REACT: Randomized Encryption with AI-Controlled Targeting for Next-Gen Secure Communication

Zhangying He and Hossein Sayadi
Department of Computer Engineering and Computer Science
California State University Long Beach
Long Beach, CA, USA 90840

***Abstract*—This work introduces *REACT* (Randomized Encryption with AI-Controlled Targeting), a novel framework leveraging Deep Reinforcement Learning (DRL) and Moving Target Defense (MTD) to secure chaotic communication in resource-constrained environments. *REACT* employs a random generator to dynamically assign encryption modes, creating unpredictable patterns that thwart interception. At the receiver's end, four DRL agents collaborate to identify encryption modes and apply decryption methods, ensuring secure, synchronized communication. Evaluation results demonstrate up to 100% decryption accuracy and a 51% reduction in attack success probability, establishing *REACT* as a robust and adaptive defense for secure and reliable communication.**

***Index Terms*—AI-Enabled Security, Chaos-Based Encryption, Internet of Things, Machine Learning, Reinforcement Learning.**

I. Introduction and Background

Advancements in Internet of Things (IoT), Artificial Intelligence (AI), and computing technologies have enabled interconnected smart systems, enhancing efficiency, convenience, and service quality. However, transmitting sensitive data over public channels poses persistent security challenges and vulnerabilities to cyber threats. Traditional cryptographic techniques, such as AES and RSA, demand substantial energy, memory, and computing power, making them less suitable for IoT devices with limited resources.

Chaos cryptography has gained prominence as a more viable alternative. Chaotic systems [1]–[3], with their simple architecture and inherently unpredictable behavior, provide robust cryptographic solutions for secure data transmission between IoT devices, embedded systems, and cloud infrastructures.

Despite advancements, significant challenges remain in securing IoT systems. Many IoT devices and their network traffic lack encryption, exposing critical components to potential threats. Resource constraints in IoT systems necessitate computationally efficient and hybrid encryption techniques. Machine learning-based methodologies provide streamlined solutions compared to traditional approaches, addressing the complexity and diversity of IoT systems. Furthermore, cryptographic methods should prioritize the complexity of the encryption process over reliance on key secrecy [4], ensuring greater unpredictability and security in IoT networks [5].

In this work, we present *REACT* (Randomized Encryption with AI-Controlled Targeting), a chaos-based, ML-enabled encryption-decryption framework for next-generation secure communication. *REACT* employs Deep Reinforcement Learning (DRL) to enhance security through a dynamic Moving Target Defense (MTD) strategy. It features a lightweight hardware-level chaotic system for IoT devices, encrypting messages into random, non-repetitive signals to ensure communication security. *REACT* incorporates a randomization-based strategy that cycles among four chaotic encryption modes on the sender's side, while four deep DRL-enabled parallel controllers on the receiver's side ensure accurate decryption and deploy a dynamic moving target defense strategy for improved efficiency. Additionally, chaotic-encrypted messages are decrypted using ML models, offering robust and adaptive communication security.

II. Proposed Methodology

1) Threat Model: Our threat model addresses adversaries targeting IoT network data both during transmission and at rest.

In-Transit Lightweight Encryption. Hackers can exploit vulnerabilities during the data generation and transmission processes, compromising individual devices and the overall connected system. To mitigate these risks, as shown in Figure 1, it is crucial to encrypt sensor data generated by wearable devices before transmission and storage [6]. Lightweight encryption methods are essential to accommodate the resource-constrained nature of IoT devices while maintaining robust security.

At-Rest Data Encryption. Attackers may intercept network transmissions to capture ciphertext and attempt to reverse engineer it to the original message. To counter such threats, sensitive data stored in IoT system databases must be encrypted. An efficient decryption mechanism is equally critical, ensuring data can only be decrypted when queried and processed, thereby minimizing exposure and maintaining security.

2) Overview of REACT: Figure 1 illustrates the *REACT* framework, our proposed AI-enhanced, dual-stage encryption and decryption system for IoT devices. In the first stage, a lightweight chaotic system performs hardware-level data encryption at the sender's end, while machine learning aids decryption at the receiver's end. We implemented five time-series classifiers in Scikit-Learn and TensorFlow to decode encrypted signals into their original messages. The second stage employs randomization techniques at the sender's side to enhance security, complemented by DRL-enabled parallel controllers for adaptive decryption at the receiver's side. We customized the RL environment extended from OpenAI's Gym baseline class gym.Env and implemented four Advantage Actor Critic (A2C)-based RL agents for parallel controllers using TensorFlow. This design addresses vulnerabilities in both data transmission and storage, ensuring robust IoT security.

The *REACT* framework comprises four key components: *1) Hardware-level Chaotic Encryption:* Lightweight encryption

978-3-9826741-0-0/DATE25/© 2025 EDAA

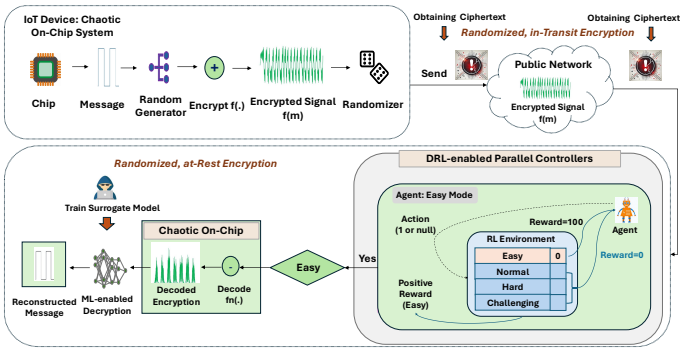

Fig. 1: Overview of *REACT* framework. The random generator dynamically selects one of four encryption modes, while trained deep reinforcement learning-based parallel controllers at the receiver accurately predict the encryption mode

implemented at the hardware level. *2) MTD-based Randomized Encryption Mode Generator:* Dynamically selects one of four encryption modes (Easy, Normal, Hard, Challenging) at the sender's side to introduce randomness and complexity. *3) DRL-enabled Parallel Controllers:* DRL agents at the receiver predict the encryption mode for adaptive decryption. For simplicity, Figure 1 shows the Easy mode agent. *4) ML-enabled Decryption:* ML models recover the original messages from encrypted signals, ensuring efficient and accurate decryption.

To achieve signal synchronization with encryption, a Chua's transmitter and receiver [7] were implemented in MATLAB Simulink, following the approach described in [1]. Four modes of Chua's signal encryption (Easy, Normal, Hard, Challenging) were developed, each generating three types of signals: *Out.m* (original message), *Out.X* (encrypted message), and *Out.Sync* (decoded encrypted message from the Chua's receiver).

III. Evaluation Results

1) ML-Enabled Signal Decryption: We evaluated various machine learning models to decrypt signals across four encryption modes. Under optimal conditions, nearly all tested models achieved perfect scores in accuracy, F1-score, precision, and recall, as shown in the first bar group in Figure 2. For normal and hard encryption modes (second and third groups), the LSTM model demonstrated exceptional decryption performance, achieving an impressive F1-score of 95%. However, for challenging signals, the LSTM's performance declined to an F1-score of 88%. In contrast, Random Forest, MLP, and KNN with DTW consistently maintained a high decryption F1-score of approximately 90%, even under challenging conditions. The results suggest that IoT systems, with knowledge of updated encryption modes, can effectively fine-tune ML models to decrypt ciphered messages reliably.

2) Effectiveness of the Randomization Strategy: Figure 3 depicts the evaluation of the proposed adaptive defense strategy (blue dots), which employs randomization on the sender's side and DRL-enabled parallel controllers on the receiver's side to predict encryption modes. This approach is benchmarked against the best-case (orange bars) and worst-case (purple bars) cipher attacks produced by attackers' surrogate models across the four encryption modes. As shown, surrogate models trained on mixed messages fail to converge, achieving F1-scores of approximately 50% across all models. The randomized

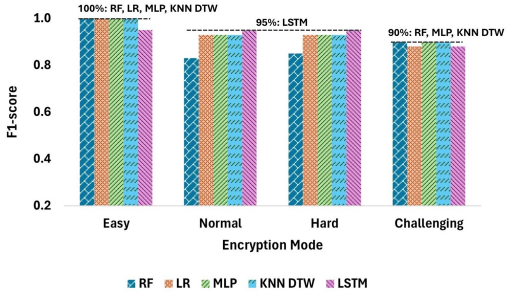

Fig. 2: ML-enabled decryption performance: Average F1-score with 5-fold cross-validation

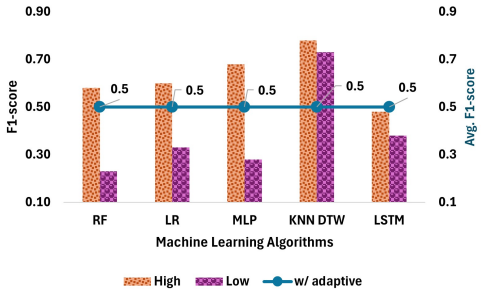

Fig. 3: Adaptive defense F1-scores across all models, compared with the highest and lowest F1-scores from the attacker's surrogate model without moving target defense

and diverse encrypted ciphertexts exposed to attackers add an additional layer of complexity, making it significantly harder and costlier for attackers to recover the protected messages. Consequently, the surrogate models remain ineffective, operating at a guess-level accuracy.

IV. Conclusion

In this paper, we introduced *REACT*, an AI-driven framework designed to enhance chaotic communication security in resource-constrained devices using reinforcement learning and randomization. *REACT* encrypts time-series sensor data via a hardware-based chaotic scheme, randomly selecting from four modes for secure public transmission with dual-randomized signals. At the receiver, four DRL agents collaboratively identify the encryption mode and apply the proper decryption model, ensuring robust and adaptive communication security.

V. Acknowledgment

This work is supported in part by the National Science Foundation under Grant Nos. 2131156 and 2139034.

References

[1] J. Hwang *et al.*, "Machine learning in chaos-based encryption: Theory, implementations, and applications," *IEEE Access*, vol. 11, pp. 125 749–125 767, 2023.

[2] L. Kocarev, "Chaos-based cryptography: a brief overview," *IEEE Circuits and Systems Magazine*, vol. 1, no. 3, pp. 6–21, 2001.

[3] A. Hedayatipour *et al.*, "A comprehensive analysis of chaos-based secure systems," in *Silicon Valley Cybersec. Conf.* Springer, 2021, pp. 90–105.

[4] W. Wen *et al.*, "Differential attack on a hyper-chaos-based image cryptosystem with a classic bi-modular architecture," *Nonlinear Dynamics*, vol. 87, pp. 383–390, 2017.

[5] K. Demir and S. Ergün, "Cryptanalysis of a random number generator based on continuous-time chaos," *IET Circuits, Devices & Systems*, vol. 14, no. 5, pp. 569–575, 2020.

[6] V. Adat and B. B. Gupta, "Security in internet of things: issues, challenges, taxonomy, and architecture," *Telecommunication Systems*, vol. 67, pp. 423–441, 2018.

[7] Z. Galias, "Positive topological entropy of chua's circuit: A computer assisted proof," *International Journal of Bifurcation and Chaos*, vol. 7, no. 02, pp. 331–349, 1997.