Neural Network Assisted IDS/IPS: An Overview of Implementations, Benefits, and Drawbacks

Kyle Rozendaal
Department of Information Assurance
Saint Cloud State University
St. Cloud, MN 56301, USA

Thivanka Dissanayake-Mohottalalage
Department of Information Assurance
Saint Cloud State University
St. Cloud, MN 56301, USA

Akalanka Mailewa
Department of Computer Science and IT
Saint Cloud State University
St. Cloud, MN 56301, USA

ABSTRACT
Modern IDS use inflexible knowledge bases, rule sets and rely on human interaction for successful threat mitigation. While this approach to network and hardware security has been effective in the past, the explosion of large data breaches in the past few years reveals a lack of effective detection for unknown or undocumented threats.We infer that a change in detection and prevention of cybercrime needs to start at the system level and use more intelligent methods of attack detection and prevention: Neural Networks and Artificial Intelligence assisted IDS. This paper gives a broad overview of the modern state of IDS/IPS systems, discusses the benefits and drawbacks of modern implementation, gives a broad overview of current research into the field of neural network-based IDS, and discusses benefits and drawbacks of NNIDS systems. Finally, we conclude with a few examples of modern implementations of NNIDS and areas for future study in the field.

Keywords
IDS/IPS, Neural Network

1. INTRODUCTION
It only takes a few short minutes browsing the news to realize that cybercrime is an increasing threat to business, government, and personal well-being in the modern age. Hackers executed hundreds of successful attacks in the past few years that com- promised millions of individuals personally identifiable information. The trend is so widespread that according to Identity Force there have been well over fifty reported successful data breaches in 2019 alone. [1]. Modern consumers expect a certain level of data security when signing up for services and keeping personally identifiable information confidential is one of the three tenets in the CIA of information security. Companies are repeatedly failing to protect consumer data and while blame falls on the company for not successfully securing customer data, financial records, or other important data, the truth is that attackers are smarter, computers are more widespread, and attack vectors are growing at a rate that is far outpacing the rate of defensive strategy production. With the increasing complexity of attack patterns old security solutions are quickly becoming obsolete; specifically, systems designed to detect network or host intrusions. Aptly named intrusion detection systems are one of the first lines of defense against would-be attackers and provide administrators with an alert about an anomalous bit of network or system traffic.
This papersets forth an argument that the antiquated approach of database-centric intrusion detection systems is quickly becoming outdated, especially with the implementation of neural networks into offensive and defensive security strategies. Furthermore, this paper provides an overview of novel methods for detecting network intrusions using artificial intelligence and neural networks. To understand the benefits and drawbacks of using neural networks in IDS the paper begins with an explanation of key terms relating to intrusion detection and neural networks. This section is followed by a review of different neural-network-based IDS implementation methods that have been discussed in scientific journals and developed at places like the California Institute of Technology, MIT, and the University of California at Santa Barbara. Afterwards there is a brief explanation of the benefits of utilizing neural networks in intrusion detection systems and an explanation of what business can gain by implementing a neural-network-assisted IDS in their security architecture. Prior to the conclusion this paper alsohighlights some of the drawbacks of using a neural network-based architecture Finally the paper concludes witha brief analysis of the future of neural networks in IDS.

2. DEFINITION AND KEY TERMS
In an intrusion detection system, there are choices that a user must make when determining how to build, design, and implement the system to protect their network from potential attack. What sort of attacks does our IDS need to detect? Is it going to be a network-based system or a hardware-based system? Is it going to be signature-based or anomaly-based? Is it going to be a supervised system, an unsupervised system, or something in between? This section aims to define each of these terms and give the reader a broader understanding of the types of systems available and then discuss how neural networks aid with intrusion detection.

2.1 Types of Attacks
Most academic research uses certain datasets to test their IDS against as a benchmark for performance. The popular datasets include KDD99 [2],NSL-KDD [3], ISCX [4], and DARPA [5]. DARPA,KDD99, and NSL-KDD use datasets captured from honeypots, whereas ISCX is a bidirectional data- flow generator that can simulate real-time network traffic for testing IDS. In the comprehensive data- sets there are four categories of attacks that IDS are tested against.

1. ***Probe:*** This type of attack may be as simple as a ping sweep, or complex as an entire network port scan. These attacks are used in an attack strategy to gather data about a network architecture and to search for potential entry points and vulnerabilities.
2. ***Denial-of-Service (DoS):***A DoS attack occurs when

substantial amounts of data are sent to a network from a unique location. These types of attack usually manifest as network requests sent at high frequency to overwhelm a host-system's resources and deny service to others attempting to access the network. ADoS attack differs from a Distributed Denial of Service attack in that a DDoS attack sends data from many attack points. These types of attacks attempt to remove the availability of information for other users or are used as diversions to distract administrators from the real intention of the attack.

3. ***Remote-to-Local (R2L):*** This type of at- tack occurs when a remote user attempts to gain local access to a machine using a remote connection service like secure shell or telnet. To be considered an attack, the remote user must not have access to a local account on the host being attacked. R2L attacks are difficult to identify because typical network traffic can closely mirror this activity.
4. ***User-to-Root (U2R):*** This type of attack occurs when a local user attempts to gain root access to a system when they are not a designated root user. This type of attack is also known as privilege escalation and can also be difficult to identify as it also mirrors normal activity on a system.

2.2 Network-Based IDS

Computer and network information security threats today are often caused by but not limited to system intrusions. Intruders use computer malware, such as viruses, Trojanhorses, and spywares [6] to gain unauthorized access to data on or transmitted by those systems. Thus, intrusion detection and prevention systems are developed and implemented in current systems, to identify and avoid misuse actions or anomalous behaviors from an intrusion [7]. There are two types of systems: Network-based IDS (NIDS) and Host-based IDS(HIDS). As the names suggest, network-based IDS are typically deployed next to the network gateway or "edge router," where it monitors and analyzes network traffic at the packet level and creates logs of all traffic travel- ling into and out of the network. Certain NIDS have the capability to perform Deep Packet Inspection wherein the packets header and content are viewed and recorded, however, since NIDS are intended to run seamlessly, full-packet inspection will significantly slow down the processing speed of the NIDS. Additionally, with the rising-popularity of encrypted packets, a DPI would be useless.

2.3 Hardware-Based IDS

HIDS are typically installed on the host machines, which act as the last defense against attacks. HIDS monitors and analyzes a workstation or computer system. This system monitors traffic into and out of the network-interface-card on a computer and watches application logs and system calls for ab- normal behaviors and work with much higher-level data than a NIDS. HIDS are OS Dependent, are computationally intensive, and are reliant on local code, local configuration, and application logs on the local system. However, HIDS do not slow down network performance and are much more adept at catching U2R attacks and R2L attacks than a NIDS.

2.4 Hybrid IDS

Hybrid intrusion detection systems are a blend of NIDS and HIDS using features from both to detect anomalies more comprehensively within a network of computers. These systems are the most resource intensive since they cover both the entrance to the network as well as activity on specific machines but also do the best job of monitoring for all types of attacks.

2.5 Signature-Based IDS

A signature-based intrusion detection system stores a database of known attack signatures and patterns and compares network traffic to detect attack patterns. A signature-based intrusion detection system is only as good as the supporting knowledgebase since all intrusions are labeled using a predefined dataset [8]. To add new attack types for the IDS to recognize knowledge base must be updated manually by administrators, patch scripts, or updates provided by the IDS manufacturer. While these systems are quite effective, as attacks get more complex the database size and processing time will increase. These IDS systems are time-consuming to keep updated and are vulnerable to altered attacks since they are programmed to interpret an attack as a static set of operations and do not dynamically adapt to slight variation in attack pattern.

2.6 Anomaly-Based IDS

These systems are based on sets of normalized data and identify instances where the data does not conform to the normalized set of data. Typically, there is a calculated normal zone determined by the software developer[8]. If any connection attempt or system call falls outside the normal zone an alert is created and sent to an administrator. An anomaly does not mean there is an intrusion, but it does mean that there is something out of the ordinary that needs to be inspected.

2.7 Supervised IDS

Supervised intrusion detection systems are systems trained by administrators using complex algorithms to group labelled data. Labelled data is data that a trained professional gives to the computer and tells it how to use it. Trained systems tend to miss unknown attacks since all attack detection is provided by a user inputting data into the training modules. Supervised Intrusion Detection Systems need constant training and retraining to be kept up to date.

2.8 Unsupervised IDS

Unsupervised intrusion detection systems use clustering to create groups of data out of unlabeled data to make assumptions about the data and determine normal vs abnormal behavior. As the name implies, unsupervised intrusion detection systems can run without the aid of human-labelled data and remove the labelling of data, making an unsupervised system the ideal candidate for a fully autonomous neural network-based IDS.

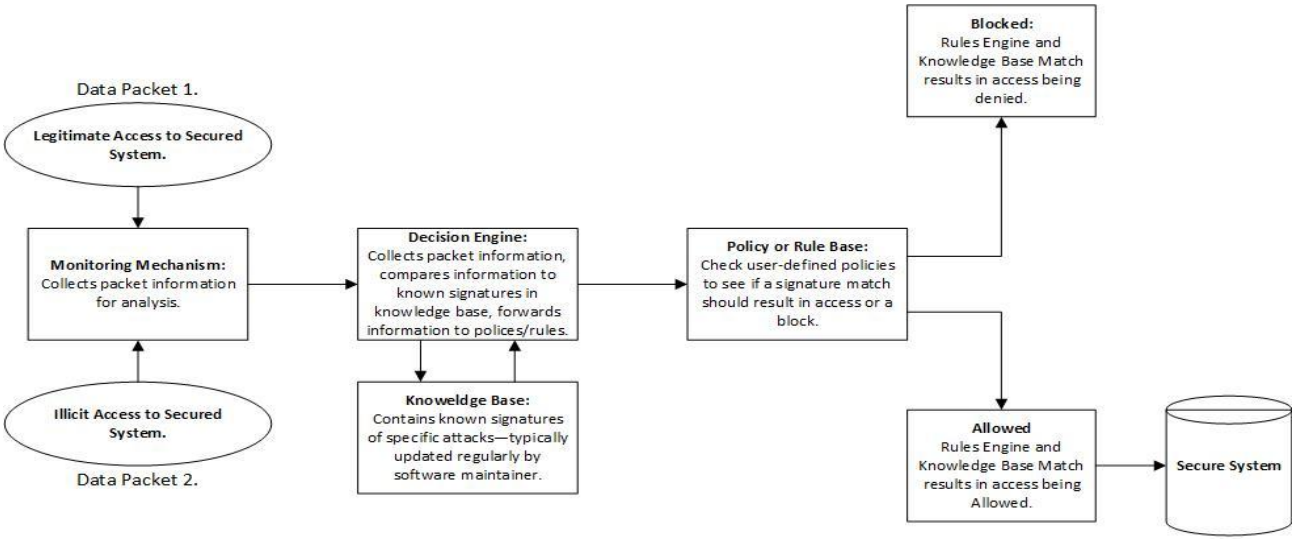

Figure 1: Basic flow within a modern signature-based intrusion detection system

3. MODERN IDS/IPS SOLUTIONS

Many intrusion detection systems in production today have common components, structure, and workflow. A traditional modern IDS usually has these fundamental components:

1. ***Knowledgebase:*** A database where regular and abnormal behaviors and patterns are stored the type of data, structure of data, and normalization patterns depends on the type of IDS.
2. ***Monitoring mechanism:*** Detects the status of the protected system and may also provide logging functionalities.
3. ***Decision engine:*** Analyzes data from monitoring mechanism and identifies if the protected system is running under proper conditions.

Intrusion Protection Systems also have "Rule bases" and "Action mechanisms" in addition to the above components. Rule bases are databases that contain customized rules or conditions that sup- ports action mechanism to take the duty of blocking any unauthorized activity identified by the decision engine [9].Monitoring mechanisms are deployed at the front line of an IDS where its pre-defined sensor units filter through all network traffic (NIDS) or process activities (HIDS). Then, the system passes data to- ward decision engine which compares the data with known behaviors and patterns stored in the knowledgebase. The decision engine identifies all event data and passes the authorized data to destinationor sends the denial signal to rule bases from an IPS. IPS takes the events from the rule base and acts to block unauthorized traffic or process activities to prevent system breach. This basic workflow is outlined nicely in the diagram one [9]:

3.1 Modern Challenges with IDS and IPS

With the rapid growth of digital information usage and technology development, there are far more purposes one can use to initiate a cyber-attack.Concurrently, techniques, tutorials, and self-learning materials are widely available online, hacking, and digital crimes have never been and faster and easier to execute than they are today. Traditional IDS employ statically stored knowledge base to support decision making and identification, and traditional IPS utilizes stored rules base to act on abnormal activities.

These traditional configurations cannot keep up with the modern trend of intrusion evolution. Administrators configure knowledge bases to "memorize" certain attack patterns, which are often defined as signatures by IT security professionals. Therefore, in real world situations, with the ever-evolving change of technology, relying on human collection of data and updating knowledge based and rule sets is an unattainable goal in helping IDS systems close in on catching the most undesirable scenarios.

The other great challenge includes minimizing false alarms and actions from IDS and IPS systems. Returning to the CIA triangle of information security principle,"A" stands for "Availability." E-commerce—being the current trend in the development of businesses—relies heavily on availability of their commercial websites for growth and profit. Within any smart grid system, system availability not only means continuous service,but may also impact physical national security if compromised. While software developers, systems administrators and IT security officers are working day and night, trying to keep these programs and systems products available 24 hours per day there is no room for false actions to stop authorized users with their needs and access.

Occasionally, actions taken to prevent legitimate intrusion, also creates unavailability. Outmoded rule sets designed to perform within an older software architecture could damage systems when incorrectly applied to a new and modified infra-structure. False alarms often stem from outdated knowledge bases, are oftentimes caused by lack of acknowledgement of new trends, and by not updating rulesets in time there is a window for attackers to make a move against the system that could have been preventable.

3.2 Assistance of IDS and IPS with AI

To serve the purpose of replicate human intelligence and neural network with machines, countless scientists have contributed to create and refine artificial intelligence as well as neural networks. Compared to human intelligence, artificial intelligence overcomes humans with calculation speed and accuracy, but is lacking weighted decision making. Artificial neural network mimics the human nervous systems in the human brain with programmed machine learning algorithms. By design, artificial neural network processes a human thinking procedure into numerous of layers, thus machines are nearly "self-adaptive" when human sets the guidelines for

them to start learning with. Therefore, artificial intelligence combined with artificial neural network could outperform human thinking in some ways, in this specific case, intrusion detection learning and decision making [10].

Whether it is HIDS or NIDS, the data that these systems filter through is small in size, high in frequency and, lower at code level, thus, it is extremely difficult for a human to track the data flow. However, machines are particularly good at dealing with digital data and many of the intrusion attack patterns can be determined automatically without human intervention.

The process of traditional IDS and IPS could mostly be automated. Algorithms assigned to clustering data can work with unlabeled data and detect anomalies without administrator assistance, listening ports can be dynamically set as incoming traffic patterns change, user rights and system logs can be observed automatically for changes in patterns. The knowledge base will automatically update with new findings and learnings making the system more secure with every decision.

4. IMPLEMENTATION OF NEURAL NETWORKS IN IDS

Modern implementations of intrusion detection systems rely on databases that require constant updates, attack definitions that are constantly in flux, and constant monitoring with human inputs in a constantly dynamic system. Integrating a neural network or artificial intelligence into intrusion detection systems, in theory, will remove the human element from the machinations and will result in a system that can dynamically react to new attack patterns in real-time based on past experiences. A system, as such described, would be able to detect attack patterns based on relevant data, past attacks, provide its knowledge base with real-time updates, and be more accurate at recognizing potential threats than a human or human-updated knowledge base system. Recent studies into the implementation of Neural Networks provide mixed results as far as detection accuracy, false positives, and implementation speed. [11] Many of the top performing neural network-based intrusion detection systems use a hybrid anomaly detection model and of the top contenders, however, a few similarities emerge among other types of automated systems that are noteworthy.

4.1 Feature Selection

Determining useful variables in the model and removing features that are either redundant or irrelevant can improve both processing performance, detection rate, and minimize the false negative rate. The use of feature selection also minimizes risk for overfitting of datasets and can help in the identification of R2L and U2R attacks by creating specific class architectures for these types of attacks.

4.2 Clustering

When providing a neural network with vast quantities of unlabeled data, the neural network needs some mechanism to sort through the data. Most neural nets need to take four assumptions as truth for the clustering method to work, namely:

1. There is significantly more normal network traffic than abnormal network traffic.
2. Anomalous network traffic is qualitatively different than normal network traffic
3. After clustering is complete, scores are attributed to clusters of data. The largest dataset is assumed to be the normal and is set as the baseline set for normal.
4. Any cluster that receives a score higher than the baseline cluster is assumed to be malicious and triggers a reaction from the IDS.

4.2.1. AI Implementation in Intrusion Detection and Prevention Systems

Artificial intelligence and machine learning plays a crucial role in the detection of intrusions. Typically, artificial intelligence enables data reduction, analysis of data in recognizing elements and recognition of the intruders. Following are a few different techniques used by AI and machine learning to aid in the detection of any intrusive events.

4.2.2. Artificial Neural Network (ANN)

Recent technology development in the field of intrusion detection and prevention systems (IDPS) has approved other approaches to intrusion detection without the need for human interaction. Various artificial intelligence techniques have been employed to help the intrusion detection process [12]. One of the significant implementations is the application of a soft computing technique known as artificial neural networks (ANN) which is a model based on biological neural networks [13]. Necessarily, this technique consists of artificial neurons which are ingroups and processes information through a computation strategy. In some cases, the Artificial Neural Network becomes a flexible system that changes its structure depending on the external or internal information which goes through the network [12]. The essence of artificial neural network implementation in the IDS system is that it ensures the involvement of an intelligent agent which can recognize patterns in both normal and abnormal connections. The intelligent agent then audits and generalizes the designs to new connections in the network. Neural network application does not require signatures or rules; all that is needed is the provision of input data regarding the event to a neural network [14]. The Artificial Neural Network technique is widely used in the detection of cyberattacks, through learning the signature patterns of cyber-attacks and the routine activities from the training data systems.

An example of a neural architecture approach is the feedforward (FFNN). In this approach, a consecutive number of layers are connected to each other by a synapse[15][16]. There are four layers, and each layer has a certain number of neurons. All the neurons have the same characteristics (Learning rate, transfer function, etc.). The four layers are grouped into input layer, hidden layers, and output layer. The input layer has forty-one neurons which are used for intrusion detection. The hidden layer has fourteen neutrons and nine neurons respectively while the output layer has two neurons. These two neurons act as filters. They filter normal packets from abnormal packets. [15].Once implemented, the FFNN uses following model:

- Dataset Training/Testing > Preprocessing Dataset > Determine the NN Architecture > Training the system > Testing the System.

Another approach that has significant research behind it is the Back Propagation Neural Network. The neural network imitates some forms of human behavior. Like every other neural network, the BPNN consists of neurons/nodes and layers. Layers contain nodes and these layers are classified into groups, inner, hidden, and outer layers. The network

starts with a set of fresh patterns as input data and set of pre-defined weights in each connection [17]. In a BPNN the results from the output neurons are returned as inputs to the input layer so that the system learns from its own outcomes and can refine future decisions based on past mistakes and successes. Each set of this movement is called a single "Epoch." A new pattern is formed after every Epoch, and this is how the network is trained.

A third type of NN is the Generalized Regression Neural Network. The GRNN is known for its nonlinear mapping function, strong network adjustability, and is known for high fault tolerance and robustness [18]. These characteristics make it very suitable to handle nonlinear attacks. The GRNN has four layers, input, mode, summation, and output layers. Data is transmitted through the layers to other layers via neurons. The number of neurons is determined by the dimension of training learning samples. All calculations are conducted in the summation layer.

4.2.3. Genetic algorithm (GA)

Genetic algorithms are techniques derived from evolutionary biology. Genetic algorithms use systems like inheritance, mutation, and recombination to evolve and solve complex problems in a dynamic fashion. The procedure of creating a genetic algorithm usually begins by choosing a particular type of chromosome that illustrates the issue to be solved [19]. Depending on the element of the problem, various postures, also known as genes, are encrypted as characters or numbers of every chromosome. An assessment is then done to find the suitability of every chromosome. Therefore, a genetic algorithm is used to find the genetic representation and the suitability function of a solution [19].Genetic algorithms are typically applied to a network connection and used to detect unexpected behaviors. The capturing modules present in the intrusion detection system, gather network traffic information, and pass it to the genetic algorithm.The IDS system then applies the genetic algorithms to the captured data. The genetic algorithm then categorizes the rules gathered from the information received [20]. Next, the IDS applies the ruleset to the captured data, which creates a new population with suitable qualities. The implementation ofgenetic algorithms in the intrusion detection system are of considerable significance because they analyze the vast volume of data that the IDS captures. The genetic algorithms deal with populations of a solution which makes it suitable for detecting behaviors on IDPS where the responses have different values [20].

5. DRAWBACKS OF NEURAL NETWORKS ASSISTED IDS

While neural network assisted intrusion detection systems offer many advantages over traditional modern systems, there are a few drawbacks that need to be considered and studied more thoroughly before widespread implementation of neural networks can become commonplace in the industry.

First, when using a genetic algorithm to map inputs through hidden layers into an output, large numbers of inputs can make it extremely difficult to logically map any single given input to a selected output. Poojithaet. Al proposed a feed forward neural network trained by back propagation [21].In their study, the set of normalized data inputs into their neural network consisted of forty-one individual input neurons. Because of the large input set, it was exceedingly difficult for them to map specific inputs to outputs, and they feared oversaturation of the data led to a lower detection rate especially among R2L and U2R attacks; 36.8% and 67.7% respectively.One solution for remedying this problem is to use the feature selection process as proposed in Section IV. However, when working with a modern enterprise system, the feature set—or number of potential variables that exist in a network packet— will be significantly higher than forty-one. Because of the sheer size of variables that exist in a modern system, a paring down of the system variables is acutely necessary. Future study is warranted into the field of redundancy elimination and feature selection to optimize training of neural networks for use in IDS.Another issue as proposed by Poojithaet. Al is that "if the neurons get saturated, then the changes in the input value will produce a very small change or no change in the output value." [21]. Therefore, normalization of data is required to accurately contrast the normal from the abnormal. However, it is still theoretically possible in a real-world scenario for an attacker to flood the neural network with a specific type of network packet, thereby training the packet to believe transmissions received are benign, and then sending an extremely similar packet with a small amount of change and slipping a piece of malware into the system. This theoretical speculation is simply a note of interest as new attacks are always developed as new technologies are implemented into networks and defense structures.

Second, too many input neurons can cause an oversaturation of data and lead to difficulty mapping and a low detection rate for certain attacks. How- ever, too specific a dataset will also have adverse effects on the output of the neural network assisted IDS. Overfitting is a state that occurs after training a neural network to be too precise in its detection of certain types of attacks. While training the neural network, if the trainer presents it with too specific of data, the neural network will learn to detect the specific type of attack and will become rigid in its assignment of certain threats. In other words, it loses its ability to generalize patterns within the attack vector and instead looks for specific instances of attacks. Overfitting, then, is equivalent to a knowledge base filled with attack patterns. In training, when most attacks follow the same patterns, the neural network will perform well, however, when entering a real defense situation, the performance will drop as the neural network will have lost the ability to recognize patterns along the generalization curve.In conclusion, too many inputs lead to lower ac- curacy when detecting certain types of attacks, and too specific of training will lead to low real-world detection rates as the neural network loses the ability to generalize attack patterns. Therefore, through feature selection and smart training methodologies, neural network assisted IDS can have quite accurate results, but extreme care must be taken to correctly implement and train the system.

Another issue arises with the economics of scale.Deep neural networks are extremely resource intensive and require lots of memory and processing power to run. [22]. Many intrusion detection systems are designed to run in real time and if the alerts fall behind due to a lag in processing time from a neural network, then the traffic will have already entered, done its damage, and exited before the neural network has an opportunity to alert the administrator. A solution to this issue would be a distributed implementation model wherein the resources are spread out across the network, but as the company scales up its network footprint, the neural network must also increase in size to maintain acceptable performance metrics.

Very few neural network assisted IDS have achieved

satisfactory performance at detecting R2L and U2R attacks [11]. While a few neural networks have proven to capture over 99% of malicious R2L and U2R attacks, many subsist around the 60% range or fall into the category of 0% where they are incapable of watching for specific host-based attacks.Those neural networks that can do well at catching the attacks are a hybrid anomaly detection model that contain running code on both the network and distributed host machines. Again, this simply in- creases memory and processing usage and decreases performance as the network protection needs to evolve and grow.

Finally, as stated by Malowidzkiet. Most neural networks are tested on datasets created in 1999 and 2000. While these datasets do an excellent job as a testbed for application processing, they do not truly test the program in a way that it would be tested in a real-world scenario. [23]. The included attacks are outdated and do not mirror reality in 2019. The team instead recommends using the CTU-13 dataset as it was created on a subnet using real malware in 2013, more closely modeling a modern attack scenario.

6. CONSIDERATIONS

While neural network assisted IDS bring many potential benefits to the table, much of the implementation and testing has been in controlled lab settings and extraordinarily little has been done testing them in real-world scenarios. Because of this it is unclear what the accuracy and detection rates would be when running a fully unsupervised NNIDS in a production environment would be. Furthermore, given the large processing and storage requirements for anomaly based NNIDS, as well as extensive training time within a production environment, utilizing a fully autonomous NNIDS in a production environment is not feasible as a replacement to current IDS.

However, the fact that NNIDS are in an infant state does not mean that research, and development are being abandoned. In 2014 DARPA ran a Cyber Grand Challenge in which contestants were tasked with creating systems using automation and neural networks that could hack and defend against attacks from other automated systems. These systems ran on a modified operating system that only contained seven different system calls. These systems also had access to immense computing power: a system with 1,280 physical cores, 16 TB of memory, and 64TB of disk space [24]. Mechanical Phish, the team from UC Santa Barbara created a system that would “analyze the [binary] code, find vulnerabilities, generate exploits to prove the existence of these vulnerabilities, and patch the vulnerable software” [24].Contestants during the Cyber Grand Challenge were allowed to interact with their automated systems to manually patch software when they discovered it but were docked a number of points during the competition for every instance that they interfered with their automated system. DARPA promoted this challenge to build on the foundation of using neural networks to assist in cyber offenses and defenses in the future. The proof-of-concept machines were successful in detecting threats and exploiting weaknesses in the target machines. However, these devices functioned at their best when a minor amount of human interaction was added to the equation to assist machines in detecting logic-paths to exploitation [24].

Shoshitaaishviliet. Al discusses a Rise of the HaCRS based on the findings of mechanical phish in that the future of cyber security is going to lie in a shift from the “tool-assisted human-centered to human assisted too-centered.” [25]. The major problems during the Cyber Grand Challenge arose from the automated systems being unable to generalize data and understand the underlying logic of specific attacks (see “Overfitting " in section V). However, both the Mechanical Phish team and the HaCRS team found that if a human could provide a small “suggestion” of a direction to take, the computer’s automated analysis processes improved dramatically. HaCRS proposes a paradigm shift to this human-assisted tool-centric methodology. Instead of fighting with computers to teach them the logic of decisions, HaCRS proposes leaving human logic, but automating as much as possible using automated neural network assisted tools. With the combination of a computer’s ability to analyze massive quantities of data in a short amount of time and a human’s ability to understand inference logic-paths, the current best model for a NNIDS is one in which the computer analyzes the data, packets, logs, and other artifacts for possible intrusion and provides the data to a human for analysis. A human’s ability to understand the attack-path, infer implications of a breach,and provide input back to the NNIDS for tuning of detections in a specific environment will lead to the future and next generation of finely tuned systems and will definitely lead to further discoveries in the usage of neural networks in IDS.

Finally, Ali et. Al proposes an intrusion detection system based on artificial neural networks, fast learning networks, and particle swarm optimization. In their proposed method, particle swarm optimization and a fast-learning network are combined to create an easier to train, more efficient model that improves training time and improves detection rates [26]. The research being done by Ali et. Al can be used to reduce the implementation time currently inherent in massive NNIDS. By reducing the training time in a production environment, Ali et. Al are working to remove one of the key barriers to successful NNIDS in production environments. Further research must be done to resolve issues related to implementing neural networks in IDS, namely resource utilization, economics of scale, generalization training, smart feature selection, and distribution of detections among hardware and network interfaces to detect all types of attacks. Given that most datasets upon which Neural Networks are trained come from the 1990’s and early 2000’s, new datasets should be developed for training which contain modern infrastructures, cloud-based models and hybrid network models, common attack structures, Ransomware signatures, and other malware and ATP threat data that has been discovered in the time since the last training set was released. Neural network-based IDS and IPS systems will need to run the course against more modern attack vectors, proving their reliability against modern attacks on modern systems before widespread implementation can become a reality. However, as technology improves, research continues, and computing hard- ware gets faster and cheaper it will not be long until neural networks are optimized and ready for use in IDS and someday IPS.

7. CONCLUSION

Given the widespread use of intrusion detection systems in modern security architecture, it is important to understand the frameworks, options, and strengths and weaknesses of current hardware-based models and network-based models. Furthermore, understanding the threat landscape and limitations of the systems at hand allows a security practitioner to better understand the holes in their security framework. With most modern systems being a combination of signature-based systems with small amounts of anomaly-

based systems baked into the detection platforms threats are still slipping through the cracks and causing massive loss of confidentiality, integrity, and availability of protected data. Therefore, it is inevitable that neural networks will be utilized in intrusion detection systems to help with unmonitored intrusion detection or semi-monitored intrusion detection in the near future

8. REFERENCES

[1] Dissanayaka, A.M., Mengel, S., Gittner, L. and Khan, H., 2020. Security assurance of MongoDB in singularity LXCs: an elastic and convenient testbed using Linux containers to explore vulnerabilities. Cluster Computing, 23(3), pp.1955-1971.

[2] Siddique, K., Akhtar, Z., Khan, F.A. and Kim, Y., 2019. KDD Cup 99 data sets: a perspective on the role of data sets in network intrusion detection research. Computer, 52(2), pp.41-51.

[3] Thomas, R. and Pavithran, D., 2018. A survey of intrusion detection models based on NSL-KDD data set. 2018 Fifth HCT Information Technology Trends (ITT), pp.286-291.

[4] Injadat, M., Salo, F., Nassif, A.B., Essex, A. and Shami, A., 2018, December. Bayesian optimization with machine learning algorithms towards anomaly detection. In 2018 IEEE global communications conference (GLOBECOM) (pp. 1-6). IEEE.

[5] Hnamte, V. and Hussain, J., 2021, November. An Extensive Survey on Intrusion Detection Systems: Datasets and Challenges for Modern Scenario. In 2021 3rd International Conference on Electrical, Control and Instrumentation Engineering (ICECIE) (pp. 1-10). IEEE.

[6] S. Abraham and I. Chengalur-Smith, "An over- view of social engineering malware: Trends, tactics, and implications," Technology in Society, vol. 32, no. 3, pp. 183–196, 2010.

[7] D. Pietro and L. V, "Intrusion detection systems," Advances in information security, vol. 38, 2008.

[8] R. Singh, H. Kumar, R. K. Singla, and R. R. Ketti, "Internet attacks and intrusion detection system," Online Information Review, vol. 41, no. 2, pp. 171–184, Oct. 2017.

[9] V. Prasanth, K. Mudireddy, J. Shanchieh, and Y. Shanchieh, "Error Analysis of Sequence Modeling for Projecting Cyber Attacks," 2019.

[10] A. Shenfield, D. Day, and A. Ayesh, "Intelligent intrusion detection systems using artificial neural networks," ICT Express, vol. 4, no. 2, pp. 95–99, 2018.

[11] A. Nisioti, A. Mylonas, P. D. Yoo, and V. Katos, "From Intrusion Detection to Attacker Attribution: A Comprehensive Survey of Unsupervised Methods," IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3369–3388, 2018.

[12] S. Patel and J. Sondhi, "A Review of Intrusion Detection Technique Using Various Technique of Machine Learning and Feature Optimization Technique," International Journal of Computer Applica- tions (0975-8887), vol. 93, no. 14, pp. 43–47, May 2014.

[13] J. Shum and H. A. Malki, "Network Intrusion Detection System Using Neural Networks," Fourth International Conferences on Natural Computation, pp. 242–246, Oct. 2018.

[14] Shun, Jimmy &MalkiHeidar. (2006). Network Intrusion Detection System Using Neural Networks.International Conference on Natural Computation, 242-246.

[15] Ahmad, A. B. Abdullah and A. S Alghamdi, "Application of Artificial Neural Network in detection of Probing Attacks, " 2009 IEEE Symposium on Industrial Electronics & Applications, Kuala Lumpur, 2009, pp. 557-562doi: 10.1109/ISIEA.2009.5356382

[16] F. Haddadi, S. Khanchi, M. Shetabi, and V. Derhami, "Intrusion Detection and Attack Classification Using Feed-Forward Neural Network," 2010 Second International Conference on Computer and Network Technology, pp. 262–266, 2010

[17] N. Sen, R. Sen and M. Chattopadhyay, "An Effective Back Propagation Neural Network Architecture for the Development of an Efficient Anomaly Based Intrusion Detection System," 2014 Inter- national Conference on Computational Intelligence and Communication Networks, Bhopal, 2014, pp. 1052-1056doi: 10.1109/CICN.2014.221

[18] F. Gao, "Application of Generalized Regression Neural Network in Cloud Security Intrusion Detection," 2017 International Conference on Robots & Intelligent System (ICRIS), Huai'an, 2017, pp. 54-57. doi: 10.1109/ICRIS.2017.21

[19] J. Maldonado and M.-C. Riff, "Improving Attack Detection of C4.5 Using an Evolutionary Algorithm," IEEE Congress on Evolutionary Computation (CEC), pp. 2229–2235, Jun. 2019.

[20] P. A. A. Resende and A. C. Drummond, "Adaptive Anomaly-Based Intrusion Detection System using Algorithm and Profiling," Security and Privacy, vol. 1, no. 4, Aug. 2018. https://doi.org/10.1002/ spy2.36

[21] G. Poojitha, K. N. Kumar, and P. J. Reddy, "Intrusion Detection using Artificial Neural Network," 2010 Second International conference on Computing, Communication and Networking Technologies, 2010.

[22] Wang, L., Ye, J., Zhao, Y., Wu, W., Li, A., Song, S.L., Xu, Z. and Kraska, T., 2018, February. Superneurons: Dynamic GPU memory management for training deep neural networks. In Proceedings of the 23rd ACM SIGPLAN symposium on principles and practice of parallel programming (pp. 41-53).

[23] M. Malowidzki, P. Berezinski, and M. Mazur, "Network Intrusion Detection: Half a Kingdom for a Good Dataset," Conference: NATO STO- IST- 139 Visual Analytics for Exploring, Analysing and Understanding Vast, Complex and Dynamic Data, pp. 1–6, Apr. 2015.

[24] Shoshitaishvili, Y., Bianchi, A., Borgolte, K., Cama, A., Corbetta, J., Disperati, F., Dutcher, A., Grosen, J., Grosen, P., Machiry, A. and Salls, C., 2018. Mechanical phish: Resilient autonomous hacking. IEEE Security & Privacy, 16(2), pp.12-22.

[25] C. Salls, R. Wang, C. Kruegel, and G. Vigna, "Rise of the HaCRS," Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security -

CCS 17, pp. 1–13, Aug. 2017.

[26] M. H. Ali, B. A. D. A. Mohammed, A. Ismail, and M. F. Zolkipli, "A New Intrusion Detection System Based on Fast Learning Network and Particle Swarm Optimization," IEEE Access, vol. 6, pp. 20255–20261, Apr. 2018