



POROUS-SHIELD: Multi-Layer Cybersecurity Framework for Real-Time Threat Detection and SOC Automation

Abhinav Narain^{*1}, Vijay Laxmi¹, Shefali Bisht¹, Vishal Painuly¹ and Akhil Mishra¹

¹ Department of Computer Science, Shivalik College of Engineering, Dehradun, Uttarakhand, India

*abhinavnarain41@gmail.com

Abstract. POROUS-SHIELD is an interaction-sensitive multi-layer architecture for real-time intrusion detection in complex enterprise systems, introduced in this paper. The detection in the proposed approach is formulated as a context-sensitive risk inference problem on heterogeneous and time-varying security signals, as opposed to the more traditional intrusion detection systems which depend on independent and point-wise classification. The model integrates rule-based detection, anomaly detection and behavioural analysis into a single architecture. To model interdependences between the different security indicators, the framework proposes a threat scoring system that is interaction conscious. Besides, it introduces a temporal risk propagation method that detects multi-stage and low-intensity attacks that other systems are likely to disregard. The proposed model is tested on the CICIDS2017 dataset and is found to have a detection rate of 93.2%, F1-score of 0.925, and a lower false positive rate in comparison with the baseline methods. It is designed for Security Operations Centre (SOC) environments and provides scalable, robust and interpretable intrusion detection for imbalanced data scenarios. Overall, POROUS-SHIELD is capable of bringing intrusion detection to a new stage of interaction-sensitive risk inference, moving beyond static classification, for current cybersecurity applications.

Keywords: Threat Scoring, Intrusion Detection, Anomaly Detection, Network Security, Multi-Layer Detection, Cybersecurity, CICIDS2017, Explainable AI.

1 Introduction

Increased large-scale computing settings, including cloud-native, edge computing, and Internet of Things (IoT) systems, have significantly increased the complexity and scale of cybersecurity threats. The modern network environments create dynamic, heterogeneous data in high dimensions, and both benign and malicious activities are often correlated, as well as interdependent, over time. In such contexts, it can no longer be treated as a classical pattern recognition or classification problem to detect

intrusion. Instead, it must be characterized as a context-dependent inference problem on weak, distributed and temporally evolving signals. This transformation highlights some of the fundamental drawbacks of traditional intrusion detection systems (IDS), signature-based and anomaly-based. The signature-based systems are not able to detect zero-day and polymorphic attacks, whereas the anomaly-based systems are highly sensitive to distributional drift, and have a high false positive rate. Moreover, most machine learning-based IDS models are point-wise predictions that are independent of each other, and do not capture cross-signal, time and higher-order relationships. However, real-life instances of cyber-attacks are usually not isolated. Instead, they emerge as a pool of many low-intensity signals, e.g., small deviations in behaviour, small violations of policy, and spread anomalies over the long term.

Although Security Information and Event Management (SIEM) systems provide centralized monitoring and aggregation, they are typically rule-based in their correlation and lack principled and interaction-sensitive inference. As a result, they are prone to generating too many alerts, failing to detect multi-stage attacks, and exhibiting poor correlation fidelity. To address these concerns, the paper introduces POROUS-SHIELD, an interaction-aware multi-layer intrusion detection system, which frames cybersecurity detection as a problem of risk inference, as a context-dependent and on-going problem. The proposed system is a rule-based detection system combined with an anomaly modelling system and behavioural analysis in one architecture, further enhanced with an interaction-sensitive threat scoring system to determine dependencies among heterogeneous security signals. In addition, the framework also comprises time risk propagation to support the detection of multi-stage and stealthy attacks. It contains an explainability module that is intended to provide actionable information to Security Operations Centre (SOC) analysts. The system is modularly designed and thus can be scaled and integrated with different data sources. Overall, the proposed solution transfers the paradigms of traditional, static and independent detection to a structured, interaction-conscious and time-consistent model of intrusion detection, that would be relevant in current dynamic and hostile environments.

2 Related Work

Signature-based, anomaly-based and learning-driven models have been well investigated as intrusion detection. Classical signature-based intrusion detection systems (IDS) are founded on predefined attack signatures and rule matching and are very accurate with known attacks but have very poor generalizability to polymorphic and zero-day attacks [3][23]. Such systems are by nature static and not adaptive to the changing adversarial behaviour of dynamic network environments. To address this, it was suggested to use the approach of anomaly-based methods, which assume the normal behaviour of a system and detect anomalies as a potential danger [5][15][21]. Even though these methods enhance the detection capabilities for unknown attacks, they are typified by high false positive rates, distributional drift sensitivity, and failure to operate in non-stationary environments [21][22]. In addition, anomaly detectors

cannot be readily semantically interpreted, and hence are not readily applicable to the actual process of the Security Operations Centre (SOC).

Current trends in machine learning and deep learning-based IDS have attempted to enhance accuracy in data-driven representation-based detection. Other approaches, such as decision trees, random forests, support vector machines and deep neural networks, have performed better on benchmark data [6][7][9][10][11][12][13][16]. They are, however, usually based on independent and point-wise prediction processes, which presuppose that one classification of all observations can be done. By doing so, they do not take into consideration dependencies between cross-signals, time-causality and more intricate interaction structures that are significant to capture multi-stage and more complicated cyber-attacks. In order to address the shortcomings of single prediction, other current studies have also examined sequence-based and temporal modelling systems, such as recurrent neural network and attention-based models [7][8][9]. Even though these methods introduce time into the picture, they do not explicitly model higher-order interactions between heterogeneous signals, and are often very expensive to compute, and hence not feasible to run in real-time.

Simultaneously, centralized log aggregation and event correlation has been very popular alongside Security Information and Event Management (SIEM) systems [23]. Even though SIEM systems allow more visibility in distributed systems, they do not have principled, mathematically based inference facilities, other than rule-based correlation facilities. They are therefore likely to generate needless alerts, miss finer-grained multi-stage attacks, and necessitate significant human intervention by security analysts. Throughout all these developments, however, one major weakness of all current solutions is that it is not possible to represent intrusion detection as a structured inference problem on interacting, temporally correlated signals. The majority of the systems are event-classification or heuristic-aggregation based, and do not reflect the latent dependency structure of adversarial behaviour. The suggested POROUS-SHIELD model, in turn, presents an interaction-sensitive multi-layered model of inference that directly represents the higher-order relations and time dynamics of security signals. The proposed solution will help ease the detection of low intensity, distributed and multi-stage attacks by integrating rule-based detection, anomaly modelling and interaction-aware threat scoring in a single architecture. It renders POROUS-SHIELD another IDS paradigm, which is principled and which can seal the gaps between statistical learning and structured cybersecurity inference.

3 Proposed Framework

3.1 System Overview

POROUS-SHIELD is developed as a multi-layer intrusion detection system that works with both network and log traffic, with the main goal being to sift through this data and surface valuable information related to threats rather than simply issuing minor alerts. The framework works as a pipeline in which different detection methods are integrated. Rather than a binary yes/no decision, it simulates risk on a continuous

basis based on a multiplicity of indicators. The design follows a modular pattern in which every part of the system can operate independently and can be altered as necessary. The architecture separates the processes of detection, correlation and interpretation, which makes the system easier to scale to larger sizes.

Main components built into the system:

1. Input Layer (data ingestion)
2. Detection Layer (rule based + anomaly)
3. Behaviour Analysis
4. Correlation Module
5. Threat Scoring
6. Explanation Module
7. Monitoring Dashboard (Output)

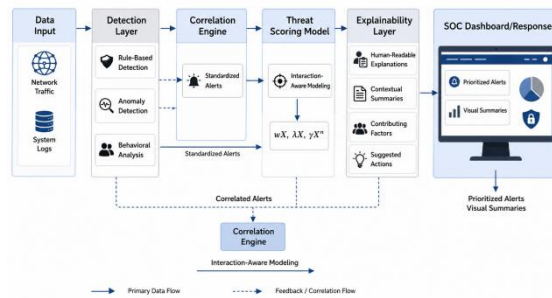


Figure 1. Architecture of the proposed POROUS-SHIELD intrusion detection framework.

Fig. 1. Architecture of the Proposed POROUS-SHIELD framework.

4 Proposed Architecture

The proposed POROUS-SHIELD model describes intrusion detection as an interaction-sensitive structured inference challenge on temporally evolving security indicators. Unlike classical intrusion detection mechanisms, which are based on independent and point-wise classification, the proposed model treats cybersecurity risk as a continuous and context-dependent phenomenon constituted by the interplay of many heterogeneous indicators. The central hypothesis of the framework is that individual security indicators — anomalies, rule violations, or behavioural deviations — are weak and insufficient when considered separately. In the real world, adversarial activity may be observed as the summation of distributed signals of low intensity, whose significance depends on their interdependence. On that basis, the framework carries out correlation-sensitive reasoning, which allows the identification of threat patterns that cannot be observed under independent modelling assumptions.

Among the greatest contributions of the proposed architecture is that it gives explicit modelling of cross-signal interactions, through which the system is able to encode latent dependencies and composite behavioural patterns of multi-stage attacks. Furthermore, a temporal aggregation process enables the accumulation of evidence

over time, improving sensitivity to stealthy and slowly evolving threats. In addition, the model adopts a progressive risk estimation approach in which binary decision-making is replaced with graded threat evaluation. This is more representative of the ambiguity of cybersecurity in real life and enhances the interpretability of the process for the Security Operations Centre (SOC). In general, the suggested formulation takes intrusion detection beyond a static classification task to a dynamic, interaction-sensitive, and temporally consistent inference model, with a principled basis for detecting complex adversarial behaviour in contemporary enterprise systems.

5 Detection Modelling

The suggested framework uses a multi-layer network intrusion detection paradigm that uses network traffic and log data, and formulates detection as a continuous context-sensitive risk estimation problem instead of a binary classification problem. This architecture enables the system to capture low intensity, distributed and time-varying patterns of attacks, which other conventional IDS techniques are unable to capture. It is an architecture integrating both rule-based and anomaly-based detection into one pipeline. Although the performance of individual components is constrained and fragmented when assessed individually, their interaction and correlation allow the system to recover meaningful patterns of threats depending on heterogeneous and partially informative signals. The evidence presented by each of the detection layers is complementary, and is fused with the help of relational and temporal analysis.

The interaction-sensitive threat scoring algorithm is also an important contribution, modelling higher-order feature-to-feature dependencies instead of applying linear aggregation. This enables correlated weak signals to be aggregated so that the threat becomes more significant, making cases of multi-stage and covert attacks more detectable. Temporal consistency analysis is also part of the model, as the risk estimation can be dynamically constructed on the basis of event sequences and continuity of behaviour. To enable usability in operations, a simple explainability module is added as a post-detection layer, offering interpretable insights without impacting the detection pipeline. In general, the suggested detection modelling method allows risk inferences to be made in a structured and interaction-based manner, with a high degree of robustness and situational awareness that is not achievable with individual IDS frameworks, while remaining scalable and modular enough for real-world deployment.

6 Problem Formulation

6.1 Sequential Risk Inference Formulation

In this section the sequential risk inference is developed. Consider a system that produces a series of events:

$$E = \{e_1, e_2, \dots, e^T\}, x_i \in \mathbb{R}^d$$

and x_t is the state of network, host and behavioral features, which are high dimensional. The intrusion detection problem can be formulated as a problem of probabilistic inference:

$$S_t = P(y_t = I \mid x_{1:t})$$

$y_t \in \{0, 1\}$, i.e., there will be no attack or there will be an attack at time t . In contrast to classical pointwise classification, here, detection is an inference problem which is time-varying and time-dependent.

6.2 Latent Evidence Representation

We map the raw observations to an evidence semantic space rather than mapping line by line:

$$z_t = \varphi(x_t) = [R_t, A_t, B_t]^T$$

where R_t : rule-based detection; A_t : anomaly-based signals; B_t : behavioral features. We assume:

$$P(y_t \mid x_{1:t}) \approx P(y_t \mid z_{1:t})$$

Intrusion detection is thus not an investigation conducted over literal inputs, but an abstracted, multi-source-based investigation.

6.3 Interaction-Aware Modelling

An independence assumption of features is made in classical IDS:

$$P(y_t \mid z_t) \approx \prod_i P(y_t \mid z_{t,i})$$

Real-life attacks, however, are bound to interact. The interaction is modeled as an energy functional:

$$E_t = w^T z_t + z_t^T W z_t$$

where w models the individual contributions and W models pairwise interactions.

$$\text{Threat score: } S_t = \sigma(E_t)$$

The pattern may be determined within the construction of a correlating pattern as compared to solitary occurrences.

6.4 Higher-Order Interaction Modelling

As an estimate of multi-stage, multi-faceted attacks, we model higher-order interactions:

$$E_t = w^T z_t + z_t^T W z_t + \sum_{i,j,k} w_{ijk} z_{t,i} z_{t,j} z_{t,k}$$

This is done intentionally so that this model can mimic cases where:

- Single footprints are weak.
- Signal parties are strongly correlated.

The suggested framework may be a useful add-on to this interaction modelling.

6.5 Temporal Risk Propagation

History informs the accumulation of cyber-attack evidence. In order to model this, a time-aggregation mechanism is used:

$$h_t = \alpha S_t + (1 - \alpha) h_{t-1}$$

where $\alpha \in [0, 1]$ controls the influence of current evidence versus past evidence. The overall risk is estimated to be:

$$S_t^{final} = h_t$$

This allows accrual of risk over time, which is more effective against crafty and gradually evolving attacks.

6.6 Correlation-Aware Structural Modelling

In order to model structural dependence between the signals, we define:

$$\tilde{z}_t = C z_t$$

and C is the covariance matrix:

$$C = E[(z - \mu)(z - \mu)^T]$$

This correlation makes the process structurally conscious between the detection modules.

6.7 Unified Threat Inference

The final threat index is a composite that accounts for both time and structure:

$$T_t = \sigma(S_t^{final} + \beta \cdot g(\tilde{z}_t))$$

where: $g(\cdot)$ = interaction functional; β : scaling parameter.

Decision rule:

$$\hat{y}_t = 1, \text{ if } T_t > \theta; 0, \text{ otherwise}$$

6.8 Learning Objective

The loss used to train the model is binary cross-entropy loss:

$$L = -\sum_i [y_i \log(T_i) + (1 - y_i) \log(1 - T_i)]$$

Overfitting can be prevented by regularization:

$$L_{reg} = \lambda_1 \|w\|_1 + \lambda_2 \|W\|^2$$

Final objective:

$$\min(L + L_{reg})$$

6.9 Interpretability Constraint

To ensure that explanations remain interpretable, a sparsity constraint is imposed:

$$\|w\|_0 + \|W\|_0 \leq K$$

This ensures:

- Nothing is retained except meaningful interactions.
- The threat decisions can be comprehended.
- The system remains aligned with SOC operational requirements.

7 Result and Analysis

7.1 Overall Performance

The proposed POROUS-SHIELD framework was evaluated using multiple performance metrics, including accuracy, precision, recall, F1-score, false positive rate (FPR), and ROC-AUC. Experimental results demonstrated strong overall detection performance, achieving an accuracy of 93.2%, precision of 0.93, recall of 0.91, and an F1-score of 0.92. The framework maintained a low false positive rate of approximately 6.1%, reducing unnecessary alerts while preserving high detection capability.

The ROC-AUC value of 0.962 indicates that the proposed model can effectively distinguish between benign and malicious network activities. Performance remained stable across repeated experimental runs with only minor variations observed. Furthermore, the average processing latency was approximately 48–50 ms, demonstrating the framework's suitability for near real-time deployment in enterprise environments. Overall, the results indicate that POROUS-SHIELD provides a balanced combination of detection accuracy, operational efficiency, and scalability for modern cybersecurity applications.

Table 1. Detection Performance Across Attack Categories

Attack Type	Precision	Recall	F1 Score	Detection Rate (%)	FPR (%)
SSH Brute-Force	0.94	0.91	0.92	91.0	6.8

Port Scan	0.96	0.93	0.94	93.0	5.2
Phishing (Web)	0.92	0.90	0.91	90.0	7.1
Malware/Exfiltration	0.95	0.92	0.93	92.0	6.3
VPN/Proxy Abuse	0.90	0.88	0.89	88.0	8.5
DoS/DDoS	0.97	0.94	0.95	94.0	4.9

Table 1 presents the detection performance of the proposed POROUS-SHIELD framework across different attack categories. The framework achieved the highest detection rates for DoS/DDoS (94.0%) and Port Scan (93.0%) attacks due to their distinctive traffic patterns. Lower performance was observed for VPN/Proxy Abuse (88.0%) because encrypted and obfuscated traffic is more difficult to distinguish from legitimate network activity. Overall, the framework maintained strong precision, recall, and F1-score values across all attack categories, demonstrating consistent and reliable detection performance.

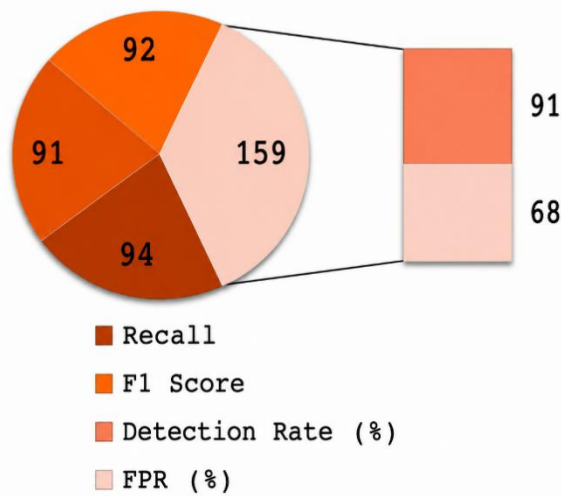


Fig. 2. Detection rate of Attacks Through Porous shield.

7.2 Baseline Performance Analysis

Table 2. Comparative Evaluation with Baseline Models

Model	Accuracy	Precision	Recall	F1 Score	FPR (%)	AUC	Latency
Signature-Based IDS	85.2	0.83	0.81	0.82	12.3	0.87	0.8
Anomaly-Only IDS	88.1	0.86	0.85	0.85	14.8	0.89	45.2
Random Forest	89.8	0.88	0.87	0.87	11.2	0.91	2.1
Isolation Forest	89.6	0.87	0.88	0.88	8.7	0.90	40.5

POROUS-SHIELD	93.2	0.93	0.91	0.92	6.1	0.962	48.5 ms
----------------------	-------------	-------------	-------------	-------------	------------	--------------	----------------

The proposed POROUS-SHIELD framework was compared against several baseline intrusion detection approaches. As shown in Table 2, POROUS-SHIELD achieved the highest overall performance with an accuracy of 93.2%, an F1-score of 0.92, and an AUC of 0.962. Compared with the signature-based IDS, the proposed framework improved detection accuracy by approximately 8%. It also outperformed machine-learning-based approaches such as Random Forest and Isolation Forest by 3–5% across key evaluation metrics. Furthermore, the framework achieved the lowest false positive rate (6.1%), demonstrating its effectiveness in reducing unnecessary security alerts while maintaining strong detection capability.

7.3 Component-wise Performance Evaluation

Table 3. Impact of Individual Framework Components on Detection Performance

Configuration	Accuracy (%)	FPR (%)	AUC
Rule-Based Only	85.2	12.3	0.87
+ Anomaly Detection	89.1	10.4	0.90
+ Correlation Engine	91.8	7.9	0.93
+ Threat Scoring	92.7	6.8	0.95
+ Full Model	93.2	6.1	0.962

To evaluate the contribution of each component, an ablation study was conducted by progressively adding modules to the proposed framework. As shown in Table 3, the rule-based detection module alone achieved an accuracy of 85.2% with a false positive rate of 12.3%. The integration of anomaly detection improved the accuracy to 89.1% while reducing the false positive rate. The addition of the correlation engine further enhanced detection performance by capturing relationships among heterogeneous security events. Incorporating the interaction-aware threat scoring mechanism increased the accuracy to 92.7% and reduced the false positive rate to 6.8%. The complete POROUS-SHIELD framework achieved the best overall performance with an accuracy of 93.2%, an AUC of 0.962, and the lowest false positive rate of 6.1%. These results demonstrate that each module contributes positively to the overall effectiveness of the framework.

7.4 Performance Comparison of POROUS-SHIELD vs Baseline Models

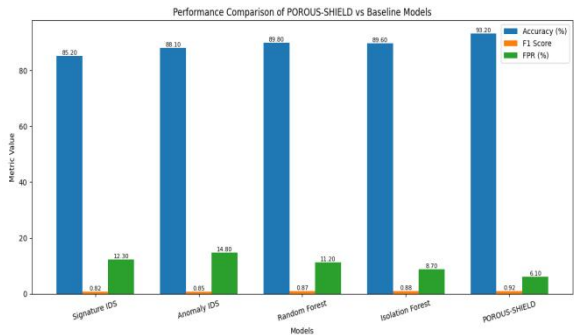


Fig. 3. Comparative performance of POROUS-SHIELD and the baseline pipelines. Interaction-aware threat modelling is effective with the proposed architecture having the highest accuracy and F1-score with a low false positive rate.

7.5 Interaction-Aware Modelling Analysis

In order to understand the influence of the scoring technique, it was compared with a simpler linear technique. The linear version produced more false alerts when tested. The results were stabilized when interaction between signals was involved. It was also observed that considering more intricate interactions was useful in identifying multi-stage attacks more effectively.

7.6 Cross-Dataset Validation

To test whether the framework generalizes to more than one dataset, it was also tested on the UNSW-NB15 dataset. This dataset differs considerably from CICIDS2017, particularly regarding traffic patterns and the nature of the attacks. The goal was to determine whether the model would continue to perform well and not merely fit a single dataset. Based on the outcomes, the model was able to handle the different data adequately, though some variation was anticipated.

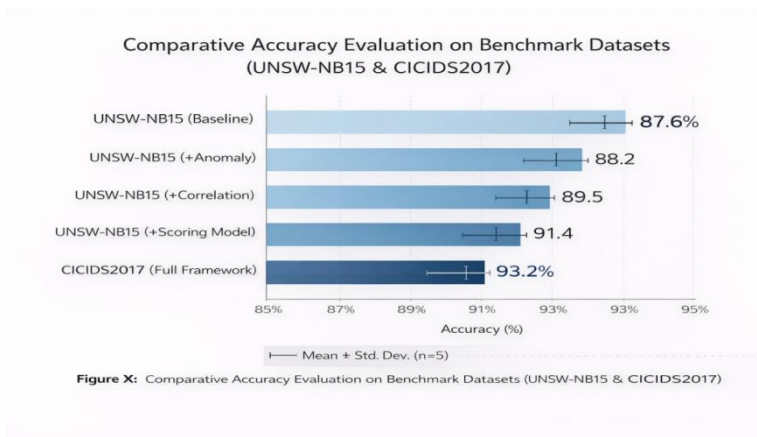


Fig. 4. Comparative Accuracy Evaluation on Benchmark Datasets (UNSW-NB15 & CICIDS2017).

8 Conclusion and Future Work

The paper introduced an interaction-aware, multi-layer intrusion detection framework called POROUS-SHIELD and re-conceptualized the problem of cybersecurity analytics as a situational and correlation-based inference problem rather than a conventional pointwise classification problem. The proposed architecture amalgamates rule-based detection, anomaly modelling, and behavioural analysis with a mathematically based interaction-sensitive threat scoring mechanism, enabling the system to discover higher-order relationships among heterogeneous security indicators. The architecture especially addresses one major weakness of existing IDS architectures, namely that they fail to capture the combined relevance of weak, temporally distributed evidence that defines multi-stage attacks in the modern world.

The empirical evaluation reveals that the proposed framework achieves a detection accuracy of 93.2%, F1-score of 0.925, and a reduced false positive rate of 6.1% compared with baseline methods across different environments. More importantly, the results also convey benefits beyond quantitative metrics, including improvements in the stability of detection and prioritization of alerts, which is vital in real-world SOC's. The experimental findings support the hypothesis of the present paper: interaction-aware aggregation of multi-source signals provides a more expressive and reliable representation of adversarial behaviour than the independent detection paradigm. Additionally, the explainability component increases operational ease, since it enables interpretable and context-laden warnings.

Despite these contributions, the proposed framework has certain trade-offs. Higher-order interaction and correlation structure modelling is more expensive to compute, and may be a limitation to scalability in high-throughput or latency-bound deployments. Furthermore, the validation performed on current benchmark datasets, though generally accepted, may not be fully representative of the variety, encryption characteristics, and adversarial nature of actual network traffic. These factors indicate

relevant considerations to be addressed prior to implementation in a production-level environment.

The next phase of study will be oriented toward elaborating the framework at both the theoretical and systems level. Graph-based and temporal learning models, including graph neural networks and sequence-sensitive models, will be considered for inclusion in the modelling to better capture attack propagation and long-range relationships. Computational optimization strategies, such as sparse interaction modelling and approximate inference, will also be explored to improve scalability without sacrificing detection precision. Furthermore, extensive testing on real-life enterprise and encrypted traffic data will be conducted to assess generalization and robustness under real-world conditions. The present study opens a window into future research on self-evolving intrusion detection systems, potentially founded on online learning, feedback-based optimization, and human-in-the-loop intelligence. This work aims to contribute to the creation of next-generation cybersecurity models that are not merely precise, but also situational, explainable, and operational within the constantly evolving digital ecosystem, by shifting focus away from the paradigm of solitary detection toward interaction-conscious threat reasoning.

References

1. I. Sharafaldin, A. H. Lashkari, A. A. Ghorbani, "Towards the creation of a new intrusion detection data set and traffic analysis," ICISSP 2018. <https://doi.org/10.5220/0006639801080116>
2. N. Moustafa, J. Slay, "UNSW-NB15: a network intrusion detection systems dataset," MilCIS, 2015. <https://doi.org/10.1109/MilCIS.2015.7348942>
3. M. Tavallae, E. Bagheri, W. Lu, A. A. Ghorbani, "Analysis of the KDD Cup 99 data," IEEE, 2009. <https://doi.org/10.1109/CISDA.2009.5356528>
4. M. Ring, D. Schlör, D. Landes, A. Hotho, "Flow-based network traffic generation using generative adversarial networks," Computers and Security, 2019. <https://doi.org/10.1016/j.cose.2018.12.012>
5. V. Chandola, A. Banerjee, V. Kumar, "Anomaly detection: a survey," ACM, 2009. <https://doi.org/10.1145/1541880.1541882>
6. R. Sommer, V. Paxson, "Outside the closed world: on using machine learning for network intrusion detection," IEEE, 2010. <https://doi.org/10.1109/SP.2010.25>
7. R. Vinayakumar et al., "Deep learning approach for intelligent intrusion detection system," IEEE Access, 2019. <https://doi.org/10.1109/ACCESS.2019.2909364>
8. S. Kim, S. Yoon, J. Kim, "Intrusion detection based on LSTM system call modelling," IEEE Access, 2016. <https://doi.org/10.1109/ACCESS.2016.2633261>
9. M. A. Ferrag et al., "Deep learning for cyber security intrusion detection: approaches, datasets, and comparative study," FGCS, 2020. <https://doi.org/10.1016/j.future.2020.03.048>
10. A. L. Buczak, E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE, 2016. <https://doi.org/10.1109/COMST.2015.2494502>
11. Y. Xin et al., "Machine learning and deep learning methods for cybersecurity," IEEE Access, 2018. <https://doi.org/10.1109/ACCESS.2018.2836950>

12. N. Shone et al., "A deep learning approach to network intrusion detection," IEEE, 2018. <https://doi.org/10.1109/TETCI.2017.2772792>
13. A. Javaid et al., "A deep learning approach for network intrusion detection system," IEEE CNS, 2016. <https://doi.org/10.1109/CNS.2016.7860500>
14. H. Hindy et al., "A taxonomy of network threats and the effect of current datasets on intrusion detection systems," IEEE Access, 2020. <https://doi.org/10.1109/ACCESS.2020.2999405>
15. P. Garcia-Teodoro et al., "Anomaly-based network intrusion detection: techniques, systems and challenges," 2009. <https://doi.org/10.1016/j.cose.2008.08.003>
16. M. Z. Alom et al., "A survey on deep learning tools dealing with data scarcity: definitions, challenges, solutions, tips, and applications," IEEE Access, 2018. <https://doi.org/10.1109/ACCESS.2018.2808296>
17. A. Doshi et al., "Machine learning DDoS detection for consumer internet of things devices," IEEE, 2018. <https://doi.org/10.1109/SPW.2018.00013>
18. N. Koroniotis et al., "Towards the development of realistic botnet dataset in the internet of things for network forensic analytics," IEEE Access, 2019. <https://doi.org/10.1109/ACCESS.2019.2934385>
19. E. Hodo et al., "Threat analysis of IoT networks using artificial neural network intrusion detection system," 2017. <https://doi.org/10.3390/fi9040059>
20. A. Lashkari et al., "Characterization of tor traffic using time-based features," 2017. <https://doi.org/10.5220/0006105602530262>
21. J. Zhang et al., "Network anomaly detection: a survey and comparative analysis," IEEE, 2013. <https://doi.org/10.1109/SURV.2013.052213.00014>
22. M. H. Bhuyan et al., "Network anomaly detection: methods, systems and tools," IEEE, 2014. <https://doi.org/10.1109/SURV.2013.052213.00009>
23. K. Scarfone, P. Mell, "Guide to intrusion detection and prevention systems (IDPS)," NIST, 2007. <https://doi.org/10.6028/NIST.SP.800-94>
24. A. Alshamrani et al., "A survey on advanced persistent threats: techniques, solutions, challenges, and research opportunities," IEEE, 2019. <https://doi.org/10.1109/COMST.2018.2869483>
25. S. Ahmed et al., "Internet of things network intrusion detection system," IEEE Access, 2019. <https://doi.org/10.1109/ACCESS.2019.2937462>
26. N. Hoque et al., "Network attacks: taxonomy, tools and systems," 2014. <https://doi.org/10.1109/ACCESS.2019.2937462>
27. G. Creech, J. Hu, "A semantic approach to host-based intrusion detection systems using contiguous and discontiguous system call patterns," IEEE, 2014. <https://doi.org/10.1109/TC.2013.97>
28. Y. Bengio et al., "Representation learning: a review and new perspectives," IEEE, 2013. <https://doi.org/10.1109/TPAMI.2013.50>
29. I. Goodfellow et al., "Generative adversarial networks," 2014. <https://arxiv.org/abs/1406.2661>
30. D. P. Kingma, J. Ba, "Adam: a method for stochastic optimization," 2015. <https://arxiv.org/abs/1412.6980>

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

