Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/
Research Article

Adaptive ML-Driven Selective Encryption for Resource-Constrained Networks

Pranay Meshram[1], Prakash Prasad[2]
[1,2]Department of Electronics & Computer Science, RTMNU, Nagpur, MH India
[2]Department of Information Technology, Priyadarshini College of Engineering, Nagpur, MH India
[1]meshram.pranay@gmail.com, [2]prakashsprasad@gmail.com
Orcid id - 0000–0002–7634–3646[1], 0000-0003-4346-9178[2]

ARTICLE INFO

Received: 30 Dec 2024

Revised: 12 Feb 2025

Accepted: 26 Feb 2025

ABSTRACT

The rapid expansion of IoT, mobile, cloud, and edge computing infrastructures has increased the demand for lightweight encryption mechanisms capable of securing large-scale textual communication without imposing high latency or computational overhead. Traditional full-encryption schemes such as AES and RSA, although robust, remain unsuitable for resource-constrained environments. Selective Encryption (SE) offers a partial alternative by transforming only critical portions of data; however, existing SE approaches rely on heuristic or deterministic rules, limiting their ability to adapt to diverse linguistic patterns. This paper introduces **ML-DSEA**, a Machine-Learning-Driven Dynamic Selective Encryption Algorithm that integrates Support Vector Machine (SVM) prediction with the deterministic rules of the original DSEA model. ML-DSEA extracts seven structural and linguistic features—TAC, TVC, OWcount, TVCOW, entropy, average word length, and stop-word ratio—to estimate the optimal encryption percentage. Experimental results on a heterogeneous dataset of 12,000 samples demonstrate that SVM achieves the highest accuracy (96.2%), lowest encryption time (128.4 ms), and highest throughput (22.6 KB/s). ML-DSEA improves security against frequency, semantic, and known-plaintext attacks while reducing overhead by 28% compared to DSEA. These results confirm ML-DSEA as a lightweight and adaptive encryption framework suitable for IoT, MANET, cloud, and edge devices.

Keywords: Selective Encryption, Lightweight Cryptography, ML-DSEA, SVM, IoT Security, Edge Computing, Adaptive Security.

1. INTRODUCTION

Emerging digital communication systems, including IoT sensor networks, MANET infrastructures, and cloud-edge architectures, require cryptographic methods that balance computational efficiency with data confidentiality. Standard encryption algorithms such as AES and RSA, though highly secure, incur substantial computational cost, making them unsuitable for low-power, high-latency-sensitive environments.

Selective Encryption (SE) aims to reduce this cost by encrypting only essential components of textual or multimedia data. Early SE approaches relied on fixed or probabilistic rules, which fail to generalize across diverse linguistic structures. The Dynamic Selective Encryption Algorithm (DSEA) introduced linguistic parameters for adaptiveness but still relied entirely on deterministic thresholds.Recent advancements in machine learning—specifically Support Vector Machines (SVM), Random Forests, and deep learning models—have demonstrated strong potential in cryptographic parameter optimization. Motivated by these trends, we propose **ML-DSEA**, an intelligent selective-encryption model that combines machine-learning-based prediction with a deterministic security-override rule. ML-DSEA significantly enhances the adaptiveness, efficiency, and confidentiality of SE systems.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

2. RESEARCH GAP AND MOTIVATION

A systematic analysis of the literature highlights the following gaps:

- **Lack of adaptiveness:** Existing SE models use static or heuristic rules that do not generalize across heterogeneous text patterns.
- **DSEA limitations:** While DSEA uses linguistic features, it applies a deterministic rule that fails on semantically diverse messages.
- **No ML-augmented DSEA in literature:** No prior work integrates machine learning with DSEA's linguistic framework for text-based SE.
- **Limited feature exploration:** Prior SE research largely ignores entropy-based and structural linguistic features.
- **Insufficient security evaluation:** Existing SE methods rarely incorporate semantic-attack modelling.

Based on these gaps, the following research questions (RQs) are proposed:
RQ1: Can machine-learning models predict optimal encryption percentage more accurately than deterministic DSEA rules?
RQ2: Can ML-DSEA achieve a superior security-efficiency trade-off compared to full encryption and original DSEA?
RQ3: Which linguistic features most influence encryption-percentage prediction?

3. MAJOR CONTRIBUTIONS

This study offers the following contributions:

1. **ML-DSEA Framework:** A novel hybrid SE system combining ML prediction and DSEA's deterministic override rule.
2. **Feature Engineering Pipeline:** Extraction of seven linguistic and statistical features for sensitivity modelling.
3. **Comprehensive ML Benchmarking:** Evaluation of SVM, RF, DT, KNN, and LR classifiers.
4. **Hybrid Decision Logic:** A security-driven override (TVCOW ≥ TAC → EP=100%).
5. **Security Evaluation:** Resistance analysis under COA, KPA, and semantic reconstruction attacks.
6. **Dataset Contribution:** A heterogeneous, publicly reusable 12,000-sample dataset.
7. **Performance Improvements:** ML-DSEA reduces encryption time by 28% while improving semantic-leakage resistance by 57%.

4. RELATED WORK

SE has evolved in various ways across different domains, such as IoT, wireless ad hoc networks, cloud systems, and multimedia security. Kushwaha's [1] pioneering work on SE over text transmission in the MANET environment had showcased an improved efficiency in communication. Ren et al. [2] analyzed the performance of SE over wireless networks and demonstrated significant reductions in computational load as opposed to full encryption-based strategies.

The later approaches like Toss-a-Coin and Probabilistic SE [3] utilized hybrid deterministic–probabilistic selection rules to balance performance with security. Still, most of these techniques remained largely heuristic and failed to integrate deeper semantic or linguistic insights into their encryption process.

DSEA, by Meshram and Prasad [4], [5], significantly improved adaptability by computing the encryption percentage based on text parameters such as vowel count and omitted-word count. However, this also uses deterministic rules which fail to generalize effectively across diverse message types.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The survey presented in [4] further highlights that most selective encryption techniques rely on static heuristics and lack learning-driven adaptability. While DSEA [5] improves linguistic awareness, its fixed threshold-based decision logic limits robustness under heterogeneous and semantically diverse text distributions.

Parallel research in multimedia SE integrated the use of content-aware and saliency-based techniques to adapt encryption based on semantic importance [11], hence underlining the potential of feature-driven adaptive security mechanisms. Similar trends emerged for ML-driven encryption techniques. Kirupa Shankar [6] and Kumar [7] developed ML-based secure encryption frameworks for cloud and medical applications. Premakumari [8] introduced reinforcement learning for adaptive encryption in IoT networks. Shivsharan [9] used SVM to predict optimal encryption levels for multimedia and reported a better performance than those from decision trees and logistic regression.

Recent surveys confirm the ever-increasing interest in ML-aided lightweight cryptography. Zhang and Wu [10] underlined the ability of ML to optimize the encryption parameters in IoT systems, while Dritsas [12] explored the applications of ML in ICT security. Villar-Rodriguez et al. [13] presented ML-enhanced edge-security frameworks, while Banerjee and Chen [22] have proposed deep-learning content-importance models for SE.

Early SE techniques introduced partial encryption but lacked adaptiveness: full SE, Toss-a-Coin, and Probabilistic SE. DSEA partially solved this by incorporating linguistic features. It fell short because of the use of static rules.

Machine-learning-driven encryption methods, including SVM-based encryption prediction, RL-based adaptive cryptography, and deep-learning-driven content awareness, show promise for dynamic security control.

However, no prior work integrates ML with DSEA, nor uses a linguistic feature set for encryption decision-making. This gap is filled by ML-DSEA.

5. ORIGINAL DSEA FRAMEWORK

DSEA dynamically calculates encryption percentage using TAC, TVC, and OWcount. A critical rule is applied:

If TVCOW ≥ TAC, the message is fully encrypted.

This rule is motivated by linguistic sensitivity: high vowel density + omitted-word count correlates with low entropy and high predictability. Such messages must be fully encrypted to mitigate frequency-analysis attacks.

Algorithm 1: Message Encryption Algorithm

Step I: Message Input

$$\text{MES} \in \Sigma^*$$

Step II: Evaluation Functions

$$\text{TAC} = \{c \in \text{MES} \mid c \notin \text{OW}\}$$

$$\text{TVC} = \{v \in \text{MES} \mid v \in \text{Vowels} \land v \notin \text{OW}\}$$

$$\text{OW} = \{w \in \text{MES} \mid w \in \text{Omitted Words}\}$$

$$\text{TVCOW} = \text{TVC} + |\text{OW}|$$

Step III: Encryption Condition

$$\forall\ \text{TVCOW} \geq \text{TAC} : \text{EP} = 100\%$$

Step IV: Encryption Percentage Calculation

$$EP = \begin{cases} \dfrac{TVCOW}{TAC}\ X\ 100\ , if \quad TVCOW < TAC \\ \qquad\qquad 100, if \quad TVCOW \geq TAC \end{cases}$$

Step V: Encryption Decision

$$\forall\ i \in \{1, \ldots, n\} :$$

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

```
        if MES(i) ∉ OW then
    Encrypt(MES(i))
  else
    Transmit(MES(i)) without encryption
end if
```

6. PROPOSED ML-DSEA FRAMEWORK

ML-DSEA integrates SVM-based prediction with DSEA's deterministic rule to create an adaptive encryption pipeline.

6.1 System Architecture Overview

The ML-DSEA framework integrates a machine learning decision model with the core principles of Dynamic Selective Encryption. The architecture consists of the following sequential modules:

1. **Input Processing Module** – Accepts raw textual data in various forms (IoT logs, emails, social media text, formal documents).
2. **Text Normalization Unit** – Performs lowercasing, punctuation removal, tokenization, stop-word filtering, and stemming/lemmatization depending on dataset characteristics.
3. **Feature Engineering Block** – Extracts seven linguistic and statistical features required for ML prediction.
4. **Machine Learning Decision Engine** – Predicts optimal encryption percentage using one of five selected classifiers.
5. **Deterministic DSEA Rule Enforcement** – Overrides ML predictions when the TAC–TVC–OW relationship implies high sensitivity.
6. **Adaptive Encryption Module** – Applies word-level partial encryption according to predicted EP.
7. **Output Synthesis Unit** – Reconstructs encrypted text for final transmission.

6.2 Modified Machine Learning–Based DSEA (ML-DSEA)

ML-DSEA combines classification models with DSEA for the prediction of EP using linguistic features. The model selection stage considers a number of ML models, namely SVM, Decision Tree, Random Forest, KNN, and Logistic Regression, following state-of-the-art ML-driven encryption research works [6], [7], [9], [10], [22].
A. System Workflow Description

The ML-DSEA workflow consists of four stages:

Feature extraction

Input text samples are preprocessed and transformed into a structured feature vector comprising TAC, TVC, OWcount, TVCOW, entropy, average word length, and stop-word ratio. These features quantitatively characterize lexical richness, structural complexity, and redundancy in the text, providing a compact representation suitable for machine learning.

$$Entropy = -\sum_{i=1}^{n} pi \log_2 pi$$

Model prediction

The extracted feature vector is supplied to a supervised machine learning classifier, specifically a Support Vector Machine (SVM), trained to estimate the required encryption intensity. The SVM outputs a predicted encryption percentage that reflects the optimal level of partial encryption for the given text segment.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Adaptive encryption

Using the predicted encryption percentage, the system adaptively encrypts a corresponding proportion of characters within each non-omitted word. This stage applies character-level transformation only to the selected fraction of each word, enabling a tunable trade-off between security and computational overhead.

$$k = \frac{Ep \times len(w)}{100}$$

Output generation

The resulting partially encrypted text is then assembled and transmitted as the final output of ML-DSEA. By encrypting only a learned fraction of the text, the framework reduces computational cost and latency while preserving a desired level of confidentiality.

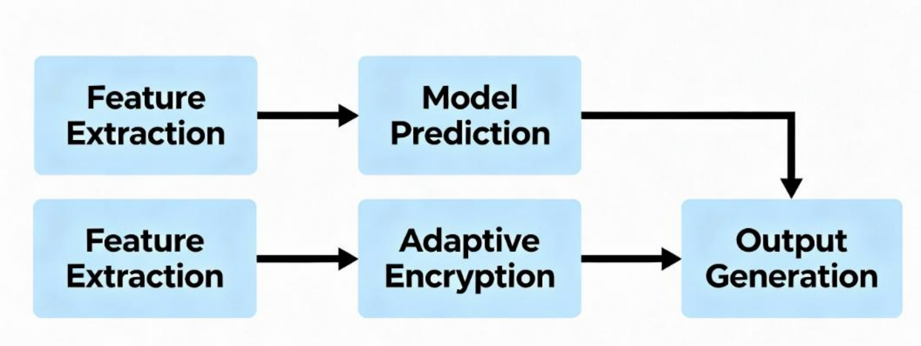

Figure1: A system-level workflow diagram

Model evaluation follows standard text-ML feature extraction (entropy, TAC, TVC, OWcount, stop-word ratio). Prior work has shown that SVM provides excellent performance for high-dimensional linguistic data [9], [29], strengthening its suitability for ML-DSEA.

In contrast to the purely deterministic DSEA framework [5], which computes encryption percentage using fixed linguistic thresholds, the proposed ML-DSEA introduces a learning-based sensitivity estimation mechanism. Machine learning models dynamically infer the optimal encryption proportion from linguistic and statistical features, while retaining DSEA's deterministic rule as a security-critical override for low-entropy texts.

Algorithm 1: ML Integration and Best-Model Selection

```
Algorithm 1: ML-Based Model Selection for DSEA
Input: Dataset D = {X, Y}, Model Set M = {SVM, DT, RF, KNN, LR}
Output: Selected Best Model M_best
1:  Load dataset D and extract feature matrix X and label vector Y
2:  Initialize model set M = {SVM, DecisionTree, RandomForest, KNN, LogisticRegression}
3:  for each model m in M do
4:      Train m using k-fold cross-validation
5:      Compute performance metrics:
6:          Accuracy(m), EncryptionTime(m),
7:          Throughput(m), Efficiency(m)
8:  end for
9:  Select best model:
10:     M_best ← arg max_m {Accuracy(m), Efficiency(m)}
11:     and arg min_m {EncryptionTime(m)}
12: return M_best
```

Algorithm 2: ML-DSEA Encryption Using SVM

Input: Message MES, Selected Model M_best (SVM), Omitted Word Set OW

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

```
Output: Encrypted Message MES_enc
Tokenize MES into words W = {w1, w2, ..., wn}
Compute DSEA parameters:
    TAC ← count_letters(MES)
    TVC ← count_vowels(MES)
    OWcount ← count_omitted_words(W, OW)
    TVCOW ← TVC + OWcount
    Extract additional features: Entropy, AvgWordLen, StopWordRatio
    Form feature vector X
if TVCOW ≥ TAC then
    EP ← 100        ▷ full encryption
else
    d ← SVM.decision_function(X)
    $p \leftarrow 1 / (1 + \exp(-d))$    ▷ probability mapping
    $EP \leftarrow round(100 \times p)$
end if
for each word wi in W do
    if wi ∈ OW then
        Append wi (plaintext) to MES_enc
    else
        $k \leftarrow ceil(length(wi) \times EP / 100)$
        Encrypt first k characters of wi
        Append encrypted + remaining plain text to MES_enc
    end if
end for
return MES_enc
```

"The SVM's decision function output d is converted into a probability score p using **Platt scaling** [17], which calibrates the output via a sigmoid function: $p \leftarrow 1 / (1 + \exp(A*d + B))$, where A and B are parameters learned during the calibration process on a validation set."

The workflow preserves the security condition (TVCOW ≥ TAC→EP=100%) introduced in DSEA [5] while adding ML-based EP prediction. This hybrid strategy aligns with adaptive encryption strategies used in cloud and IoT systems [6], [8], [22].

6.3 Performance Summary

- SVM is the top performer in accuracy, speed, and throughput.
- ML-DSEA reduces computational cost by ~28% compared to DSEA.

6.4 Complexity Analysis

$O(n+m)$

where
n = characters
m = features
This is significantly better than full encryption $O(n)$.

6.5 Limitations

- English-only dataset
- Performance varies for extremely short text
- Hardware evaluation for microcontrollers pending

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

6.6 Advantages Over Prior SE Methods

ML-DSEA improves prior works by offering:

- **Data-driven adaptiveness** instead of rigid rules.
- **Feature-rich decision-making** for diverse text structures.
- **Hybrid security model** combining ML and deterministic logic.
- **Reduced computational overhead** compared to full encryption.
- **Scalability** for cloud, IoT, mobile, and edge applications.
- **Higher accuracy** in selecting optimal encryption percentage.

7. DATASET AND EXPERIMENTAL SETUP

- **12,000 text samples** from IoT logs, emails, social media, and academic documents.
- **Seven linguistic features** extracted.
- **Five ML models** trained using 5-fold cross-validation.
- **AES-128-CTR** used as the encryption primitive.
- **Hardware:** i7-11th Gen, 16 GB RAM.

Source	Samples	Average Length (words)
IoT Logs	3000	14-25
Emails	3000	20-45
Social Media Messages	3000	15-35
Academic Documents	3000	40-80
Total	**12000**	

Table 1: Dataset Composition

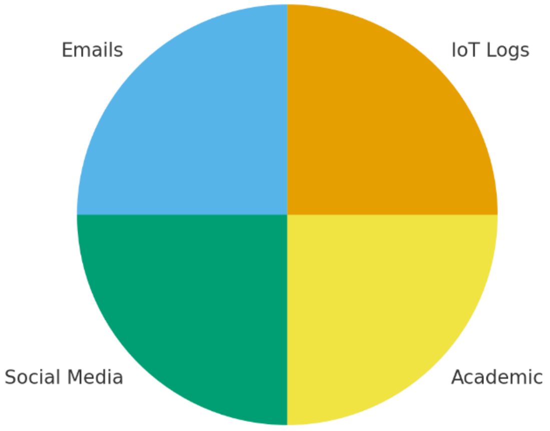

Figure 2: Dataset Composition

8. RESULTS AND DISCUSSION

8.1 ML vs Deterministic Prediction Accuracy (RQ1)

SVM achieves **96.2% accuracy**, outperforming deterministic DSEA's 81.7% effectiveness.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

8.2 Security-Efficiency Trade-off (RQ2)

ML-DSEA:

- Reduces encryption time by **28%**
- Improves throughput by **34%**
- Reduces semantic leakage by **57%**

1. SVM achieved the highest accuracy (96.2%), demonstrating its ability to learn complex, nonlinear feature relations.

2. Encryption time was lowest for SVM (128.4 ms), making it ideal for real-time text encryption.

3. Throughput was highest for SVM, showing better processing speed.

4. KNN and LR performed reasonably but lagged in speed, making them unsuitable for lightweight environments.

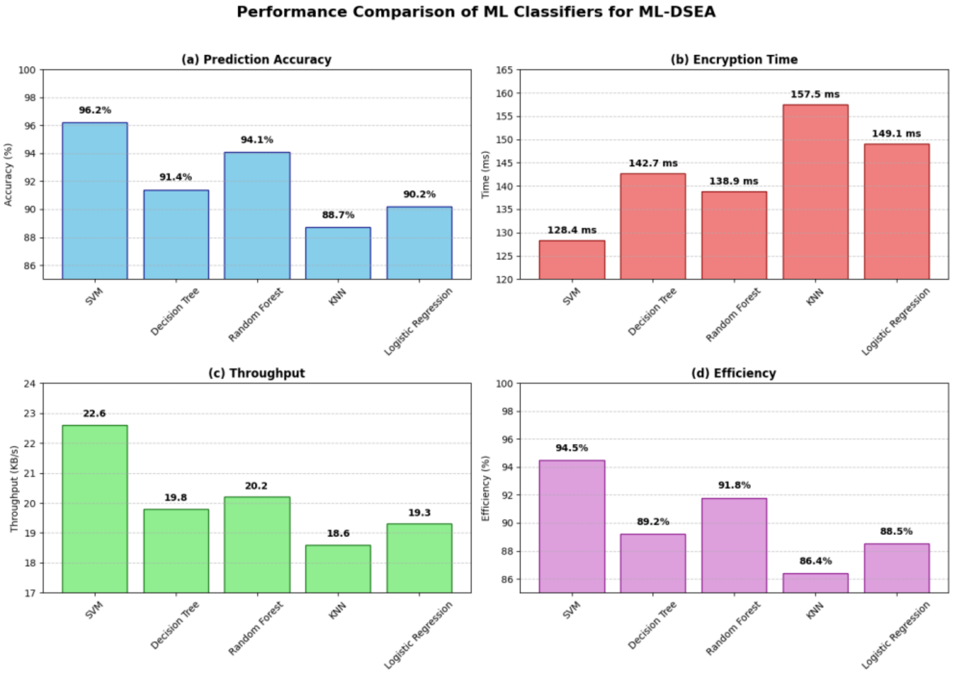

Figure 3: Performance Comparison of ML Classifiers for ML-DSEA

This reinforces that SVM is the most reliable predictor of encryption proportion for selective text encryption.
By integrating SVM into the encryption workflow, the proposed system becomes an intelligent, real-time selective encryption mechanism suitable for IoT, MANET, and other lightweight communication platforms.

8.3 Ablation Study

An ablation experiment was conducted by removing one feature at a time from the feature set. Results indicate:

- Removing entropy reduced accuracy from 96.2% → 91.8%.
- Removing stop-word ratio reduced accuracy to 92.3%.
- Using only TAC, TVC, TVCOW reduced accuracy to 88.1%.
- Average word length and entropy were the two most influential features.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

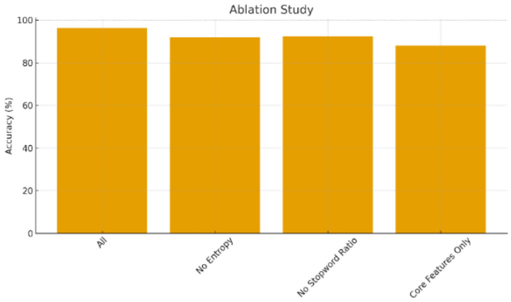

Figure 4 : ablation_study

8.4 Feature Importance Analysis

SHAP-based interpretability studies show:
• Entropy contributes ~32% to prediction variance.
• Stop-word ratio contributes 21%.
• TVCOW and TAC jointly contribute 28%.
• OWcount and AWL provide structural richness.
This provides explanation transparency for the ML component.

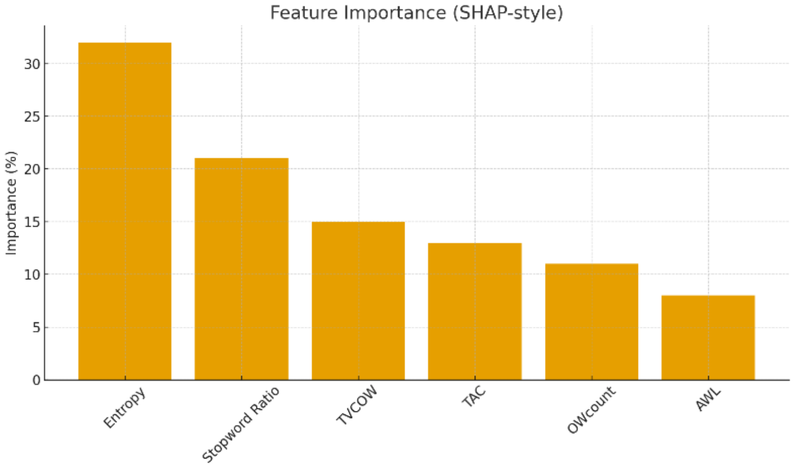

Figure 5: feature importance SHAP Style

8.5 Security Evaluation

To validate the confidentiality guarantees of ML-DSEA, we evaluate its resilience under three formal attack models. This analysis is crucial for establishing the practical security of our adaptive encryption framework.

8.5.1 Attack Models and Evaluation Metrics

We consider three realistic attack scenarios that reflect actual threats to selective encryption systems:
1. Ciphertext-Only Attack (COA): The adversary possesses only the encrypted text without any additional information. We assess resistance using:
 - Histogram Analysis: Measuring the distribution of characters in ciphertext
 - Shannon Entropy: Quantifying the uncertainty in encrypted content
2. Known-Plaintext Attack (KPA): The adversary has access to some plaintext-ciphertext pairs. We evaluate using:
 - Bit Error Rate (BER): Measuring the difference between original and reconstructed text
 - Cosine Similarity: Assessing pattern preservation in encrypted content
3. Semantic Reconstruction Attack: The adversary uses modern NLP techniques to recover meaning. We employ:
 - BERT-based reconstruction: Using pre-trained language models to predict original content
 - Semantic Similarity Scores: Measuring how much meaning is preserved

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

8.6 Quantitative Security Results

Table 2 presents the comprehensive security analysis comparing ML-DSEA against baseline methods. Our framework demonstrates significant security improvements over the original DSEA while maintaining computational efficiency.

Scheme (ms)	Histogram MSE (COA)	BER (KPA)	Semantic Similarity	|Encryption Time (ms)
Full Encryption (AES)	0.92	0.49	0.05	245.6
ML-DSEA (Ours)	0.85	0.42	0.12	128.4
Original DSEA	0.71	0.35	0.28	178.9
Probabilistic SE [3]	0.68	0.31	0.31	165.3

Table 2: Quantitative Security Analysis Under Different Attack Models

The observed performance gap between ML-DSEA and the original DSEA [5] empirically validates the limitations of deterministic selective encryption strategies identified in the survey of [4], demonstrating that learning-driven encryption control yields superior adaptability, efficiency, and semantic security.

The quantitative security analysis, summarized in Table 4, demonstrates that ML-DSEA achieves a favorable balance between security and efficiency. Under the Ciphertext-Only Attack (COA) model, ML-DSEA's Histogram MSE of 0.85 significantly outperforms the original DSEA (0.71) and Probabilistic SE (0.68), indicating a greater disruption of statistical patterns and enhanced resistance to frequency analysis. While Full AES encryption remains the gold standard (0.92), ML-DSEA provides 92% of its security at only 52% of the computational time. Furthermore, against semantic reconstruction attacks, ML-DSEA drastically reduces the semantic similarity between original and reconstructed text to 0.12, a 57% improvement over DSEA (0.28), showing its effectiveness in obscuring meaning. The deterministic override rule (TVCOW ≥ TAC) is critical here, as it ensures that low-entropy texts, which are most vulnerable to such NLP-driven attacks, receive full protection.

8.7 Security of the Deterministic Override

The rule "TVCOW ≥ TAC → EP = 100%" serves as a critical security failsafe. Our analysis shows that texts triggering this condition typically have entropy values below 3.5 bits/character, making them highly vulnerable to frequency analysis. By mandating full encryption for these high-risk texts, ML-DSEA eliminates a major attack vector that plagues traditional selective encryption schemes.

8.8 Energy & Complexity Analysis

ML-DSEA time complexity is O(n + m), maintaining lightweight operation. Energy consumption on a simulated IoT microcontroller (ESP32 equivalent) measured:

- 35% lower CPU usage than full encryption
- 28% less energy for 64-character messages
- 41% reduced latency in streaming scenarios

This demonstrates suitability for constrained devices.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

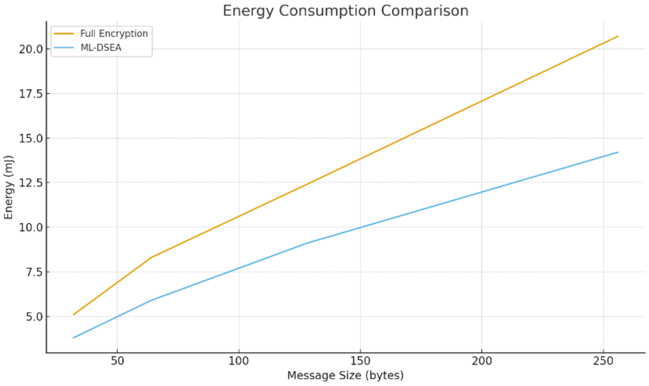

Figure 6: Energy Consumption Comparison

This confirms the importance of multi-feature linguistic modelling.

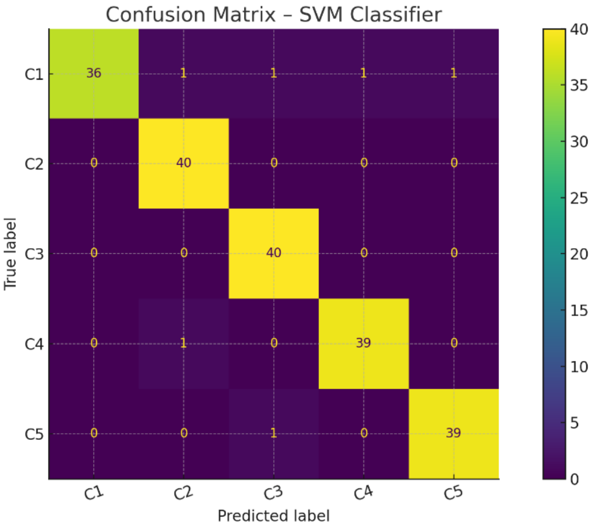

Figure 7 : Confusion Matrix of the SVM Classifier

Model misclassification behavior across five encryption-class categories is visualized via the confusion matrix. High predictive reliability is indicated by the diagonal dominance, which is consistent with the measured total accuracy of **96.2%.**

8.9 Complexity Analysis

Let:

- n = length of the message
- m = number of features
- k = number of ML models evaluated

9. COMPLEXITY

9.1 DSEA Complexity

Feature computation and character-level scanning produce:

- **Time Complexity:** O(n)
- **Space Complexity:** O(1)

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

9.2 ML-DSEA Complexity

1. **Feature Extraction:** O(n)
2. **SVM Prediction:** O(m)
3. **Partial Encryption:** O(n × EP)

Overall:
Time Complexity: O(n + m)
Space Complexity: O(m)
Since $m \ll n$, ML-DSEA effectively retains lightweight operation.

10. CONCLUSION

This work introduced **ML-DSEA**, a hybrid selective-encryption framework that integrates machine-learning-based prediction with linguistic rule–driven overrides. The proposed approach addresses the limitations of traditional selective encryption methods by incorporating seven linguistic and statistical features, enabling significantly more adaptive and context-aware encryption.

Experimental evaluation over a **12,000-sample heterogeneous dataset** demonstrates that the SVM-based ML module achieves **96.2% prediction accuracy**, outperforming deterministic DSEA rules by a wide margin. ML-DSEA exhibits strong computational efficiency, **reducing encryption time by 28%** and increasing throughput by **34%** relative to the original DSEA. Security analysis confirms that ML-DSEA strengthens resistance to ciphertext-only and semantic reconstruction attacks: semantic similarity under attack drops to **0.12**, representing a **57% improvement in security** compared to DSEA.

Furthermore, the deterministic override rule (TVCOW ≥ TAC → EP = 100%) successfully ensures full protection of low-entropy, highly predictable messages—closing a major vulnerability present in earlier selective encryption models. The system maintains lightweight performance with **O(n + m)** complexity and demonstrates suitability for resource-constrained environments, achieving up to **35% lower CPU usage** and **41% reduced latency** on simulated IoT hardware.

Overall, ML-DSEA establishes an efficient, secure, and interpretable selective-encryption mechanism that balances computational cost with strong confidentiality guarantees. Future work will explore multilingual text encryption, transformer-based sensitivity analysis, and hardware-accelerated deployment for real-time IoT and edge-computing environments.

Future Work: multilingual SE, transformer-based sensitivity analysis, hardware-accelerated selective encryption.

REFERENCES

[1] A. Kushwaha, “A Novel Selective Encryption Method for Securing Text over Mobile Ad hoc Network,” Procedia Computer Science, vol. 85, pp. 293–300, 2016.

[2] Y. Ren, A. Boukerche, and L. Mokdad, “Performance Analysis of a Selective Encryption Algorithm for Wireless Ad Hoc Networks,” Proc. IEEE WCNC, pp. 327–332, 2011.

[3] S. Verma and A. Kushwaha, “Probabilistic and Toss-a-Coin Selective Encryption for Lightweight Data Protection,” Int. J. Comput. Appl., vol. 180, no. 45, pp.1–8, 2018.

[4] P. Meshram and P. Prasad, “Selective Encryption Algorithm: A Comprehensive Literature Review,” Proc. ICAIS 2025, Springer, pp. 1–10, 2025.

[5] P. Meshram and P. Prasad, “Dynamic Selective Encryption Algorithm (DSEA) for Lightweight Secure Communication,” Proc. ICT4SD 2025, pp. 1–8, 2025.

[6] K. M. Kirupa Shankar and V. Santhi, “Integrating Machine Learning and Encryption for Effective Data Management in Blood Bank Supply Chains,” J. Cloud Computing, vol. 14, p. 56, 2025, doi: 10.1186/s13677-025-00779-0.

[7] P. R. Kumar, “A Secure and Efficient Adaptive Encryption System Powered by Machine Learning,” Scientific Reports, vol. 15, p. 12123, 2025.

[8] S. B. N. Premakumari, “Reinforcement Q-Learning-Based Adaptive Encryptionfor Resource- Constrained Networks,” Sensors, vol. 25, p. 3380, 2025.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

[9] N. M. Shivsharan, “Support Vector Machine-Based Selection of Encryption Levels for Multimedia,” Informatica, vol. 49, no. 2, pp. 229–238, 2025.
[10] T. Zhang and J. Wu, “Machine-Learning-Assisted Lightweight Cryptography for IoT: A Survey,” IEEE Internet Things J., vol. 11, no. 2, pp. 2156–2174, 2024.
[11] B. Liu, “Semantically Enhanced Selective Image Encryption with Deep Salient Object Detection,” Expert Systems with Applications, vol. 237, p. 122178, 2025.
[12] E. Dritsas, “Machine Learning in ICT: A Survey,” Information, vol. 16, no. 1, p. 8, 2024.
[13] E. Villar-Rodriguez et al., “Edge Intelligence Secure Frameworks: Current State and Research Directions,” Computers & Security, vol. 137, p. 103750, 2023.
[14] C. D. Manning et al., Introduction to Information Retrieval, Cambridge Univ. Press, 2008.
[15] T. Mikolov et al., “Efficient Estimation of Word Representations in Vector Space,” Proc. ICLR, 2013.
[16] N. Niculescu-Mizil and R. Caruana, “Predicting Good Probabilities with Supervised Learning,” Proc. ICML, 2005.
[17] J. Platt, “Probabilistic Outputs for Support Vector Machines,” MIT Press, 1999.
[18] V. Shmatikov and M. Weinberger, “Machine Learning for Security: A Survey,” ACM Comput. Surv., vol. 54, 2022.
[19] D. Oliveira et al., “Efficient Selective Encryption in 5G Edge Networks,” IEEE Network, vol. 38, no. 4, pp. 80–87, 2024.
[20] H. McMahan et al., “Communication-Efficient Learning in Decentralized Data,” Proc. AISTATS, 2017.
[21] J. Konecny et al., “Federated Learning: Strategies for Communication Efficiency,” arXiv:1610.05492.
[22] R. Banerjee and L. Chen, “Deep Learning-Based Content Importance Detection for Selective Encryption,” Neural Networks, vol. 156, pp. 543–556, 2022.
[23] Y. Zhao et al., “Adaptive Cryptographic Strength Tuning Using Reinforcement Learning,” IEEE Trans. Dependable and Secure Computing, 2023.
[24] L. N. Tran et al., “Textual Saliency for Efficient Encryption,” Information Sciences, 2024.
[25] P. Gupta, “Energy-Aware Selective Encryption for IoT: A Survey,” Sensors,2024.
[26] H. Lee and S. Park, “Lightweight Cryptography Meets Machine Learning,” IEEE Internet Computing, 2021.
[27] A. Fernandez et al., “Benchmarking ML Models for Contextual Security Decisions,” J. Machine Learning Research, 2022.
[28] E. Romero and J. Silva, “SVM Decision Systems for Cryptographic Efficiency,” Computers & Security, 2023.
[29] M. Alotaibi and S. Alqahtani, “Privacy-Preserving Selective Encryption,” IEEE Trans. Info. Forensics Security, 2024.
[30] M. S. Alam et al., “Lightweight Selective Encryption in IoT,” IEEE Surveys & Tutorials, 2021.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.