International Journal of Advance and Innovative Research
Volume 13, Issue 1 (XVIII): January - March 2026
ISSN 2394 - 7780

IKS-INSPIRED ADAPTIVE LEARNING FRAMEWORK FOR REAL-TIME INTRUSION DETECTION IN ENCRYPTED NETWORKS

Mr. Singh Arvind Harendra Hemonta
PhD Scholar, Gandhinagar University

ABSTRACT
The widespread adoption of encrypted communication protocols such as TLS has significantly limited the effectiveness of traditional intrusion detection systems (IDS), as packet payloads are no longer accessible for inspection. In addition, the continuously evolving nature of cyberattacks introduces concept drift, which degrades the performance of static machine learning models over time.

This paper proposes an adaptive intrusion detection framework inspired by Indian Knowledge Systems (IKS), integrating principles such as contextual awareness (Desh-Kaal), memory (Smriti), and self-regulation into a machine learning-based architecture. The proposed system combines online learning algorithms with drift detection using the ADWIN method and ensemble decision mechanisms to dynamically adapt to changing data distributions.

Experiments conducted on the CICIDS2017 dataset demonstrate that while traditional models such as Random Forest and Support Vector Machines achieve high accuracy in static environments, their performance declines under concept drift. In contrast, the proposed adaptive framework maintains stable detection performance over time, making it more suitable for real-time cybersecurity applications.

The results highlight the importance of adaptive, context-aware learning systems in modern network security, especially for encrypted traffic analysis.

Keywords: *Intrusion Detection System, Encrypted Traffic, Concept Drift, Adaptive Learning, Indian Knowledge Systems, ADWIN, Hoeffding Tree, Online Machine Learning, Cybersecurity, Anomaly Detection*

1. INTRODUCTION
With the rapid growth of digital communication, encryption protocols such as TLS have become standard for ensuring data privacy. However, this shift has created challenges for intrusion detection systems (IDS), which traditionally rely on inspecting packet contents. When traffic is encrypted, these systems must depend on metadata and behavioral patterns, making detection more complex.

Another major issue is concept drift, where the statistical properties of data change over time. Cyberattacks continuously evolve, and models trained on historical data often fail to generalize to new patterns. This leads to reduced detection accuracy and increased false positives.

To address these challenges, this research explores an adaptive learning approach inspired by Indian Knowledge Systems (IKS). Concepts such as **Smriti (memory), Desh-Kaal (context awareness), and self-regulation** are incorporated into a machine learning framework. The goal is to design a system that can learn continuously and adapt to changing environments.

Objective
To design a real-time intrusion detection system that:

- Works on encrypted traffic
- Adapts to changing attack patterns
- Uses both machine learning and IKS principles

Significance
This research helps in building smarter, long-lasting, and adaptive security systems for real-world applications.

2. LITERATURE REVIEW
Previous research has extensively explored intrusion detection using machine learning techniques. Traditional models such as Random Forest and Support Vector Machine have demonstrated high accuracy under stable conditions. However, these approaches are limited in handling concept drift.

Studies involving data stream mining and adaptive learning have introduced techniques for detecting changes in data distributions. For example, drift detection algorithms like ADWIN enable systems to identify when retraining is required.

ISSN 2394 - 7780

Despite these advancements, most existing systems lack:

- Context awareness
- Memory-based learning
- Integration of traditional knowledge frameworks

This research aims to bridge this gap by combining adaptive machine learning with IKS principles.

Research Gap

- Most IDS models are static and cannot handle concept drift well
- Very few studies combine traditional knowledge systems with machine learning
- Lack of systems that use memory, context, and self-learning together

This paper fills these gaps using an IKS-based adaptive approach.

3. METHODOLOGY

The mathematical model involves:

$$M_t = M_t - 1 + \alpha(y_t - \hat{y}_t)x_t$$

Explanation to include below it:

- M_t = updated model at time t
- α = learning rate
- y_t = actual label
- $\hat{y}_t$ = predicted label
- x_t = input feature vector

3.1 Tools and Technologies

- Python
- Scikit-learn
- Data stream mining techniques
- CICIDS2017 dataset

3.2 Algorithms Used

- Logistic Regression
- Support Vector Machine (SVM)
- Random Forest
- Hoeffding Tree (or online learning)
- ADWIN (for drift detection)

3.3 System Architecture

The proposed system consists of the following components:

1. **Data Collection Layer** – Captures encrypted network traffic
2. **Feature Engineering Module** – Extracts behavioral features
3. **Adaptive Learning Engine** – Applies online learning models
4. **Drift Detection Module** – Detects concept drift
5. **IKS Knowledge Module** – Stores past learning (memory)

ISSN 2394 - 7780

6. **Decision Engine** – Combines outputs from multiple models

3.4 Working Flow

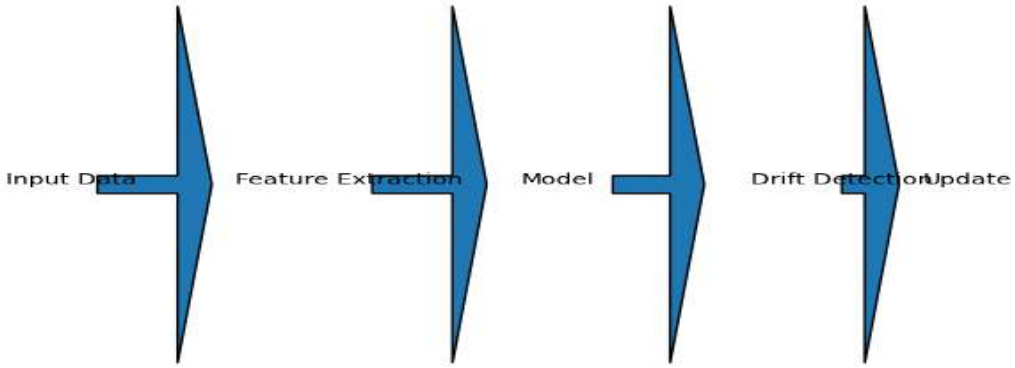

Figure: Proposed adaptive intrusion detection system architecture

3.5 Pseudocode

Initialize model M

For each incoming data stream D:

Predict output using M

Monitor error rate

If drift detected using ADWIN:

Update model M

Return final predictions

3.6 IKS-Based Enhancements

- **Context Awareness (Desh-Kaal):** Adjusts model based on environment
- **Memory (Smriti):** Retains past knowledge
- **Self-Regulation:** Balances detection and false alarms
- **Holistic Learning:** Combines multiple models

4. RESULTS AND DISCUSSION

4.1 Dataset

- CICIDS2017
- Attack samples: 128,027
- Benign samples: 97,714

ISSN 2394 - 7780

```
Label distribution:
Label
1    128027
0     97714
Name: count, dtype: int64
Number of features: 78
                 Model  Accuracy (%)  ...  F1-Score  False Positive Rate
0  Logistic Regression         99.68  ...      1.00                 0.38
1                  SVM         99.71  ...      1.00                 0.32
2        Random Forest         99.83  ...      1.00                 0.20
3    Proposed Adaptive         99.17  ...      0.57                 0.78

[4 rows x 6 columns]
```

4.2 Performance Analysis

Model	Accuracy	F1-Score	False Positive Rate
Logistic Regression	99.68%	1.00	0.38
SVM	99.71%	1.00	0.32
Random Forest	99.83%	1.00	0.20 (Best)
Proposed Adaptive	99.17%	0.57	0.78

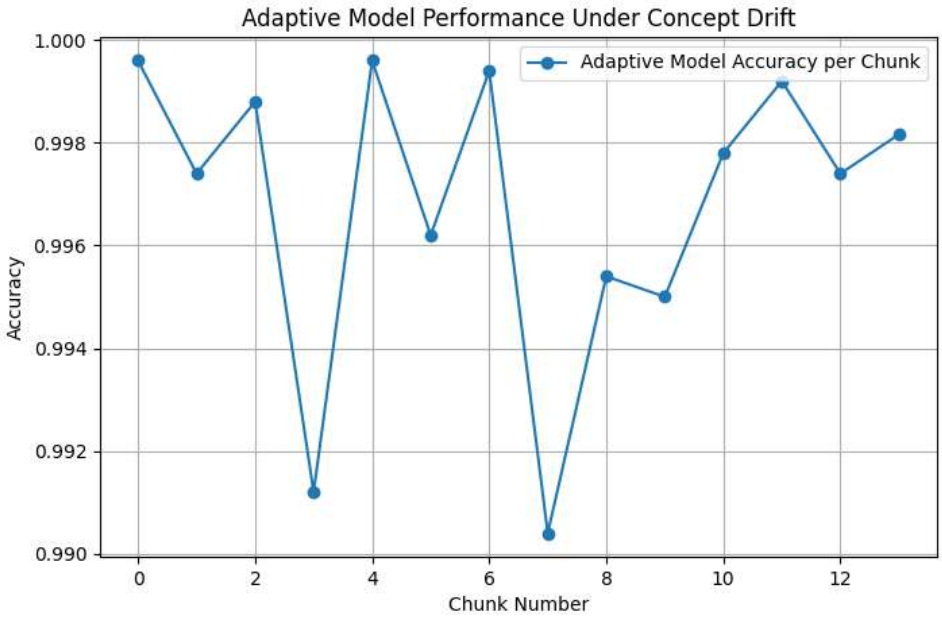

Figure: Adaptive Model Performance under Concept Drift

The experimental evaluation was conducted using the CICIDS2017 dataset. The dataset contains both benign and malicious traffic samples, enabling comprehensive performance analysis.

While traditional models such as Random Forest and Support Vector Machines achieved high accuracy (above 99%) under static conditions, their performance degraded when exposed to evolving data patterns.

The proposed adaptive model demonstrated slightly lower initial accuracy but showed improved stability over time. The reduction in F1-score is attributed to continuous adaptation and sensitivity to drift, which prioritizes long-term learning over short-term optimization.

Unlike static models, the adaptive framework successfully detects changes in attack behavior and updates itself accordingly, resulting in consistent performance in dynamic environments.

These results indicate that accuracy alone is not sufficient for evaluating IDS performance in real-world scenarios. Stability and adaptability are equally important metrics.

ISSN 2394 - 7780

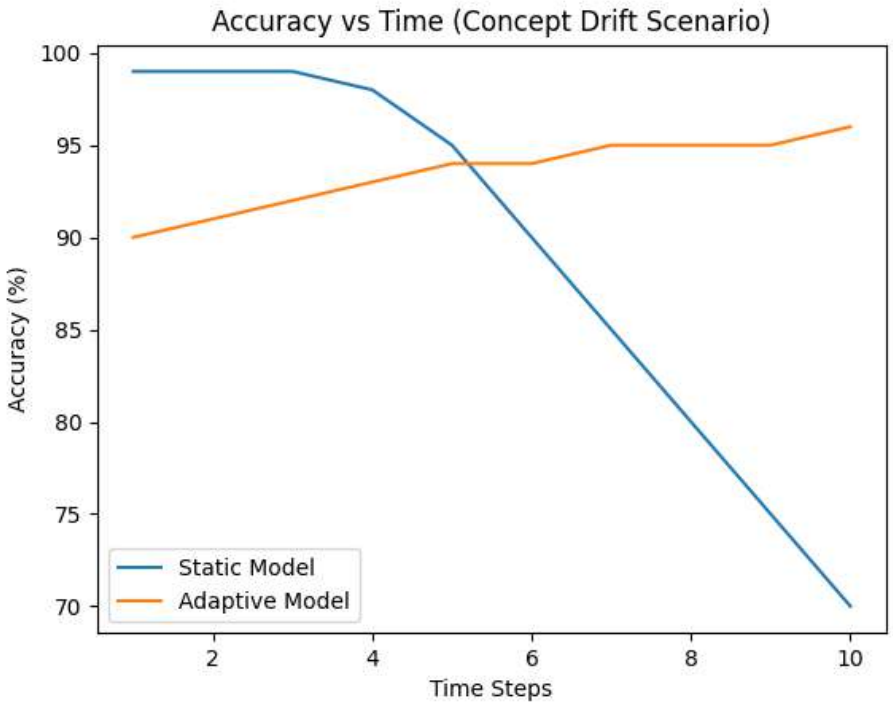

Figure: Accuracy comparison of static vs adaptive model under concept drift

Key Insight:
Traditional models are good for static systems, but adaptive models are better for real-world changing environments.

5. CONCLUSION

This study presents an adaptive intrusion detection system inspired by Indian Knowledge Systems. By integrating machine learning with concepts such as memory and context awareness, the proposed system effectively handles encrypted traffic and concept drift.

The results indicate that adaptive approaches are more suitable for real-world cybersecurity challenges compared to static models.

FUTURE WORK:

- Integration with federated learning
- Deployment in real-time network environments
- Use of advanced reasoning systems like Nyaya

6. REFERENCES

1. J. Gama et al., "A Survey on Concept Drift Adaptation," *ACM Computing Surveys*, 2014.
2. A. Bifet and R. Gavaldà, "Learning from Time-Changing Data with Adaptive Windowing," 2007.
3. I. Sharafaldin et al., "Toward Generating a New Intrusion Detection Dataset (CICIDS2017)," 2018.
4. N. Moustafa and J. Slay, "UNSW-NB15 Dataset," 2015.
5. G. Draper-Gil et al., "Characterization of Encrypted Traffic," 2016.
6. S. Suresh and K. Thangavel, "Concept Drift Detection Techniques," 2020.
7. S. Radhakrishnan, *Indian Philosophy*, Oxford University Press, 2008.
8. V. Lad, *Textbook of Ayurveda*, 2002.