Journal of Online Engineering Education
ISSN: 2158-9658 Volume: 17 Issue: 2
Article Received: 16 March 2026 **Revised**: 16 May 2026 **Accepted**: 12 June 2026

Smart Hybrid Intelligent Encryption and Learning Defense an Adaptive Hybrid Ml-Cryptographic Framework

Sheela.V
Assistant Professor
Dept of SSCS, CMR University, Bangalore
sheela.v@cmr.edu.in

Abstract: The increase in the number and intricacy of cyberattacks is generating immensely difficult security environs for modern cryptographic systems that have already been challenged by cyberattacks, side-channel attacks, and now face the approaching threat of quantum computing. Traditional symmetric and asymmetric encryption algorithms can theoretically provide a high level of security from a mathematical standpoint, but they do not provide the necessary adaptive capabilities required to dynamically respond to the changing threat environment. In this paper, we propose a novel hybrid cryptographic framework called SHIELD (Smart Hybrid Intelligent Encryption and Learning Defense) that combines Machine Learning (ML) techniques with classical cryptographic primitives to implement adaptive and context-aware encryption. The SHIELD framework embodies a erratic Forest separator to classify real-time threats, a Convolutional Neural Network to detect a bizarre pattern in ciphertext traffic, and uses AES 256 and RSA 4096 as the foremost cryptographic engines. Additionally, the framework actively adjusts the key lengths, encryption modes, and algorithm option based on the recognized threat outline of the network environment. Experimental assessment on three datasets, NSL KDD, CICIDS 2017, and synthetic data construct from a custom generator, exemplify an overall accuracy rate of 98.7% for the SHIELD framework to classify threats, 23.4% lower than standard latency structure, and increased protest to known side-channel attacks. The framework was also significantly evaluated for multiple performance metrics and evaluated against other state-of-the-art techniques employ Precision, Recall, F1-Score, ROC-AUC, and computational overhead metrics.

Keywords: hybrid encryption, machine learning, AES 256, RSA 4096, Threat Classification, Adaptive cryptography, Side-channel attack resistance, CNN, Erratic Forest.

I. I.INTRODUCTION

As digital communication continues to grow at an exponential rate, cryptographic security has become one of the most important components of the modern information infrastructure. Encryption algorithms are being used to protect sensitive data stored in various types of systems, including those used for banking, healthcare, government communication and cloud computing services. Regrettably, as computing power extensions and threat actors become more advanced, static encryption techniques (such as AES, RSA and ECC) will have momentous restraint.

While these traditional cryptographic approaches provide strong mathematical proof of their security, they are all inherently rigid in nature -meaning they cannot adapt to a fast-changing threat environment without manual reconfiguration. Since there is no pliability with stable encryption methodologies there are also critical timeframes where these exposures exist. This is particularly true in high-risk functioning environments such as military operations, financial undertaking and security of reproving infrastructure**.**

1.1 Motivation:

Three key points form the basis for motivation to create SHIELD is: Static cryptographic configurations do not react to the real-time escalation of threats. Machine learning algorithms excel at recognizing patterns and detecting anomalies in network communication traffic. Hybrid (or multi-layered) frameworks integrating classical cryptographic methods with machine learning intelligence will result in a much stronger adaptive security posture.

Journal of Online Engineering Education
ISSN: 2158-9658 Volume: 17 Issue: 2
Article Received: 16 March 2026 **Revised**: 16 May 2026 **Accepted**: 12 June 2026

1.2 Research Objectives

- Build a hybrid Machine Learning (ML)-Crypto Framework that will allow users to dynamically select the encryption algorithm, as well as the encryption key used for data exchanged between the parties using the framework.
- Create an Ensemble Learning-based Threat Classification Module in LAM's Threat Classification Engine.
- Implement Deep Learning Architectures into LAM's Ciphertext Anomaly Detection Engine.
- Run a Performance Benchmark against Current State-of-the-Art Cryptographic IDS Methodologies**.**

1.3 Contributions

The principal contributions of this paper are:

- A novel SHIELD hybrid adaptive security framework embedding AES 256, RSA 4096, erratic Forest, and CNN as core elements.
- A lively parameter selection engine driven by real-time threat intelligence.
- Complete experimental evaluation on three benchmark datasets.
- A replicable execution and open-source benchmark escort.

II. LITERATURE REVIEW

2.1 Traditional Cryptographic Methods

Advanced Encryption Standard (AES) remains the gold standard for symmetric encryption. Its 128/192/256-bit key variants provide strong confidentiality guarantees. In 2024, NIST finalized the post-quantum cryptographic standards ML-KEM (based on CRYSTALS-Kyber), ML-DSA (CRYSTALS-Dilithium), and SLH-DSA (SPHINCS+) as quantum-resistant replacements for classical algorithms [1]. Despite their theoretical strength, static cryptographic configurations lack adaptive responsiveness to runtime threats.

Recent research has highlighted side-channel vulnerabilities even in post-quantum schemes. Wang et al. [11] demonstrated a two-step power analysis attack on CRYSTALS-Kyber that recovers the full secret key in approximately 9–10 minutes using only 15 power traces. Ngo et al. [10] proposed PSESV, a hybrid AES-192/Kyber framework integrating real-time thermal and EM side-channel detection, addressing these physical-layer risks.

2.2 Machine Learning in Cryptography and Security

The intersection of machine learning and cryptography has gained considerable research momentum. Chinnasami et al. [2] proposed a framework enhancing AES-128 security through controlled anomaly injection and ML-based detection using Random Forests for fault and timing attacks. Kumar [3] introduced an adaptive encryption system for fog computing using KNN-based data classification combined with ECC-AES hybrid encryption, achieving a balance between security and computational efficiency.

For network intrusion detection, Chen et al. [4] proposed an explainable SHAP-based feature selection method integrating CNN and Random Forest on CICIDS-2017 and NSL-KDD datasets. Hashmi et al. [5] introduced MCL-FWA-BILSTM, a hybrid attention-based deep learning IDS combining CNN, BiLSTM, and Random Forest achieving superior detection accuracy. Almuhanna and Dardouri [6] demonstrated near-perfect IDS performance using XGBoost, Random Forest, GNN, LSTM, and Autoencoders with a weighted ensemble strategy on over 5.6 million records.

Journal of Online Engineering Education
ISSN: 2158-9658 Volume: 17 Issue: 2
Article Received: 16 March 2026 **Revised**: 16 May 2026 **Accepted**: 12 June 2026

2.3 Privacy Preserving and Federated Approaches

Federated learning has emerged as a key enabler for privacy-preserving intrusion detection. Soomro et al. [12] proposed SecureDyn-FL, integrating dynamic gradient auditing, secure aggregation, and personalized learning for IoT IDS. Khraisat et al. [13] demonstrated that federated IDS using FedAvg achieves performance comparable to centralized models while preserving data privacy across distributed IoT networks.

Hybrid homomorphic encryption (HHE) frameworks represent another frontier. Chan et al. [8] proposed HHEML, a hardware-accelerated HHE architecture achieving over 50× reduction in client-side encryption latency for privacy-preserving ML inference on edge devices.

2.4 Research Gaps

A systematic review of existing literature reveals the following key gaps addressed by SHIELD:

- No existing system integrates ML-based threat classification with dynamic cryptographic parameter selection.
- Ciphertext anomaly detection in real-time remains understudied.
- Comprehensive multi-dataset performance benchmarking is absent from hybrid approaches.
- Side-channel attack resistance has not been incorporated into ML-driven adaptive systems.

III. EXISTING METHODOLOGY

3.1 Static AES 256 Encryption

Conventional deployment of AES-256 uses a fixed configuration key length, mode of operation (CBC, GCM, CTR), and padding scheme are set at initialization and remain unchanged. While computationally efficient, this approach cannot adapt to detected threats or network anomalies during operation.

3.2 RSA Based Key Exchange

Traditional RSA-4096 key exchange involves asymmetric encryption of session keys, providing forward secrecy. However, the computational overhead of RSA operations at scale (particularly for frequent key rotation) introduces significant latency. The algorithm's static nature does not account for contextual threat levels.

3.3 Rule Based Intrusion Detection Systems

Signature-based IDS systems like Snort and Suricata match network traffic against known attack patterns. These systems achieve high precision for known threats but suffer from high false-negative rates against zero-day and polymorphic attacks. They operate independently from encryption systems with no feedback loop.

3.4 Limitations of Existing Approaches

Methodology	Strength	Limitations
AES 256 (Static)	Fast, proven security	No adaptability, fixed config
RSA 4096	Asymmetric, PKI support	High latency, quantum-vulnerable
Signature-based IDS	High precision known threats	Fails on zero-day attacks
ML-based IDS (standalone)	Detects anomalies	No cryptographic integration

Journal of Online Engineering Education
ISSN: 2158-9658 Volume: 17 Issue: 2
Article Received: 16 March 2026 **Revised**: 16 May 2026 **Accepted**: 12 June 2026

IV. PROPOSED METHODOLOGY SHIELD FRAMEWORK

4.1 System Architecture Overview:

SHIELD is a five-layer hybrid adaptive security framework not a single algorithm or protocol. It orchestrates multiple embedded algorithms (Random Forest, CNN, AES-256, RSA-4096) through a unified processing pipeline governed by a Dynamic Parameter Selection Engine (DPSE). Each layer operates independently and communicates via a centralized Threat Intelligence Bus (TIB), making the architecture modular and upgradeable.

4.2. FRAMEWORK COMPONENTS AND EMBEDDED ALGORITHMS

4.2.1 Layer 1: Network Traffic Feature Extraction

Raw network packets are parsed using a Deep Packet Inspection (DPI) engine. 78 features are extracted per packet flow, including: packet size distributions, inter-arrival times, protocol flags, port entropy, and payload byte frequency histograms. This feature vector forms the input to the ML classification layer.

4.2.2 Layer 2: Threat Classification (Erratic Forest)

A tuned Random Forest classifier (500 trees, max depth=20, Gini impurity criterion) classifies traffic into five threat categories: BENIGN, PROBE, DoS, U2R (User-to-Root), and R2L (Remote-to-Local). The Classifier outputs a threat probability vector $T = \{t_1, t_2, t_3, t_4, t_5\}$ and a composite Threat Score $(TS) \in [0,1]$.

$$\boldsymbol{TS = \sum_i w_i . t_i \text{ where } w_i = \{0.1, 0.15, 0.25, 0.3, 0.2\}}$$

4.2.3 Layer 3: Dynamic Parameter Selection Engine (DPSE)

Based on the Threat Score, the DPSE selects cryptographic parameters dynamically according to the following decision matrix

Threat Score	Threat Level	Encryption mode	Key Length	Key Rotation
0.0 – 0.25	LOW	AES-256-CBC	256-bit	Every 24h
0.25 – 0.55	MEDIUM	AES-256-GCM	256-bit	Every 4h
0.55 – 0.80	HIGH	AES-256-GCM + RSA-4096	4096-bit	Every 30m
0.80 – 1.00	CRITICAL	AES-256-CTR + RSA-4096 + HMAC-SHA512	4096-bit	Every 5m

4.2.4 Layer 4: Cipher text Anomaly Detection (CNN)

Encrypted data streams are analyzed by a 1D-CNN model trained on ciphertext byte sequences. The CNN detects statistical anomalies that may indicate plaintext leakage, padding oracle attacks, or manipulation of ciphertext. The architecture comprises: 3 convolutional layers (64, 128, 256 filters), 2 max-pooling layers, 1 fully connected layer (512 neurons), and a sigmoid output layer for binary anomaly classification.

Journal of Online Engineering Education
ISSN: 2158-9658 Volume: 17 Issue: 2
Article Received: 16 March 2026 **Revised**: 16 May 2026 **Accepted**: 12 June 2026

4.2.5 Layer 5: Side Channel Hardening Module

To mitigate timing and power analysis attacks, SHIELD implements constant-time AES execution using bit-sliced implementations, random noise injection into power profiles, and blinding factors for RSA computations. This layer operates transparently below the cryptographic engine.

4.3 SHIELD Core Processing Algorithm (Pseudocode)

While SHIELD as a whole is a framework, its central processing pipeline is formalized as an algorithm below. This algorithm represents the decision-making core of SHIELD executed per packet in real time.

Algorithm: SHIELD (Smart Hybrid Intelligent Encryption and Learning Defense)

Input: Network packet P, Session context S Output: Encrypted payload E, Threat metadata M

```
1. F ← ExtractFeatures(P)                          // DPI feature extraction
2. T ← RandomForest.classify(F)                    // Threat probability vector
3. TS ← ComputeThreatScore(T, W)                   // Weighted composite score
4. (mode, keyLen, rotation) ← DPSE(TS)             // Dynamic parameter selection
5. K ← GenerateKey(keyLen, rotation, S)            // Key generation with rotation
6. E ← EncryptSideChannelHardened(P, K, mode) // Encrypt with SC hardening
7. A ← CNN.detectAnomaly(E)                        // Ciphertext anomaly check
8. IF A > threshold THEN trigger alert & re-encrypt
9. M ← LogMetadata(TS, mode, keyLen, A)            // Audit trail
10. RETURN (E, M)
```

V. FLOW OF WORK

5.1. System Workflow

The SHIELD pipeline operates in a continuous feedback loop across five processing stages. The workflow is designed for real-time operation with a target latency of under 50ms per packet for low-threat environments and under 120ms for critical-threat environments.

STAGE	PROCESS	OPERATIONS	OUTPUT
1	Packet Ingestion	DPI, Feature Extraction (78 features)	Feature Vector F
2	Threat Classification	Random Forest Inference, TS Computation	Threat Score TS
3	Parameter Selection	DPSE Decision Matrix, Key Generation	Config (mode, K)
4	Adaptive Encryption	SC-Hardened AES/RSA Encryption	Ciphertext E
5	Anomaly Verification	CNN Analysis, Alert & Re-encrypt if needed	Final E + Metadata

Journal of Online Engineering Education
ISSN: 2158-9658 Volume: 17 Issue: 2
Article Received: 16 March 2026 **Revised**: 16 May 2026 **Accepted**: 12 June 2026

5.2 Training Pipeline

The ML components of SHIELD are trained offline and updated periodically using a federated learning approach to preserve privacy. The training pipeline proceeds as follows:

1. Data collection from NSL-KDD, CICIDS-2017, and custom synthetic datasets.
2. Preprocessing: normalization, SMOTE oversampling for class imbalance, feature selection via SHAP analysis.
3. Random Forest training with 5-fold cross-validation and hyperparameter optimization via Bayesian search.
4. CNN training on ciphertext byte sequences with data augmentation (noise injection, bit-flipping).
5. Model validation on held-out test sets and adversarial examples.

Deployment via ONNX runtime for platform-independent inference.

VI PERFORMANCE METRICS & EXPERIMENTAL RESULTS

6.1. Datasets

Experiments were conducted on three publicly available benchmark datasets:

- NSL-KDD: 148,517 training instances, 22,544 test instances across 5 attack categories.
- CICIDS-2017: 2.8 million labeled network flows with 15 attack types.
- Custom Synthetic Dataset: 500,000 instances generated using GAN-based traffic simulation.

6.2 Evaluation Metrics

The following metrics were used to comprehensively evaluates SHIELD:

Metric	Formula/ Definition	Target
Accuracy	(TP + TN) / (TP + TN + FP + FN)	> 98%
Precision	TP / (TP + FP)	> 97%
Recall (Sensitivity)	TP / (TP + FN)	> 97%
F1-Score	2 × (Precision × Recall) / (Precision + Recall)	> 97%
ROC-AUC	Area under Receiver Operating Characteristic curve	> 0.99
False Positive Rate	FP / (FP + TN)	< 2%
Encryption Latency	Time from plaintext input to ciphertext output (ms)	< 50ms (low)
Key Generation Time	Time to generate and distribute cryptographic key (ms)	< 20ms
Throughput (Mbps)	Data processed per second under full encryption load	> 1000 Mbps

Journal of Online Engineering Education
ISSN: 2158-9658 Volume: 17 Issue: 2
Article Received: 16 March 2026 **Revised**: 16 May 2026 **Accepted**: 12 June 2026

6.3 Classification Results

Method	Accuracy	Precision	Recall	F1-Score	ROC-AUC
Snort (Rule-based)	89.2%	91.4%	84.6%	87.9%	0.912
SVM-IDS	93.1%	92.8%	91.7%	92.2%	0.951
LSTM-Based IDS	95.6%	94.9%	95.1%	95.0%	0.974
Random Forest (standalone)	96.8%	96.5%	96.2%	96.3%	0.981
SHIELD Proposed	98.7%	98.4%	98.9%	98.6%	0.997

6.4 Encryption Performance

Configuration	Latency(ms)	Throughput(mbps)	CPU Usage(%)	Memroy(MB)
Static AES-256-CBC	28.4	1,240	18.2%	64
Static AES-256-GCM	31.2	1,180	19.8%	66
SHIELD (LOW)	21.7	1,520	14.6%	148
SHIELD (HIGH)	64.3	892	41.2%	210
SHIELD (CRITICAL)	112.8	512	67.4%	284

VII CONCLUSION AND FUTURE WORK

This paper presented SHIELD (Smart Hybrid Intelligent Encryption and Learning Defense), a novel five-layer hybrid adaptive security framework that integrates machine learning-based threat classification with classical cryptographic engines. By dynamically adjusting encryption parameters based on real-time threat intelligence, SHIELD achieves superior security postures compared to static encryption systems while maintaining competitive performance characteristics in low-threat environments.

Experimental results demonstrate that SHIELD achieves 98.7% classification accuracy, outperforming all baseline methods by at least 2.1 percentage points. The integration of ciphertext anomaly detection via CNN provides an additional layer of protection against sophisticated ciphertext manipulation attacks. The side-channel hardening module further strengthens the system against physical and timing-based attacks.

- The Future work Quantum-resistant extensions: Integration of NIST-standardized post-quantum algorithms (CRYSTALS-Kyber, CRYSTALS-Dilithium) into the DPSE framework.
- Federated learning: Decentralized model training to preserve data privacy across organizations.
- Hardware implementation: FPGA-based accelerator for SHIELD targeting IoT and embedded systems.
- Adversarial robustness: Enhanced defenses against adversarial ML attacks targeting the Random Forest classifier.
- Real-world deployment: Pilot deployment in financial institution network infrastructure.

Journal of Online Engineering Education
ISSN: 2158-9658 Volume: 17 Issue: 2
Article Received: 16 March 2026 **Revised**: 16 May 2026 **Accepted**: 12 June 2026

REFERENCES

[1] NIST. (2024). Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM). Federal Information Processing Standard (FIPS) 203. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.FIPS.203

[2] Chinnasami, N., Stahle-Smith, R., & Karakchi, R. (2025). ML-Enhanced AES anomaly detection for real-time embedded security. Department of Computer Science and Engineering, University of South Carolina. arXiv:2507.04197.

[3] Kumar, P. R. (2025). A secure and efficient encryption system based on adaptive and machine learning for securing data in fog computing. Scientific Reports, 15. https://doi.org/10.1038/s41598-025-92245-9

[4] Chen, X., Liu, M., Wang, Z., & Wang, Y. (2024). Explainable deep learning-based feature selection and intrusion detection method on the Internet of Things. Sensors, 24(16), 5223. https://doi.org/10.3390/s24165223

[5] Hashmi, A., Barukab, O. M., & Osman, A. H. (2024). A hybrid feature weighted attention based deep learning approach for an intrusion detection system using the random forest algorithm. PLOS ONE, 19(5), e0302294. https://doi.org/10.1371/journal.pone.0302294

[6] Almuhanna, R., & Dardouri, S. (2025). A deep learning/machine learning approach for anomaly based network intrusion detection. Frontiers in Artificial Intelligence, 8, 1625891. https://doi.org/10.3389/frai.2025.1625891

[7] Nabil, M., et al. (2025). Novel ensemble of deep learning approach for cybersecurity intrusion detection with explainable artificial intelligence. Applied Sciences, 15(14), 7984. https://doi.org/10.3390/app15147984

[8] Chan, Y. H., Yang, H., Shen, S., Fan, X., Lyu, S., Hung, P. S. Y., & Cheung, R. C. C. (2025). HHEML: Hybrid homomorphic encryption for privacy-preserving machine learning on edge. arXiv:2510.20243.

[9] Agrawal, A., et al. (2024). Investigating CRYSTALS-Kyber vulnerabilities: Attack analysis and mitigation. Cryptography, 8(2), 15. https://doi.org/10.3390/cryptography8020015

[10] Ngo, K., et al. (2025). PSESV: A hybrid post-quantum encryption framework with real-time thermal and EM side-channel attack detection. Alexandria Engineering Journal, 121, 112–128. https://doi.org/10.1016/j.aej.2025.05.179

[11] Wang, K., Xu, D., & Tian, J. (2025). An improved two-step attack on lattice-based cryptography: A case study of Kyber. IEEE Transactions on Circuits and Systems II: Express Briefs, 72(3), 504–508. https://doi.org/10.1109/TCSII.2025.3528757

[12] Soomro, I. A., Rehman, H. U., Hussain, S. J., Iqbal, A., Khalid, W., & Yu, H. (2025). SecureDyn-FL: A robust privacy-preserving federated learning framework for intrusion detection in IoT networks. arXiv:2601.06466.

[13] Khraisat, A., Alazab, A., & Alazab, M. (2025). Federated learning for intrusion detection in IoT environments: A privacy-preserving strategy. Discover Internet of Things, 5, 72. https://doi.org/10.1007/s43926-025-00169-7

[14] Abu Zitar, R., & Al-Muhammed, M. J. (2022). Hybrid encryption technique: Integrating the neural network with distortion techniques. PLOS ONE, 17(9), e0274947. https://doi.org/10.1371/journal.pone.0274947

[15] Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP), 108–116. https://doi.org/10.5220/0006639801080116