning: It is the advanced subset of machine learning methods where many abstract layers communicate with one another. Each layer is strongly connected to one of the previous layer and the decision making is based on the output generated by the previous layer. In Artificial Intelligence, deep learning is termed as subset of machine learning that has networks which supports unsupervised learning of data. This unsupervised learning network can be of following types: Auto encoders, Deep Belief Networks, Generative Adversarial Networks.

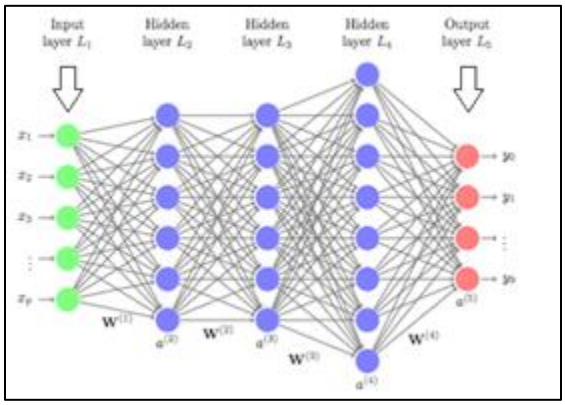

Figure 1.2 *Deep Learning working Model[2]*

1.2.1 Autoencoder Neural Networks: Autoencoder are termed as the neural networks which have 3 layers: first as input layer, second as hidden layer & the last as layer of decoding. Here network are designed to recreate all its inputs, that makes the hidden layer to get to learn effective presentations of the inputs provided. The autoencoders are comes under unsupervised Machine learning algorithms with back propagation, that set the target values must be the same as the inputs. An autoencoder is designed to copy back its input to the self output. Internally, the hidden layer is the one that describes a code that is used to describe the input [2]. A deep auto encoder comprises of two deep-belief networks that are symmetrical that generally have 4-5 layer showing the encoding portion of the network, and the second set of 4-5 layers that explains the decoding half [3].

II. RELATED WORK

In the past many researchers proposed different Network Intrusion Detection approaches for efficient and accurate detection of threats. In this section we have given a short description of existing works carried out by different authors.

Hamidreza Sadreazami et. al [4] This paper presented a very novel anomaly and intrusion detection method for looking at the importance of Security and privacy concerns in Cyber systems. Proposed framework for intrusion detection and sensor measurements are used by this framework as the graph signal that is target & utilizes statistical properties for intrusion detection. The similarity matrix for graph is also created using both types of data measured with the sensors & sensor's proximity which results in a data adaptive & aware structure monitoring system. Finally, Experiments are done to carry out the performance of the method proposed authors concluded found that the observations found provides better result for proposed intrusion detection system superior to the performance compared to the existing ones.

Jaime Zuniga-Mejia et. al [5] discusses the wireless networks that are reconfigurable like wireless sensor and ad hoc networks which doesn't depend on fixed infrastructure. Dynamic & open nature of this network makes them vulnerable to routing attacks. In this paper, a different approach is put forward for intrusion detection in linear based theory that is based on reconfigurable network routing. Using this method, routing attacks can be determined by using the system's 'z-plane' poles. This technique does not depend on the matrix of the number of attack detection & doesn't need extreme dimensionality reduction. Also 2 other host-based intrusion detection techniques are also analyses and presented by providing a case study. For both of the techniques the accuracy was higher.

Panagiotis I et. Al [6] gives a detailed review of smart grid design for electrical systems as it is a big technological advancement in grid systems. The benefits of smart grid like protection of the physical environment, better quality of service, increased reliability, and utilizing efficiently the existing infrastructure and the regenerative energy resources are also discussed in this paper. But it also possess some security & privacy challenges. Therefore a need of an efficient intrusion prevention and detection system to prevent various security threats is must. In this paper, after examining the contribution level of the IDPSs in the Smart Grid systems analysis of different cases is discussed. On the basis of analysis the limitations of smart grid electrical system and an urgent need of IDPS system is found as these systems provide a defence mechanism, which enhances performances by timely detecting or preventing security threats.

Amol Borkar et. al [7] describes in this paper that Intrusion detection is another level of security technique that scans computer networks to avoid suspicious activities. A survey of literature of Intrusion Detection System & Internal Intrusion Detection System is presented here where various forensic and data mining methods are used for actual time operation. Data mining techniques are also presented for cyber analysis to support intrusion detection. System proposed in this paper reduces the rate of false positives. The new system find out the intruders in real time system and presents an intruders list and their actions and it is less time consuming, as compared to the survey, while developing a new IDS, in real time systems these features may be used to detect the attackers and their malicious activities. A valid IDS is the one which will verify intruder accurately in the real time system.

Rui Zhao et. al [8] shows that application of Deep learning is spreading in big range of areas like image segmentation, recognition of object, machine translation and recognition of speech. The motive of authors in this paper is to provide a summary of the growing research work on the deep learning. The introduction to deep learning techniques, along with the applications areas of deep learning in the monitoring systems

of health by machine are also reviewed in this paper from many scenarios. Auto encoder, Restricted Boltzmann Machines, Deep Belief Network, Deep Boltzmann Machine, CNN and Recurrent Neural Networks are also reviewed. Also new trends of deep learning based machine system are also discussed.

Nikolov et. al [9] in their paper shows the impacts of problem of learning project on a student in Technology school Electronic systems. The intrusion detection system is majorly based on the recurrent neural network classifier that is named as the long short term memory units. Along with highly challenging task a project based study was presented. The concept for Apache HTTP Server's network intrusion detection system is based on neural network that is recurrent classifier was put forward by using the advance technologies. The effects of PBL on student from Technology school Electronic system include enhanced skills of project management, better knowledge acquiring , improved critical thinking skills and experience with the new machine learning models

Amureesh Saxsena et. al [10] discussed that the intrusion detection system are utilized for detecting the abnormal activity which extends on the public network. Intrusion detection System are very important tool of security for identifying system from attacks on computer networks and devices. The various types of IDS like host-based, anomaly, hybrid and network-based IDS, specifically IDS using the Agent based technology in network that are real, are discussed in this paper. There have been incredible research in this area of network security to develop an IDS which is agent based for security, that means a mobile agent within the network is present to check or observe packet & detect activities. Another observation is that the IDS that can increase the flexibility of mobile agents is the IDS that uses grid computing is very useful.

Bo Dong et. al [11] throws light on the fact that deep learning has attracted many people due to its strong potential. Deep learning techniques are used in many areas, like recognizing kinds of classification and patterns that are made. Intrusion detection analyzing get data from scanning security actions. This paper explains various techniques that were used for classifying traffic over the network. Authors has decided to make use of other methods on present data set & perform analysis with existing techniques to get excellent way for intrusion detection. Analysis of the large datasets and the deeper systems analysis are done because of the Deep belief and the Deep coding techniques.

Anuja Desai et. al [12] considers that communication based on internet, due to various types of vulnerabilities present, attacks possibility in network is increasing rapidly. It is becoming very difficult for intrusion detection systems to identify the intruders. SQL injection is a type of attack, which may be performed by internal attackers. The objective of external intruder is to cause malicious act in remote system. To prevent system from these 2 categories of attacks, an intrusion detection system which must be robust is required. The authors of the paper, implemented intrusion detection system that is hybrid, in which identification of external & internal threats. Algorithm of signature matching is also implemented in this paper to verify internal attacks. The newly put forward system is hybrid and works in well manner in an online environment

Mohammad et. al [13] describes an approach to detect potential threats by implementing techniques like Random forest, decision free, & KNN. To overcome the limits of the existing system which are not capable to detect basic attacks. The newly put forward system produce the effective result in identifying IP based attacks. The effectiveness of algorithm was evaluated to find Detection accuracy, precision, recall.

Dewan Md. Farid et. al [14] discussed challenges of data mining like missing values, reduction of noise and handling continuous attributes . Due to the huge size of properties which are dynamic in nature, of intrusion behaviours as well as data, some techniques based on data mining for intrusion detection have been used in existing systems. Authors proposed an algorithm which uses naive Bayesian classifier for adaptive network intrusion detection & also to perform detections a decision tree is used & false positives are kept at acceptable mark for various types of attacks in network. The efficiency of the proposed algorithm is tested by using on the KDD99 benchmark intrusion detection dataset. The outcomes of the experiment shows that the new algorithm provides the detection rates at high level & reduces false positives.

***Table 2.1** : Review of based on Objective , Advantage and Limitation*

Reference Paper	*Author*	*Objective*	*Advantage*	*Limitation*
4	*Hamidreza Sadreazami, Amir Asif and Konstantinos N. Plataniotis, Arash Mohammadi*	*The usage of the statistical approach which is graph based for intrusion detection.*	*Graph matrix and sensor signals improves detection accuracy.*	*It is applicable in distributed networks but complexity increases.*
5	*Jaime Zuniga Mejia, Cesar Vargas Rosales and Andreas Spanias, Rafaela Villalpando Hernandez*	*To design an IDS for Reconfigurable Wireless Networks.*	*Helpful in detecting intrusions in wireless networks.*	*Complexity increases with size of network and scalability is needed to be analyzed.*
6	*Panagiotis I. Radoglou Grammatikis,*	*To make smart grids secure and safe by using IDPS.*	*Smart grids system with IDPS are efficient and*	*The advancement brings new challenges which*

	Panagiotis G. Sarigiannidis		*environment friendly.*	*need to be tackled.*
7	*Amol Borkar, Anjali Kumari, Akshay Donode*	*To study the existing IDS and IIDPS.*	*The study suggests that when detection of intruders in real time, It consumes less time.*	*In large scale networks we get processing delays.*
8	*Rui Zhao, Ruqiang Yan, Zhenghua Chen, Kezhi Mao, Peng Wang & Robert X.Gao*	*To give summary of growing research in deep learning.*	*Latest trends based on machine monitoring for deep learning are stated.*	*Simple deep learning methods can't work with large datasets.*
9	*Dimitar Nikolov, Iliyan Kordev and Stela Stefanova*	*To analyze the impact of problem based learning projects on students.*	*Such projects improve critical thinking & enhance project management skills.*	*Cost of such a project is high, Skilled trainers are required for giving training.*
10	*Aumreesh Ku. Saxena, Dr. Sitesh Sinha and Piyush Shukla*	*A review of agent based IDS.*	*Benefits of agents in IDS are, DynamicAdaptation, Platform Autonomy, Accessibility, Independent Execution & Scalability*	*The detection accuracy remains a concern.*
11	*Bo Dong &Xue Wang*	*Comparison of deep learning method with regular methods in NIDS*	*Deep learning methods are promising to be used in IDS.*	*The system is having some limits which is sanctity of data.*
12	*Anuja S. Desai and D. P. Gaikwad*	*Implementation of intrusion detection system in hybrid manner for identification of internal and external attacks.*	*New hybrid system is compatible in offline and online environment both.*	*Some attacks are hard to detect.*
13	*Mohammad et. al*	*To accurately detect potential attacks.*	*Detect interactive and accurate outcomes in IPV4-based attacks.*	*IPV6 attacks cannot be detected yet*
14	*Dewan Md. Farid, Nouria Harbi, and Mohammad Zahidur Rahman,*	*To present a new approach for dealing with challenges of data mining by combining Naive Bayes and Decision tree.*	*The accuracy and implementation of IDS improved.*	*Some challenges still remain while dealing with data mining.*

III. RESEARCH GAPS AND FINDINGS

From our study of many existing systems or research work in this field of NIDS, we have found many drawbacks in traditional systems which need to be improved for reducing false alarms and increasing reliance on IDS for detecting malicious activities done by Intruders. The findings of our literature work are mentioned below in a point wise manner.

- Honey pots have been used in some existing algorithms to trap intruders but they have immature aspects i.e. how to enhance the safety of their own. Therefore we need to use more efficient security honey net to replace the honey pot.

- Existing system used simple machine learning techniques which fell short to fight the new challenges and provide effective security.

IV. CONCLUSION AND FUTURE WORK

4.1 Conclusion : This paper gives a brief introduction of IDS and NIDS. The main goal of this paper is to examine the existing system and provide a detailed literature survey to form the basis on which we can propose a new approach for better and efficient NIDS for securing computer networks from attacks. Deep learning termed, a subset of machine learning has very bright scope in the field of IDS in the near future.

4.2 Future Work: Our paper presented summary of existing approach but still there is a lot of scope for improvement. We can apply new Genetic Fuzzy System hybridized technique by using neural networks to overcome the classification problem seen in intrusion detection systems. New methods will use deep learning with imbalanced class problems which will be developed, using CNN models with integration of bootstrapping methods & cost-sensitive training for implementation on large datasets.

REFERENCES

[1] Sinem Osken; Ecem Nur Yildirim; Gozde Karatas; Levent Cuhaci, “Intrusion Detection Systems with Deep Learning: A Systematic Mapping Study”, Scientific Meeting on Electrical-Electronics & Biomedical Engineering and Computer Science (EBBT), 2019, pp. 1-9

[2] Dong YuanTong, “Research of Intrusion Detection Method Based on IL-FSVM”, IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), 2019, pp. 108-128.

[3] Anish Halimaa A.; K. Sundarakantham, “Machine Learning Based Intrusion Detection System”, 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2019, pp. 1-16.

[4] Hamidreza Sadreazami, Arash Mohammadi, Amir Asif and Konstantinos N. Plataniotis, “Distributed-Graph-Based Statistical Approach for Intrusion Detection in Cyber-Physical Systems”, IEEE Transactions on Signal and Information Processing over Networks, Vol. 4, 2018, pp. 137-147,.

[5] Jaime Zuniga Mejia, Rafaela Villalpando Hernandez, Cesar Vargas Rosales and Andreas Spanias, "A Linear Systems Perspective on Intrusion Detection for Routing in Reconfigurable Wireless Networks”, Vol.7, 2019, pp. 60486-60500.

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

[7] Amol Borkar, Akshay Donode and Anjali Kumari, “A Survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and Protection System”, Proceedings of the International Conference on Inventive Computing and Informatics, 2017, pp. 949-953.

[8] Rui Zhao, Ruqiang Yan, Zhenghua Chen, Kezhi Mao, Peng Wang, and Robert X. Gao, “Deep Learning and Its Applications to Machine Health Monitoring: A Survey”, 2015, pp. 1-14.

[9] Dimitar Nikolov, Iliyan Kordev, Stela Stefanova, “Concept for network intrusion detection system based on recurrent neural network classifier”, Proc. XXVII International Scientific Conference Electronics, 2018, pp.13-16.

[10] Aumreesh Ku. Saxena, Dr. Sitesh Sinha, Dr. Piyush Shukla, “General Study of Intrusion Detection System and Survey of Agent Based Intrusion Detection System”, International Conference on Computing, Communication and Automation, 2017, pp.417-421.

[11] Bo Dong, Xue Wang, “Comparison Deep Learning Method to Traditional Methods Using for Network Intrusion Detection”, International Conference on Communication Software and Networks, 2018,pp. 581- 585.

[12] Anuja S. Desai and D. P. Gaikwad, “Real Time Hybrid Intrusion Detection System usingSignature Matching Algorithm and Fuzzy-GA”, IEEE International Conference on Advances in Electronics, Communication and Computer Technology, 2016,pp. 291-294.

[13] Mohammed Anbar, Rosni Abdulah, Izan H. Hasbullah and Omar E. Elejla, “Comparative Performance Analysis of classification algorithm for Internal Intrusion Detection”, 14th Annual Conference on Privacy Security and Trust, 2016, pp. 109-120.

[14] Dewan Md. Farid, Nouria Harbi, and Mohammad Zahidur Rahman, “Combining Naive Bayes and Decision tree for Adaptive Intrusion Detection”, airccse.org/journal, 2017, pp. 12-25.