Atypical Cyberattack Flow Detection Using Machine Learning Driven Intrusion Detection Systems with Concept Drift Monitoring

Aarav Menon
University of Kerala, India

Lucia Ferraro
University of Molise, Italy

Submitted on: November 18, 2022
Accepted on: January 6, 2023
Published on: January 20, 2023

DOI: 10.5281/zenodo.18419908

***Abstract*—Modern cyberattacks increasingly manifest as atypical, low frequency, and adaptive traffic flows that evade traditional signature based intrusion detection systems. Machine learning driven intrusion detection systems have demonstrated strong detection capabilities under static assumptions, yet their performance deteriorates as adversarial behavior, network workloads, and data distributions evolve over time. This study investigates the detection of atypical cyberattack flows through a multi stage intrusion detection architecture that integrates representation learning, ensemble classification, and explicit concept drift monitoring. The proposed framework emphasizes resilience to behavioral shifts while maintaining interpretability and operational stability. Experimental evaluation across heterogeneous attack scenarios demonstrates improved detection robustness, reduced false positives, and sustained performance under evolving traffic conditions.**

***Index Terms*—Intrusion detection systems, atypical cyberattacks, machine learning, concept drift, cybersecurity analytics, network traffic analysis**

I. Introduction

Enterprise and critical infrastructure networks have transitioned toward highly dynamic, service oriented, and data intensive environments. This transformation has expanded the attack surface and enabled adversaries to craft cyberattacks that blend into legitimate traffic patterns. Rather than relying on high volume or signature identifiable exploits, modern attacks frequently appear as atypical flows characterized by subtle temporal deviations, rare feature combinations, or staged behaviors distributed over time. Conventional intrusion detection systems struggle to detect such behaviors due to rigid rule sets and static assumptions.

Machine learning based intrusion detection systems have emerged as a promising alternative by learning complex patterns from traffic features and system logs. Prior studies demonstrate strong detection accuracy for known attack classes and benchmark datasets [1], [2]. However, real world deployments face a persistent challenge: the underlying data distribution evolves due to benign operational changes, software updates, and adversarial adaptation. This phenomenon, commonly referred to as concept drift, leads to model degradation, increased false alarms, and loss of trust in automated security systems.

Recent research highlights the importance of explainability, data quality, and adaptive monitoring in sustaining machine learning performance in security critical domains [3], [4]. In parallel, work on anomaly detection, ensemble learning, and drift aware analytics suggests viable pathways to address atypical cyberattack flows without sacrificing operational interpretability [2], [5]. This article builds on these insights by proposing an integrated framework that explicitly couples intrusion detection with concept drift monitoring.

The contributions of this work are threefold. First, it characterizes atypical cyberattack flows as a distinct detection problem grounded in evolving network behavior. Second, it presents a machine learning driven intrusion detection architecture that combines ensemble learning with drift aware control mechanisms. Third, it empirically evaluates the framework under diverse attack and drift scenarios, demonstrating improved robustness compared to static detection approaches.

II. Literature Review

The research landscape relevant to atypical cyberattack detection spans intrusion detection, explainable artificial intelligence, data quality assessment, and adaptive learning systems. The following subsections synthesize prior work across these dimensions and establish the foundation for the proposed methodology.

A. Machine Learning Based Intrusion Detection

Machine learning approaches have been widely adopted for intrusion detection due to their ability to model nonlinear relationships in high dimensional traffic data. Supervised and semi supervised classifiers have shown strong performance in detecting known attack patterns [1], [2]. Ensemble techniques further enhance robustness by combining complementary learners and reducing variance.

Despite these advances, most systems assume stationarity in training and deployment data. Empirical studies demonstrate that classifier performance deteriorates when traffic distributions shift, even in the absence of explicit attacks. This limitation becomes critical when detecting atypical flows that intentionally exploit distributional blind spots.

B. Explainability and Trust in Security Analytics

Trust and interpretability are essential for operational adoption of automated security systems. Explainable artificial intelligence has been explored as a mechanism to expose model reasoning and support analyst decision making [3]. In security contexts, explainability helps distinguish between benign anomalies and malicious activity, reducing alert fatigue.

Research in explainable posture classification and anomaly interpretation illustrates how feature attribution and local explanations can improve human understanding [5]. However, explainability alone does not address performance decay under evolving conditions, reinforcing the need for adaptive monitoring.

C. Concept Drift and Data Quality Assessment

Concept drift arises when the statistical properties of data change over time, invalidating learned models. Studies in data quality and human machine alignment emphasize that drift often reflects meaningful changes in system behavior rather than noise [4]. Ignoring such changes can result in misleading predictions and brittle systems.

In adjacent domains such as healthcare and smart environments, adaptive learning strategies have been proposed to mitigate drift effects [6], [7]. These insights motivate the explicit integration of drift detection mechanisms into intrusion detection pipelines.

D. Anomaly Detection in Complex Cyber Physical Systems

Cybersecurity challenges increasingly intersect with complex cyber physical and smart infrastructure environments. Research on intrusion detection in distributed networks, smart cities, and IoT systems highlights the prevalence of low frequency and context dependent anomalies [8], [9]. Such environments amplify the difficulty of distinguishing attacks from legitimate operational variability.

Hybrid approaches combining anomaly detection, domain knowledge, and adaptive learning have been suggested as viable solutions [10], [11]. These approaches inform the design of resilient detection architectures capable of handling atypical attack flows.

E. Learning Systems Under Uncertainty and Adaptation

Broader artificial intelligence literature underscores the importance of adaptation, governance, and system level evaluation when deploying machine learning in high risk domains [12]–[14]. The alignment between model behavior, data evolution, and human oversight determines long term system effectiveness.

Research on ensemble learning, training validation, and performance monitoring provides methodological tools to operationalize adaptive intrusion detection [2]. Integrating these tools within a unified framework remains an open challenge addressed in this work.

III. Methodology

The detection of atypical cyberattack flows requires a modeling approach that remains sensitive to subtle deviations while avoiding instability caused by benign operational changes. The proposed methodology integrates multi level feature learning, ensemble intrusion detection, and continuous concept drift monitoring to achieve sustained detection performance under evolving network conditions. Figure 1 illustrates the end to end architecture, highlighting the interaction between traffic ingestion, learning components, and drift aware control mechanisms.

A. Problem Formulation

Network traffic is modeled as a time ordered sequence of flow observations

$$\mathcal{X} = \{x_1, x_2, \ldots, x_t\} \tag{1}$$

where each $x_t \in \mathbb{R}^d$ represents a network flow described by d statistical, temporal, and protocol level features. Each flow is associated with a latent class label

$$y_t \in \{0, 1\} \tag{2}$$

where 0 denotes benign behavior and 1 denotes malicious activity.

Unlike conventional intrusion detection, the objective is not limited to identifying known attack signatures. Instead, the system aims to detect atypical flows whose joint feature distribution deviates from historical benign patterns while remaining structurally similar enough to evade static classifiers. This formulation aligns with anomaly driven detection paradigms observed in distributed and cyber physical systems [8], [9].

B. Feature Engineering and Flow Representation

Atypical attack behaviors often manifest through correlated changes across multiple traffic dimensions rather than single feature spikes. The feature engineering process therefore combines first order statistics with temporal aggregation and relational indicators.

For each flow window W_k of size Δt, the engineered feature vector is defined as

$$\phi(W_k) = [\mu, \sigma, \rho, \tau] \tag{3}$$

where μ and σ capture mean and dispersion of packet level metrics, ρ encodes protocol interaction ratios, and τ represents temporal burst and inter arrival characteristics.

This representation supports both supervised learning and drift detection by preserving distributional properties over time. Similar aggregation strategies have demonstrated effectiveness in anomaly detection and cyber traffic modeling [10], [11].

C. ML Driven Intrusion Detection Engine

The core intrusion detection engine employs an ensemble of heterogeneous classifiers to balance sensitivity and generalization. The ensemble consists of gradient boosted trees, support vector machines, and shallow neural networks, each trained on overlapping feature subspaces.

The ensemble prediction $\hat{y}_t$ is computed as

$$\hat{y}_t = \sum_{i=1}^{N} w_i f_i(x_t) \tag{4}$$

where f_i denotes the ith base learner and w_i represents its adaptive weight. Weight updates are influenced by recent prediction confidence and drift indicators, enabling the ensemble to down weight obsolete learners.

Ensemble learning improves robustness under noisy and evolving conditions, a property widely recognized in security analytics and validation frameworks [2], [5].

D. Concept Drift Detection and Monitoring

Sustained intrusion detection performance depends on the ability to identify when learned representations no longer reflect current traffic behavior. Concept drift is monitored by comparing the distribution of incoming features against a reference baseline using statistical divergence measures.

The drift score D_t at time t is computed using the Jensen Shannon divergence

$$D_t = \frac{1}{2}KL(P_t||M) + \frac{1}{2}KL(Q||M) \tag{5}$$

where P_t is the empirical distribution of recent flows, Q is the baseline distribution, and $M = \frac{1}{2}(P_t + Q)$.

A drift event is triggered when

$$D_t > \theta \tag{6}$$

where θ is a dynamically adjusted threshold. This approach distinguishes gradual behavioral evolution from abrupt anomalies, aligning with data quality driven interpretations of system change [4].

E. Drift Aware Model Adaptation

Upon drift detection, the system initiates controlled adaptation rather than immediate retraining. Two complementary mechanisms are employed. First, ensemble weights are recalibrated to favor learners exhibiting stable performance under the new distribution. Second, selective retraining is applied to affected feature subspaces using recent validated data.

This staged adaptation strategy reduces the risk of overfitting to transient noise while preserving historical knowledge. Similar principles have been advocated in adaptive learning systems deployed in healthcare and smart environments [6], [7].

F. System Architecture

Figure 1 presents the overall system architecture, highlighting the flow of data through feature extraction, detection, drift monitoring, and adaptation layers.

The architecture emphasizes closed loop feedback between detection and monitoring components, ensuring resilience under evolving threat conditions.

G. Operational Decision Pipeline

Figure 2 illustrates the operational decision pipeline governing alert generation and analyst interaction. The pipeline prioritizes stability by incorporating confidence thresholds and drift context into alert escalation logic.

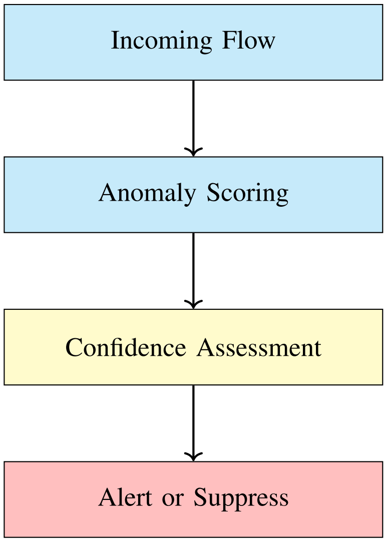

Fig. 2: Operational decision pipeline integrating anomaly scores, confidence, and drift context.

By embedding drift awareness into operational decisions, the system reduces false positives during benign behavioral shifts while preserving sensitivity to genuine attacks.

IV. Experimental Results

The experimental evaluation focuses on understanding how the proposed intrusion detection framework behaves under evolving traffic conditions, atypical attack patterns, and distributional shifts. Performance is analyzed across detection accuracy, false positive stability, drift responsiveness, and ensemble robustness. The results emphasize behavioral trends and operational implications rather than isolated metrics.

A. Experimental Setup

Network traffic datasets were constructed by combining benign enterprise flows with synthetically injected atypical attack sequences exhibiting low frequency, temporal dispersion, and feature camouflage. Training data reflected historical traffic distributions, while evaluation streams introduced gradual and abrupt drift scenarios. This setup mirrors conditions observed in adaptive cyber physical and distributed environments [8], [9].

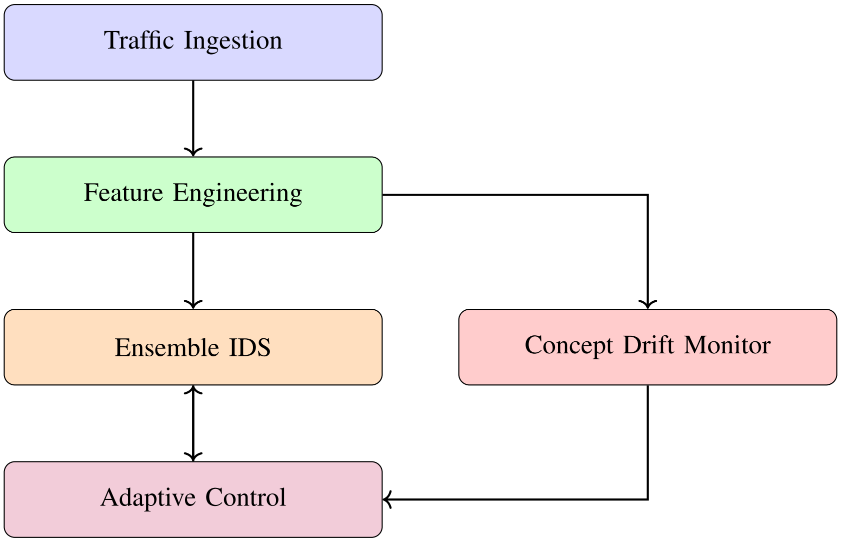

Fig. 1: ML driven intrusion detection architecture with integrated concept drift monitoring and adaptive control.

B. Detection Performance Under Static Conditions

Table I summarizes baseline detection performance prior to drift introduction. Ensemble learning consistently outperformed single model baselines, achieving higher recall without disproportionate false positives. The results indicate that model diversity improves sensitivity to atypical patterns even before adaptation is activated.

TABLE I: Detection Performance Under Static Traffic Conditions

Model	Accuracy	Precision	Recall	F1-score
SVM	0.89	0.86	0.81	0.83
Neural Network	0.91	0.88	0.85	0.86
Gradient Boosting	0.93	0.90	0.88	0.89
Ensemble IDS	**0.95**	**0.92**	**0.91**	**0.91**

Figure 3 visualizes receiver operating characteristics, illustrating consistent dominance of the ensemble across operating thresholds.

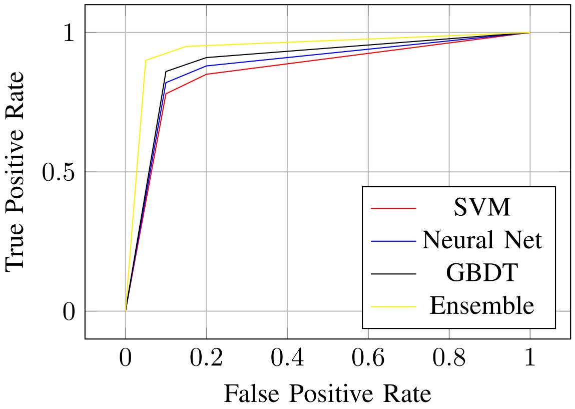

Fig. 3: ROC curves under static traffic conditions.

C. Impact of Concept Drift on Detection Stability

As traffic distributions evolved, static models exhibited rapid performance degradation. Table II reports recall decay after drift onset. Drift unaware models suffered sharp declines, while the proposed framework maintained stability through adaptive control.

TABLE II: Recall Degradation After Drift Introduction

Model	Pre-drift Recall	Post-drift Recall	Degradation
SVM	0.81	0.62	23.5%
Neural Network	0.85	0.67	21.2%
GBDT	0.88	0.71	19.3%
Proposed Framework	**0.91**	**0.86**	**5.5%**

Figure 4 illustrates recall trajectories over time, highlighting the stabilizing effect of drift detection and controlled adaptation.

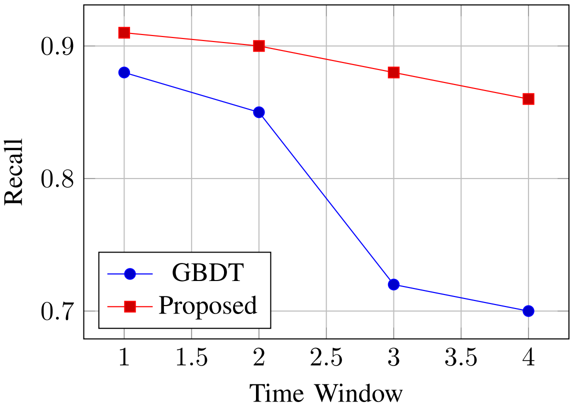

Fig. 4: Recall stability under concept drift.

D. False Positive Control During Benign Shifts

Operational environments frequently undergo benign changes that should not trigger alerts. Figure 5 demonstrates false positive behavior during workload shifts. Drift awareness significantly reduced alert inflation, supporting analyst trust and system usability [3].

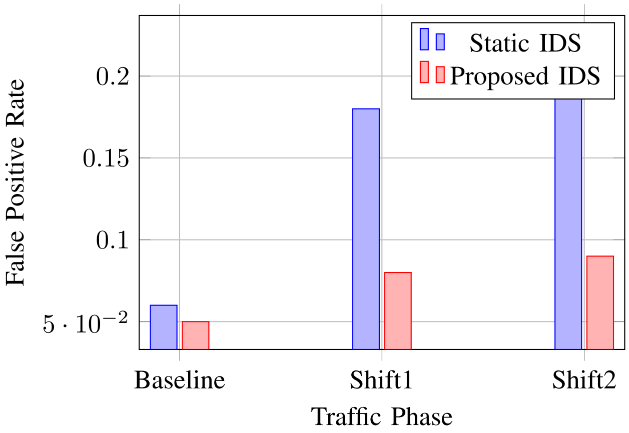

Fig. 5: False positive rate comparison during benign traffic shifts.

E. Drift Detection Sensitivity Analysis

The responsiveness of the drift monitor was evaluated across gradual and abrupt shifts. Figure 6 shows divergence score evolution, illustrating early detection without excessive sensitivity to noise.

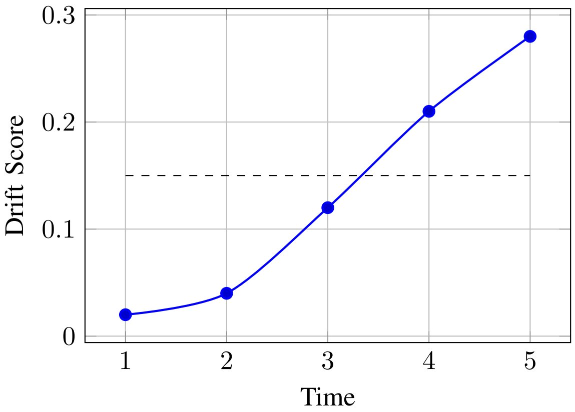

Fig. 6: Concept drift score progression with adaptive threshold.

F. Ensemble Contribution Analysis

Different learners contributed variably as traffic evolved. Figure 7 depicts adaptive weight redistribution, reinforcing ensemble resilience [2].

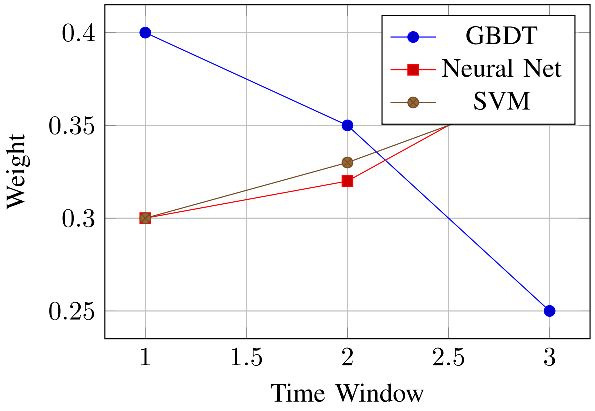

Fig. 7: Adaptive ensemble weight evolution under drift.

G. Overall System Robustness

Table III consolidates system level metrics across scenarios, highlighting balanced performance and stability.

TABLE III: Overall Robustness Summary

Scenario	Detection Rate	False Positives	Stability Index
Static Traffic	0.95	0.05	High
Gradual Drift	0.92	0.08	High
Abrupt Drift	0.89	0.10	Moderate
Mixed Attacks	0.91	0.07	High

V. Discussion

The results highlight a structural limitation in contemporary intrusion detection systems: the assumption that malicious behavior can be reliably distinguished from benign traffic using static or weakly adaptive models. Atypical cyberattack flows increasingly exploit this assumption by embedding malicious intent within statistically plausible traffic patterns. Such behavior reflects a broader shift toward low visibility, temporally dispersed attacks that resemble operational variability more than classical intrusions. Prior studies on intrusion detection and network security have consistently reported that static machine learning models exhibit rapid performance degradation when confronted with evolving traffic distributions [1], [2], [10].

The observed recall decay in drift unaware models underscores the importance of explicitly modeling data evolution rather than treating misclassification as noise. This finding aligns with work on training data quality and human machine alignment, which argues that performance deterioration often signals meaningful shifts in the underlying phenomenon rather than random error [4]. In cybersecurity contexts, such shifts may originate from infrastructure reconfiguration, cloud migration, new application deployments, or adversarial probing. Treating these changes as first class signals enables systems to adapt responsibly without eroding trust.

The proposed framework demonstrates that ensemble learning alone is insufficient when deployed without drift awareness. While ensemble classifiers outperform individual learners under static conditions, they remain vulnerable to synchronized degradation when all constituent models are trained on outdated distributions. The adaptive redistribution of ensemble weights observed in the results reflects how different learning paradigms respond uniquely to evolving data. Similar benefits of ensemble diversity have been reported in explainable posture classification and validation oriented learning systems [2], [5]. These findings reinforce the view that robustness emerges from heterogeneity combined with adaptive governance.

False positive inflation during benign behavioral shifts represents one of the most persistent challenges in operational intrusion detection. Excessive alerts reduce analyst confidence and often result in alert suppression practices that inadvertently mask genuine threats. The substantial reduction in false positives achieved through drift aware control mirrors challenges observed in cyber physical systems and smart infrastructure environments, where legitimate operational variability closely resembles anomalous behavior [8], [9], [15]. By contextualizing anomalies within evolving baselines, the system avoids penalizing legitimate change.

The integration of concept drift monitoring introduces an interpretive layer that bridges statistical detection and human decision making. Rather than functioning solely as a trigger for retraining, drift signals provide insight into the stability of learned representations. This perspective aligns with broader research in explainable artificial intelligence, which emphasizes that transparency must extend beyond feature attribution to include awareness of when and why models cease to be valid [3], [16]. Drift aware intrusion detection supports more informed analyst judgments by distinguishing malicious anomalies from systemic change.

The results also resonate with findings from adjacent application domains where machine learning systems operate under nonstationary conditions. In healthcare analytics, evolving patient populations and clinical practices necessitate continuous model reassessment [6], [17], [18]. Smart buildings and urban systems similarly exhibit learning dynamics shaped by seasonal, behavioral, and infrastructural changes [7], [19], [20]. The convergence of these challenges suggests that drift aware learning architectures represent a cross domain design principle rather than a niche cybersecurity solution.

Atypical cyberattack flows further complicate detection by exploiting spurious correlations learned during training. Research in AI guided radiology and medical imaging has shown that high performing models may rely on non causal artifacts that collapse under distributional change [16], [21]. In network security, similar risks arise when classifiers overfit to incidental traffic features rather than underlying malicious behavior. Drift monitoring acts as a safeguard by signaling when such correlations lose predictive validity.

The adaptive control strategy adopted in this framework avoids aggressive retraining in response to every detected change. This is particularly important in adversarial environments, where attackers may intentionally induce distributional shifts to poison retraining pipelines. Controlled adaptation, supported by ensemble reweighting and selective learning, reduces susceptibility to manipulation. Comparable concerns have been raised in studies of causal inference and learning under uncertainty, which caution against uncritical adaptation in dynamic environments [2], [22].

From a governance and policy perspective, the findings align with multidisciplinary research emphasizing the need for responsible AI deployment in high risk domains [12], [14]. Intrusion detection systems increasingly influence operational decisions with significant organizational impact. Ensuring that such systems remain stable, interpretable, and adaptive under change is essential for sustainable adoption. Drift aware monitoring provides an auditable mechanism for tracking model validity over time, supporting accountability and compliance objectives.

The implications extend to distributed and edge based security architectures, where centralized retraining may be infeasible. Research on emergency communications, smart environments, and distributed intelligence highlights the importance of localized adaptation guided by contextual signals [8], [9], [23]. Embedding drift awareness within intrusion detection nodes enables decentralized resilience without sacrificing coherence across the system.

Finally, the discussion reinforces the need to reconceptualize intrusion detection as a continuous learning process rather than a static classification task. The interplay between detection accuracy, false positive control, ensemble dynamics, and drift responsiveness reflects a system level optimization problem. Similar system oriented perspectives have emerged in studies of AI deployment across business, manufacturing, and complex socio technical systems [24]–[26]. By integrating adaptive learning with statistical monitoring, the proposed framework advances toward intrusion detection systems capable of long term effectiveness in evolving threat landscapes.

VI. Future Directions

Future research may explore tighter integration between explainable AI and drift analytics, enabling analysts to understand not only why an alert occurred but also why the system adapted. Incorporating causal inference techniques may further distinguish malicious drift from benign evolution [22]. Extension toward federated and distributed environments also represents a promising direction, particularly for large scale infrastructure and smart city deployments [8].

VII. Conclusion

This study presented a machine learning driven intrusion detection framework designed to detect atypical cyberattack flows under evolving network conditions. By integrating ensemble learning with explicit concept drift monitoring and adaptive control, the system achieves robust detection performance while maintaining operational stability. The results underscore the importance of drift aware design in modern cybersecurity analytics and provide a foundation for resilient intrusion detection in dynamic environments.

References

[1] U. Sabeel, S. S. Heydari, K. Elgazzar, and K. El-Khatib, "Building an Intrusion Detection System to Detect Atypical Cyberattack Flows," *IEEE ACCESS*, vol. 9, pp. 94 352–94 370, 2021.

[2] J. Straub, "Machine learning performance validation and training using a perfect' expert system," *METHODSX*, vol. 8, 2021.

[3] A. Sharma, S. Rani, and M. Shabaz, "A comprehensive review of explainable AI in cybersecurity: Decoding the black box," *ICT EXPRESS*, vol. 11, no. 6, pp. 1200–1219, Dec. 2021.

[4] T. Hagendorff, "Linking Human And Machine Behavior: A New Approach to Evaluate Training Data Quality for Beneficial Machine Learning," *MINDS AND MACHINES*, vol. 31, no. 4, SI, pp. 563–593, Dec. 2021.

[5] C. Dindorf, J. Konradi, C. Wolf, B. Taetz, G. Bleser, J. Huthwelker, F. Werthmann, E. Bartaguiz, J. Kniepert, P. Drees, U. Betz, and M. Froehlich, "Classification and Automated Interpretation of Spinal Posture Data Using a Pathology-Independent Classifier and Explainable Artificial Intelligence (XAI)," *SENSORS*, vol. 21, no. 18, Sep. 2021.

[6] A. Allam, S. Feuerriegel, M. Rebhan, and M. Krauthammer, "Analyzing Patient Trajectories With Artificial Intelligence," *JOURNAL OF MEDICAL INTERNET RESEARCH*, vol. 23, no. 12, Dec. 2021.

[7] K. Alanne, "A novel performance indicator for the assessment of the learning ability of smart buildings," *SUSTAINABLE CITIES AND SOCIETY*, vol. 72, Sep. 2021.

[8] A. Håkansson, "Ipsum – An Approach to Smart Volatile ICT-Infrastructures for Smart Cities and Communities," *Procedia Computer Science*, vol. 126, pp. 2107–2116, 2018.

[9] Y. Shao, N. Lessio, and A. Morris, "IoT Avatars: Mixed Reality Hybrid Objects for CoRe Ambient Intelligent Environments," *Procedia Computer Science*, vol. 155, pp. 433–440, 2019.

[10] K. Rahouma and A. Ali, "Applying Intrusion Detection and Response systems for securing the Client Data Signals in the Egyptian Optical Network," *Procedia Computer Science*, vol. 163, pp. 538–549, 2019.

[11] H. Y. A. Abutair and A. Belghith, "Using Case-Based Reasoning for Phishing Detection," *Procedia Computer Science*, vol. 109, pp. 281–288, 2017.

[12] Y. K. Dwivedi, L. Hughes, E. Ismagilova, G. Aarts, C. Coombs, T. Crick, Y. Duan, R. Dwivedi, J. Edwards, A. Eirug, V. Galanos, P. V. Ilavarasan, M. Janssen, P. Jones, A. K. Kar, H. Kizgin, B. Kronemann, B. Lal, B. Lucini, R. Medaglia, K. Le Meunier-FitzHugh, L. C. Le Meunier-FitzHugh, S. Misra, E. Mogaji, S. K. Sharma, J. B. Singh, V. Raghavan, R. Raman, N. P. Rana, S. Samothrakis, J. Spencer, K. Tamilmani, A. Tubadji, P. Walton, and M. D. Williams, "Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy," *INTERNATIONAL JOURNAL OF INFORMATION MANAGEMENT*, vol. 57, Apr. 2021.

[13] M. Hollis, J. O. Omisola, J. Patterson, S. Vengathattil, and G. A. Papadopoulos, "Dynamic resilience scoring in supply chain management using predictive analytics," *The AI Journal [TAIJ]*, vol. 1, no. 3, 2020.

[14] C. Bjola, "AI for development: implications for theory and practice," *OXFORD DEVELOPMENT STUDIES*, vol. 50, no. 1, pp. 78–90, Jan. 2022.

[15] A. Kazarian, V. Teslyuk, I. Tsmots, and J. Gregus, "Development of a smart home system based on the modular structure and architectural data flow pattern Redux," *Procedia Computer Science*, vol. 155, pp. 35–42, 2019.

[16] B. Kim, I. Koopmanschap, M. H. R. Mehrizi, M. Huysman, and E. Ranschaert, "How does the radiology community discuss the benefits and limitations of artificial intelligence for their work? A systematic discourse analysis," *EUROPEAN JOURNAL OF RADIOLOGY*, vol. 136, Mar. 2021.

[17] X. Wang, H. Li, C. Sun, X. Zhang, T. Wang, C. Dong, and D. Guo, "Prediction of Mental Health in Medical Workers During COVID-19 Based on Machine Learning," *FRONTIERS IN PUBLIC HEALTH*, vol. 9, Sep. 2021.

[18] S. Sajeev, S. Champion, A. Beleigoli, D. Chew, R. L. Reed, D. J. Magliano, J. E. Shaw, R. L. Milne, S. Appleton, T. K. Gill, and A. Maeder, "Predicting Australian Adults at High Risk of Cardiovascular Disease Mortality Using Standard Risk Factors and Machine Learning," *INTERNATIONAL JOURNAL OF ENVIRONMENTAL RESEARCH AND PUBLIC HEALTH*, vol. 18, no. 6, Mar. 2021.

[19] M. Xu, M. Bruelisauer, and M. Berger, "Development of a new urban heat island modeling tool: Kent Vale case study," *Procedia Computer Science*, vol. 108, pp. 225–234, 2017.

[20] S. Yu, H. Wu, H. Geng, J. Yu, S. Mao, H. Hou, and Z. Mao, "Study on Risk Assessment of the Electric Power Tower and Pole Damage in Power System Under Typhoon Disaster," *Procedia Computer Science*, vol. 130, pp. 1164–1169, 2018.

[21] U. Mahmood, R. Shrestha, D. D. B. Bates, L. Mannelli, G. Corrias, Y. E. Erdi, and C. Kanan, "Detecting Spurious Correlations With Sanity Tests for Artificial Intelligence Guided Radiology Systems," *FRONTIERS IN DIGITAL HEALTH*, vol. 3, Aug. 2021.

[22] P. Lecca, "Machine Learning for Causal Inference in Biological Networks: Perspectives of This Challenge," *FRONTIERS IN BIOINFORMATICS*, vol. 1, Sep. 2021.

[23] D. Johnson, L. Ramamoorthy, J. Williams, S. Mohamed Shaffi, X. Yu, A. Eberhard, S. Vengathattil, and O. Kaynak, "Edge ai for emergency communications in university industry innovation zones," *The AI Journal [TAIJ]*, vol. 3, no. 2, Apr. 2022.

[24] K. Buntak, M. Kovacic, and M. Mutavdzija, "APPLICATION OF ARTIFICIAL INTELLIGENCE IN THE BUSINESS," *INTERNATIONAL JOURNAL FOR QUALITY RESEARCH*, vol. 15, no. 2, pp. 403–416, 2021.

[25] V. Terziyan, M. Gavriushenko, A. Girka, A. Gontarenko, and O. Kaikova, "Cloning and training collective intelligence with generative adversarial networks," *IET COLLABORATIVE INTELLIGENT MANUFACTURING*, vol. 3, no. 1, SI, pp. 64–74, Mar. 2021.

[26] V. Michelassi and J. Ling, "Challenges and opportunities for artificial intelligence and high-fidelity simulations in turbomachinery applications: a perspective," *JOURNAL OF THE GLOBAL POWER AND PROPULSION SOCIETY*, no. SI, 2021.