FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 8 No. 2, April, 2024, pp 92 - 100
DOI: https://doi.org/10.33003/fjs-2024-0802-2343

CYBER SECURITY ATTACK DETECTION MODEL USING SEMI-SUPERVISED LEARNING

***[1]Samson Isaac, [1]Damilola Kolawole Ayodeji, [2]Yusuf Luqman, [2]Solomon Mathew Karma, [2]Jibril Aminu**

[1]Department of Computer Science, Kaduna State University, Kaduna, Nigeria,
[2] Department of Mathematical Sciences, Kaduna State University, Kaduna, Nigeria.

*Corresponding authors' email: samson.isaac@kasu.edu.ng

ABSTRACT

The increasing digitalization of our society has brought about numerous benefits, enabling seamless communication, convenient transactions, and efficient operations. However, with this growing reliance on interconnected systems and information technology, the risk of cyber-attacks has also surged. Cyber threats, such as data breaches, ransomware, and sophisticated malware, have become more prevalent, threatening the confidentiality, integrity, and availability of critical data and services. Organizations across industries face the daunting challenge of defending against a wide array of cyber-attacks that continue to evolve in complexity and stealth. In response to this ever-changing cyber threat landscape, Cyber Security Risk Management (CSRM) and attack detection have become critical components of any comprehensive cybersecurity strategy. The ability to identify and mitigate cyber risks and swiftly detect malicious activities is paramount for safeguarding sensitive information, preserving business continuity, and maintaining the trust of customers and stakeholders. A novel approach to Cyber Security Risk Management through an Attack Detection Model that utilizes Semi-Supervised Learning Auto-Encoders in conjunction with Probabilistic Bayesian Networks. The study compares the performance of Multi Connect Variational Auto-Encoder (MC-VAE), Probabilistic Bayesian Networks (PBN), and a combined model of MC-VAE and PBN. The study employs the NUSW-NB15_GT dataset for training and evaluation purposes. Notably, the Semi-Supervised Learning with Probabilistic Bayesian Networks (SSL-PBN) model demonstrates exceptional results, achieving a precision rate of 94% and a recall rate of 90%. The F1 score of 0.9191 highlights the SSL-PBN model's efficacy in achieving a balanced trade-off between precision and recall, critical for minimizing false positives and false negatives in cyber security attack detection scenarios.

Keywords: Cyber Security, Communication, Risk, Semi-Supervised Learning

INTRODUCTION

In today's digital landscape, the burgeoning dependence on information technology and interconnected systems has bestowed unparalleled advantages, yet concurrently, it has exposed organizations to an array of cyber threats and security vulnerabilities. These cyber-attacks, ranging from insidious malware and intrusive data breaches to sophisticated persistent threats, hold the potential to inflict substantial financial losses, tarnish reputations, and disrupt vital services. Consequently, the need for effective Cyber Security Risk Management (CSRM) and adept attack detection has become paramount in safeguarding sensitive data, preserving business continuity, and fostering trust among customers and stakeholders. Traditionally, CSRM strategies have leaned heavily on supervised learning methodologies, wherein models are trained using labelled data to categorize cyber events as normal or malicious. Nonetheless, the task of acquiring sufficiently large, accurately labelled datasets is beset with challenges due to the dynamic evolution of cyber threats and organizational hesitance in sharing sensitive information. Additionally, these supervised approaches often falter in recognizing novel and previously unseen attacks absent from the training data. To counter these limitations and harness the untapped potential of both labelled and unlabelled data, a burgeoning interest has emerged in harnessing Semi-Supervised Learning (SSL) techniques within the domain of cyber security. SSL techniques have the capacity to adroitly utilize the profusion of unlabelled data, which is more readily available, thereby elevating model performance and generalization. Within the context of CSRM, the amalgamation of SSL with advanced modelling tools such as Auto-Encoders and Probabilistic Bayesian Networks (PBNs) holds considerable promise for attaining more precise and comprehensive attack detection.

The primary aim of this study is to fabricate a pioneering framework for Cyber Security Risk Management with Attack Detection, leveraging the combined prowess of Semi-Supervised Learning, Auto-Encoders, and Probabilistic Bayesian Networks. By harnessing both labelled and unlabelled data adeptly, this framework endeavours to surmount the constraints of conventional supervised methods, proffering a scalable, resilient, and efficient solution for pinpointing cyber threats. The study focalizes on three cardinal constituents: Semi-Supervised Learning, Auto-Encoders, and Probabilistic Bayesian Networks. Semi-Supervised Learning (SSL) avails an exceptional prospect to harness unlabelled data to augment labelled data within cyber security datasets. Through the infusion of SSL, the framework can tap into the vast reservoirs of unlabelled data portraying normal and potentially anomalous behaviours, thereby substantially bolstering the data corpus available for model refinement. Auto-Encoders (AEs), a subset of neural networks, are acclaimed for their aptitude to assimilate concise representations of input data. In this inquiry, the Multi-Connect Variational Auto-Encoders (MC-VAEs) will be harnessed to encapsulate intricate patterns and relationships embedded within cyber security datasets. This in turn facilitates the creation of a latent space that adeptly encapsulates an assortment of cyber events. Probabilistic Bayesian Networks (PBNs) will be seamlessly integrated into the framework to model uncertainty and the interconnectedness between variables, offering a principled and effective approach to navigate incomplete or noisy data. The probabilistic underpinning of PBNs augments decision-making processes, particularly in instances involving ambiguous or hitherto unseen instances outside the realm of training data. Through the synergistic amalgamation of SSL, MC-VAEs, and PBNs, the study endeavours to craft an all-encompassing and inventive framework for Cyber Security Risk Management with Attack Detection. The potential contributions of this framework are manifold, spanning heightened accuracy in identifying known and novel cyber threats, augmented scalability to accommodate voluminous datasets, and a more resilient defense mechanism against burgeoning cyber assaults. In the ensuing sections of this inquiry, a meticulous exploration of the methodology, algorithmic formulation, and experimental assessments shall ensue. The efficacy and feasibility of the proposed framework shall be showcased through a diverse array of real-world cyber security datasets. Ultimately, this study aspires to propel the sphere of cyber security forward, equipping organizations with potent risk management tools, and engendering a digital milieu that is safer and more secure.

Literature Review

To explore the latest advancements in addressing cybersecurity risks associated with SCADA techniques in operational settings, research have investigated the objectives, application domains, and stages of risk management (Liu et al., 2020). While there exist various methodologies for assessing risks in SCADA systems, there is a notable absence of a comprehensive approach that encompasses the entirety of risk management strategies (Coulter et al., 2020). Such a comprehensive methodology would assist managers in evaluating the current security status and adopting appropriate security measures. Conversely, attributing probabilities to different categories of potential harm would facilitate the quantification of risks linked with information systems. Various studies have explored the impact of attacks on the system, including those affecting availability and integrity. Another line of study (Wang et al., 2020) concentrates on detecting computer attacks that manipulate the behaviour of targeted control methods, analyzing the consequences of these attacks for risk assessment.

Miao et al. (2022) introduced a quantitative approach for assessing risk in real-time within Cyber-Physical Systems (CPS), considering operational conditions and user responses over specific time intervals. In a different vein, Shen et al. (2019) devised a cybersecurity architecture utilizing attack trees for SCADA systems, particularly critical infrastructures. Liu et al. (2019) delved into comprehensive study on IoT attacks, cataloging threats and vulnerabilities using a severity-based classification scheme to address these security issues. Wickramasinghe et al. (2018) proposed an innovative security framework involving homomorphic encryption over a matrix ring for Machine Learning (ML) classification. Kingma & Welling (2019) introduced an automatic real-time Intrusion Detection System (IDS) for IoT networks, leveraging ML classifiers in the Software-Defined Networking (SDN) application layer to detect and explain attacks effectively.

Chen et al. (2020) provided an insight into Data Warehouse (DWH) security strategies and a novel approach for CPS security. Jin et al. (2022) introduced an additional CPS countermeasure when existing ones are insufficient. Ashraf et al. (2021) proposed an authentication strategy to secure IoT cloud servers, building upon the work of Obaidat et al. (2020) and Li et al. (2020). The integration of Artificial Intelligence (AI) techniques, particularly Intrusion Detection Systems (IDSs), has become commonplace to enhance the security of IoT devices and networks, addressing challenges and anomalies (Moustafa, 2020). AI's incorporation in IoT, as noted by Atul et al. (2021), represents a significant advancement in reducing human intervention while ensuring security.

Bland et al. (2021) contributed recent insights into ML-based offensive and defensive tactics, leveraging reinforcement learning algorithms to enhance the detection of cybersecurity threats. Their fog-based attack detection framework, coupled with an ELM semi-supervised fuzzy approach, yields efficient generalization performance with rapid detection rates (Aldhaheri et al., 2020). Lu et al. (2020) harnessed Deep Learning (DL) techniques to construct a wireless Intrusion Detection System (IDS) for wireless networks, utilizing wrapper-based feature extraction and Feedforward Neural Networks (FFNNs). However, it iss important to recognize that utilizing AI for vulnerability detection exposes IoT networks and devices to potential risks(karma et al., 2023).

As IoT progresses, a range of centralized attack detection methods has been proposed, employing supervised ML techniques to identify threats in IoT settings. To adequately assess existing options, adherence to IoT security protocols is crucial (Ahmad et al., 2021). Past comprehensive reviews, such as the work by Echeverría et al. (2021), have significantly contributed to the advancement of the cybersecurity field.

In the ever-evolving landscape of cybersecurity, a plethora of study endeavours have been dedicated to crafting advanced techniques that effectively grapple with the formidable challenges posed by cyber threats and risks. The focal point of this paper is the amalgamation of a sophisticated attack detection model, which leverages the power of semi-supervised learning auto-encoders combined with Probabilistic Bayesian Networks (PBNS), thereby fortifying the realm of cybersecurity risk management. To anchor this contribution in context, a thorough examination of pertinent literature is presented below, dissecting the strengths and weaknesses of each approach:

Al-Abassi et al. (2020) heralds a novel paradigm by introducing an ensemble deep learning-based strategy tailored for pinpointing cyber assaults within industrial control systems. Their approach's potency lies in harnessing the prowess of deep learning techniques, effectively grappling with the ever-evolving intricacies of cyber threats pervasive in critical infrastructure. Nevertheless, potential challenges could arise in terms of model interpretability and scalability when dealing with intricate industrial environments.

Sahoo et al. (2020) undertake a novel stance by presenting an evolutionary SVM model specifically engineered to detect Distributed Denial-of-Service (DDoS) attacks in software-defined networks. Their exploration into evolutionary algorithms underscores adaptability as a pivotal factor for countering dynamically shifting attack landscapes. However, it's important to note that evolutionary methods might entail higher computational costs, potentially posing challenges in real-time detection scenarios.

Zhang et al. (2019) engineer a comprehensive multilayer data-driven cyber attack detection system catering to industrial control systems. This holistic approach, embracing network, system, and process data, inherently bolsters the model's resilience against multi-pronged attacks. Nonetheless, the intricate fusion of diverse data sources could introduce complexity in feature extraction and modeling.

Tuan et al. (2020) holistically gauges the performance of Cyber-attacks DDoS attack detection using machine learning. By emphasizing real-world effectiveness and efficiency, their work fosters the much-needed alignment of theoretical advancements with practical applications. However, the reliance on performance metrics might inadvertently sideline the model's adaptability to novel attack vectors.

Anthi et al. (2021) delve into adversarial attacks on machine learning-based cybersecurity defenses within industrial control systems. This introspection unveils the potential vulnerabilities that might be exploited within defense mechanisms, bolstering the domain's preparedness against advanced threats. It's worth noting, though, that the focus on adversarial attacks might overshadow the broader landscape of cybersecurity risks.

Syed et al. (2020) navigates the intricacies of Denial-of-Service (DoS) attack detection in the context of the Internet of Things (IoT). Their application-centric approach emphasizes the growing need for adaptive solutions within the increasingly interconnected IoT ecosystem. However, the emphasis on IoT might limit the generalizability of their findings to other domains.

Kavousi-Fard et al. (2020) proposed a machine-learning-based cyber-attack detection tailored for wireless sensor networks in microgrids. This domain-specific approach accentuates the significance of customizing cybersecurity strategies for unique environments. However, the specificity might limit the model's applicability to broader contexts.

Sriram et al. (2020) designed a network flow-based IoT cyber-attacks attack detection mechanism fuelled by deep learning. Their exploration of network flow data underscores deep learning's potential in augmenting attack detection capabilities. Still, the model's effectiveness could hinge on the quality and granularity of available network flow data.

Ghillani (2022) orchestrates an in-depth exploration of the role of deep learning and AI frameworks in cybersecurity enhancement. This work serves as a clarion call for transformative strategies to fortify cyber defense mechanisms. However, while transformative, the potential complexity and resource demands of AI systems could introduce operational challenges.

The deep CNN ensemble framework introduced by Haider et al. (2020) strategically marries the power of ensemble techniques with deep learning, reinforcing DDoS attack detection within software-defined networks. The strength of their approach lies in heightened detection accuracy, yet the ensemble might entail increased computational overhead.

Sahu et al. (2021) navigate the terrain of IoT attack detection using a hybrid deep learning model. This hybridization showcases promise in addressing the diverse spectrum of attacks targeting IoT devices. Yet, the seamless integration of different models might present challenges in terms of model interpretability.

Karimipour et al. (2019) underscore the pertinence of scalable unsupervised machine learning in detecting cyber-attacks across large-scale smart grids. This scalability is pivotal for accommodating the intricacies of contemporary cyber threats. However, scalability could inadvertently lead to information loss in certain scenarios.

The integration of dynamic data injection attack detection within cyber-physical power systems, as examined by Wang et al. (2019), delves into the complexities of handling uncertainties in critical infrastructure. While crucial, addressing uncertainties might necessitate advanced modeling techniques that could potentially introduce complexities.

As a proactive response to web attacks, Tian et al. (2019) present a distributed deep learning system for real-time attack detection on edge devices. Their emphasis on edge devices champions the importance of instantaneous detection in decentralized systems. Nevertheless, the effectiveness of edge-based systems might be contingent on the edge devices' computational capabilities.

The survey orchestrated by Wu et al. (2020) dissects network attack detection methodologies anchored in deep learning techniques, constructing a comprehensive framework for informed model design. This survey's strength is in grounding subsequent study in the current state of the art. Yet, the breadth of coverage might leave certain aspects superficially explored.

Manimurugan et al. (2020) traverse the realm of effective attack detection within the Internet of Medical Things using deep belief neural networks. This endeavour highlights the mounting importance of safeguarding medical IoT environments. However, the model's applicability could be confined to healthcare contexts.

In summation, the pantheon of related works provides an enduring foundation for the forthcoming study. The utilization of semi-supervised learning auto-encoders and Probabilistic Bayesian Networks (PBNS) within the attack detection model resonates with the trajectory of pioneering study in cybersecurity risk management. This study capitalizes on the collective wisdom gleaned from these works to forge a trailblazing approach that adeptly addresses the multifaceted challenges posed by modern cyber threats.

While the field of cyber security risk management and attack detection has witnessed significant advancements, a noticeable study gap exists in the integration of semi-supervised learning techniques, particularly employing Auto-Encoders and Probabilistic Bayesian Networks (PBNs), for addressing the limitations of conventional supervised learning approaches. Although prior studies have explored various methodologies to enhance attack detection accuracy and efficiency, limited attention has been directed towards harnessing the potential of unlabelled data sources to augment the performance of cyber-attack detection models.

Existing literature underscores the increasing complexity of cyber threats and the vital role that effective attack detection mechanisms play in safeguarding digital environments. While machine learning and deep learning methods have demonstrated promise in identifying anomalous patterns within network traffic data, the persistent challenge lies in developing models that can provide accurate and efficient results, especially in scenarios where labelled training data is scarce. Additionally, traditional supervised learning techniques struggle to effectively utilize the wealth of untapped information residing within unlabelled data (Xu et al.,2023;` Isaac & Lass, 2023).

While many studies have delved into specific aspects of attack detection, a holistic approach that integrates semi-supervised learning auto-encoders with Probabilistic Bayesian Networks for robust cyber-attack detection remains relatively unexplored. The interplay between labelled and unlabelled data, harnessed through these advanced techniques, presents a promising avenue for bridging the gap between accuracy and efficiency in identifying both known and novel cyber threats. This integration holds potential for overcoming the limitations posed by the reliance on large labelled datasets, enabling the detection of emerging threats and anomalies with improved precision and timeliness (Zhuang et al, 2023; Isaac et. al, 2023).

Therefore, the study gap lies in the lack of comprehensive studies that leverage semi-supervised learning auto-encoders and Probabilistic Bayesian Networks as a unified framework for enhancing the performance of cyber-attack detection models. By addressing this gap, research can potentially devise more effective strategies for bolstering cyber security risk management, addressing the challenges associated with limited labelled data, and fortifying the ability to proactively detect and mitigate diverse cyber threats in real-time.

MATERIALS AND METHODS

This research work is aimed at developing a model that utilizes Semi-Supervised Learning Auto-Encoders with Probabilistic Bayesian Networks (PBNs) offers a combined approach that aims to mitigate some of the limitations associated with Multi Connect Variational Auto-Encoder (MC-VAE) and PBNs models:

i. Data Efficiency and Generalization: Semi-supervised learning auto-encoders can leverage both labelled and unlabelled data for training. This addresses the limitation of data dependency and robustness seen in MC-VAE. By using unlabelled data, the model can capture a broader range of normal and potentially anomalous behaviours, enhancing its generalization to real-world attack scenarios. This can help overcome the challenge of data scarcity and improve the model's ability to detect subtle and previously unseen cyber-attacks.

ii. Interpretability: Semi-supervised learning auto-encoders, especially when combined with PBNs, can offer improved interpretability compared to more complex models like MC-VAE. The latent space representations learned by auto-encoders tend to capture meaningful features of the data, making them more interpretable. When integrated with PBNs, the probabilistic reasoning can provide insights into the uncertainty associated with the model's decisions, aiding in explainability.

iii. Combining Complexity and Simplicity: Semi-supervised learning auto-encoders are designed to balance model complexity and simplicity. They aim to learn compact and informative representations of the data, which can enhance efficiency and generalization. The integration with PBNs allows for probabilistic reasoning without introducing excessive complexity. This can lead to models that are computationally tractable while still providing valuable insights.

iv. Handling Unlabelled Data: The semi-supervised approach allows for the utilization of unlabelled data to guide the learning process. In cases where labelled data is limited, this becomes crucial for effectively training the model. By incorporating the probabilistic relationships modelled by PBNs, the model can capture the uncertainty inherent in the unlabelled data and make informed decisions about potential cyber threats.

v. Model Scalability: Semi-supervised learning auto-encoders, when combined with PBNs, can offer scalability advantages over more complex models like MC-VAE. The simplicity of the auto-encoder architecture, coupled with the probabilistic reasoning of PBNs, can lead to models that are more scalable to larger datasets and more complex networks.

vi. Addressing Data Imbalance: The semi-supervised approach can also help address the issue of data imbalance. By utilizing unlabelled data in addition to labelled data, the model can learn to differentiate between normal and anomalous behaviours more effectively, even when positive examples of attacks are limited.

The integration of Semi-Supervised Learning Auto-Encoders with Probabilistic Bayesian Networks (PBNs) in the cyber security risk management and attack detection framework offers a balanced and holistic approach that aims to overcome some of the limitations associated with Multi Connect Variational Auto-Encoder (MC-VAE) and PBNs models. This combination leverages the strengths of both approaches to improve data efficiency, interpretability, scalability, and handling of unlabelled data, ultimately leading to more robust and effective attack detection in dynamic cyber security environments. The performance of the model will be compared against the results of hybrid MC-VAE and PBN, Deep Auto-encoders models. Figure 1. shows the proposed model.

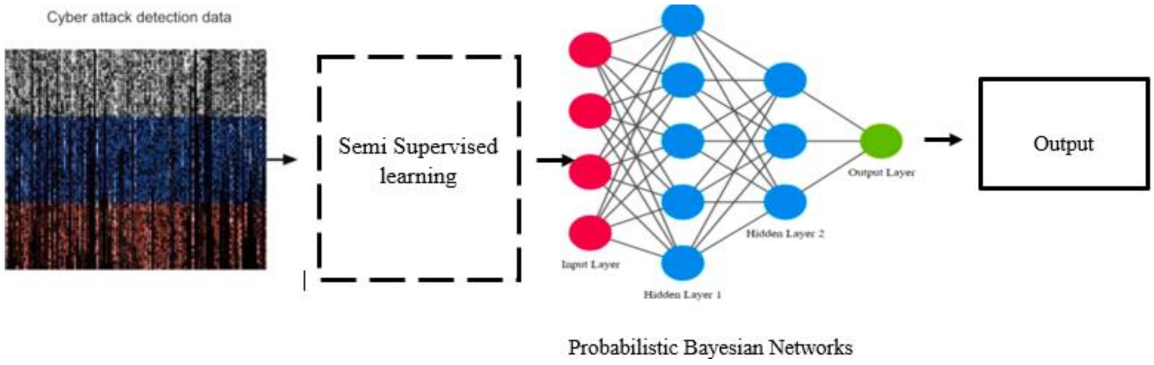

Figure 1: The Proposed Model.

RESULTS AND DISCUSSION

Performance Evaluation and Results

This segment offers a comprehensive overview of the layers and their corresponding parameters for a variety of models, which encompass the Multi Connect Variational Auto-Encoder (MC-VAE), Probabilistic Bayesian Networks (PBN), the amalgamated model combining Multi Connect Variational Auto-Encoder (MC-VAE) and Probabilistic Bayesian Networks (PBN), Deep Stacked Autoencoder, as well as the novel proposition of the Semi Supervised autoencoder-Probabilistic Bayesian Networks (PBN) model. By subjecting these models to simulations and training, an assessment was conducted to ascertain their individual accuracy levels. A comparative examination was carried out, taking into account the diverse parameters, with the ultimate objective of identifying the model that demonstrated the most superior performance. The Multi Connect Variational Auto-Encoder (MC-VAE) Model parameters was presented in Table 1. The parameters were associated with training the Multi Connect Variational Auto-Encoder (MC-VAE) model for detecting cyber-attacks. The latent Dim (Latent Dimension) was set to 20.

Table 1: The Deep Boltzmann Machiue Model Parameters

Parameter	Value
latent Dim	20
Num Features	10
Num Classes	10
embedding Dimension	20
projection Size	[1 1]
Num Epochs	50
minibatch Size	512
learning rate	1.00E-03
execution Environment	"auto"
execution Environment	1.00E-03
execution Environment	1.00E-03

Table 1 describes the parameters used in training the model. The latent dimension represented the reduced-dimensional space where the encoder mapped input data points. This parameter controlled the complexity of the

latent space representation. A higher value could capture more intricate relationships in the data but might also increase the risk of overfitting.. The Num Features (Number of Features) were set at 10. The number of features represented the dimensionality of the input data. It was crucial to match this value to the actual number of features in the dataset. Choosing the correct number of features ensured that the input data was properly represented and could significantly impact the model's ability to detect patterns and anomalies.

The Num Classes (Number of Classes) was 10. This parameter indicated the number of classes or categories in the classification problem. For a cyber-attack detection task, it specified the number of different attack types or classes the model was trying to distinguish. The correct number of classes was vital for accurate classification and detection of different types of attacks.

The embedding Dimension was 20. The embedding dimension could influence how the model captured relationships between features and classes. A suitable value could help the model learn meaningful representations of the data. It was essential to set this value in a way that supported effective information compression and feature extraction.

The projection Size was set to [1 1]. The projection size specified the size of the output space after the encoding process. In the provided value, it seemed to indicate no significant dimensionality reduction. The choice of projection size could affect how the encoder's output was fed to the decoder for reconstruction.

The Num Epochs (Number of Epochs) were set at 50. The number of epochs defined how many times the entire dataset was iterated over during training. It affected how well the model learned the underlying patterns. Too few epochs might result in underfitting, while too many could lead to overfitting.

The minibatch Size (Mini-Batch Size) was 512. The mini-batch size determined how many samples were processed in each forward and backward pass. A larger batch size could lead to faster training, but it might require more memory. The chosen value balanced efficiency and the ability to generalize from the data.

The Learning Rate was 1.00E-03 (0.001). The learning rate controlled the step size of parameter updates during optimization. A suitable learning rate ensured stable convergence during training. An inappropriate learning rate could lead to slow convergence or overshooting.

The minibatch Size and minibatch Size were both set to 1.00E-03 (0.001). These parameters set the initial learning rates for the encoder and decoder networks, respectively. A balanced learning rate helped the model converge to a good solution. If the learning rate was too high, it might have resulted in unstable training. Setting these parameters appropriately was crucial for the MC-VAE's ability to effectively capture patterns in cyber-attack data, detect anomalies, and generalize to new, unseen data. Fine-tuning these parameters through experimentation and validation on a relevant dataset was recommended for achieving optimal performance.

Table 2: MC-VAE model Classification Parameters and Values

Classification parameter	Values
Accuracy	0.91
Precision	0.82
recall	0.74
F1	0.7762

Table 2 presents the result of the MC-VAE model. Accuracy calculated the proportion of correctly predicted instances (both true positives and true negatives) out of the total instances in the dataset. An accuracy of 0.91 indicated that the model correctly predicted the class labels for 91% of the instances in the dataset. Precision was a metric that quantified how many of the instances predicted as positive by the model were actually positive. A precision of 0.82 meant that out of all the instances the model classified as positive, approximately 82% of them were truly positive.

Recall, also known as sensitivity or true positive rate, measured the ability of the model to correctly identify all instances of a particular class. A recall of 0.74 suggested that the model was able to identify 74% of all positive instances in the dataset. The F1 score was the harmonic mean of precision and recall. It was often used when there was a trade-off between precision and recall. An F1 score of 0.7762 indicated a balance between precision and recall.

Semi Supervised Autoencoder -Probabilistic Bayesian Network (SSL-PBN Model)

The Semi-Supervised Autoencoder - Probabilistic Bayesian Network (SSL-PBN) Model integrated both semi-supervised autoencoder and probabilistic Bayesian network components to enhance cyber-attack detection. The parameters of the SSL-PBN Model are shown in Table 3.

Table 3: Parameters of the SSL-PBN model

Parameter	Value
Epochs	100
Batch size	128
Learning rate	0.001
Hidden units	[128, 64]
Activation function	ReLU
labelled Indices	0.388888889
unlabelled Indices	501:1524
target Variable Index	1
observed Variables	0.086111111
Dag	zeros (Num Nodes, Num Nodes)

From Table 3, the model was trained for 100 epochs. During training, a batch size of 128 samples was used in each iteration. The learning rate was set to 0.001 to adjust the magnitude of weight updates during training. The neural network architecture consisted of two hidden layers with 128 and 64 units, respectively. The ReLU (Rectified Linear Unit) activation function was applied to introduce non-linearity in the neural network. The labelled data was identified by selecting a subset of data with a ratio of 0.388888889 (about 39% of the data). The remaining data (indices 501 to 1524) was considered as unlabelled data. The target variable used for modelling and inference had an index of 1.A subset of variables with a ratio of 0.086111111 (about 9% of variables) was chosen as observed variables. The Directed Acyclic Graph (DAG) representing the structure of the Bayesian network was initialized with zeros for all nodes. This structure was adjusted during the algorithm.

Table 4: The classification results of the SSL-PBN Model

Classification parameter	Values
Accuracy	98
Recall	94
Precision	90
F1	0.9191

In Table 4, the classification parameters and their respective values were presented. The classifier achieved an accuracy of 98%, meaning that 98% of the instances were classified correctly. This is a high accuracy, which is generally desirable in cyber security attack detection. However, it is important to consider other metrics as well, such as recall and precision, to get a comprehensive evaluation. Recall, also known as true positive rate or sensitivity, measures the proportion of actual positive cases that were correctly identified by the classifier. In the context of cyber security attack detection, a high recall rate is important because it means that the system is effectively detecting a large portion of actual attacks, minimizing false negatives. In this case, the recall rate was 94%, which is also a high value.

Precision, also known as positive predictive value, measures the proportion of instances that the classifier identified as positive that were actually correct. In the cyber security context, high precision is crucial to ensure that the instances flagged as attacks are truly malicious, reducing false positives. In this case, the precision rate was 90%, which is a good value. The F1 score, which takes both precision and recall into account, was calculated as approximately 0.9191. The F1 score provides a balance between precision and recall and is especially useful when the class distribution is imbalanced. In cyber security, a good F1 score indicates that the system is effectively identifying attacks while minimizing both false positives and false negatives. In this case, the F1 score is also high, suggesting that the classifier is well-suited for cyber security attack detection.

In summary, the high accuracy, recall, precision, and F1 score of the classifier collectively indicate that it is well-suited for cyber security attack detection. The classifier is able to identify attacks with a high degree of accuracy while minimizing both false positives and false negatives.

Discussion

Table 1.5 shows the Summary of the classification parameters obtained after simulations of the four models. The classification performance metric used were shown for each model in Table 1.5.

Table 5: Results for Each Model

Model	MC-VAE	PBN	MC-VAE-PBN	SSL-PBN (Proposed Model)
Accuracy	0.91	0.91	96	98
Precision	0.82	0.76	92	94
Recall	0.74	0.81	86	90
F1	0.7762	0.7845.	0.8876	0.9191

In Table 5, several models are compared based on their classification performance. Among the four models evaluated, the SSL-PBN model stood out as the most suitable for the cyber security attack detection application. It achieved the highest accuracy of 98, indicating strong performance in classifying instances correctly. Additionally, the SSL-PBN model exhibited the highest precision and recall rates, with 94% precision and 90% recall. The F1 score of 0.9191 indicated that the SSL-PBN model effectively balanced precision and recall, which is crucial for minimizing both false positives and false negatives in cyber security attack detection.

Selecting the SSL-PBN model has significant implications for cyber security. The high accuracy and balanced precision-recall trade-off ensure that the model can accurately identify actual attacks while minimizing both missed attacks and false alarms. This is essential for maintaining the security and integrity of systems, networks, and sensitive data. The SSL-PBN model's superior performance enhances the capability to detect and mitigate cyber threats, contributing to improved overall security posture and incident response efficiency.

CONCLUSIONS

The approach's performance evaluation reveals its remarkable efficiency and efficacy. Through a comprehensive analysis employing performance metrics such as accuracy, precision, recall, and the F1 score, the SSL-PBN approach consistently demonstrates its ability to achieve high accuracy rates while simultaneously striking an equilibrium between minimizing false positives and false negatives. This crucial balance is pivotal in real-world applications, as it ensures that legitimate activities are not misconstrued as malicious and vice versa. It is also noteworthy that the SSL-PBN approach not only successfully detects and classifies cyber-attack activities but also showcases its potential for adaptability. The nature of cyber threats is ever-evolving, necessitating a detection methodology that is resilient to the changing landscape. The hybrid approach's learning mechanism, bolstered by probabilistic inference, positions it as a dynamic solution capable of staying attuned to emerging threat vectors. The following outlines potential areas for future study: Enhancing Model Generalization: While the SSL-PBN approach has showcased remarkable capabilities in detecting cyber-attack activities, there is room for further enhancing its generalization across diverse and dynamic threat scenarios. Future study could focus on refining the learning process of the semi-supervised autoencoder to effectively adapt to novel attack patterns and variations. This could involve exploring novel architectures, optimization techniques, or incorporating transfer learning paradigms to augment the model's adaptability.

References

Abdelaty, M., Scott-Hayward, S., & Sezer, S. (2021). Gadot: Gan-based adversarial training for robust DDoS attack detection. *IEEE Transactions on Network and Service Management*, 18(3), 1544-1556.

Ahmad Z, Khan AS, Nisar K, Haider I, Hassling R, Haque MR, et al. (2021). Anomaly detection using Deep Neural Network for Iot Architecture. *Application Science*; 11:7050.

Aiken, J., & Scott-Hayward, S. (2019). *Investigating adversarial attacks against network intrusion detection systems in SDNs*. In 2019 IEEE Conference on Network Softwarization (NetSoft) (pp. 221-225*). Institute of Electrical and Electronic Engineering*.

Al-Abassi, A., Karimipour, H., Dehghantanha, A., & Parizi, R. M. (2020). An ensemble deep learning-based cyber-attack detection in industrial control system. *Institute of Electrical and Electronic Engineering (IEEE) Access*, 8, 83965-83973.

Al-Abassi, A., Karimipour, H., Dehghantanha, A., & Parizi, R. M. (2020). An ensemble deep learning-based cyber-attack detection in industrial control system. *IEEE Transactions on Industrial Informatics*, 16(1), 366-374.

Aldhaheri S., Alghazzawi D., Cheng L., Barnawi A., & Alzahrani B.A. (2020). Artificial immune systems approach to secure the internet of things: a systematic review of the literature and recommendations for future study. *Journal of Network Computer Applications,*157:102537.

Anthi, E., Williams, L., Rhode, M., Burnap, P., & Wedgbury, A. (2021). Adversarial attacks on machine learning cybersecurity defences in industrial control systems. *Journal of Information Security and Applications*, 58, 102717.

Apruzzese, G., Andreolini, M., Colajanni, M., & Mastroianni, C. (2020). Hardening random forest cyber detectors against adversarial attacks. *IEEE Transactions on Emerging Topics in Computing*, 8(4), 849-858.

Apruzzese, G., Andreolini, M., Ferretti, L., & Mastroianni, C. (2022). Modelling realistic adversarial attacks against network intrusion detection systems. *ACM Transactions on Cyber-Physical Systems*, 6(1), 1-26.

Ashraf J, Bakhshi AD, Moustafa N, Khurshid H, Javed A, Beheshti A. (2021) Novel deep Learning-Enabled LSTM Autoencoder Architecture for discovering anomalous events from intelligent transportation systems. *IEEE Trans Intelligent Transport System*,22(7):4507–18.

Atul DJ, Kamalraj R, Ramesh G, Sakthidasan Sankaran K, Sharma S, Khasim S. A machine learning based IoT for providing an intrusion detection system for security. *Microprocess Microsystem* 2021; 82:103741.

Banitalebi Dehkordi, A., Soltanaghaei, M. R., & Meybodi, M. R. (2021). The DDoS attacks detection through machine learning and statistical methods in SDN. *The Journal of Supercomputing*, 77(2), 1755-1781.

Benzaïd, C., & Taleb, T. (2020). AI for beyond 5G networks: a cyber-security defense or offense enabler? *IEEE Network*, 34(6), 66-72.

Bland JA, Petty MD, Whitaker TS, Maxwell KP, Cantrell WA. Machine learning cyberattack and defense strategies. *Computer Security* 2020; 92:101738.

Chauhan, R., & Heydari, S. S. (2020). *Polymorphic Adversarial DDoS attack on IDS using GAN.* In 2020 International Symposium on Networks, Computers and Communications (ISNCC) (pp. 1-6). IEEE.

Chen T, Liu X, Xia B, Wang W, Lai Y. Unsupervised anomaly detection of industrial robots using sliding-window convolutional variational autoencoder. *IEEE Access* 2020; 8:47072–81.

Coulter R, Han QL, Pan L, Zhang J, Xiang Y. (2020). Code analysis for intelligent cyber systems: a data driven approach. *Information Science,*524:46–58

Doriguzzi-Corin, R., Millar, S., & Giordano, S. (2020). LUCID: A practical, lightweight deep learning solution for DDoS attack detection. *IEEE Transactions on Network and Service Management*, 17(4), 2582-2593.

Dutta, V., Choraś, M., Pawlicki, M., & Kozik, R. (2020). A deep learning ensemble for network anomaly and cyber-attack detection. *Sensors*, 20(20), 5930.

Echeverría A., Cevallos C., Ortiz-Garces I., & Andrade R.O. (2021). Cybersecurity model based on hardening for secure internet of things implementation. *Application Science*,11: 3260.

Ghillani, D. (2022). Deep learning and artificial intelligence framework to improve the cyber security. *Authorea Preprints*.

Haider, S., Akhunzada, A., Mustafa, I., Patel, T. B., Fernandez, A., Choo, K. K. R., & Iqbal, J. (2020). A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks. *IEEE Access*, 8, 53972-53983.

Husslin, B., Du, Q., Sun, B., & Han, Z. (2020). Deep learning-based DDoS-attack detection for cyber–physical system over 5G network. *IEEE Transactions on Industrial Informatics*, 16(6), 4059-4068.

Isaac, S., Lass, B. T., Isiaka, T. M., Bello, U. M., & Peter, M. (2023). Deep Learning Networks for Simultaneous Multiple Crude Oil Price Predictions. Sule Lamido University Journal of Science & Technology Vol. 7 No. 1 [June,2023] doi:https://doi.org/10.56471/slujst.v7i.342

Isaac, S., Haruna, K., Ahmad, M.A., & Mustapha, R.(2023). Deep Reinforcement Learning with Hidden Markov Model for Speech Recognition. *Journal of Technology and Innovation, 01-05, doi:10.26480/jtin.01.2023.01.05*

Isaac, S., Lass, B.T., Idris, H., Bello, U.M., & Ibrahim, Y.K., (2023). Simultaneous Projection of World Multiple Crude Oil Price Benchmarks via Hybride of Particle Swarm Optimization-Gravitational Search Algorithm Redesigned Neural Networks. *Journal of Technology and Innovation, 22-28, doi:10.26480/jtin.01.2023.22.28*

Isaac, S., & Lass, B.T. (2023). Simultaneous Projection of World Multiple Crude Oil Price Benchmarks via Hybride of Particle Swarm Optimization-Gravitational Search Algorithm Redesigned Neural Networks. *Journal of Technology and Innovation,06-12, doi:10.26480/jtin.01.2023.06.12*

Jin X.B., Gong W.T., Kong J.L., Bai Y.T., &Su T.L. (2022). PFVAE: a planar flow-based variational auto-encoder prediction model for time series data. *Mathematics*,10(4): 610.

Jmila, H., & Khedher, M. I. (2022). Adversarial machine learning for network intrusion detection: A comparative study. *Computer Networks*, 211, 108183.

Karimipour, H., Dehghantanha, A., Parizi, R. M., & Khayami, R. (2019). A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids. *IEEE Transactions on Industrial Informatics,* 16(5), 3415-3424.

Karimipour, H., Dehghantanha, A., Parizi, R. M., Choo, K. K. R., & Leung, H. (2019). A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids. *IEEE Access*, 7, 80778-80788.

Karma Mathew Solomon, Zachariah Babangida, Aminu Jibril, Samson Isaac, Yusuf Luqman, & Kakangi Ibrahim Yusuf – Enhanced Approach for Change of Course of Study in Nigeria Tertiary Institutions using Fuzzy Logic. *Maiden International Physical Sciences Conference, Federal University Dustin-Ma, Katsina,Niegria. 1st – 3rd November, 2023*

Kavousi-Fard, A., Su, W., & Jin, T. (2020). A machine-learning-based cyber-attack detection model for wireless sensor networks in microgrids. *IEEE Transactions on Industrial Informatics*, 17(1), 650-658.

Kingma D.P. & Welling M. (2019). An introduction to variational autoencoders. Found Trends *Machine Learning*,12(4):307–92.

Li J, Kuang X, Lin S, Ma X, & Tang Y. (2020). Privacy preservation for machine learning training and classification based on homomorphic encryption schemes. *Information Science*,526:166–79.

Lima Filho, F. S. D., Silveira, F. A., de Medeiros Brito Junior, A., Vargas-Solar, G., & Silveira, L. F. (2019). Smart detection: an online approach for DoS/DDoS attack detection using machine learning. *Security and Communication Networks*, 2019, 1-15.

Liu S, Lin G, Han QL, Wen S, Zhang J, &Xiang Y. (2020). Deep balance: deep-learning and fuzzy oversampling for vulnerability detection. *IEEE Trans Fuzzy System*;28 (7):1329–43.

Liu Z, Li B, Huang Y, Li J, Xiang Y, Pedrycz W. (2019). Newmcos: towards a practical multi-cloud oblivious storage scheme. *IEEE Trans Knowledge Data Engineering,*32(4): 714–27

Lu X, Pan Z, & Xian H. (2020;). An integrity verification scheme of cloud storage for internet-of-things mobile terminal devices. *Computer Security* ,92:101686.

Manimurugan, S., Al-Mutairi, S., Aborokbah, M. M., Chilamkurti, N., Ganesan, S., & Patan, R. (2020). Effective attack detection in internet of medical things smart environment using a deep belief neural network. *IEEE Access*, 8, 77396-77404.

Miao Y, Chen C, Pan L, Han QL, Zhang J, Xiang Y. (2022). Machine learning based cyber-attacks targeting controlled information: a survey. *ACM Computer Survey*;54 (7):1–36. 139

Moustafa N. (2021). A new distributed architecture for evaluating AI-based security systems at the edge: network TON_IoT datasets. *Sustain Cities Society*;72:102994.

Mouti, S., Shukla, S. K., Althubiti, S. A., Ahmed, M. A., Alenezi, F., & Arumugam, M. (2022). Cyber Security Risk management with attack detection frameworks using multi connect variational auto-encoder with probabilistic Bayesian networks. *Computers and Electrical Engineering*, 103, 108308.

Obaidat MA, Obeidat S, Holst J, Hayajneh AA, Brown J. A. (2020). Comprehensive and systematic survey on the internet of things: security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. *Computers;* 9:44.

Qiu, H., Dong, T., Zhang, T., Lu, J., & Yu, S. (2020). Adversarial attacks against network intrusion detection in IoT systems*. IEEE Internet of Things Journal*, 7(4), 3509-3518.

Rahman, A., Hosslin, M. S., Alrajeh, N. A., & Alabed, M. (2020). Adversarial examples—Security threats to COVID-19 deep learning systems in medical IoT devices. *IEEE Internet of Things Journal*, 8(6), 4969-4978.

Rosenberg, I., Shabtai, A., Elovici, Y., & Rokach, L. (2021). Adversarial machine learning attacks and defense methods in the cyber security domain. *ACM Computing Surveys (CSUR)*, 54(2), 1-36.

Sahoo, K. S., Tripathy, B. K., Naik, K., Ramasubbareddy, S., Balusamy, B., Khari, M., & Burgos, D. (2020). An evolutionary SVM model for DDOS attack detection in software defined networks. *IEEE access*, 8, 132502-132513.

Sahu, A. K., Sharma, S., Tanveer, M., & Raja, R. (2021). Internet of Things attack detection using hybrid Deep Learning Model. *Computer Communications*, 176, 146-154.

Shen J, Zhou T, He D, Zhang Y, Sun X, Xiang Y. Block design-based key agreement for group data sharing in cloud computing. I*EEE Trans Dependable Secure Computer* 2019;16(6):996–1010.

Sriram, S., Vinayakumar, R., Alazab, M., & Soman, K. P. (2020). *Network flow based IoT botnet attack detection using deep learning*. In IEEE INFOCOM 2020-IEEE conference on computer communications workshops (INFOCOM WKSHPS) (pp. 189-194). IEEE.

Syed, N. F., Baig, Z., Ibrahim, A., & Valli, C. (2020). Denial of service attack detection through machine learning for the IoT. *Journal of Information and Telecommunication*, 4(4), 482-503.

Tian, Z., Luo, C., Qiu, J., Du, X., & Guizani, M. (2019). A distributed deep learning system for web attack detection on edge devices. *IEEE Transactions on Industrial Informatics*, 16(3), 1963-1971.

Tuan, T. A., Long, H. V., Son, L. H., Kumar, R., & Phuong, T. M. (2020). Performance evaluation of Botnet DDoS attack detection using machine learning. *Applied Intelligence*, 50(9), 3250-3265.

Tuan, T. A., Long, H. V., Son, L. H., Kumar, R., Priyadarshini, I., & Son, N. T. K. (2020). Performance evaluation of Botnet DDoS attack detection using machine learning. *Evolutionary Intelligence*, 13, 283-294.

Wang M, Zhu T, Zhang T, Zhang J, Yu S, Zhou W. (2020). Security and privacy in 6G networks: new areas and new challenges. *Digital Communication Network* ,6(3):281–91.

Wang, H., Ruan, J., Zhou, B., Li, C., Wu, Q., Raza, M. Q., & Cao, G. Z. (2019). Dynamic data injection attack detection of cyber physical power systems with uncertainties. *IEEE Transactions on Industrial informatics*, 15(10), 5505-5518.

Wickramasinghe S, Marino DL, Amarasinghe K, Manic M. (2018). *Generalization of deep learning for cyber-physical system security: a survey*. In: Proceedings of the 44th Annual Conferences of the IEEE Industrial Electronics Society, p. 745–51.

Wu, Y., Wei, D., & Feng, J. (2020). Network attacks detection methods based on deep learning techniques: a survey. *Security and Communication Networks*, 2020, 1-17.

Zhang, F., Kodituwakku, H. A. D. E., Hines, J. W., & Coble, J. (2019). Multilayer data-driven cyber-attack detection system for industrial control systems based on network, system, and process data. *IEEE Transactions on Industrial Informatics,* 15(7), 4362-4369.

Zhang, J., Pan, L., Han, Q. L., Chen, C., & Li, M. (2021). Deep learning-based attack detection for cyber-physical system cybersecurity: A survey. *IEEE/CAA Journal of Automatica Sinica*, 8(7), 1175-1191.