SMU Data Science Review

Volume 6
Number 2 *Summer 2022*

Article 20

2022

Self-Learning Algorithms for Intrusion Detection and Prevention Systems (IDPS)

Juan E. Nunez
Southern Methodist University, enunezgonzalez@smu.edu

Roger W. Tchegui Donfack
Southern Methodist University, rtcheguidonfack@mail.smu.edu

Rohit Rohit
Southern Methodist University, rchanne@mail.smu.edu

Hayley Horn
Southern Methodist University, hhorn@mail.smu.edu

1 Introduction

In recent years, there has been an increase in cybersecurity incidents due to the frequency, diversity, and elevated sophistication of cyberattacks. The Internet Crime Report 2020 from the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) reported a 265% increase in total complaints from the American public from its inception in 2016 to 2020 and a 69% increase from 2019 to 2020. Between 2016 and 2020, "IC3 received 2,211,396 complaints, reporting a loss of $13.3 billion (about $41 per person in the US)" [14]. In 2021 the IC3 continued receiving an increasing number of complaints. The number of complaints received rose to 847,376, a 7% increase compared to 2020. These complaints affected American consumers and businesses, resulting in more than $6.9 billion (about $21 per person in the US) in potential losses. The top 3 incidents reported in 2021 are ransomware, business e-mail compromise (BEC), schemes (phishing), and the criminal use of cryptocurrency [26].

Current security measures are often insufficient to protect networks from increased cyberattacks. Cyber threats are evolving as malicious activity grows increasingly intertwined with traditional foreign intelligence threats and emerging technologies [26]. Additionally, the ever-evolving threats and trends we face from malign cyber actors combined with the size and complexity of modern enterprise networks generate an enormous amount of data in the form of log files.

Traditionally, organizations collect log files to monitor the health of networked devices and user activities to help forensic analysis of cyber incidents. This information is often displayed on dashboards to help administrators detect cyberattacks as they happen.

Network administrators often rely on Security Information and Event Management (SIEM) software products and services to help them analyze and extract value from these large volumes of data. This is a time-consuming activity that requires the expertise of one or more network engineers to configure the SIEM. Network engineers create custom scripts that fit the network architecture of an organization to monitor the logs and send notifications when network events happen. These events are then analyzed and prioritized. If a networking event is severe enough to cause disruptions to a critical system, an immediate response may be required—and this can happen at any time, day, or night.

Furthermore, many of the cybersecurity controls organizations implement like firewalls, SIEMs, and traditional Intrusion Detection and Prevention Systems (IDPS) rely on a database of previously identified threat patterns to detect and prevent cyberattacks. Unfortunately, these approaches are reactive because they aim to implement remedies after cyberattacks occur.

The sophistication of cyberattacks and the volume of data involved in preventing cybersecurity incidents require that any enterprise-level cybersecurity program

implement equally sophisticated solutions and response times. Artificial Intelligence (AI) techniques, which can mine data to find malicious patterns, and Machine Learning (ML) methods, which can enable IDPS to detect threats at near-real-time speeds, are needed to address these cybersecurity challenges.

This research aims to explore Artificial Intelligence algorithms that can improve the efficiency of training models that can increase the detection rate and accuracy of Intrusion Detection and Prevention Systems. By using supervised and unsupervised machine learning models, this study demonstrates how to implement self-learning machine learning models that can eliminate the need to rely on databases of previously identified threat patterns (pre-labeled data) to identify malicious activity. These algorithms must be trained in the network they intend to defend to achieve this goal. This training implies that the algorithm learns the patterns of life of the network traffic in that network, thus facilitating anomaly detections as they occur. This research aims to improve cyberthreat detection rates by implementing Bayesian Neural Networks to improve the accuracy of network traffic classification based on header-derived statistics instead of the host's IP address or port.

The expected result is a model that can be deployed to alleviate the workload on network administrators because an IDPS enabled with these models can automatically classify a threat and isolate it in near real-time. This allows cybersecurity resources to respond to a threat as it is happening, even when it is a zero-day exploit. On the other hand, anomalies can be originated from new devices or applications added to the network, unusual user activity, and other events which may not be malicious. Isolating traffic or the source of the event that resulted in an anomaly gives the staff responsible for the health of a network the opportunity to analyze a threat report and train the model to recognize the new pattern as benign. This gives the network staff more flexibility and reduces the risk of disrupting the operation of critical systems.

There are some commercial implementations of self-learning AI for anomaly detection in networks. However, they are cost-prohibitive for smaller businesses. One additional benefit of this research is to demonstrate that self-learning AI can be implemented to alleviate the cost of intrusion detection and prevention systems that can evolve to meet the challenge posed by emerging threats. Applications of this sort can contribute to lowering adoption barriers to this technology.

2 Literature Review

2.1 Self-learning AI for intrusion detection and prevention

According to a study by Shril, A. V. (2022), modern organizations' higher dependence on digital infrastructure makes them more vulnerable to cyber-crimes. As Shril notes, "The existing literature suggests that the most frequently chosen weapons of hackers

are Internet of things (IoT) attacks, phishing attacks, malware attacks, distributed denial of service (DDoS) attacks, and structured query language (SQL) injection attacks" [19 p. 2].

Machine learning and deep learning can aid IDPS improvements to counteract cybersecurity threats. However, incorporating AI-based technology into business operations may have undesirable ethical consequences that cybersecurity specialists must address to ensure that legal liability risks are managed without compromising cybersecurity, as noted in a research paper by Yang & Fang (2018). For instance, some users of assistive technology may be affected by the implementation of AI-based systems due to their access patterns and interactions being different from users who do not use assistive technology. Fortunately, in a system enabled by the algorithms explored in this research, such patterns can be included in the baseline by labeling them as benign traffic—once the system detects them—thus preventing disruptions to assistive technology users.

On the other hand, due to its potential to automate tasks, AI is an enabler that can enhance accessibility for people with disabilities. AI can automate tasks requiring human intelligence to aid visual perception, predictive text auto-completion, and decision-making. AI-powered solutions can significantly enhance the lives of people with disabilities by enabling them to live independently and acquire new skills to perform jobs, including cybersecurity jobs [20].

2.2 Mechanisms for IDPS

Cybersecurity refers to technologies that protect computers, networks, programs, and data from unauthorized access, modification, and destruction [5]. Network security systems include both network and computer security systems. Firewalls, antivirus software, and IDPS are all sub-parts forming a multilayer security system. For example, the overall mechanism of detecting, determining, and recognizing unauthorized access and user behavior, such as the usage, copying, modification, and destruction of data, is aided by IDPS.

Unauthorized access from outside threat actors and unauthorized access from within a company are security risks. The three primary types of network traffic analysis that IDPS makes are (1) signature-based, (2) misuse-based, and (3) anomaly-based. The fourth kind of network analysis is called (4) hybrid network analysis. This analysis integrates signature-based and anomaly-based analysis to detect and prevent malicious attacks. This is achieved by identifying what is classified as anomalous in the baseline used by signature-based analysis [7]. The previously listed network traffic analysis is utilized to recognize common types of attacks while reducing the number of false alarms the network sets off. In legacy systems, network administrators are responsible for manually updating the rules and signatures of the SIEM database. As a result, it is challenging to analyze new assaults and tailor rules that combine a thorough understanding of the organization and anticipate an adequate response to every attack

vector the administrators can imagine. Consequently, this can leave organizations vulnerable to missed attack vectors known as zero-day exploits [13]. Zero-day exploits are vulnerabilities that have not been previously identified or shared with a broad audience and for which no known mitigations are implemented.

Analyzing a network's typical behavior to identify deviations from the norm is the basis of using an anomaly-based strategy. One of the strengths of this analysis is that the IDPS can recognize assaults that use zero-day exploits. Typical activity profiles can be adapted to the requirements of each system, application, and network. The profiles are specific to each entity, which makes it difficult for attackers to decide which activities they can conduct covertly because the profiles are unique. In addition, the data detected by anomaly-based algorithms can be utilized to define misuse-detecting signatures. The possibility of high false-positive rates is one of the most significant drawbacks of using anomaly-based approaches. This can be mitigated by stacking supervised and unsupervised machine learning algorithms to alleviate the initial learning curve of unsupervised machine learning and help create the initial baseline [13]. The hybrid detection approach incorporates both the identification of misuse and the detection of anomalies into its workflow. The result simultaneously reduces the incidence of false positives for previously unknown cyberattack vectors and increases the detection rate of previously recognized cyber intrusions. For this reason, a hybrid approach has become prevalent in cybersecurity programs incorporating machine learning and deep learning [8].

2.3 IDPS that utilize artificial intelligence models

IDPS aid in continuous monitoring of network traffic, Information technology systems-based operations, and user actions that breach the organization's policies, generating records or logs that are passed on to network administrators and management. This monitoring can be done remotely or locally, where an AI-based IDPS is an essential component of a multilayered security architecture [2]. IDPS intercepts network traffic between all devices to analyze traffic and log malicious behavior [3]. The utilization of IA-based IDPS becomes significant due to the near impossibility of developing a completely secure network impervious outside and inside threat actors.

2.4 Wireless Intrusion Detection and Prevention System (WIDPS)

A study by Mitchell & Chen (2014) describes an anomaly-based solution that analyses protocol-based attacks and multi-dimensional data that can defend real-time systems from being compromised by infiltrators. Implementing a hybrid detection methodology, which combines the two intelligent approaches of abuse and abnormality, is a way to increase the detection capabilities of a pre-existing Wireless Intrusion Detection and Prevention System [4]. These two intelligent approaches are known as abuse and abnormality WIDPS. Researchers have developed a hybrid IDPS by integrating the misuse-based intrusion detection and prevention system with an

anomaly-based packet header for network traffic anomalies. This has resulted in the creation of a hybrid IDPS. The key idea that supports hybrid detection is that abuse identifies known assaults while anomaly identifies unknown ones. This allows hybrid detection to discover previously unknown assaults. In addition, the methodologies of multi-agent-based computational intelligence and intelligence based on multiple agents have been combined to provide a new architecture known as collaborative-WIDPS. At the wireless local area network (WLAN) protocol level, WIDPS may detect issues such as policy violations and misconfigurations [1].

2.5 Bayesian Algorithms

Models based on Bayesian algorithms are well suited for anomaly detection in network traffic because Bayesian models become more accurate with increased complexity. Modern networks are a complex mixture of traditional network appliances, servers, endpoints, hybrid clouds, and the Internet of Things (IoT). All these devices generate large and complex network traffic patterns with numerous features and often incomplete data. These datasets are a challenge for Markov chain Monte Carlo (MCMC) theory-based models like hierarchical, graphical, AI, diffusion, and hidden trees models, because they require increasing computational power with increases in complexity, despite the evolution of the research in these types of models that continually takes advantage of the advances in parallel computing and GPU.

By contrast, imprecise models, incomplete information, and summarized data are ideal conditions for approximate inference models because approximate computational inference dramatically reduces the dimension and size of the raw data while capturing its essential aspects. Approximate models and algorithms may thus be at the core of the next computational revolution [Page 85, 17].

Bayesian algorithms are an answer to the need for approximate models. Using a Neural Network trained on Bayesian Classifier will help drastically scale down the network traffic (flow) workloads of mid to large-sized applications. Tom Auld, A. W. demonstrated that a sophisticated Bayesian trained neural network can classify flows, based on header-derived statistics and no port or host (IP address) information, with up to 99% accuracy [Page 15, 21].

2.6 Recurrent Neural Networks Algorithms

This research project explores using Recurrent Neural Networks (RNN) as a potential classification algorithm in combination with Convolutional Neural Networks (CNN) to improve the detection results of a new model, as presented by Manuel Lopez-Martin et al. A model based on layering a combination of Convolution Neural Network (CNN) plus (Recurrent Neural Networks) RNN gives the best detection results, being these results better than other published works with alternative techniques. A simple RNN model already provides particularly satisfactory results. Still, it is interesting to

appreciate that these results improve when the input to the RNN model is provided by a CNN model in a previous layer [Page 8, 25].

3 Methods

3.1 Data

The network traffic dataset used in this research includes information about network traffic, attack types, and internal network logs. The CSE-CIC-IDS2018 on AWS project, a collaborative effort between the Communications Security Establishment (CSE) & the Canadian Institute for Cybersecurity (CIC), enables the creation of network traffic datasets for training and testing anomaly detection models. This research project utilizes machine learning algorithms to automate the generation of profile-based datasets representing real-life infrastructure traffic, anonymous users' behavior, and several known and novel attack patterns. The AWS project also provides a feature extraction module that allows users to add more data points and features for comprehensive model building. The project website offers an experimental dataset that is used in this research. The dataset has been organized by day. The raw data was recorded daily, including the machine's network traffic and event logs (windows and Ubuntu event Logs). The feature extraction process from the data used the CICFlowMeter-V3 to extract more than 80 traffic features that were saved as a CSV file per machine [12]. The dataset includes ten days of data with multiple examples of attack patterns and intrusion types (Ref. Table.1). The data features do not include IP addresses or ports.

Table.1 Different Intrusion Types available in the dataset.

Intrusion Type	Total Network Traffic Events	Percentage Traffic
Benign	13484708	83.08%
DDOS attack-HOIC	686012	4.23%
DDoS attacks-LOIC-HTTP	576191	3.55%
DoS attacks-Hulk	461912	2.85%
Bot	286191	1.76%
FTP-BruteForce	193360	1.19%
SSH-Bruteforce	187589	1.16%
Infiltration	161934	1.00%
DoS attacks-SlowHTTPTest	139890	0.86%
DoS attacks-GoldenEye	41508	0.26%
DoS attacks-Slowloris	10990	0.07%

The data contains timestamps for each network flow event with statistics for forward or incoming packages (Ref. Fig.1), backward or outgoing network packets (Ref Fig. 2), and flow duration if network packet transfers (Ref Fig. 3). This is useful for algorithms like RNNs, which can leverage the time slices as features within its hidden layers.

Fig.1 Hourly comparison for Log Average Network Packets contained in Benign and Intrusive network flows forward (Incoming)

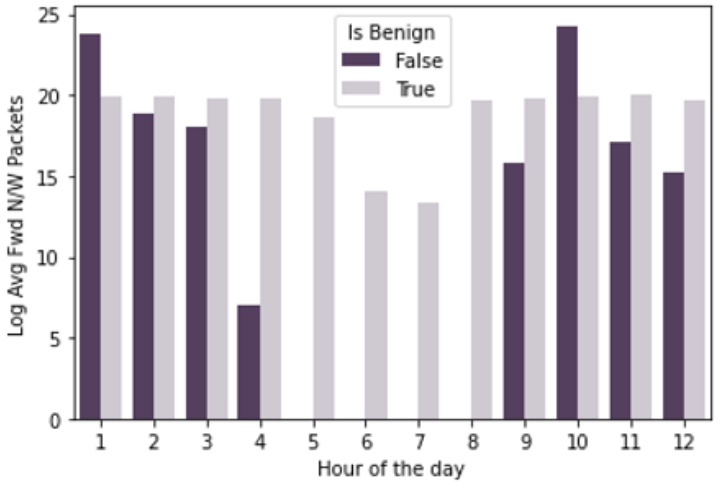


Fig.2 Hourly comparison for Log Average Network Packets contained in Benign and Intrusive network flows backward (Outgoing)

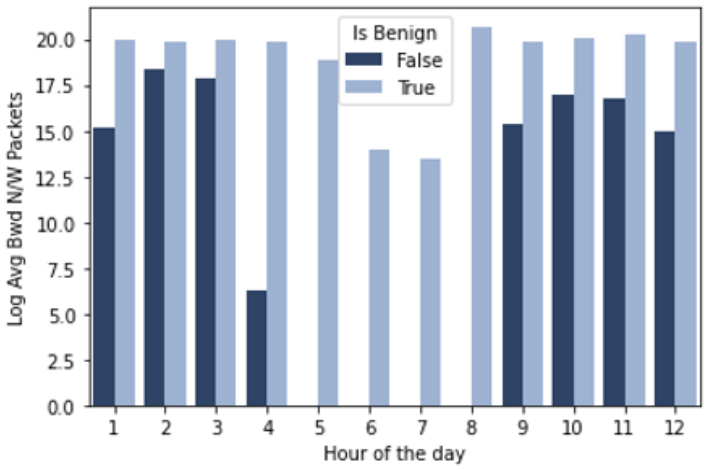
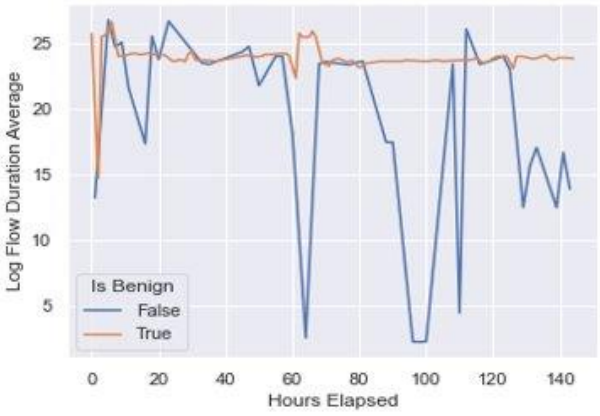


Fig.3 Figure shows the Log Average duration of attacks vs benign traffic patterns



3.2 Techniques

This research project explores the uses of self-learning artificial intelligence models as defense mechanisms. First, the algorithm will be trained with the network data to learn the typical behavioral patterns of the network. Then, different attack patterns will be simulated by introducing data that is abnormal for this network. Finally, the predictions generated by the most successful model will have the classes: benign, quarantine, notify and drop, depending on the type of traffic encountered.

Bayesian algorithms tend to do better as the network and traffic complexity increases. Further, a neural network can be used to produce a probability distribution over the classes for a given network flow. Therefore, combining the two approaches, using Linear Bayesian functions stacked with hidden layers of Neural Networks, will help us fine-tune the required precision and accuracy for predicting attacks [21]. Choosing an appropriate loss function for the network is essential to avoid overfitting data on the Training set. Introducing weighted loss can help compensate for potential imbalances within objective functions [24]. For this technique, we chose a hybrid of cross-entropy loss and reverse KL-divergence loss. Weights have been assigned to KL-divergence to optimize prior probabilities in the Bayesian functions [27].

The study also explored RNNs as an alternative approach, as they have the intrinsic ability to account for temporal dependencies in sequence learning. Consequently, this approach can benefit network traffic flows with a semblance of periodicity [16]. However, since RNNs are computationally expensive algorithms, using an optimized version of RNN, namely Long Short-term Memory (LSTM) or Gated Recurrent Unit (GRU), would help address performance and cost concerns while training the model. For example, a recent study on speech recognition datasets shows that LSTM achieves the best word error rates. Nevertheless, the GRU optimization is faster, achieving word error rates close to LSTM [23].

4 Results

4.1 Interpretation

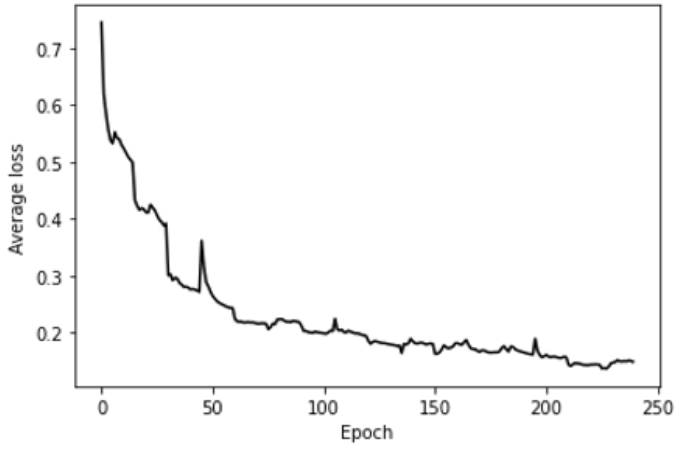
This research considered that the resulting models should show detection rates with an F1-score greater than 0.9 to be effective. The key assessment metric is the F1 score, which is a balance between precision and accuracy with equal weights on both metrics. This would help to choose an optimized approach for both true positives and negatives to avoid blockage of valid traffic and simultaneously prevent intrusive attacks with high precision. Performance of the model is also a key consideration in assessment as it should not add latency to the overall turnaround for the network flow.

Table 2. Overall performance is based on the parameters that can be interpreted.

ANN-based mechanism	F1 score	Category	Attack types	Output Label	Action
Bayesian Neural Network (BNN)	**0.97**	**True Positive**	**DDoS**	**Quarantine**	**Notify Admin**

After training the Bayesian NN with one hidden layer of linear NN and classifier for 200 epochs, the model displayed a 97% F1 score for traffic correctly identified as DDoS. Consequently, this traffic was labeled as quarantined. The resulting action, in this case, would be to notify the network administrator.

Fig.4 Figure shows progression of the average loss value after each training iteration.



The study used a Validation Data set that was not part of the training files to simulate real-world applications. The model showed optimal training performance at approximately 200 epochs (Ref Fig. 4) beyond that the model tends to overfit the test data. PyTorch facilitated the implementation of these models. The optimal model for this data set contained one Linear NN layer stacked with two Bayesian NN layers and with Rectified Linear Unit function (ReLU) as the activation function between these NN layers.

5 Discussion

5.1 Research limitations and ethical considerations

The data collected will not involve human subjects. The dataset utilized is purposefully generated for this type of research and it does not contain Personal Identifiable Information (PII). This research project assumes that the dataset provided by the CSE-CIC-IDS2018 on AWS project observed the following ethical considerations: while collecting data, researchers must ensure that any third party involved in the data

collection gave their explicit consent to the data collection and all data acquired stand true to their facts. There should not be any means of copyright infringement or plagiarism, and the research would make the best use of tangible and intangible resources.

The researchers will not collect data from existing networks due to the limitations imposed by organizational policies about releasing sensitive information and exposing network vulnerabilities to third parties. Any network data collected from existing networks in later stages will be used solely for research purposes and destroyed once the research is completed. Any real-life data collected will be stored securely and monitored by the researchers. If information system assets are used, they should be protected carefully, and false positives, unintentional bias, and false negatives would be carefully verified.

Furthermore, there are ethical considerations around protecting information systems assets from unauthorized access or disruption by threat actors. Even after the models have been trained, there is the possibility of encountering false positives due to the introduction of unaccustomed users, new applications, the addition of devices, and changes to network configurations. That is why the models will default to quarantine new events, to allow the network administrators to evaluate further and determine if the new event is a threat or a false positive that should be allowed and therefore incorporated into the baseline of what is typical for this network.

This study explored layering RNN with BNN to improve detection performance. However, the dataset was not suitable for training RNN.

5.2 Application

The findings of this study imply that Bayesian Neural Networks are an excellent candidate for applications that require highly adaptable and economical anomaly detection with autonomous learning capabilities. Such capabilities are a good match for cybersecurity applications to help identify threats and try to prevent them in near real-time. However, these same methods can meet the requirements in other areas such as sensor networks, industrial quality control, and even semi-unsupervised image labeling.

5.3 Future research

The research design is presented as an overall strategy for integrating components to implement intrusion detection and prevention systems using unsupervised learning ML. Future studies can investigate different approaches to automate network intrusion detection and prevention and focus on critical aspects like transferability using deep learning intrusion detection. There will be four approaches to investigate:

1. The capacity to transfer learning between neural networks that have been trained with various inputs.
2. To develop the ability to move information between different neural networks to automate network intrusion detection and prevention.
3. The further refinement of the algorithm's performance to facilitate the implementation in operational networks like Supervisory Control and Data Acquisition (SCADA). SCADA has a lower tolerance for the automation of intrusion prevention because false positives can stop production, derail operations, and even result in physical damage to costly industrial equipment.
4. Layering of combinations of Recurrent Neural Network (RNN) and Convolutional Neural Networks CNN) to improve detection results.
   a) "RNNs have the intrinsic ability to account for temporal dependencies in sequence learning" [4].
   b) Consequently, network traffic flows with periodicity can benefit from this approach
   c) The timestamp features for each network event would need to be broken down into a time window for creating the Time Distributed layer for the RNN network

Another research area to explore in future studies is the implementation of AI-driven frameworks to defend digital assets once quantum computers defeat RSA. Multiple players, including IBM and nation-states like Japan, China, and India, aim to release commercial quantum computers by 2023. According to Sanders, the introduction of commercially available quantum computers will not immediately create a change in basic assumptions in the speed of digital transformation of societies. However, in the long term, quantum computers will create new challenges for attackers and defenders of digital assets [15].

6 Conclusion

This research reviewed unsupervised machine learning algorithms used in intrusion detection and prevention systems to expedite anomaly detection and intrusion prevention. It explored algorithms that have proven effective in anomaly detection applied to detecting and preventing cyberattacks. The study found that the Bayesian Neural Network models were more efficient at the automatic detection of anomalies in networks. These models can automate intrusion prevention with characteristics that emulate the body's immune system. The success criteria for the models were measured by an F1 score greater than 90%. The most successful model yielded by this study, the Bayesian Neural Network model achieved a 97% F1 score. This was the result of stacking traditional Neural Networks with Bayesian linear function as hidden layers, to be effective, minimize false positives, and to create autonomous learning capabilities. The purpose of this research is to equip companies with tools to protect their data assets from hackers. This research can be useful for businesses seeking to enhance their network defense capabilities by adding IDPS enhanced with self-learning AI. This

study has shown Bayesian Neural Network model to be effective. Due to reduced demand on computer resources, speed of training, and the autonomous learning and intrinsic memory capability of Bayesian Neural Network models.

Bayesian algorithms have proven effective in anomaly detection applications to detect and prevent cyberattacks. Using heuristics instead of a list of previously identified threats as pre-labeled data facilitates the detection of zero-day exploits and atypical patterns that could indicate compromise in near-real time. Algorithms and compute optimization are essential for efficient ML training The development of approximate inference models based on Bayesian Algorithms are worth pursuing since they can reduce the cost barrier for many organizations because they train faster, reduce cost associated with data preparation and compute resources, and result in better performing models when compared with LSTM models. Thus, clearing the way so that more organizations can implement AI-enhanced IDPS and remain focused on their core business instead of the specter of a cyberattack.

7 Acknowledgment

This paper was completed with assistance from SMU's Librarians on AI models. Their contributions included research on current trends and their practical application to address cybersecurity incidents. The input from the advisor Hayley Horn was instrumental in helping refine this document and added focus to this research.

References

[1] [Al-Shourbaji, I., & Al-Janabi, S. (2017). Intrusion Detection and Prevention Systems in Wireless Networks. Kurdistan Journal of Applied Research, 2(3), 267-272. Available at https://www.kjar.spu.edu.iq/index.php/kjar/article/view/117

[2] Bashir, U., & Chachoo, M. (2014, March). Intrusion detection and prevention system: Challenges & opportunities. In 2014 International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 806-809). IEEE. Available at https://ieeexplore.ieee.org/abstract/document/6828073/

[3] Dilek, S., Çakır, H., &Aydın, M. (2015). Applications of artificial intelligence techniques to combat cyber-crimes: A review. arXiv preprint arXiv:1502.03552. Available at https://arxiv.org/abs/1502.03552

[4] Mitchell, R., & Chen, R. (2014). A survey of intrusion detection in wireless network applications. Computer Communications, 42, 1-23. Available at https://www.sciencedirect.com/science/article/abs/pii/S0140366414000280

[5] Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from a machine learning perspective. Journal of Big data, 7(1), 1-29. Available at https://link.springer.com/article/10.1186/s40537-020-00318-5

[6] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE transactions on emerging topics in computational intelligence, 2(1), 41-50. Available at https://ieeexplore.ieee.org/abstract/document/8264962

[7] Thapa, S., & Mailewa, A. (2020, April). The role of intrusion detection/prevention systems in modern computer networks: A review. In Conference: Midwest Instruction and Computing Symposium (MICS) (Vol. 53, pp. 1-14). Available at file:///C:/Users/User/Downloads/EasyChair-Preprint-3278%20(1).pdf

[8] Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., ... & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. Ieee access, 6, 35365-35381. Available at https://ieeexplore.ieee.org/abstract/document/8359287

[9] Yang, K., Liu, J., Zhang, C., & Fang, Y. (2018, October). Adversarial examples against the deep learning-based network intrusion detection systems. In MILCOM 2018-2018 IEEE military communications conference (MILCOM) (pp. 559-564). IEEE. Available at https://ieeexplore.ieee.org/abstract/document/8599759

[10] Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. Ieee Access, 5, 21954-21961. Available at https://ieeexplore.ieee.org/abstract/document/8066291

[11] Zhang, C., Ruan, F., Yin, L., Chen, X., Zhai, L., & Liu, F. (2019, October). A deep learning approach for network intrusion detection based on the NSL-KDD dataset. In 2019 IEEE 13th International Conference on Anti-counterfeiting, Security, and Identification (ASID) (pp. 41-45). IEEE. Available at https://ieeexplore.ieee.org/abstract/document/7777224

[12] Canadian Institute for Cybersecurity. (2018). CSE-CIC-IDS2018 on AWS. Retrieved from University of New Brunswick: https://www.unb.ca/cic/datasets/ids-2018.html
[13] DarkTrace. (2018). DarkTrace IA: Combining Unsupervised and Supervised Machine Learning. Retrieved from DarkTrace: https://www.darktrace.com/en/resources/wp-machine-learning.pdf
[14] Deputy Director, Paul Abbate. (2020). Internet Crime Report 2020. Federal Bureau of Investigations. Washington, D.C.: Internet Crime Complaint Center.
[15] Keane, J. (2022, June 6). The race toward a new computing technology is heating up — and Asia is jumping on the trend. Retrieved from CNBC: https://www.cnbc.com/2022/06/07/quantum-computing-more-asian-countries-are-getting-in-on-the-trend.html
[16] Monidipa Das, M. P. (2019). MUSE-RNN: A Multilayer Self-Evolving Recurrent Neural Network for Data Stream Classification. Retrieved from https://ieeexplore-ieee-org.proxy.libraries.smu.edu/stamp/stamp.jsp?tp=&arnumber=8970794&tag=1
[17] Peter J. Green, K. P. (2015, July). Bayesian computation: a summary of the current state, and samples backwards and forwards. Retrieved from Stat Comput 25, 835–862 (2015): https://doi.org/10.1007/s11222-015-9574-5
[18] SAS Institute Inc. (2019, December 13). Introduction to Bayesian Analysis Procedures. Retrieved from SAS/STAT User's Guide: https://documentation.sas.com/doc/en/pgmsascdc/9.4_3.4/statug/statug_introbayes_sect015.htm
[19] Shril, A. V. (2022, January). Cyber Security: A Review of Cyber Crimes, Security Challenges and Measures to Control. Vision The Journal of Business Perspective, OnlineFirst, 1-2.
[20] SmartClick. (2020). How AI Can Improve the Lives of People with Disabilities. Retrieved from SmartClick: https://smartclick.ai/articles/how-ai-can-improve-the-lives-of-people-with-disabilities/
[21] Tom Auld, A. W. (2007, January). Bayesian Neural Networks for Internet Traffic Classification. (N. 1. IEEE TRANSACTIONS ON NEURAL NETWORKS VOL. 18, Producer) Retrieved June 2022, from IEEE Explore: https://ieeexplore-ieee-org.proxy.libraries.smu.edu/stamp/stamp.jsp?tp=&arnumber=4049810
[22] Vadapalli, P. (2021, February 4). Bayes Theorem in Machine Learning: Introduction, How to Apply & Example. Retrieved from upGrad: https://www.upgrad.com/blog/bayes-theorem-in-machine-learning/
[23] Apeksha Shewalkar, Deepika Nyavanandi, Simone A. Ludwig (2019, March 10) Performance evaluation of deep neural networks applied to speech recognition: RNN, LSTM and GRU
[24] Remco van der Meer, Cornelis W. Oosterlee, Anastasia Borovykh (2021, March 24) Optimally weighted loss functions for solving PDEs with Neural Networks: https://doi.org/10.1016/j.cam.2021.113887
[25] Manuel Lopez-Martin, Antonio Sanchez-Esguevillas, Belen Carro, Jaime Lloret (2017, August 17) Network Traffic Classifier with Convolutional and

Recurrent Neural Networks for Internet of Things: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8026581

[26] Paul Abbate, Deputy Director, Federal Bureau of Investigation. (2021). Internet Crime Report. Retrieved from The Internet Crime Complaint Center (IC3): https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

[27] Andrey Malinin, Mark Gales Reverse (2019, December). KL-Divergence Training of Prior Networks: Improved Uncertainty and Adversarial Robustness: https://proceedings.neurips.cc/paper/2019/file/7dd2ae7db7d18ee7c9425e38df1af5e2-Paper.pdf