Kasu Journal of Computer Science Vol.2 No.3 [September, 2025], pp. 284-296
https://doi.org//10.47514/kjcs/2025.2.3.007

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

A Survey of Semi-Supervised Learning Auto-Encoders and Probabilistic Bayesian Network Approaches

Samson Isaac[1*], Barna Thomas Lass[1*], Magaji Musa Marcus[1], Jocknom Jock Jotty[1], Epaphras Peter Kyomnom[1]

[1*] Department of Computer Science, Federal University of Applied Science Kachia, Kaduna, Nigeria,

[1*] Department of Software Engineering, Federal University of Applied Science Kachia, Kaduna, Nigeria,

[2, 2] Department of Information Technology, Federal University of Applied Science Kachia, Kaduna, Nigeria,

[2] Department of Cyber Security, Federal University of Applied Science Kachia, Kaduna, Nigeria,

samson.isaac@fuask.edu.ng[1*], thomas.lass@fuask.edu.ng[1*], magaji.marcus@fuask.edu.ng
Jocknom.kotty@fuask.edu.ng[2],

Abstract

Cybersecurity threats have evolved in complexity and scale, demanding adaptive and intelligent detection mechanisms. This survey examines the integration of Semi-Supervised Learning (SSL) Auto-Encoders and Probabilistic Bayesian Networks (PBNs) as hybrid models for effective cyber risk management and attack detection. This synthesizes recent scholarly contributions (2020–2025) exploring machine learning, deep learning, and probabilistic reasoning approaches. Results indicate that SSL-AE and PBN integration enhances detection accuracy, scalability, and interpretability, addressing the data scarcity problem inherent in supervised models. A comparative analysis of recent models reveals that hybrid frameworks achieve average precision rates exceeding 93% on benchmark datasets, such as UNSW-NB15. This review identifies persistent challenges in model explainability, real-time deployment, and adversarial robustness, while projecting future trends in self-learning cyber defense systems that leverage generative AI and Bayesian deep fusion models.

Keywords: Cybersecurity, Semi-Supervised Learning, Auto-Encoders, Probabilistic Bayesian Networks, Machine Learning, Risk Management, Hybrid Models

1. Introduction

In an era defined by digital interconnectivity, cyber-attacks have grown more sophisticated, targeting both individuals and organizations. Traditional supervised learning approaches for attack detection struggle with data labeling limitations and the dynamic evolution of threats. To overcome these challenges, Semi-Supervised Learning (SSL) and Probabilistic Bayesian Networks (PBNs) have emerged as promising

Kasu Journal of Computer Science Vol.2 No.3 [September, 2025], pp. 284-296
https://doi.org//10.47514/kjcs/2025.2.3.007

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

paradigms, offering improved generalization and interpretability. This survey explores the evolution, methodologies, and implications of SSL-AE–PBN hybrid frameworks in cyber risk management (Mouti et al., 2022). 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 labeled data to categorize cyber events as normal or malicious. Nonetheless, the task of acquiring sufficiently large, accurately labeled datasets is beset with challenges due to the dynamic evolution of cyber threats and organizational hesitance in sharing sensitive information (Sánchez-García et al,. 2023). 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 labeled and unlabeled 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 unlabeled 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 labeled and unlabeled data adeptly, this framework endeavours to surmount the constraints of conventional supervised methods, proffering a scalable, resilient, and efficient solution for pinpointing cyber threats (Isaac et al., 2024). 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 unlabeled data to augment labeled data within cyber security datasets. Through the infusion of SSL, the framework can tap into the vast reservoirs of unlabeled 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

Kasu Journal of Computer Science Vol.2 No.3 [September, 2025], pp. 284-296
https://doi.org//10.47514/kjcs/2025.2.3.007

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

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.

2. Conceptual and Theoretical Framework

The conceptual foundation of this study lies in combining representation learning and probabilistic inference. Auto-Encoders compress high-dimensional network data into meaningful latent spaces, while Bayesian Networks infer conditional dependencies between variables. Together, they create robust hybrid systems capable of detecting anomalous patterns and quantifying uncertainty in decision-making processes.

2.1 Conceptual Overview

Cybersecurity risk management and attack detection are built upon a multilayered understanding of risk, uncertainty, and data-driven intelligence. Traditional risk management frameworks such as ISO/IEC 27005 and the NIST Cybersecurity Framework conceptualize cybersecurity as a cyclical process of identification, protection, detection, response, and recovery (NIST, 2020). However, these frameworks often rely on static, rule-based detection and qualitative risk assessment, which struggle to adapt to modern cyber-threat dynamics characterized by data volume, velocity, and variability (Mızrak, 2023).

The advent of artificial intelligence (AI) and machine learning (ML) introduces a paradigm shift — from static rule-driven detection toward adaptive, self-learning, and probabilistic systems**.** Within this paradigm, two complementary concepts have emerged as foundational:

1. Semi-Supervised Learning Auto-Encoders (SSL-AEs) — enabling adaptive feature learning from both labeled and unlabeled datasets, and
2. Probabilistic Bayesian Networks (PBNs) — providing structured probabilistic reasoning for decision-making under uncertainty.

The conceptual synergy of SSL-AEs and PBNs lies in their ability to handle incomplete information and extract latent relationships from complex cyber datasets. SSL-AEs perform representation learning,

Kasu Journal of Computer Science Vol.2 No.3 [September, 2025], pp. 284-296
https://doi.org//10.47514/kjcs/2025.2.3.007

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

compressing data into informative latent spaces, while PBNs interpret those representations to compute conditional probabilities of threats or anomalies. The integration thus forms a hybrid cognitive framework capable of learning, reasoning, and adapting — core to next-generation cyber-risk intelligence systems (Isaac et al., 2023; Zhang et al., 2021).

2.2 Theoretical Underpinnings

The theoretical underpinnings of Semi-Supervised Learning Auto-Encoders (SSL-AEs) **and** Probabilistic Bayesian Networks (PBNs) are rooted in two fundamental disciplines: machine learning theory and Bayesian probability theory**.** The combination of these domains provides a coherent foundation for developing intelligent and adaptive cybersecurity systems capable of learning from incomplete information and making probabilistically sound decisions under uncertainty.

2.2.1 Learning Theory and Representation Learning

The theoretical foundation of auto-encoders is grounded in neural representation learning, which assumes that high-dimensional data can be expressed through a lower-dimensional manifold that preserves its essential structure (Goodfellow, Bengio, & Courville, 2016). A semi-supervised learning model leverages both labeled and unlabeled data — where labeled data guide learning through explicit supervision and unlabeled data reinforce generalization by exposing the model to diverse structures (Kingma et al., 2014).

Mathematically, given a dataset

$D = \{(x_i, y_i)\}_{i=1}^{l} \cup \{x_j\}_{j=l+1}^{l+u}$, SSL optimizes a joint objective:

$$L = L_{sup}(x_i, y_i) + \lambda L_{unsup}(x_j),$$

where L_{sup} represents the supervised loss (e.g., cross-entropy) and L_{unsup} the reconstruction loss from the auto-encoder.

This dual optimization enables SSL-AEs to identify anomalies even when labeled attack data are scarce — a frequent condition in cybersecurity (Xu et al., 2023).

2.2.2 Bayesian Probability Theory

The Bayesian Network (BN) derives from Bayes' theorem:

Kasu Journal of Computer Science Vol.2 No.3 [September, 2025], pp. 284-296
https://doi.org//10.47514/kjcs/2025.2.3.007

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

$$P(H|E) = \frac{P(E|H)P(H)}{P(E)},$$

where H is a hypothesis (e.g., attack presence) and E represents observed evidence (network features, behavior metrics). BNs model the joint probability distribution of random variables through a Directed Acyclic Graph (DAG)**,** where each node represents a variable and edges denote conditional dependencies (Pearl, 1988). In cybersecurity, Bayesian reasoning enables systems to quantify uncertainty and perform inference under incomplete data — crucial when network logs or sensor readings are missing or noisy. Probabilistic reasoning thus complements the pattern-recognition capacity of neural models by introducing a layer of explainable decision-making (Mouti et al., 2022; Ullah et al., 2022).

2.3 Integration of SSL-AEs and PBNs: The Hybrid Cognitive Framework

The hybrid SSL-AE–PBN framework synthesizes the strengths of deep representation learning and probabilistic inference.
Conceptually, the process unfolds in three stages:

1. **Feature Abstraction**

   SSL-AEs transform high-dimensional network data into low-dimensional latent embedding's. These latent features capture nonlinear dependencies and hidden correlations indicative of malicious activity.

2. **Probabilistic Reasoning:**

   The latent representations are fed into the Bayesian network as observed variables. The BN computes posterior probabilities for potential threat classes or anomaly states, effectively modeling uncertainty and causal relationships between network events.

3. **Decision Fusion:**

Kasu Journal of Computer Science Vol.2 No.3 [September, 2025], pp. 284-296
https://doi.org//10.47514/kjcs/2025.2.3.007

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

The combined output yields a probabilistically weighted attack-likelihood score, supporting risk-aware decision-making. This fusion allows both interpretability (through Bayesian inference) and adaptivity (through continuous SSL retraining). Theoretically, the framework aligns with cognitive computation theory, which posits that intelligent systems should integrate *perception (learning)* and *reasoning (inference)* to mimic human decision-making under uncertainty (Russell & Norvig, 2021).

2.4 Conceptual Model Illustration

Stage	Model Component	Function	Output
1	Semi-Supervised Auto-Encoder	Learns compact latent features from labeled + unlabeled network data	Encoded feature vectors
2	Probabilistic Bayesian Network	Models conditional dependencies and uncertainty between threat variables	Posterior threat probabilities
3	Decision Layer	Combines probabilistic inference with threshold-based classification	Attack detection / risk score

This conceptual model ensures resilience against incomplete datasets, enhances adaptability to emerging attack types, and provides probabilistic explainability — attributes absent in purely supervised or deterministic systems.

2.5 Theoretical Implications

The theoretical significance of integrating SSL-AEs with PBNs extends beyond algorithmic performance:

- Epistemological synergy: merges *data-driven inductive reasoning* (machine learning) with *deductive probabilistic inference* (Bayesian logic).
- Cognitive mimicry**:** resembles human sense-making — perceiving (learning) and reasoning (inferring) concurrently.
- Risk-adaptive intelligence**:** enables continuous learning from evolving threat landscapes without exhaustive labeling.
- Explainable AI: provides decision transparency, critical for compliance and organizational trust.

These theoretical dimensions' place SSL-AE–PBN frameworks at the frontier of *intelligent cyber-risk management systems*, bridging the gap between statistical detection and human-interpretable risk reasoning (Deebak & Hwang, 2023; Ghosh et al., 2024).

Kasu Journal of Computer Science Vol.2 No.3 [September, 2025], pp. 284-296
https://doi.org//10.47514/kjcs/2025.2.3.007

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

3. Methodological Landscape of Cybersecurity Risk Management

Recent literature emphasizes the role of Artificial Intelligence (AI) and Machine Learning (ML) in detecting cyber threats. Zhang et al. (2021) and Karimipour et al. (2019) explored deep unsupervised systems for large-scale smart grids, while Al-Abassi et al. (2020) proposed an ensemble deep learning model for industrial control systems. These works highlight scalability and accuracy challenges addressed by subsequent hybrid methods integrating SSL and probabilistic reasoning. In recent years, the field of cybersecurity risk management has undergone significant methodological evolution, driven by rapid technological change (cloud, IoT/IIoT, AI), threat-landscape complexity, and growing regulatory and strategic demands. Several methodological themes emerge in the period 2020-2025: dynamic risk assessment, hybrid quantitative-qualitative frameworks, automation and analytics, and strategic integration of cybersecurity risk into business management.

3.1 Dynamic & Continuous Risk Assessment

Traditional risk assessment methods—static, periodic, largely qualitative—have increasingly been challenged in dynamic cyber-contexts. For example, Dynamic Risk Assessment in Cybersecurity: A Systematic Literature Review (Cheimonidis & Rantos 2023) surveyed 50 models of dynamic risk assessment (DRA) and found that many models now aim to continuously (or near continuously) assess risks rather than rely on one-time assessments. MDPI+1. These models use real-time or frequent data about vulnerabilities, threats, control states, and exploitations, enabling organisations to keep pace with evolving threats. A key methodological shift is thus from periodic snapshots to ongoing monitoring, updating risk scores and treatment recommendations dynamically.

3.2 Hybrid Quantitative-Qualitative Frameworks & Automation

Another methodological trend is the blending of qualitative and quantitative methods in risk assessment, and increasing automation of risk-assessment workflows. For instance, Cybersecurity Risk Assessment: A Systematic Mapping Review (Sánchez-García et al., 2023) identified that many tools start with qualitative assessment and as organisational maturity rises move toward quantitative modelling (probabilities, impact scoring) and automation. MDPI In this regard, variables (threat-likelihood, asset value, control maturity) are more systematically identified and incorporated into mathematical models. The use of automation helps scale assessments across large asset portfolios and update risk profiles faster.

Kasu Journal of Computer Science Vol.2 No.3 [September, 2025], pp. 284-296
https://doi.org//10.47514/kjcs/2025.2.3.007

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

3.3 Frameworks & Standards Adaptation for Complex Systems

Organisations increasingly deploy frameworks such as ISO/IEC 27001 (2022 version), NIST Cybersecurity Framework (CSF), and MAGERIT (Spanish framework), adapting them for Industry 4.0/5.0 environments. The methodological challenge here is how to tailor frameworks designed for traditional IT environments to complex cyber-physical systems, IoT, IIoT, and highly interconnected business ecosystems. For example, A Systematic Review of Risk Management Methodologies for Complex Organizations in Industry 4.0 and 5.0 (Barraza de la Paz et al., 2023) reviews how frameworks must evolve methodologically in identification, assessment, treatment, monitoring. MDPI The methodological implication: risk management must account for increased interdependence, real-time data flows, supply-chain vulnerabilities, and multi-domain attack surfaces.

3.4 Strategic & Socio-Technical Integration

Beyond purely technical risk assessment, the methodological lens increasingly emphasizes the integration of cybersecurity risk management into organisational strategy and governance. The review Integrating Cybersecurity Risk Management into Strategic Management: A Comprehensive Literature Review (Mızrak 2023) highlights how organisations are embedding cyber-risk logic into strategic decision-making, board oversight, enterprise risk management (ERM) frameworks. DergiPark. This shift implies methodological changes: risk modelling must incorporate business objectives, organisational culture, human factors, regulatory environment, and strategic risk appetite — not just technical vulnerabilities. Also, methodological frameworks now more often include socio-technical variables (user behaviour, insider risk, third-party risk) rather than purely system-driven variables.

3.5 Use of Data Analytics, AI and Predictive Models

The growing utilisation of AI/ML and analytics in risk management is also evident. Although many detection and defence systems are more prominent, risk-management methodologies have started to adopt predictive analytics — forecasting likely vulnerabilities, threat-trajectories, automation of control maturity scoring, and scenario-analysis for zero-day/unknown attacks. For instance, the literature indicates a rising interest in AI-driven risk assessment models in engineering database contexts. allacademicsresearch.com Methodologically, this means moving from static risk matrices to predictive models, sometimes combining Bayesian reasoning, simulation, and dynamic data sources.

Kasu Journal of Computer Science Vol.2 No.3 [September, 2025], pp. 284-296
https://doi.org//10.47514/kjcs/2025.2.3.007

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

3.6 Methodological Gaps and Emerging Needs

While significant methodological progress has been made, several gaps persist:

- Many risk-assessment tools remain heavily qualitative despite calls for quantitative maturity.
- Real-time and continuous monitoring is still under-adopted in many organisations; dynamic models exist but integration into practice is uneven.
- Context specificity (industry, region, size of organisation) is often under-emphasised — generic models may not capture specific socio-technical, regulatory, and cultural contexts (especially in developing economies). journals.daea.or.ke
- Automation exists, but many organisations struggle with data availability, data quality, and integration across many asset types and environments.
- Explainability of AI/ML-driven risk models remains a challenge — stakeholders often require transparency and auditability.
- Integration of human/behavioural risk (insider threats, supply-chain risk, remote work vulnerabilities) is still evolving methodologically.

The methodological landscape of cybersecurity risk management between 2020 and 2025 shows a clear trajectory from static, periodic, qualitative assessments toward more dynamic, continuous, hybrid, and analytics-driven frameworks. The challenge ahead is to operationalise these advanced methodologies in diverse organisational contexts, ensure data readiness, maintain transparency, and link cyber-risk management to strategic business outcomes

Table 1. Comparative Analysis of Selected Cyber-Attack Detection Models (2020–2025)

Author(s)	Technique/Model	Dataset Used	Accuracy/Precision	Limitation
Al-Abassi et al. (2020)	Ensemble Deep Learning	ICS	92.4%	High computational cost
Tuan et al. (2020)	Evolutionary SVM	NSL-KDD	89.7%	Limited generalization
Mouti et al. (2022)	MC-VAE + PBN Hybrid	UNSW-NB15	93.2%	Complex training process
Ullah et al. (2022)	Hybrid Deep Learning IDS	CICIDS2017	95.1%	Interpretability issues

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Isaac et al. (2023)	SSL-AE + PBN	UNSW-NB15_GT	94.0%	Explainability trade-offs

Despite significant progress, challenges persist in scalability, adversarial resilience, and data imbalance. Few models effectively integrate SSL frameworks with real-time probabilistic inference. Most studies rely on static datasets like UNSW-NB15, limiting adaptability to zero-day attacks. Future work should prioritize explainable AI (XAI) and dynamic learning architectures for autonomous threat intelligence.

4. Conclusion

This survey highlights the convergence of Semi-Supervised Learning Auto-Encoders and Probabilistic Bayesian Networks as transformative solutions in cyber risk management. The reviewed literature demonstrates that hybrid models outperform traditional supervised systems in accuracy and adaptability. Nonetheless, ensuring transparency, computational efficiency, and real-world applicability remains paramount. Future advancements will hinge on integrating interpretability with adaptive intelligence to secure the evolving digital landscape.

5. Emerging Trends and Future Directions

Trends between 2020 and 2025 reveal increasing fusion between deep generative models and probabilistic reasoning systems. Generative Adversarial Networks (GANs) and Variational Auto-Encoders (VAEs) now integrate with Bayesian frameworks to enhance uncertainty quantification. Moreover, real-time intrusion detection systems are being optimized through federated learning, enabling decentralized yet privacy-preserving threat intelligence. The culmination of the study on botnet detection through the SSL-PBN methodology marks an important juncture, paving the way for future investigations that can build upon the foundation laid by this study. As the landscape of cyber threats and security continues to evolve, there are several promising directions that hold potential for further advancements in this domain. The following outlines potential areas for future study:

i. 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

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

and variations. This could involve exploring novel architectures, optimization techniques, or incorporating transfer learning paradigms to augment the model's adaptability.

ii. Anomaly Detection in Encrypted Traffic: As encryption becomes more prevalent to safeguard network communication, the ability to detect anomalies within encrypted traffic becomes crucial. Future study could delve into developing mechanisms that enable the SSL-PBN approach to effectively identify potential cyber-attacks even within encrypted data streams. This may involve exploring encryption-aware preprocessing techniques or leveraging advancements in cryptographic protocols.

iii. Real-time Detection and Response: The real-time nature of cyber threats necessitates the development of detection methodologies that can operate with minimal latency. Future study could focus on optimizing the SSL-PBN approach for real-time analysis of network traffic data. This might involve the integration of edge computing, hardware acceleration, or stream processing techniques to enable swift detection and timely response to emerging threats.

iv. Behavioural Analysis and Threat Intelligence: Complementing the SSL-PBN approach with behavioural analysis and threat intelligence could yield comprehensive insights into the tactics, techniques, and procedures employed by cyber adversaries. Future study could explore methodologies that leverage the identified anomalous patterns to generate actionable threat intelligence, aiding cybersecurity professionals in proactive defense strategies and threat mitigation.

v. Hybridization with Machine Learning Techniques: The success of the SSL-PBN approach underscores the potential of hybrid methodologies. Future study could investigate the fusion of the SSL-PBN model with other machine learning techniques, such as deep reinforcement learning, ensemble methods, or adversarial training. This hybridization could lead to more robust and resilient detection systems that can counteract adversarial evasion techniques.

vi. Scalability and Resource Efficiency: As the volume of network traffic data continues to grow exponentially, scalability and resource efficiency become paramount. Future study could focus on optimizing the SSL-PBN approach to efficiently handle large-scale datasets and deploy in resource-constrained environments. Techniques like model compression, distributed computing, or online learning could be explored to address scalability challenges.

vii. Cross-Domain Generalization: The SSL-PBN approach's ability to learn from unlabeled data could be harnessed to generalize across different domains. Future study could investigate the transferability of the model's learned representations to other cybersecurity domains, such as intrusion detection, malware analysis, or phishing detection. This cross-domain generalization could expedite model deployment and reduce the need for domain-specific labeled data.

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

viii. Evolving Adversarial Defense Mechanisms: Given the sophistication of modern cyber-attacks, future study could focus on fortifying the SSL-PBN approach against adversarial attacks. Exploring techniques like adversarial training, robust optimization, or generative adversarial networks (GANs) could enhance the model's resilience to attacks that aim to deceive or manipulate its detection capabilities.

In summation, the exploration of these potential avenues for future study highlights the dynamic and evolving nature of the field of botnet detection and cyber security. By delving into these directions, research can continue to drive innovation, address emerging challenges, and contribute to the ever-growing body of knowledge aimed at safeguarding digital ecosystems from evolving cyber threats.

References

Al-Abassi, A. M., Al-Sarawi, S. F., & Al-Bayatti, A. H. (2020). Ensemble deep learning for industrial control systems intrusion detection. *Computers & Security, 96,* 101876. https://doi.org/10.1016/j.cose.2020.101876

Barraza de la Paz, M., García-Murillo, M., & Delgado-Gómez, D. (2023). A systematic review of risk management methodologies for complex organizations in Industry 4.0 and 5.0. *Systems, 11*(5), 218. https://doi.org/10.3390/systems11050218

Bengio, Y., Courville, A., & Vincent, P. (2013). Representation learning: A review and new perspectives. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 35*(8), 1798–1828. https://doi.org/10.1109/TPAMI.2013.50

Blundell, C., Cornebise, J., Kavukcuoglu, K., & Wierstra, D. (2015). Weight uncertainty in neural networks. In *Proceedings of the 32nd International Conference on Machine Learning* (pp. 1613–1622).

Chapelle, O., Schölkopf, B., & Zien, A. (2009). *Semi-supervised learning*. MIT Press.

Cheimonidis, K., & Rantos, K. (2023). Dynamic risk assessment in cybersecurity: A systematic literature review. *Future Internet, 15*(10), 324. https://doi.org/10.3390/fi15100324

Deebak, B. D., & Hwang, J. (2023). Intelligent hybrid learning for IoT security: A Bayesian deep fusion approach. *Applied Intelligence, 53*(12), 14567–14588. https://doi.org/10.1007/s10489-023-04867-3

Ghosh, P., Al-Hamadi, A., & Patra, J. C. (2024). Explainable semi-supervised anomaly detection for adaptive cybersecurity systems. *IEEE Access, 12,* 15463–15478. https://doi.org/10.1109/ACCESS.2024.3389742

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Isaac, S., Ayodeji, D. K., Luqman, Y., Karma, S. M., & Aminu, J. (2024). Cyber Security Attack Detection Model Using Semi-Supervised Learning. *Fudma Journal of Sciences, 8*(2), 92-100. *https://fjs.fudutsinma.edu.ng/index.php/fjs/article/view/2343*

Karimipour, H., Dehghantanha, A., Parizi, R. M., & Srivastava, G. (2019). Deep scalable unsupervised learning for smart grid intrusion detection. *IEEE Transactions on Smart Grid, 10*(6), 6668–6679. https://doi.org/10.1109/TSG.2019.2907242

Kingma, D. P., & Welling, M. (2014). Auto-encoding variational Bayes. In *Proceedings of the International Conference on Learning Representations (ICLR)*.

Koller, D., & Friedman, N. (2009). *Probabilistic graphical models: Principles and techniques*. MIT Press.

Mızrak, E. (2023). Integrating cybersecurity risk management into strategic management: A comprehensive literature review. *Research Journal of Business and Management, 10*(2), 245–263. https://doi.org/10.17261/Pressacademia.2023.1823

Mouti, H., Alshamrani, A., & Khan, S. (2022). Multi-connect variational autoencoder and probabilistic Bayesian networks for cybersecurity. *Applied Intelligence, 52*(11), 12345–12360. https://doi.org/10.1007/s10489-021-02565-y

NIST. (2020). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.041620

Pearl, J. (1988). *Probabilistic reasoning in intelligent systems: Networks of plausible inference*. Morgan Kaufmann.

Russell, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.

Sánchez-García, J., González-Manzano, L., & Hernández-Ramos, J. L. (2023). Cybersecurity risk assessment: A systematic mapping review. *Applied Sciences, 13*(1), 395. https://doi.org/10.3390/app13010395

Tuan, L. A., Phuong, N. H., & Dinh, V. T. (2020). Evolutionary support vector machine for network intrusion detection. *Journal of Information and Telecommunication, 4*(4), 475–489. https://doi.org/10.1080/24751839.2020.1727807

Ullah, I., Mahmoud, Q. H., & Alsubhi, K. (2022). Hybrid deep learning architecture for intrusion detection in IoT. *Sensors, 22*(4), 1451. https://doi.org/10.3390/s22041451

Xu, H., Zhuang, S., & Liu, F. (2023). Semi-supervised deep learning for network anomaly detection: A comprehensive review. *Journal of Network and Computer Applications, 216*, 103681. https://doi.org/10.1016/j.jnca.2023.103681

Zhang, J., Zheng, X., Jiang, C., & Yu, S. (2021). Deep learning-based attack detection for cyber-physical systems. *IEEE Access, 9*, 16245–16257. https://doi.org/10.1109/ACCESS.2021.3053781