A Study on Artificial Intelligence based security for Intrusion Detection Systems

Dr.N MUTHUMANI
M.Sc., M.Phil. NET., Ph.D., PRINCIPAL,
PPG College of Arts & Science, Coimbatore.

Mr. G SURESHKUMAR
PhD, Research Scholar,
Department of Computer Science,
PPG College of Arts & Science, Coimbatore.

Abstract - An Intrusion Detection System (IDS), which is an effective security system that can detect, prevent, and maybe react to computer threats, is one of the standard components of security infrastructures. It monitors target sources of activity in computer or network systems, such as audit and network traffic data, and employs various methodologies to deliver security services. An intrusion detection system (IDS) is the second line of defence against network anomalies and threats. Intrusion Detection Systems (IDS) are critical in network security. A variety of approaches are used to create IDSs for various scenarios and applications. Because both network security personnel and cybercriminals have access to more advanced technology, most IDS systems nowadays are AI-based. Artificial intelligence is widely regarded as the better way to adapt and build IDS and plays a critical role in detecting intrusions. For detecting cyber attacks or malicious activity (IDS), the Intrusion Detection System is the most important component in network security. Artificial intelligence technologies such as neural networks, support vector machines, and fuzzy logic, which can address real-time problems, have gained popularity in recent years. Researchers are using honeypot-style protections to strengthen up machine learning, which is a promising step in the fight against adversarial AI. Various AI-based methodologies have been examined in this study, with a focus on IDS development. This paper also examines various dynamic models of Intelligent Intrusion Detection Systems based on Al intrusion detection techniques. These Artificial Intelligence (AI)-based solutions have a big role to play in the development of IDS, and they have a lot of advantages over the current methods.

Keywords: Network Security, Intrusion Detection System (IDS), Artificial Intelligence (AI), Cyber-attacks.

1. INTRODUCTION

As a result of the present interest and advancement in the development of internet and communication technologies during the preceding decade, network security has emerged as a crucial study topic. Firewalls, antivirus software, and intrusion detection systems (IDS) are used to defend the network's security and all of its linked assets within a cyberspace. Rapid improvements in the internet and communication fields have also resulted in a tremendous increase in network size and data volume. As a result, many of new attacks are emerging, making it difficult for network security to properly detect breaches.. Furthermore, intruders with the intent of launching various assaults within the network cannot be overlooked. An intrusion detection system (IDS) is a tool that inspects network traffic for confidentiality, integrity, and availability, protecting the network from possible intrusions. Despite the best efforts of the academics, IDS continues to struggle with increasing detection accuracy while lowering false alarm rates and detecting new intrusions. IDS systems based on Artificial Intelligence (AI) have lately been adopted as feasible options for promptly identifying network intrusions. This paper reviews various Artificial Intelligence approaches for Intrusion Detection.This article defines IDS and then presents taxonomy based on the most widely used AI approaches in intrusion detection systems (IDS).

II. RELATED WORKS

Many scholars have proposed that AI and IDS be combined. Some dealt with unknown attacks, while others dealt with well-known attacks. Artificial Intelligence based techniques have recently been applied in IDSs and have shown to be effective in detecting intrusive behaviours.

2.1 Machine Learning-based IDS

Any IDS must be able to differentiate between two different sorts of behaviour patterns: normal and malicious[4]. K-nearest neighbour and K-means are two popular machine learning techniques for clustering behaviour patterns

around a centroid[5]. The supervised technique Support Vector Machines (SVM), which divides the data plane into smaller hyper planes and automates feature selection, has also been examined. Many studies have used adaptive machine learning-based techniques for IDS to improve classification accuracy, such as the work published in, which proposed a validation procedure by presenting an automated and adaptive testing prototype[6]. Many studies have used adaptive machine learning-based methodologies for IDS to increase classification accuracy, includes the researchers presenting an automated and adaptive testing prototype as part of a validation approach. Adaptive Model Generation (AMG) [7] as a model generator that would execute IDSs adaptively in real time. AMG automates data collection, detection model construction, and deployment, and allows for real-time data analysis.

2.2 Deep Learning based IDS

Various different researchers have used deep learning algorithms to study IDS and have produced remarkably accurate results. The authors of [8] investigated the capabilities of a Deep Belief Network (DBN) in detecting invasive patterns. In [9], the authors created a hybrid IDS methodology that used DBN as a feature selector and SVM as a classifier by combining DBN and SVMs. The accuracy percentage of the hybrid technique was 92 percent. The authors of [10] proposed a partial supervised learning strategy in which the classifier was primarily trained on regular traffic, allowing any knowledge of harmful behaviour to evolve dynamically. For anomaly identification, the authors used the Discriminative Restricted Boltzmann Machine (DRBM) as an energy-based classifier. The authors in [11] employed an auto encoder in the early stage of an IDS to reduce dimensionality and extract features for a DBN to classify anomalous and normal behaviour patterns in order to reduce dimensionality and extract features for a DBN to identify anomalous and normal behaviour patterns.

2.3 Reinforcement learning based IDS

Reinforcement learning (RL) is a type of machine learning in which agents take activities in order to maximise the concept of rewards. The reinforcement learning method has previously been employed in IDSs in several studies. The researchers created a distributed reinforcement learning system in which each agent (sensor) analyses state observations and communicates them to a central agent in the system [12]. Agents at the top of the hierarchy have the knowledge to analyse the collected data and notify the network operator of a general abnormal state. In [13], the authors used a Monrovian reward process (MRP) to model the behaviour of system call series, where the intrusion detection problem is transformed into MRP value function forecasting. Pursuit Reinforcement Competitive Learning was used in the work reported in [14] to develop an online clustering technique for detecting intrusion utilising Pursuit Reinforcement Competitive Learning (PRCL). The researchers in [15] presented an adaptive neural network solution to intrusion detection that uses reinforcement learning to identify new threats autonomously.

III. INTRUSION DETECTION SYSTEM

Cyber-attacks are growing more complex, causing greater hurdles in detecting intrusions effectively. Intrusion is defined as unauthorised access to information within a computer or network system in order to compromise its integrity, confidentiality, or availability. A detection system, on the other hand, is a security instrument that can be used to detect illegal activity. The practise of intelligently monitoring and analysing events in a computer system or network for evidence of security policy violations is known as intrusion detection. An Intrusion Detection System (IDS) is a security tool that monitors host and network traffic for anomalous activity that violates security policies and jeopardises data confidentiality, integrity, and availability. The goal of IDS is to detect various sorts of malicious network traffic and computer activity that a traditional firewall could miss. This is essential for achieving high levels of protection against actions that jeopardise the availability, integrity, or secrecy of computer systems. If malicious behaviour is detected, the IDS will send an alert to the host or network administrators. If malicious behaviour is detected, the IDS will send an alert to the host or network administrators.

IV. CLASSIFICATION OF IDS

IDS systems are classified into two types based on the methods employed to detect intrusions. Signature-based Intrusion Detection System (SIDS) and Anomaly-based Intrusion Detection System (AIDS) are two of them. Misuse detection is a method for detecting assaults that follow a specific pattern or signature. The major problem of abuse detection is that it will miss any unique network or system attacks because it relies on a recognised pattern to detect attacks. On the other hand, anomaly detection is used to detect unknown assaults.

4.1 Signature-based intrusion detection systems (SIDS)

Signature intrusion detection systems (SIDS) use pattern matching techniques to identify a known attack. They are also known as Misuse Detection or Knowledge-based Detection. SIDS uses matching algorithms to track down a previous breach. In other words, when an intrusion signature matches the signature of a previous intrusion

that already exists in the signature database, an alert signal is triggered. SIDS looks through a host's logs for commands or behaviours that have already been identified as malware.

The SIDS technique is based on creating an intrusion signature database, comparing current activity to previous signatures, and raising an alarm if a match is detected. For commonly identified intrusions, SIDS usually provides good detection accuracy. SIDS, However, identifying zero day attacks is difficult since no matching signature exists in the database until the new attack's signature is collected and recorded. SIDS are used in a number of common tools, including as Snort and Net STAT.

4.2 Anomaly based Intrusion Detection System (AIDS)

AIDS uses machine learning, statistical, and knowledge-based methodologies to create a standard model of a computer system's behaviour. A large divergence between observed behaviour and the model, which can be seen as an incursion, is classified as an anomaly. The two stages in the development of AIDS are the training and testing phases. In the training phase, the usual traffic pattern is utilised to create a model of normal activity, and in the testing phase, a fresh data set is used to determine the system's ability to generalise to previously unexpected incursions. Based on the training method employed, AIDS can be classified into a variety of categories, including statistical, knowledge-based, and machine learning.

Because it does not rely on a signature database to detect aberrant user behaviour, AIDS has the ability to detect zero-day attacks.

On the basis of data sources, IDS is divided into two categories: host-based IDS (HIDS) and network-based IDS (NIDS). Data from the host system and audit sources including the operating system, window server logs, firewall logs, application system audits, and database logs are examined by HIDS. HIDS can detect insider attacks that do not require network traffic.

NIDS is a network traffic monitoring system that uses packet capture, Net Flow, and other network data sources to monitor network traffic collected from a network. IDS that is network-based can monitor a large number of machines connected to a network. External malicious activities that may be started as a result of an external threat can be monitored by NIDS early on, before the risks propagate to other computer systems. NIDSs are limited in their ability to analyse all data in a high bandwidth network due to the volume of data travelling via modern high-speed communication networks.

V. AI TECHNIQUES FOR IDS

This section provides a review of contemporary AIDS approaches for enhancing detection accuracy and lowering false alarms. Anomalies can be discovered in a variety of methods. In order to detect abnormalities, many machine learning approaches are used. Methods for combating AIDS can be divided into three categories: Machine learning is based on statistics, knowledge, and machine learning is based on statistics. Gathering and analysing every data record in a class of items, as well as constructing a statistical model of typical user behaviour, are all part of the statistics-based strategy. Machine-learning approaches, on the other hand, learn to match intricate patterns from training data, whereas knowledge-based methods seek to detect required actions from existing system data such as protocol specifications and network traffic instances.

5.1 Statistics-based Techniques

An ID based on statistics builds a normal behaviour profile distribution model, then detects low probability events and flags them as suspected intrusions. Statistical AIDS takes into account statistical metrics such as the median, mean, mode, and standard deviation of packets. In other words, rather than analysing data traffic, each packet is examined, yielding a fingerprint for the flow. Statistical AIDS are used to find out if there are any differences between current and normal behaviour. Univariate, multivariate, and time series models are some of the most often used models in statistical IDS.

5.2 Knowledge-based techniques

A collection of procedures is referred to as an expert system technique. The construction of a knowledge base that appropriately reflects the legitimate traffic profile is required for this strategy. Intrusions are defined as actions that vary from the regular profile. The standard profile model, unlike the other types of AIDS, is usually based on human expertise and expressed as a set of rules that seek to characterise typical system behaviour.

Because the system is aware of all routine operations, knowledge-based systems have the ability to eliminate false-positive warnings. This type of IDS, however, requires a frequent update on knowledge about projected normal behaviour in a constantly changing computing environment, which is a time-consuming procedure due to the difficulties of gathering information about all usual behaviours. Some of the commonly used models in statistical IDS include Finite State Machines (FSM), Description Languages and Expert Systems.

5.3 Machine Learning Techniques

Machine learning is a technique for extracting knowledge from large volumes of data. Machine learning models are made up of a set of rules, methods, or complex "transfer functions" that may be used to detect and predict behaviour as well as discover significant data patterns. Machine learning techniques have been extensively applied in the field of AIDS research. Clustering, neural networks, association rules, decision trees, genetic algorithms, and nearest neighbour methods are some of the algorithms and techniques that have been used to extract knowledge from intrusion datasets.

VI. ANALYSIS OF AI METHODS IN SECURITY

Chevrolet et al. investigated Bayesian networks (BN) and Classification Regression Trees (CRC) were used to compare the performance of two feature selection procedures, and these methods were combined for increased accuracy.

Bajaj et al. introduced Information Gain (IG) and Correlation Attribute Evaluation were used in a feature selection technique that incorporated feature selection algorithms. They examined the performance of the selected features using a variety of classification approaches, including C4.5, naive Bayes, NB-Tree, and Multi-Layer Perception.

These et al. suggested A Random Tree model was used by NIDS to improve accuracy and lower the false alarm rate.

Subramanian et al. recommended Using decision tree approaches to classify the NSL-KDD dataset and develop a model based on its metric data, as well as analyzing the performance of decision tree techniques.

Xiao et al. observed ML-based protection approaches to preserve data privacy from unauthorised access and malware control, taking into account several attack models such as DoS/DDoS, jamming, spoofing, MITM, and soft-switch.

VII. AI IN THREAT PREDICTION

Artificial intelligence (AI) has several advantages and applications in a variety of disciplines, including cyber security. With today's rapidly evolving cyber attacks and widespread device proliferation, AI and machine learning can help keep up with cyber criminals, automate threat detection, and respond more quickly than traditional software-driven or manual operations.

Artificial intelligence (AI) can be used to detect cyber threats and potential harm. Traditional software solutions are unable to keep up with the massive amount of new malware that is created every week; as a result, artificial intelligence can be extremely effective in this domain. With sophisticated AI based algorithms, Before malware or ransom ware attacks reach the system, systems are being trained to detect malware, perform pattern recognition, and detect even the tiniest characteristics of malware or ransom ware attacks.

VIII. CONCLUSION

A comprehensive overview of several AI-based intrusion detection (ID) algorithms is presented in this paper. In numerous investigations of artificial intelligence (AI) based techniques in ID, many features such as the source of audit data, processing criteria, technique employed, classifier design, dataset, feature reduction technique used, and classification classes are compared. By considering appropriate base classification techniques, training sample size, and combination strategy, the detection accuracy of hybrid and/or ensemble approaches can be increased. AI-based cyber security solutions can provide the most up-to-date knowledge of global and industry-specific dangers, allowing you to priorities threats based on which is most likely to be used to attack your systems rather than what could be used to attack your systems.

REFERENCES

[1] S. Chevrolet, A. Abraham, and J. P. Thomas, "Feature deduction and ensemble design of intrusion detection systems," Computers & Security, vol. 24, no. 4, pp. 295–307, 6// 2005

[2] C.Nagarajan and M.Madheswaran - ‘Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter’ - Journal of ELECTRICAL ENGINEERING, Vol.63 (6), pp.365-372, Dec.2012.

[3] Bajaj K, Aurora A (2013) Dimension reduction in intrusion detection features using discriminative machine learning approach. IJCSI International Journal of Computer Science Issues 10(4):324–328

[4] C.Nagarajan and M.Madheswaran - ‘Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques’- Taylor & Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011.

[5] S. Thaseen and C. A. Kumar, "An analysis of supervised tree based classifiers for intrusion detection system," in 2013 international conference on pattern recognition, informatics and Mobile engineering, 2013, pp. 294–299

[6] L. Dali, A. Bentajer, E. Abdelmajid, K. Abouelmehdi, H. Elsayed, E. Fatiha, and B. Abderahim. A survey of intrusion detection system. In 2nd World Symposium on Web Applications and Networking (WSWAN), pages 1–6, March 2015.
[7] Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012
[8] Stefano Zanero and Sergio M. Savaresi.Unsupervised learning techniques for an intrusion detection system. In ACM Symposium on Applied Computing, SAC '04, pages 412–419, New York, NY, USA, 2004. ACM.
[9] NicoGörnitz, Marius Kloft, KonradRieck, and Ulf Brefeld.Active learning for network intrusion detection. InProceedings of the 2Nd ACM Workshop on Security and Artificial Intelligence, AISec '09, pages 47–54, New York, NY,USA, 2009. ACM.
[10] J. Straub. Testing automation for an intrusion detection system. In IEEE Autotestcon, pages 1–6, Sept 2017.
[11] M. Z. Alom, V. Bontupalli, and T. M. Taha.Intrusion detection using deep belief networks. In National Aerospace andElectronics Conference (NAECON), pages 339–344, June 2015.
[12] M. Z. Alom, V. Bontupalli, and T. M. Taha.Intrusion detection using deep belief networks. In National Aerospace andElectronics Conference (NAECON), pages 339–344, June 2015.
[13] Ugo Fiore, Francesco Palmieri, Aniello Castiglione, and Alfredo De Santis. Network anomaly detection with therestricted boltzmann machine. Neurocomputing, 122:13 – 23, 2013.
[14] Yuancheng Li, Rong Ma, and Runhai Jiao. A hybrid malicious code detection method based on deep learning. 9:205–216,05 2015.
[15] C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011.