PROJECT REVIEW 1

ADAPTIVE CRYPTOGRAPHIC KEY MANAGEMENT USING MACHINE LEARNING BASED INTRUSION DETECTION

Arshia -1409
Nidhi -1429
Haseena - 1449

TABLE OF CONTENTS

INTRODUCTION

- Communication is the backbone of today’s digital world.
- Safety of information and data is very important.
- Attackers use cryptanalysis to break keys, so there is a need to detect and respond fast.
- Intrusion Detection Systems (IDS) are used to detect unusual activities.
- Present IDS face issues like limited adaptability,cost and slow response.

SECURE COMMUNICATION IN NETWORKS: A COMPREHENSIVE SURVEY OF LIGHTWEIGHT ENCRYPTION AND KEY MANAGEMENT TECHNIQUES

1. Standard cryptographic schemes (e.g., RSA, full AES) exceed energy and compute budgets, making them impractical for real-time aerial missions.
2. Literature highlights the urgency of designing cryptographic solutions that align with constraints—low power, limited memory, and latency sensitivity.
3. ASCON, ChaCha20, and AES variants strike a balance between security and efficiency, optimized for constrained platforms without sacrificing robustness.
4. Algorithms are assessed on computational complexity, memory footprint, energy consumption, and latency critical for mission-critical responsiveness.
5. Key compromises include:
    - Speed vs. memory usage
    - Security strength vs. energy efficiency
    - Latency vs. throughput
6. Lightweight cryptography enables scalable, secure communication , supporting dynamic keying and low-latency encryption.

ENHANCING SECURITY FEATURES IN WSNS USING AUTOENCODER-BASED INTRUSION DETECTION AND ECC WITH DYNAMIC KEY ROTATION

- **SVM-AES:** High accuracy (84%) but energy-heavy; lacks dynamic routing and key agility due to static AES overhead.
- **RF-KSS:** Suffers from node desynchronization, increasing latency and exposure to coordinated replay attacks.
- **XGBoost-FR:** Performs well on static data but fails under zero-day threats and dynamic traffic shifts.
- **ES-ML Models:** Use balancing and reduction techniques; improve detection on skewed data but lack replay resilience and adaptive key/session handling.
- **Dual Classifiers (SVM-AES + RNN):** Enhance temporal modeling but introduce high latency and static encryption, limiting scalability.
- **Missing Foundations:** No current model integrates dynamic key rotation, energy-aware routing, or adaptive learning under concept drift.

DYNAMIC KEY CRYPTOGRAPHY AND APPLICATIONS

1. Old cryptography is weak → fixed keys (Caesar, monoalphabetic) are easy to break; even modern ciphers (DES, AES) fail if a static key is stolen.
2. Dynamic key idea → keys change continuously (per session, block, or round), so attackers never get enough data with one key.
3. Approach → build on existing block ciphers by auto-generating new subkeys without heavy computation.
4. Advantages → backward-compatible, efficient, and much more secure (resists brute force, frequency, differential, linear attacks).
5. Applications → secure communication (mobile, banking, e-commerce, military), especially where long-term secrecy is critical.

EVALUATING THE PERFORMANCE OF CLASSIFICATION ALGORITHMS ON THE UNSW-NB15 DATASET FOR NETWORK INTRUSION DETECTION

- Intrusion Detection Systems (IDS) aim to secure networks by analyzing traffic using both misuse-based and anomaly-based detection methods.
- Machine learning algorithms such as Decision Trees, Support Vector Machines (SVM), K-Nearest Neighbors (KNN), and Neural Networks are widely applied for threat detection.
- Feature selection and dimensionality reduction techniques like PCA (Principal Component Analysis) improve accuracy and reduce computational cost.
- IDS models are often trained and tested using benchmark datasets such as KDD Cup 99, NSL-KDD, or UNSW-NB15.
- The ultimate objective is to build real-time, adaptive, and scalable IDS with high detection rates and minimal false alarms.

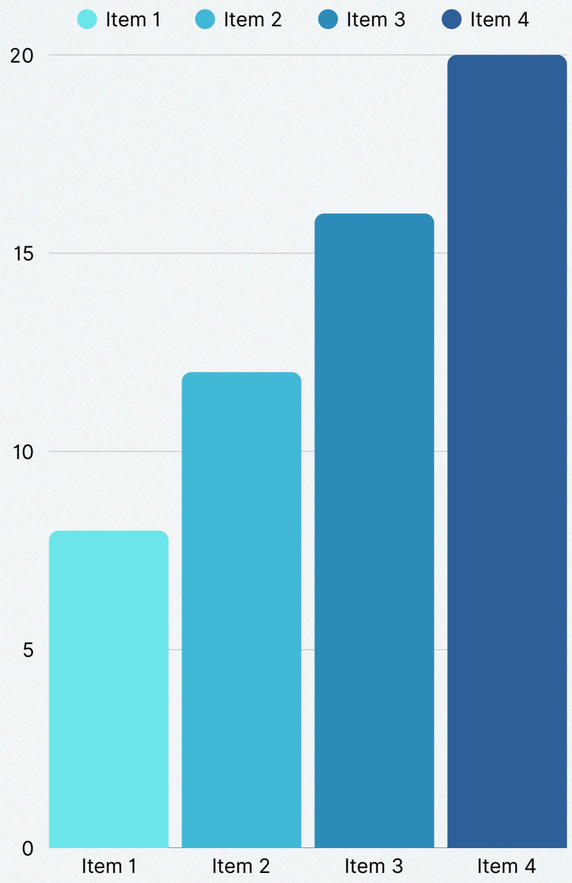
MACHINE LEARNING BASED NETWORK ANOMALY DETECTION

1. Two-Phase Model – The authors propose a two-phase anomaly detection system:
2. Phase 1: Random Forest is used to detect anomalies and generate a feature called “attack-or-not”.
3. Phase 2: A Neural Network uses this feature to further classify the type of attack.
4. Dataset Used – The model is trained and tested on the UNSW-NB15 dataset, which contains 2.5 million+ records with 47 features, covering nine modern attack families (e.g., DoS, Exploits, Worms, Backdoors).
5. Performance of Algorithms – Out of 11 classifiers tested, Random Forest achieved the highest accuracy (98%), followed by Decision Tree and CART (97%). Other algorithms like SVM and Naïve Bayes performed worse.
6. Result :- In anomaly detection phase, the model achieved 0.99 Precision and Recall, showing high effectiveness in detecting whether traffic is normal or malicious.
7. In attack categorization phase, the Neural Network achieved 0.93 Precision and 0.88 Recall, but struggled with differentiating certain attack types.

PERFORMANCE EVALUATION OF INTRUSION DETECTION BASED ON MACHINE LEARNING USING APACHE SPARK

- Traditional IDS approaches (misuse and anomaly detection) suffer from issues like frequent updates, high false positives, and low accuracy. The paper aims to overcome these challenges with machine learning.
- Among all algorithms tested, Random Forest performed best with the highest accuracy (97.49%), sensitivity (93.53%), and specificity (97.75%). It also had the fastest prediction time, though Naïve Bayes was the fastest to train.

Methods	Accuracy	Sensitivity	Specificity	Training Time	Prediction Time
SVM	92.28	92.13	91.15	38.91	0.20
Naïve Bayes	74.19	92.16	67.82	2.25	0.18
Decision Tree	95.82	92.52	97.10	4.80	0.13
Random Forest	97.49	93.53	97.75	5.69	0.08



REASERCH ON DATA-SETS

- **KDD CUP 99**

Large scale, highly redundant, simulated attacks,biases model learning

- **NSL-KDD**

Removes duplicates, more representative, still lacks real network scenarios

- **UNSW-NB15**

Mix of real and synthesized traffic, 49 features, covers modern attacks, Lacks data of protocol type and mostly used

FINALISED DATASET AND IT'S PARAMETERS

(LINK IN REFERENCES)

- The dataset consists of network-based and user behavior-based features. Each feature provides valuable information about potential cyber threats. It is Licensed MIT .
- The dataset is useful for supervised machine learning, where a model learns from labeled attack patterns.

network_packet_size
(Packet Size in Bytes)

protocol_type
(Communication Protocol)

encryption_used
(Encryption Protocol)

login_attempts
(Number of Logins)

session_duration
(Session Length in Seconds)

failed_logins
(Failed Login Attempts)

ip_reputation_score
(Trustworthiness of IP Address)

browser_type
(User's Browser)

Target Variable
(attack_detected)

CONCLUSION

Problem: Hackers exploit static cryptographic keys → compromises communications.
Solution: Adaptive framework combining: **Machine Learning-based Intrusion Detection (IDS) Real-time Cryptographic Key Rotation**

Intrusion Detection System (IDS):

- Uses supervised ML algorithms
- Trained on previously described datasets
- Detects anomalous traffic patterns with high accuracy

Key Rotation Mechanism:

- On detecting intrusion , the system automatically updates encryption keys
- AES for data encryption
- Diffie-Hellman / Elliptic Curve Diffie-Hellman (ECDH) for secure key exchange

Evaluation Metrics:

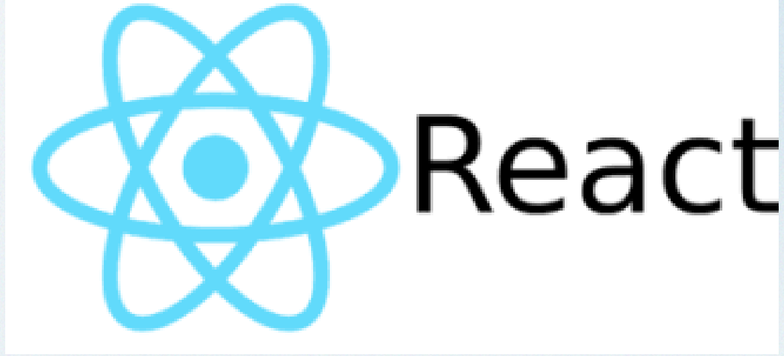
- Detection Accuracy
- False Positive Rate
- Latency Impact
- Throughput changes after key rotation

EXPECTED RESULT

Results will be:

1. Stronger network security
2. Attack window minimized
3. Fast and optimised intrusion detection
4. Low performance overhead → practical for enterprise & cloud environments

TECH STACK



REFERENCES

Dataset

- https://www.kaggle.com/datasets/dnkumars/cybersecurity-intrusion-detection-dataset

Research Papers

- Dynamic Key Cryptography and Applications
- Secure Communication in Networks: A Comprehensive Survey of Lightweight Encryption and Key Management Techniques
- Enhancing Security Features in WSNs using Autoencoder-Based Intrusion Detection and ECC with Dynamic Key Rotation
- Machine Learning Based Network Anomaly Detection
- Performance evaluation of intrusion detection based on machine learning using Apache Spark
- Evaluating the Performance of Classification Algorithms on the UNSW-NB15 Dataset for Network Intrusion Detection

THANK YOU