IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 13 October 2023, accepted 30 October 2023, date of publication 8 November 2023, date of current version 13 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3331320

TOPICAL REVIEW

Machine Learning in Chaos-Based Encryption: Theory, Implementations, and Applications

JINHA HWANG[1], GAURI KALE[2], PERSIS PREMKUMAR PATEL[1], RAHUL VISHWAKARMA[1], (Graduate Student Member, IEEE), MEHRDAD ALIASGARI[1], AVA HEDAYATIPOUR[2], (Member, IEEE), AMIN REZAEI[1], (Member, IEEE), AND HOSSEIN SAYADI[1], (Member, IEEE)

[1]Department of Computer Engineering and Computer Science, California State University Long Beach, Long Beach, CA 90840, USA
[2]Department of Electrical Engineering, California State University Long Beach, Long Beach, CA 90840, USA

Corresponding author: Ava Hedayatipour (Ava.Hedayatipour@csulb.edu)

This work was supported by the National Science Foundation under Grant 2131156.

ABSTRACT Chaos-based encryption is a promising approach to secure communication due to its complexity and unpredictability. However, various challenges lie in the design and implementation of efficient, low-power, attack-resistant chaos-based encryption schemes with high encryption and decryption rates. In addition, Machine learning (ML) has emerged as a promising tool for enhancing the growing security and efficiency concerns and maximizing the potential of emerging computing platforms across diverse domains. With the rapid advancements in technology and the increasing complexity of computing systems, ML offers a unique approach to addressing security challenges and optimizing performance. This paper presents a comprehensive study on the application of ML techniques to secure chaotic communication for wearable devices, with an emphasis on chaos-based encryption. The theoretical foundations of ML for secure chaotic communication are discussed, including the use of ML algorithms for signal synchronization, noise reduction, and encryption. Various ML algorithms, such as deep neural networks, support vector machines, decision trees, and ensemble learning methods, are explored for designing chaos-based encryption algorithms. This paper places a greater emphasis on methodological aspects, metrics, and performance evaluation of machine learning algorithms. In addition, the paper presents an in-depth investigation into state-of-the-art ML-assisted defense and attacks on chaos-based encryption schemes, covering their theoretical foundations and practical implementations. Furthermore, a review of the potential advantages and limitations associated with the utilization of ML techniques in secure communication systems and encryption is provided. The study extends to exploring the diverse range of applications that can benefit from ML-assisted encryption, such as secure communication in the Internet of Things (IoTs), cloud computing, and wireless networks. Overall, we provide insights into the applications of ML for secure chaotic communication in wearable devices, its challenges, and opportunities, offering a foundation for further research and development and facilitating advancements in the field of secure chaotic communication.

INDEX TERMS Quantum computing, quantum-safe, chaos, chaotic map, encryption, side channel attacks, machine learning, artificial intelligence, hardware security.

I. INTRODUCTION

The amount of data created over the next three years will be greater than the data created in the past 30 years combined [1]. According to a study by the International Data Corporation (IDC), the global datasphere, which includes all the data created, captured, and replicated, is expected to grow from 33 ZettaBytes (ZB) in 2018 to 175 ZB by 2025 (Fig. 1). This represents a Compound Annual Growth Rate (CAGR) of 61%. The growth in data is being driven by the data generated from IoT sensors, wearable devices [2], [3], and medical data records. Moreover, financial institutions [4] can store

The associate editor coordinating the review of this manuscript and approving it for publication was Alberto Cano.

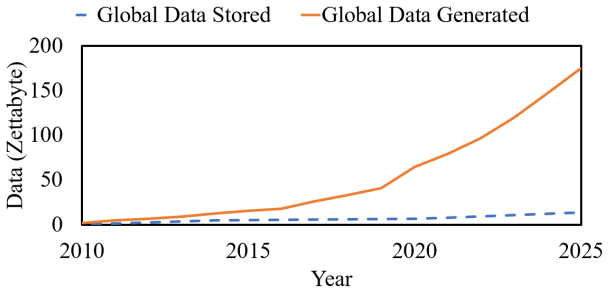


FIGURE 1. Global data growth trajectory from 2010 to 2025 - This figure illustrates the escalation in global data generation and the corresponding data storage capacity over fifteen years.

mission-critical data for several years or even indefinitely, to comply with anti-money laundering regulations [5] and to facilitate customer service and support as mandated by the Securities and Exchange Commission (SEC) in the United States.

Today, a vast amount of data is generated by the healthcare sector, accounting for approximately 30% of the global data volume, which provides invaluable insights and opportunities for advancements in patient care and medical research [6]. With a projected CAGR of 36% for health data by 2025, harnessing and effectively utilizing this data becomes even more crucial for driving evidence-based decision-making, personalizing treatments, and improving health outcomes [7]. With wearable devices finding their way into our healthcare system, it is specifically important to secure high-risk sensitive healthcare wearable systems including implantable pacemakers, biofluidic-based wearables, and skin-based wearables; considering the corner cases where an attacker can access the data and manipulate it to cause life-threatening situations.

Cryptographic methods [8] for security in today's world are generally composed of two categories of symmetric and asymmetric solutions. Numerous algorithms are developed for asymmetric encryption, such as Rivest-Shamir-Adleman (RSA), the Digital Signature Algorithm (DSA), and Elliptic Curve Cryptography (ECC). The security of RSA and ECC relies on the difficulty of integer factorization and discrete logarithm problems. Symmetric algorithms can be classified into two main types: block algorithms and stream algorithms. Block algorithms encrypt data block by block, which can lead to potential security gaps due to the wait time for complete blocks. Stream algorithms, on the other hand, encrypt data byte by byte or even bit by bit, providing increased security as data is not retained in the system's memory without encryption. Examples of encryption algorithms include Data Encryption Standard (DES), Triple DES, Advanced Encryption Standard (AES), RC2, and Blowfish. Hash-based, digital signature, DeoxyriboNucleic Acid (DNA)-based cryptography [9], and quantum cryptography [10] also play a vital role in ensuring secure communication and data protection in various applications and systems. However, with the advent of quantum computers, RSA and ECC solutions will not be secure [11]. This poses a serious concern, as these algorithms are the most commonly used algorithms for secure key exchange. On a theoretical level, Shor's factoring algorithm [12] can solve the problems in polynomial time, and this heads toward a new area of cryptography, i.e., Post-Quantum Cryptography (PQC) [13] that aims to develop new algorithms and techniques that can resist attacks from quantum computers.

National Institute of Standards and Technology (NIST), an organization that promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure [14] is following steps to initiate a standardization effort in PQC. The industry is already transitioning to the PQC era [15] from a proactive approach to security. The CRYSTALS-Kyber [16] is a quantum-safe algorithm developed by IBM Research that was also selected by NIST as one common encryption algorithm to access secure websites.

In recent years, researchers have been exploring the use of chaotic maps in cryptography, particularly in the context of PQC. One approach that has been proposed is to use Chebyshev polynomials [17], which are based on a chaotic map, for encryption. However, this approach was quickly broken in the first round of the NIST PQC and it was withdrawn from the competition. This raises the question of whether the attack was inherent to Chebyshev polynomials or whether the specific cryptosystem used in the competition was poorly chosen. To address this issue, researchers have been exploring other options for using chaotic maps in cryptography. One promising approach is to use a Lorenz chaotic map [18] for secret-key exchange. This approach has been shown to be effective in a hash algorithm for a stream cipher that is designed for the PQC era. By leveraging the chaotic behavior of the Lorenz map and other chaotic equations, it is possible to create a secure and robust encryption scheme that is resistant to attacks from quantum computers.

An alternate approach to using chaos-based techniques for designing cryptosystems can be implemented by creating a hyper-chaotic circuit and carefully choosing the components that will increase the key space for encryption. Once such an approach is demonstrated in [19] which uses memristive components as tunable keys and also implements the concept of logic locking [20] for enhanced security. However, the main challenge even after designing the encryption algorithm is retrieving the information at the destination (decryption), as during chaotic encryption, the original signal is mixed with the chaotic system. Synchronization between the encryptor and decryptor is a key component of a chaotic cryptosystem. To solve this issue, Machine Learning (ML) approaches can be used to synchronize the output signal.

In this paper, we first look at the methods of chaotic map-based cryptosystems as a hardware implementation and at the application of ML approaches to the synchronization of the output signal. We also review ML as a tool to attack

chaotic systems. The paper is organized as follows: We provide a detailed background on chaotic maps in Section II and in Section III we discuss the ability of ML, and specifically reservoir computing, to predict chaotic behavior. Further, in Section IV an ML approach to synchronizing the signals is implemented using different clustering and categorizing algorithms. We then evaluate the various ML-based attacks on the chaotic encryption systems in Section V. Finally, in Section VI we provide the overall discussion, followed by the conclusion in Section VII.

II. THE HISTORY OF CHAOS

In 1963, Lorentz presented the first well-known chaotic system. This marked the start of chaos theory, a branch of nonlinear system theory that has been studied intensively in recent years. Chaos can be applied to signals in two main ways (i.e., discrete-time vs. continuous-time chaotic systems), with distinct advantages and challenges in terms of encryption strength and security considerations.

A. DISCRETE-TIME CHAOS

Discrete-time chaotic systems are mathematically described with nonlinear functions where the output is an iterated function of the input. The general form of discrete-time chaotic systems can be expressed as follows:

$$x_{n+1} = f(C, x_n) \tag{1}$$

As shown in Eq. (1), the next state of the system, x_{n+1} is a function of the present state, x_n, and the control parameter, C. This nonlinear function is called a chaotic map. Depending on the number of state variables, chaotic maps are of two kinds: (i) One-dimensional maps, where only one deterministic equation is involved to describe the evolution of a single state variable. Examples of this kind are sine maps [29], tent maps [30], and logistic maps [31]. (ii) Multi-dimensional chaotic maps, that involve more than one deterministic equation to define the evolution of multiple state variables. Hénon map [32] falls into this second category. The simple mathematical expression of chaotic maps can be suitable for applications like FPGA-based image encryption [33]. However, it is reported that the CMOS-based compact implementation of classic chaotic maps becomes highly hardware-hungry. As a solution to this issue, researchers have been exploring how to leverage the built-in non-linearity in transistors to design simple, hardware-effective discrete maps with meaningful chaotic properties [34], [35], [36].

In recent years various new chaotic equations have been developed. A novel two-dimensional parametric polynomial chaotic system (2D-PPCS) was developed for various engineering applications like secure communication, image and data encryption, biological and physiological modeling, and many more [37]. Unlike existing chaotic systems with various limitations, the 2D-PPCS offers benefits such as continuous chaotic parameter ranges, robust chaos, and reduced occurrence of chaos degradation. This was achieved by utilizing modular quantification applied to two parametric polynomials, allowing for customization of Lyapunov exponents and desired complexity [38]. The study provided theoretical analysis and presented two examples, supported by numerical experiments, demonstrating the robust chaotic behavior of the 2D-PPCS [39]. As an application of this chaotic system, a pseudorandom number generator was developed to showcase practical applications, exhibiting superior performance compared to representative 2-D chaotic maps in generating higher randomness pseudorandom numbers [40].

Our primary focus lies in continuous-time signals, as our objective is to encrypt and transmit signals from resource-constrained devices and systems, all while avoiding the use of energy-intensive components and data conversion processes.

B. CONTINUOUS-TIME CHAOS

Continuous-time chaos generators are dynamic systems described by nonlinear differential equations, which encompass both Ordinary Differential Equations (ODEs) and Delay-Differential Equations (DDEs). The inherent instability within these chaotic dynamical systems leads to long-term unpredictability and positive entropy. To achieve desirable characteristics such as multiple equilibrium points and attractive regions, various equations incorporating nonlinear components are employed, including polynomial forms, sinusoidal, delay-based, and PieceWise-Linear (PWL) functions.

One of the most renowned examples of a chaotic system is the Lorenz attractor [21], [22], [23], known for its intricate and butterfly-like pattern. However, the original equations suffered from the complexity introduced by two multipliers, posing implementation challenges [24]. To address this drawback, a modified Lorenz system [25], [26] was introduced, represented by three differential equations without multipliers. This modified system successfully captures the essential behavior of the Lorenz attractor, including the generation of the butterfly effect, as well as modified and unsymmetrical Lorenz systems. Additionally, researchers have proposed various other variations of the Lorenz system, such as the four-dimensional Lorenz-Stenflo system [27], [28] with four parameters, aimed at improving stability and unpredictability. Table 1 summarizes continuous-time chaos approaches with the equations that can produce continuous chaos, along with their implementation based on scroll type and function. As seen in this table, Chaos can be implemented using various equations, with the common thread being the incorporation of a crucial nonlinear element featuring multiple equilibrium points. This fundamental characteristic underpins the intriguing nature of chaotic systems where, despite their inherent unpredictability, they remain confined within what are known as "attractive regions." Among the nonlinear elements that facilitate chaos are integrators, sinusoidal waveform generators, delay-based systems, and polynomial forms, as well as the notable inclusion

TABLE 1. Continuous-time chaotic communication approaches. These equations can be categorized based on their scroll type and function.

Name	Equation *	Scroll Type	Function
Lorenz [21], [22], [23]	$x' = \lambda\sigma(y - x)$ $y' = \lambda((\beta - z)x - y)$ $z' = \lambda(xy - \rho z)$	Double Scroll, Multi Scroll	Operational Transconductance Amplifier, Multiplier
Modified Lorenz [24], [25], [26]	$x' = \sigma(y - x)$ $y' = K(\beta - z) + m$ $z' = (\lvert x\rvert - \rho z)$	Double Scroll	Operational Transconductance Amplifier
Lorenz Stenflo [27], [28]	$x' = \sigma(y - x) + \lambda\omega$ $y' = (\beta - z)x - \theta y)$ $z' = xy - \epsilon z$ $\omega' = -x - \rho\omega$	Multi Scroll	Operational Transconductance Amplifier, Product

*: λ σ, β, ϵ, θ and ρ are parameters whose choice of value results in a chaotic system.
K is a bipolar switching constant which is 1 for x $\geq$ 0 and -1 for x $<$ 0

of piecewise-linear (PWL) functions. PWL functions, are especially adept at generating chaos due to their use of linear segments with abrupt transitions, thereby yielding complex behavior contingent upon their specific piecewise-linear structure. The realm of chaotic systems however extends beyond just PWL functions. Various other nonlinear systems and equations, such as the Rössler attractor, the Chua circuit, and the Duffing oscillator, further exemplify the diversity of chaotic behavior stemming from different forms of nonlinearity. In all these cases, the presence of nonlinear elements and equations featuring multiple equilibrium points can be the catalyst for chaotic dynamics. Notably, chaos is often marked by its sensitive dependence on initial conditions, where even slight alterations in the system's starting state can lead to vastly divergent trajectories over time. A comparative analysis of these methods has been done in our previous work [41].

A secure communication scheme for chaotic modulation based on the synchronization of the Lorenz system is proposed by Zapatorio et al. [42]. In this secure communication, the intensity limit, stability of the transmitted signal, characteristics of broadband, and requirements for the accuracy of electronic components have been presented by simulation and experiments. Following this work, Xiong et al. [43] proposed some improvements to the measurement method and the experimental circuit to facilitate the synchronization, with and without the signal. The possibility of synchronizing coupled analog and digital systems was experimentally proven. The digital model obtained with a semi-implicit numerical integration method gives fast and stable computer simulation. There are three different cases of synchronization: analog-to-analog, digital-to-analog, and analog-to-digital. El-Maksoud et al. [44] demonstrated that chaotic systems with chaotic dynamics have different communication, security, and computation applications consisting of high-speed and low-cost hardware for three-dimensional chaotic flows without equilibrium. As a proof of concept, they implemented their solution in hardware with low computational overhead on an FPGA board.

Various other chaotic attractors are also illustrated by FPGAs. Bonny et al. [45] proposed implementing chaotic attractors as True Random Bit Generators (TRBGs) on FPGA's. The high-speed TRBGs realized on a modular FPGA hardware platform use two switching-type chaotic oscillators. For that purpose, two different implementations are described for each TRBG: a throughput-optimized architecture and a resource-optimized architecture that utilizes fewer FPGA blocks. Wang et al. [46] investigated different modes of implementation, comparing the advantages and disadvantages of higher-dimensional chaotic oscillators on the throughput, hardware requirements, and security of the generated bitstreams. This investigation reveals that a real-time encryption process in analog circuitry can be achieved using off-the-shelf components.

For a range of applications, including e-government, e-identity cards, e-passports, e-visas, e-commerce, and public and private keys, chaos systems are used to produce random numbers. Bonny et al. [47] have proposed a complete hardware/software comparison and security analysis of three-dimensional chaotic and four-dimensional hyper-chaotic oscillator systems. Hyper-chaotic systems can exhibit a higher level of complexity in comparison with chaotic systems. The experimental results showed that the hyper-chaotic oscillator has a higher level of security than the chaotic one, but it is slower and utilizes more FPGA resources. This work explores the features of each oscillator system, such as throughput, FPGA resource utilization, operating clock frequency, and security of the generated bitstreams, to show a compromise solution for these features.

A comparative linearization of the chaos system is a promising direction for investigation. Linear circuits are useful as they can amplify and process electrical signals without introducing any distortion. A system is considered non-linear if the equation defining it comprises square or higher-order input/output components, products of input/output and their derivatives, or constants. Chua's equation is considered to have more linear elements and a chaos generator known as Chua's chaotic system, with many multi-scroll chaotic oscillators derived from the double-scroll Chua's equation [41]. In contrast to typical oscillators, an oscillator with infinite equilibria solely contains nonlinear components (quadratic, absolute, and cubic). The oscillator's unique qualities make it appropriate for security applications. Simulations and an electronic circuit have been used to learn more about

the oscillator's behavior. Lyapunov exponents, bifurcation diagrams, chaotic attractors, and the boosting feature are discussed [48].

As no external signal interferes with the system, Chua's circuit is autonomous, which means the chaotic state variables in an autonomous system can be synchronized [49]. A typical autonomous Chua's circuit, which has been reported as the equation with the least amount of hardware required, consists of three main components: resistors, capacitors, and inductors, and these components need to contain at least one nonlinear element, one locally active resistor, and three energy-storage elements. Real-world insight into controlling chaotic phenomena is beneficial in many fields, including secure communication, the medical field, and fractal theory, which encourages the implementation of these devices on-chip. However, the design of chaotic oscillators is challenging due to their sensitivity and fabrication variations, which may cause the mathematical model to suppress chaotic behavior.

Recent years have witnessed a significant advancement in biomedical applications of chaotic systems, specifically in image encryption. Although image encryption does not fit the focus of this paper, below are some examples of modern multi-dimensional chaos. A novel, lightweight approach to image encryption was devised for Medical Internet of Things (MIoT) networks, incorporating compressive sensing and a modified seven-dimensional (MSD) hyperchaotic map [50]. The 7D hyperchaotic map underwent initial modification to generate highly secure and intricate secret keys. Leveraging the NonSubsampled Contourlet Transform (NSCT), further improvements were made in compressive sensing, and measurement matrices were derived using the secret keys generated by MSD. The encryption process entailed applying diffusion and permutation techniques to compressed images using the secret keys obtained from MSD. Comprehensive analyses substantiated the approach's resilience, security, and statistical effectiveness. A separate study introduced a swift image encryption algorithm based on an enhanced 6-D chaotic system, entailing the design of a hyper-chaotic system with heightened chaotic behavior [51], [52]. This algorithm showcased exceptional security prowess, robustness, and rapid encryption and decryption speeds. An asymmetric image encryption method based on elliptic curve ElGamal cryptography and chaotic theory was introduced to address concerns regarding key management in symmetric encryption schemes [53], [54]. This method exhibited elevated security, efficiency, and resistance against attacks [55]. An investigation was conducted to evaluate the efficiency of chaotic-based image block ciphering in spatial and Fractional Fourier Transform (FrFT) domains. Various chaotic maps were scrutinized, considering FrFT parameters as supplementary encryption keys. The outcomes demonstrated the efficacy of chaotic-based image encryption in the FrFT domain, with the Cat-FrFT scheme demonstrating superior resistance against channel noise attacks [56]. Utilizing 3D adversarial attacks within chaotic systems introduces a new dimension

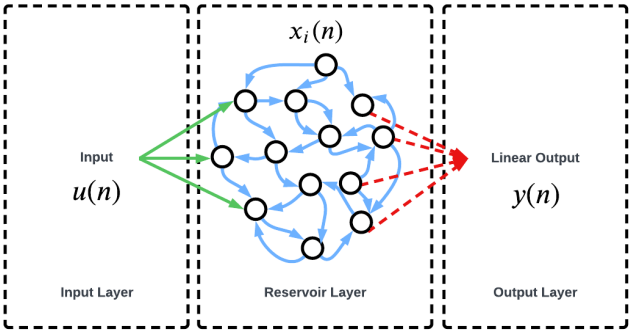


FIGURE 2. The three-layer structure of a reservoir computing system, showing the flow from input signal $u(n)$ through the dynamic reservoir $xi(n)$ to the linear output $y(n)$, encapsulating the core process of information transformation [61].

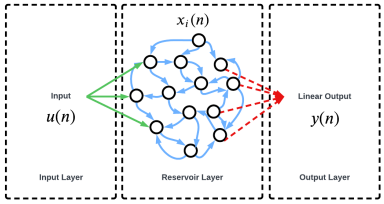
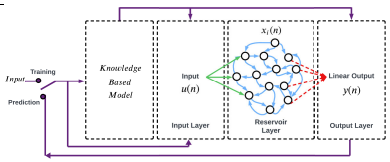
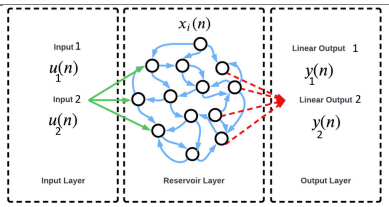
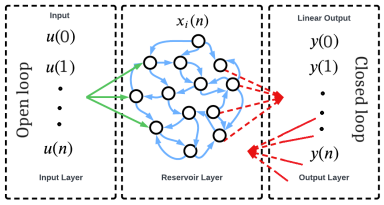
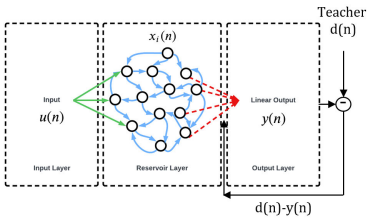
of security challenges. These attacks strategically exploit the complex behavior of chaotic systems, aiming to manipulate their trajectories and disrupt their intended functionality. By targeting the vulnerabilities inherent in chaotic dynamics, adversaries can potentially compromise the integrity and reliability of critical applications, highlighting the need for robust defenses in this evolving landscape of cybersecurity [57], [58].

Further, as with any other hardware block being fabricated, various hardware security concerns also arise when designing chaotic encrypters [56]. Therefore, many different methods were researched to encrypt the chaotic system, use fractional differential equations to overcome interfering environmental factors such as temperature and voltage change, and improve the synchronization of the signals in chaotic communication. Here we explore ML as a tool to improve the chaotic behavior and synchronization of the chaotic system on the chip and also look into ML-based attacks on chaotic communication systems.

III. MACHINE LEARNING FOR CHAOS PREDICTION

Numerous papers have been published that delve into the realm of chaotic and analog encryption systems. However, the fact that none of these works really address the critical issue of security or provide an estimate of the computational efforts necessary to break these systems raises a notable concern. The prevailing assumption in most of these papers is that the system's security is primarily derived from the obscurity of the encryption method itself. As a result, it is commonly believed that cryptanalysts would find it exceedingly challenging to launch an attack based solely on knowledge of the ciphertext [59]. Nonetheless, the lack of comprehensive security analyses and computational assessments poses potential vulnerabilities in the practical implementation of these encryption techniques. In recent years, reservoir computing has been introduced as a method to predict the numbers that will be generated by the original system τ seconds in advance (Table. 2) [60].

TABLE 2. Comparison table for chaos prediction using machine learning.

Name	Proposed Method
Fan et al. [61] Classic reservoir Computing	
Pathak et al. [62] hybrid forecasting scheme that combines a knowledge-based model with reservoir computing for chaos synchronization	
Zhang et al. [63] sense phase coherence between coupled chaotic oscillators	
Borra et al. [64] modeling dynamics in multiscale systems	
Weng et al. [65] use of reservoir computing for synchronizing chaotic systems	
Pathak et al. [66] Estimate Lyapunov exponents from input data	Classic reservoir computing [61] extracted positive and zero Lyapunov exponents of a chaotic system from data.
Weng et al. [67] a viable alternative to conventional dynamical equations	Classic reservoir computing [61] demonstrate that successful dual synchronization can be achieved between a chaotic system and its learned reservoir system.

Fan et al. [61] introduced the use of reservoir computing for predicting the evolution of chaotic dynamical systems without relying on a model, as shown in Fig. 2. The proposed scheme incorporates infrequent updates of the actual state of the target system, allowing for an arbitrarily long prediction horizon for a variety of chaotic systems. The robustness of the proposed approach is based on the theory of temporal synchronization. The reservoir system can correct its trajectory and accurately predict the evolution of the target system, even over a long prediction horizon, through a physical understanding of synchronization. When the trajectories of the reservoir and original systems diverge, the reservoir system can be corrected with a real measurement as small as a single data point. This synchronization enables the reservoir system to reset the prediction horizon and continue to predict accurately. While the proposed scheme demonstrates robustness in predicting the state evolution of chaotic systems, it has some limitations due to the exponential divergence between the trajectories of the reservoir and true systems, which restricts the prediction horizon achieved.

Pathak et al. [62] introduced a hybrid forecasting scheme that combines a knowledge-based model with reservoir computing. By leveraging the advantages of both approaches, the hybrid technique consistently outperforms individual components, showcasing improved performance and making predictions at smaller reservoir sizes, thus saving computational resources. Moreover, even in cases where the knowledge-based model exhibits flaws, the hybrid approach still produces accurate predictions, demonstrating its robustness. Furthermore, both the hybrid scheme and the reservoir-only model exhibit training reusability, enabling multiple subsequent predictions without the need for retraining. This approach holds significant potential in various applications, including weather forecasting and chaos system synchronization.

ML approaches have also been applied to predict phase coherence in chaotic systems. Zhang et al. [63] utilized reservoir computing to sense phase coherence between coupled chaotic oscillators. Results revealed that an integrated input scheme can discern different degrees of phase coherence, whereas an independent input scheme fails to sense phase coherence. This finding holds implications for predicting large chaotic systems using parallel reservoirs.

Borra et al. [64] address the challenge of understanding and modeling dynamics in multiscale systems by employing reservoir computing to build data-driven effective models. The study demonstrates that predictability can be improved by hybridizing the reservoir with an imperfect model, allowing accurate predictions even with smaller reservoirs. The potential of this approach extends to more complex, high-dimensional, multiscale systems through the use of multi-reservoir architectures in parallel.

Weng et al. [65] explore the use of reservoir computing for synchronizing chaotic systems and their ML models. By employing an ML technique with reservoir computing, synchronization can be achieved among chaotic systems and their fitted reservoir computers using just one observational measure.

In a different study, Pathak et al. [66] presented an ML model for chaotic dynamical systems using reservoir computing to estimate Lyapunov exponents from data. The technique successfully approximated the ergodic properties of the true system and accurately calculated positive and zero Lyapunov exponents. However, calculating the numerical value of the negative Lyapunov exponent remains challenging due to its high magnitude.

Weng et al. [67] re-examined the reservoir computing approach for modeling chaotic systems. This ML method provides a viable alternative to conventional dynamical equations when analytical models are inaccessible. The study demonstrated that the temporal and spatial scales of trained reservoir systems mirror those of observed chaotic systems, and successful dual synchronization can be achieved between a chaotic system and its learned reservoir system.

In conclusion, the integration of ML and knowledge-based models has shown great promise for forecasting and understanding chaotic dynamical systems. These approaches offer innovative solutions, enabling accurate predictions, synchronizations, and modeling even in the absence of complete mechanistic knowledge. The combination of these techniques holds significant potential for advancing chaos system synchronization and forecasting in various fields of science and engineering.

IV. MACHINE LEARNING FOR CHAOS SYNCHRONIZATION

Chaotic signal encryption finds applications in secure communication, data privacy, image and video encryption, biometric security, secure control systems, financial transactions, and IoT security. To focus on a specific example, here we look into the utilization of chaotic signal encryption to enhance the security of communication systems, such as wireless networks, satellite communication, and internet-based communication. By exploiting the complex and unpredictable nature of chaotic signals, encryption algorithms based on chaos theory can provide robust protection against eavesdropping and unauthorized access.

In the various communication system implementations reviewed in Section II, a similar circuit serves as both the transmitter and receiver. Here we use Chua's system as an example to show the signal synchronization. The message to be transmitted is encrypted in the transmitter and sent through a public channel visible to unauthorized users. At the receiver, chaotic synchronization is used to decrypt the message. The decrypted message still requires further processing to reconstruct the original message.

A. TRADITIONAL METHODS FOR SIGNAL SYNCHRONIZATION

In the system shown in Fig. 3, the original message is represented by the signal "Message" and its encrypted version before being transmitted through the public channel as "Encrypted". The goal is to ensure that no data can be extracted from the encrypted message, as it should exhibit no correlation with the original message. The data that is decoded by the receiver is represented by "Decrypted", which, although not a perfect 0 and 1 representation, is correlated with the original message. The accuracy of the reconstruction is evaluated by calculating the accumulated number of false positives and false negatives divided by the total number of data points. Although the original and the decrypted messages do have a correlation, the accuracy

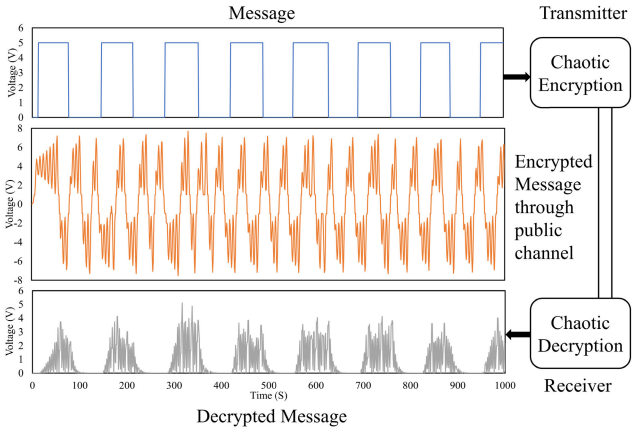


FIGURE 3. Visualization of chaotic encryption for secure communication - The top plot presents the original binary message signal. The middle plot displays the message after chaotic encryption, signifying transmission over a public channel. The bottom plot shows the signal post chaotic decryption, illustrating the restoration of the original message at the receiver's end. The temporal axis is marked in seconds, providing a clear depiction of the encryption-decryption dynamics over time.

does not exceed 80% when common classification methods like threshold and averaging are used [68], which cannot be trusted for data transfer specifically in biomedical devices.

Compared to traditional methods such as averaging, moving average, and thresholding, machine learning emerges as a superior tool for error correction and signal synchronization. Chaotic signals often exhibit complex and non-linear dynamics, making their synchronization a challenging task. Machine learning algorithms, especially deep learning models, possess the capability to adapt and learn intricate patterns from chaotic signal data, allowing them to correct errors with a remarkable level of accuracy. These models excel at capturing and deciphering chaotic behavior, even in the presence of noise and unpredictability. Unlike conventional methods that rely on fixed heuristics, machine learning continuously refines its error correction strategies as it encounters more data, making it a potent tool for achieving precise synchronization in the chaotic signal domain. This adaptability and ability to handle complex, dynamic systems positions machine learning as an invaluable asset in advancing the state-of-the-art in chaotic signal synchronization research.

ML has become a popular asset for signal synchronization, but its application in chaotic encryption is still a relatively new field. There are various ML algorithms that offer the potential for improved encryption security and the development of practical decoders for error correction in digital communication devices, addressing previous limitations and achieving better frame error rates for various codes. Next, we will explain the need for synchronization in chaotic communication, explore the current research on signal synchronization using ML, its limitations, and how chaotic encryption with ML can overcome these limitations due to its robustness. Furthermore, we will discuss the latest research

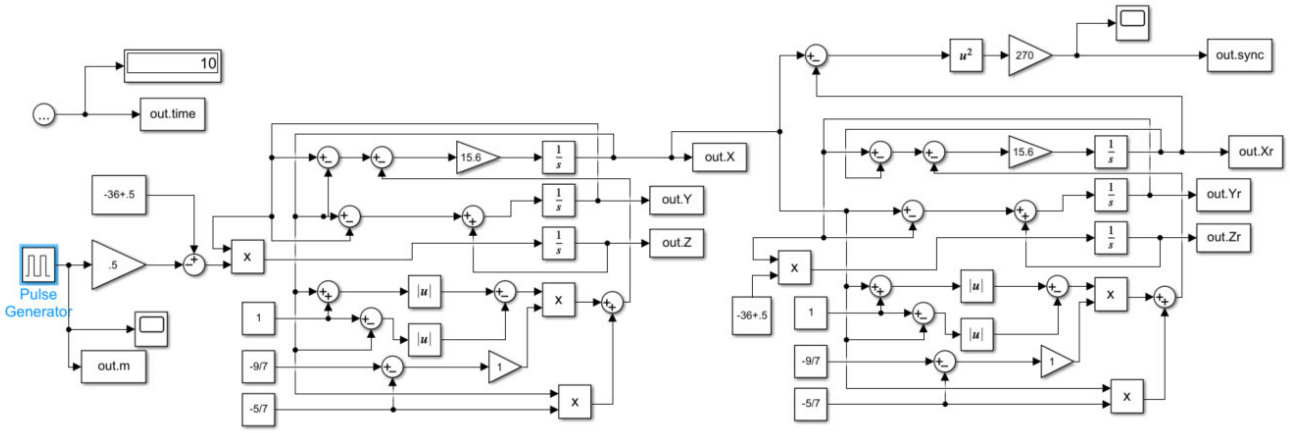


FIGURE 4. Design used for data extraction using matlab simulink showing the transmitter block on the left and receiver block on the right. This transmitter performs message encryption over a public channel using Chua's chaotic system and the receiver decrypts the message using chaotic synchornization.

on ML in chaotic encryption and how it has the potential to revolutionize the field.

B. MACHINE LEARNING METHODS FOR SIGNAL SYNCHRONIZATION

ML is widely used in signal synchronization. Popovici et al. [69] proposed a novel clustering method for the evaluation of signal data based on the similarity of their pattern, which contains more information than the signal intensity and dominant frequencies. Novel clustering method is a creative technique to group data points into a cluster based on unique algorithms or techniques that are usually not covered using traditional clustering algorithms in machine learning and data analysis. The signals are transformed into symbol strings, and the edit distance is used to determine the similarity between strings. Based on this similarity, the data streams are clustered using a Self-Organizing Map (SOM)-type network that adapts incrementally to the input sensor data stream. The method is particularly useful for the inspection of signal streams in the context of online monitoring and offline analysis.

The proposed ML techniques for signal synchronization, such as clustering and feature extraction, show great promise in effectively analyzing and processing large and complex datasets in real-time applications. Clustering is the process of grouping similar data points together based on their shared characteristics or proximity in a dataset. Feature extraction is the process of selecting and transforming relevant information from raw data to create a more concise representation, facilitating effective analysis and pattern recognition. There have been examples of these methods handling complicated real-time data, like ECG [70] and EEG [71], [72], where even slight errors can result in severe consequences. Therefore, using ML in chaotic synchronization could make the decrypted signal in the receiver more robust and even more effective.

Support Vector Machine (SVM) is a powerful and versatile supervised learning algorithm used for classification and regression, with a focus on classification problems. SVMs were introduced in the 1960s and refined in the 1990s, and their unique implementation sets them apart from other ML algorithms. Their popularity stems from their ability to handle multiple continuous and categorical variables [73]. In SVM, a model represents different classes in a hyperplane in multidimensional space. SVM iteratively generates a hyperplane to minimize error and divides datasets into classes to find the Maximum Marginal Hyperplane (MMH). Support vectors are the closest data points to the hyperplane that help define the separating line. The hyperplane is a decision plane or space that separates a set of objects with different classes, and its margin is calculated as the perpendicular distance from the line to the support vectors. Here, a larger margin is considered better than a smaller margin.

Weng et al. [65] chose to use chaotic synchronization as a method for secure communication. They described a new approach to synchronizing chaotic systems using ML, specifically the reservoir computing technique, as discussed in Section III. Reservoir computing is a machine learning technique that uses a fixed, randomly generated "reservoir" of neurons to process temporal data, making it particularly suitable for tasks involving sequential or time-series data. This method allows for accurate prediction of chaotic systems without prior knowledge of their equations. By transmitting a single scalar signal, trained reservoir computers can synchronize with learned chaotic systems, and cascading synchronization can also be achieved. One of the limitations of the method proposed in the paper is that it requires a large number of parameters to be tuned in order to achieve optimal synchronization. This can be time-consuming and computationally expensive, especially for complex systems with many degrees of freedom. Additionally, the method assumes that the dynamics of the systems being synchronized are well-known, which may not always be the case in practical

applications. Finally, the methods based on linear feedback control may not be sufficient for achieving synchronization in systems with highly nonlinear dynamics. However, the limitations of [61] and [65] can be resolved by adopting different ML techniques.

Combining ML and chaotic synchronization techniques could provide a more secure and efficient solution for real-time signal synchronization and analysis, with potential applications in healthcare, telecommunications, and other fields where secure data transmission is critical.

C. DATA PREPARATION

The initial phase of our study involved meticulous data preparation to ensure the quality and appropriateness of the dataset for our experiments. Key steps included:

Data Acquisition: Using the system setup in Fig.4, we obtained a dataset consisting of 2,743 samples. The dataset was exported from a CSV file, and the columns of primary interest were 'Reference,' 'Time,' and 'Out Sync.'

Feature Selection: Among the available attributes, we focused on 'Reference' as the input signal, 'Out Sync' as the output signal following transmission through a chaos receiver, and 'Time' as the temporal information.

Data Normalization: To facilitate consistent and meaningful model training, we applied Min-Max scaling to normalize the 'Reference' and 'Out Sync' signals to the range of [0, 1].

D. MODEL SELECTION

Our choice to utilize classification models, as opposed to regression models, is rooted in the fundamental objective of our research. Our primary focus revolves around classifying the 'Out Sync' signal, which spans a continuous numerical range encompassing various float values. In contrast, the corresponding 'Reference' input message assumes one of two distinct values: either 0 or 1. Our primary aim is to deduce, in the absence of any supplementary contextual information, whether the 'Out Sync' signal corresponds to the 'Reference' value of 0 or 1.

This undertaking presents us with a complex challenge-mapping a continuous linear signal into discrete categories-effectively ''synchronizing'' the 'Out Sync' signal with the underlying 'Reference' message. To tackle this synchronization task, we have turned to classification models, purpose-built for precisely this type of problem. These models excel in categorizing data points into distinct classes.

By classifying the 'Out Sync' signal into two discrete classes, 0 or 1, we establish a direct correspondence between the observed signal and the original message it signifies. This strategic choice empowers us to distill intricate continuous information into a binary decision-making process, echoing the essence of chaotic synchronization-a sophisticated endeavor effectively encapsulated through classification.

In summary, our selection of classification models is deeply rooted in the inherent challenge of mapping a linear 'Out Sync' signal into discrete categories, mirroring the binary nature of the underlying 'Reference' message. This choice aligns seamlessly with our overarching objective: achieving synchronization between the output and input signals, even in the absence of additional contextual information. Here is an expanded explanation of the rationale behind each model selection:

Neural Networks (NN): Neural Networks are renowned for their versatility and success across diverse domains. We opted for NNs due to their adaptability and their ability to effectively handle complex patterns inherent in our data.

Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM): Our task relies heavily on sequential dependencies, making RNNs and LSTMs ideal choices. LSTMs, in particular, were chosen to address the well-documented vanishing gradient problem commonly associated with standard RNNs.

Support Vector Machine (SVM): SVMs have demonstrated noteworthy accomplishments in the classification of Electromyography (EMG) signals, serving as a reference point for their potential applicability to our task.

This diverse selection of models reflects our commitment to thoroughly investigate and address the unique challenges posed by our synchronization task, leveraging the strengths of each model to advance our understanding and achieve our research objectives.

E. METRICS FOR ML PERFORMANCE EVALUATION

In the context of ML-based signal synchronization, precise assessment of learning algorithms is essential to ensure the selection of the most suitable method for ensuring the security and reliability of the system. The choice of appropriate performance metrics plays a pivotal role in quantifying the quality of synchronization outcomes. Here, we review the key metrics employed for the evaluation of machine learning techniques in signal synchronization tasks.

Mean Absolute Error (MAE): MAE calculates the average absolute difference between the predicted and actual values in a linear regression problem as follows:

$$\text{MAE} = \frac{1}{n}\sum_{i=1}^{n}|y_i - \hat{y}_i|$$

MAE metric is resilient to outliers offering a streamlined interpretation. A lower MAE demonstrates a better-fitting model, with errors represented in the same units as the target variable.

Mean Squared Error (MSE): This metric measures the average of the squared differences between predicted and actual values as described below:

$$\text{MSE} = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2$$

MSE amplifies larger errors, making it sensitive to outliers. MSE is frequently used in regression problems such signal synchronization preventing negative and positive errors from offsetting each other. This metric underscores the importance

of accurate predictions by giving larger errors more weight in the evaluation process.

Root Mean Squared Error (RMSE): RMSE metric is the square root of the MSE, shown in the same units as the target variable: (RMSE $= \sqrt{\text{MSE}}$). RMSE offers a similar interpretation to MAE but penalizes larger errors more heavily. It is often employed in linear regression problems where the emphasis is on the importance of larger prediction errors.

R-squared (R^2): R-squared calculates the proportion of variance in the dependent variable that is predictable from the independent variables in the regression model:

$$R^2 = 1 - \frac{\sum_{i=1}^{n}(y_i - \hat{y}_i)^2}{\sum_{i=1}^{n}(y_i - \bar{y})^2}$$

R-squared metric ranges from 0 to 1, with higher values indicating a better fit. While this metric offers insights on how well a model is fit, it does not reveal whether the model's predictions are systematically too high or too low. Hence, it needs to be considered in association with other performance metrics when being used for evaluating the performance of ML models.

F1 Score: The F1 score harmonizes precision and recall, providing a balanced measure of classification performance. It assesses the trade-off between true positives and false positives, offering a holistic view of model accuracy.

Accuracy: Accuracy represents the proportion of correctly classified instances out of the total, serving as a general indicator of model performance.

Confusion Matrix: The confusion matrix provides a granular breakdown of classification outcomes, elucidating true positives, true negatives, false positives, and false negatives. It enables a detailed understanding of model behavior.

F. EVALUATION METRICS SELECTION

In the classification tasks, the confusion matrix stands as an indispensable tool, unveiling critical facets of a model's performance. It serves as a comprehensive blueprint, dissecting the landscape of classification accuracy and errors. The nuanced insights it imparts shed light on the subtleties of model behavior, allowing for a richer understanding of its capabilities.

Additionally, the inclusion of accuracy and the F1 score further enriches our evaluation. Accuracy acts as a straightforward yet vital metric, quantifying the proportion of correctly classified instances-a fundamental measure of the model's overall correctness. The F1 score, on the other hand, delves deeper, capturing the balance between precision and recall, particularly crucial when handling imbalanced datasets. These metrics enhance our ability to assess the model's efficacy from multiple angles.

G. ML IMPLEMENTATION FOR SIGNAL SYNCHRONIZATION

Unsupervised clustering algorithms, such as K-means clustering, K-Nearest Neighbors (KNN), and Density-Based Spatial Clustering of Applications with Noise (DBSCAN), can be used to simplify the tuning of parameters in the reservoir computing technique. By clustering similar data points, the number of parameters that need to be tuned can be reduced, making the process less time-consuming and computationally expensive. Furthermore, the use of unsupervised clustering algorithms can address the issue of overfitting by identifying the most relevant features for the synchronization task. The use of ML methods, such as reservoir computing, can also be complemented with more traditional control theory techniques to overcome the limitations of linear feedback control.

To test different ML algorithms for signal synchronization, a Chua's transmitter and receiver were implemented in Mathlab Simulink. The data extracted from the **out.m**, **out.X** and **out.Sync** of the circuit is shown in Fig.4. The **out.m** represents the message, in our case, a pulse train that needs to be ciphered and sent through the public channel. **out.X** represents the message through the public channel. No meaningful data (0 or 1 in our message) should be extracted from this signal. In other words, **out.X** should show no correlation with the message (**out.m**). **out.sync** is the data that is decoded by the receiver; although it is not a perfect 0 and 1 scheme, this deciphered message is correlated with the message. Here is where we aim to use different machine learning algorithms to improve the correlation of **out.sync** and **out.m**.

Fig. 5 presents the results of the experimentation conducted to achieve signal synchronization between the input data (**out.m**) and the desired output signal using various ML algorithms. The objective of this study is to accurately retrieve the original message from the encrypted message. Fig. 5a depicts the original message (**out.m**), while Fig. 5b illustrates the decoded message (**out.sync**) obtained through the traditional method of thresholding. Thresholding in machine learning is the process of applying a predefined threshold value to the output of a model or algorithm to make binary decisions, such as classifying data points as ''positive'' or ''negative'' based on their scores or probabilities, resulting in a Mean Squared Error (MSE) of 13.00. To improve synchronization and reduce MSE, alternative ML methods were explored. For Fig. 5c, LSTM, or Long Short-Term Memory, is a type of recurrent neural network (RNN) architecture in machine learning designed to model and make predictions for sequences of data while effectively addressing the vanishing gradient problem. Using LSTM resulted in a reduced MSE of 6.96. Furthermore, the application of K-means clustering in Fig. 5d led to an MSE of 6.96. The MSE decreased in both cases compared to the traditional method. K-means is a clustering algorithm in machine learning that groups data points into 'K' clusters by minimizing the distance

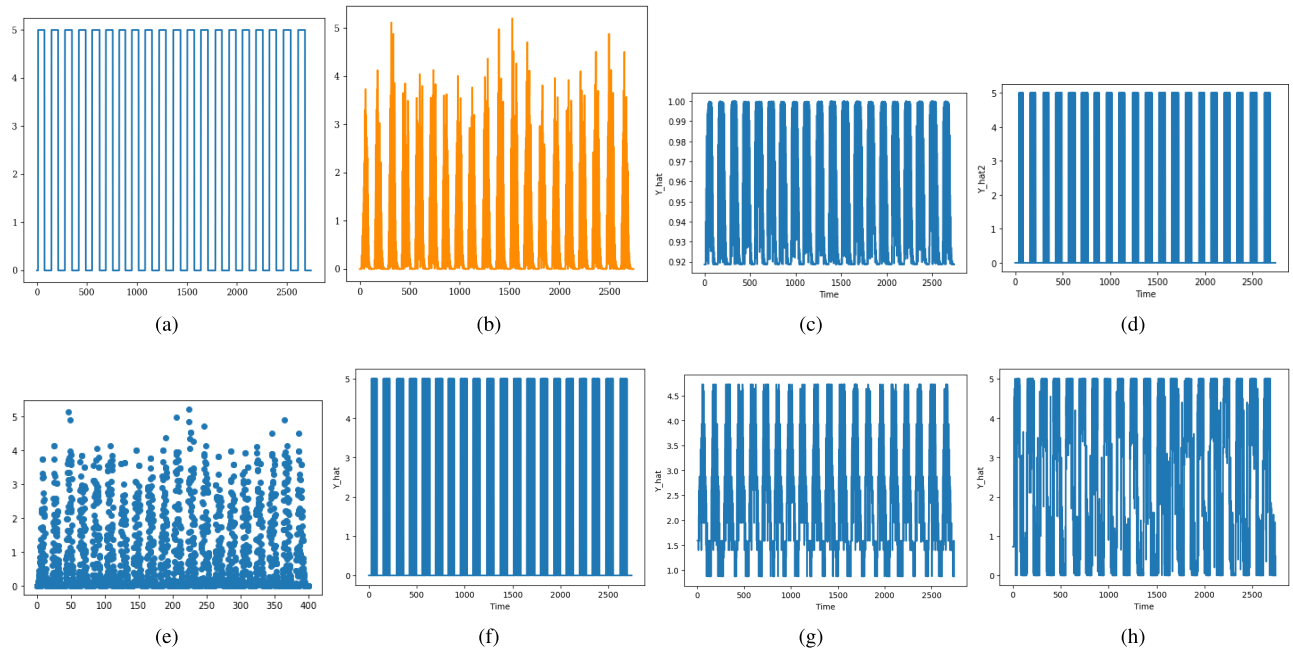


FIGURE 5. Comparative analysis of machine learning algorithms in signal synchronization - Subfigures (a) through (i) depict the signal processing results using various machine learning techniques for secure communication. Subfigure (a) represents the original binary message signal. Subfigure (b) shows the decoded message with a Mean Squared Error (MSR) of 13.00. Subfigures (c) to (i) display the synchronization results achieved by LSTM, k-means, DBSCAN, SVM, and AdaBoost algorithms with respective MSR values provided, illustrating each algorithm's efficacy in reconstructing the signal with synchronization errors quantified for comparative evaluation.

between data points and their cluster centroids. Additionally, it was observed that DBSCAN in Fig. 5e produced an MSE of 12.56, indicating sub-optimal performance. DBSCAN is a density-based clustering algorithm in machine learning that identifies clusters by analyzing data point densities and effectively handles noisy data. Among notable findings is the significant enhancement achieved using SVM in Fig. 5f, with an impressively low MSE of 5.25. Furthermore, employing Adaptive Boosting (AdaBoost) in Fig. 5g resulted in an MSE of 3.52, and utilizing Random Forest (RF) in Fig. 5h resulted in an MSE of 4.00, both demonstrating promising outcomes for signal synchronization.

However, it is important to note that although MSE is a valuable evaluation metric, it may not always fully capture the effectiveness of synchronization. Other evaluation methods should also be considered to provide a comprehensive assessment of the synchronization performance.

To implement more metrics in the use of machine learning in signal synchronization, we have examined four distinct models: the Long Short-Term Memory (LSTM), an improved LSTM variant, the Convolutional Neural Network (CNN), and the Support Vector Machine (SVM). The objective was to ascertain their capability to synchronize chaotic signals and classify them into discrete categories, specifically '0' or '5.'

1) LONG SHORT-TERM MEMORY (LSTM)

In our initial exploration, we employed a standard LSTM architecture with a training duration of 100 epochs. The model exhibited commendable performance, achieving an F1 score of 0.8463, an accuracy rate of 85.19%, and a Mean Squared Error (MSE) of 0.1481. The confusion matrix revealed 243 true positives, 23 false positives, 58 false negatives, and 223 true negatives (Fig. 6a).

2) IMPROVED LONG SHORT-TERM MEMORY (LSTM)

Building upon our initial findings, we advanced to an enhanced LSTM model, extending the training duration to 150 epochs, employing the Adam optimizer, and implementing a cross-entropy loss function. This model demonstrated substantial improvement, boasting an impressive F1 score of 0.9212, an accuracy of 91.77%, and a significantly reduced MSE of 0.0823. The corresponding confusion matrix unveiled 239 true positives, 27 false positives, 18 false negatives, and 263 true negatives (Fig. 6b).

3) CONVOLUTIONAL NEURAL NETWORK (CNN)

Our exploration extended to the domain of Convolutional Neural Networks (CNN), where the model underwent rigorous training spanning 500 epochs. The CNN showcased competitive performance, yielding an F1 score of 0.8634, an accuracy rate of 86.29%, and an MSE of 0.1371. The accompanying confusion matrix detailed 235 true positives, 31 false positives, 44 false negatives, and 237 true negatives (Fig. 6c).

4) SUPPORT VECTOR MACHINE (SVM)

In parallel, we introduced the Support Vector Machine (SVM), a classical machine learning algorithm known for

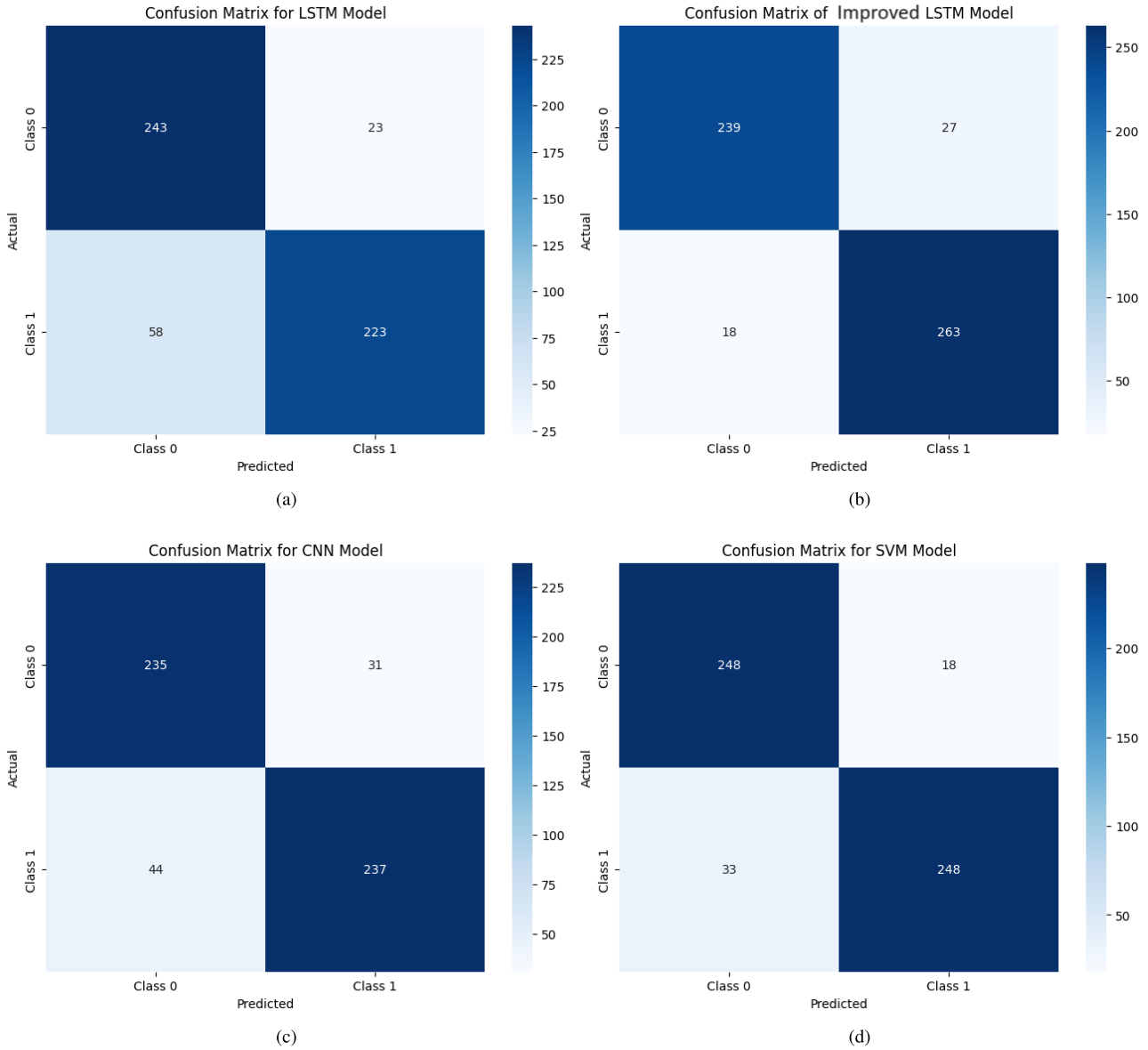


FIGURE 6. Comparative confusion matrices for synchronization models (a) Confusion Matrix of Long Short-Term Memory(LSTM) Model(b) Confusion matrix of improved LSTM model with more epochs and adam optimizer (c) Confusion matrix of convolutional neural network model (d) Confusion matrix of support vector machine (SVM) Model. Despite a lower number of training epochs compared to the CNN model, Figure (b) illustrates that the LSTM model showed better performance, excelling in both accuracy and mean squared error (MSE).

its robust classification capabilities. The SVM model, while not as complex as neural networks, delivered compelling results. It achieved an F1 score of 0.9068 and an accuracy rate of 90.68%. The associated MSE stood at 0.0932. The confusion matrix portrayed 248 true positives, 18 false positives, 33 false negatives, and 248 true negatives (Fig. 6d).

The results from these experiments illuminate significant variations in model performance, with the improved LSTM model emerging as the frontrunner in synchronization and classification tasks. This model, benefitting from an increased number of epochs, an optimized optimizer, and a sophisticated loss function, achieved the highest F1 score, accuracy rate, and the lowest MSE among all models considered. These findings underscore the pivotal role of model architecture and training parameters in achieving synchronization and classification accuracy within chaotic signal systems.

Factors such as computational efficiency, real-time capabilities, and generalization to different datasets are also crucial aspects to be taken into account during the review and selection of the most suitable algorithm for practical applications of signal synchronization.

V. MACHINE LEARNING ATTACKS ON ENCRYPTION SYSTEMS

In this section, we review the recent studies focused on ML-based attacks in encryption systems. Although traditional encryption algorithms used in resource-limited devices

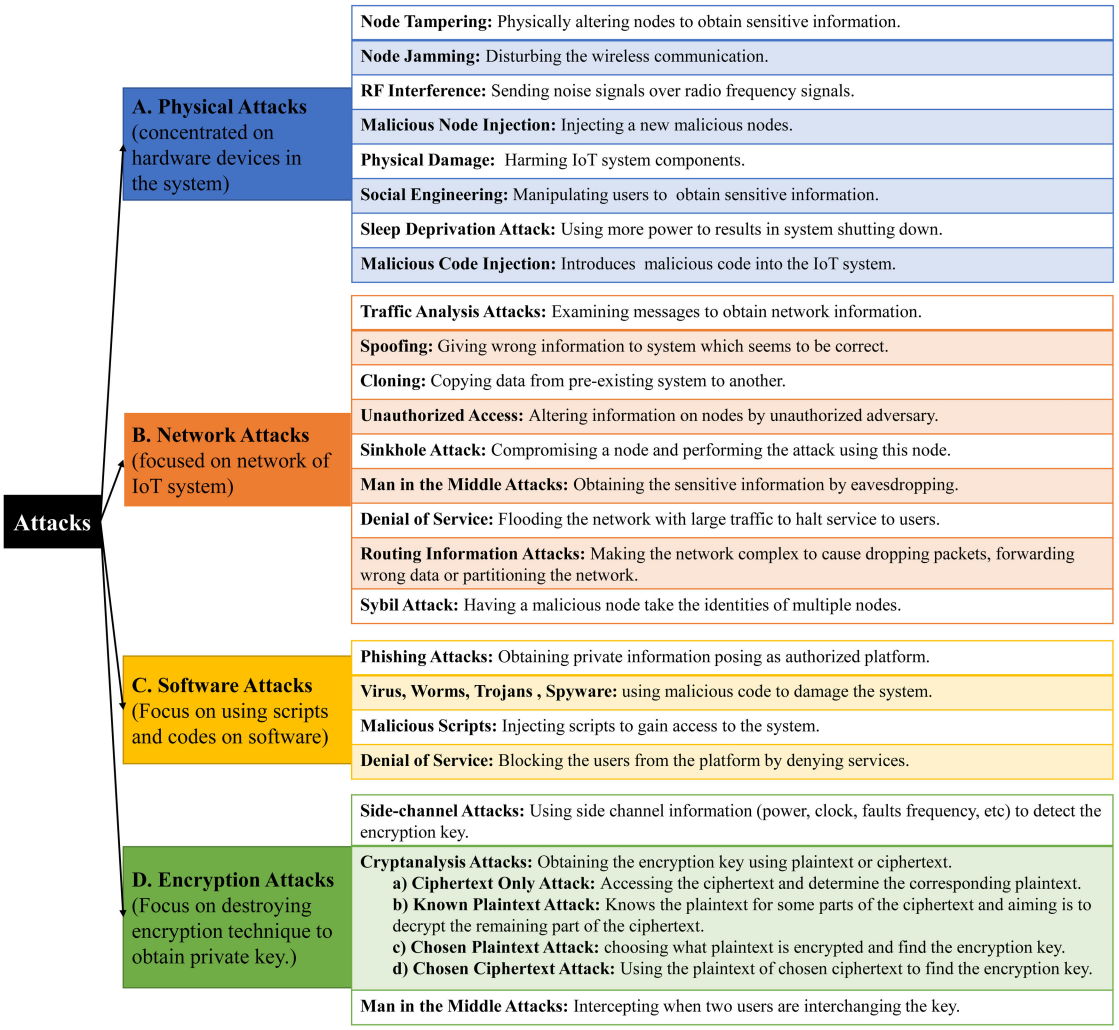


FIGURE 7. Common attacks for communication focused on attacks appropriate for IoT, wearable, and resource-limited devices.

are capable of fulfilling their intended functions, they fall short in ensuring the security of the personal data generated by these devices and their sensors, making them susceptible to frequent security breaches. To make our resource-limited devices secure and reliable, it is crucial to implement security measures at each layer, as depicted in Fig. 7, which shows the potential security attacks that these devices may face [74].

Instances of security breaches have compelled the technology we use daily to prioritize research in the field of cryptography. Notably, there have been many data leaks, specifically from wearables and IoT devices. As an example, the data of over 61 million users worldwide who were using Fitbit and Apple devices [75] was exposed recently. Wearable medical devices, such as cardiac implants [76], [77], implantable insulin delivery pumps [78], [79], and neurological implants [80], [81], are also vulnerable to targeted attacks. As a result, there is a growing impetus to enhance traditional encryption algorithms and explore new ways of encryption that aim to bolster the overall security and reliability of wearable devices and safeguard the sensitive data and health information of users.

A discussion of common attacks on chaotic encryption is discussed in our previous work [82]. ML has been researched as a tool to attack chaotic encryption schemes by utilizing its powerful pattern recognition capabilities against the inherent unpredictability and complexity of chaotic systems. Although the examples are not many, here we take a look at the use of ML in attacking chaos. Most ML attacks on chaotic systems focus on algorithms that can be trained to exploit patterns and regularities within chaotic encrypted data, leading to successful decryption attacks. These attacks leverage the ability of ML models to recognize underlying patterns and relationships, even in seemingly random encrypted data, as discussed in Section III. Apart from this application, ML can also be used in predicting encryption keys, as a plaintext attack, and to predict key system parameters.

He et al. [83] developed a proof of concept for breaking chaos-based image encryption schemes. The approach

avoided the need for manual examination of encryption keys to recreate decrypted images by using a low-dimensional feature space and a deconvolutional generator. Encrypted images were effectively decoded with both static and dynamic keys using the proposed method. As stated by the authors, the accuracy rates of the regenerated images were 97.87% and 92.04%, respectively. The authors reached the conclusion that their suggested method is automatic and key-independent, thus making it more effective than previous approaches.

Wang et al. presented a deep learning-based known-plaintext attack for chaotic cryptosystems [84]. The authors proposed to encrypt images using two chaotic encryption techniques, generating ''plaintext-ciphertext'' pairs that are subsequently used to train two convolutional neural networks as the decryption model. CNN, or Convolutional Neural Network, is a deep learning architecture designed for image and spatial data processing, using convolutional layers to automatically learn hierarchical features and patterns from data. Encoder-decoder networks transform input data into a fixed-length representation and generate output sequences from it. The authors used two encoder-decoder neural networks, UNet and MSEDNet, as experimental models and compared their efficiency and accuracy when attacking the classic one-dimensional chaotic map and the proposed hybrid chaotic map, which encrypts the R, G, and B channels of the image separately for color images.

We can find the parameters in hyper-chaotic systems by using ML algorithms. Time-delay nonlinear systems inhibit their capability to exhibit hyper-chaos in a phase space that has infinite dimensions, which makes it impossible for systems with low dimensions to achieve this. We can offer a higher level of computational security against embedding reconstruction by using this characteristic of time-delay systems. In time-delay communication and signal coding (CSC) systems, the crucial element to ensure secure communication among the pairs is the time-delay signature (TDS). In case an unauthorized hostile attacker manages to breach TDS, the system's key space gets eventually reduced, and the dynamics of CSC systems get completely reconstructed. Thus, the identification process is considered a critical aspect for assessing the security level of such a system in the TDS of a time-delay CSC system. Gao et al. introduced an approach utilizing CNN-based image recognition to extract the TDS [85]. Chen et al. also used a CNN-based deep learning method to extract the TDS in a time-delayed chaotic system [86]. Simulations to demonstrate the effectiveness of this method in handling robust nonlinearity were used in the works mentioned above, thus addressing the shortcomings of current techniques. Not only for controlling and synchronizing chaotic systems but also for their application in various other fields, the understanding of time delays holds significant importance in this process.

The worthy discussion of adversarial ML can also be identified as a form of attack in any system using ML. Moreover, adversarial ML is defined as the practice of using malicious input data to deceive or misguide an ML model. Adversarial ML has been commonly used to execute an attack or cause a malfunction in an ML system where the same instance of an adversary can be manipulated accordingly to fool multiple models of different databases or architectures. After further discussions and implementations, it is stated that it can be deployed in a variety of applications, including attacking encryption systems.

An adversary or attacker is a person or entity who seeks to infiltrate a system to achieve specified aims. As shown in Fig. 8 an opponent may launch attacks against ML at two stages: training and testing. During training, the attacker may try to influence the model or the dataset by introducing fake data or changing existing data. After the model has been trained, testing or inference attacks occur. In ''Data Access'', the attackers possess some level of access to the dataset, enabling them to construct an alternate model that can be utilized during the testing stage. The act of poisoning involves the attackers changing either the dataset or the model to create a modified trained model. To carry out ''Poisoning,'' the attackers can use various methods, such as manipulating the current training set, introducing fake data into the training set, or corrupting the learning algorithm through logic manipulation. Locate adversarial examples that can bypass accurate outputs from the model, also known as an ''Evasion'' attack. ''Oracle'' attacks consist of several methods, such as ''Extraction'' attacks, where the attacker endeavors to extract the model's parameters by analyzing its predictions, ''Inversion'' attacks, where the attacker seeks to reconstruct the training set, including private information; and ''Membership Inference'' attacks, where the attacker strives to ascertain whether the input data was part of the model's training set.

VI. CHALLENGES AND OPPORTUNITIES

In this section, we explore the research challenges and opportunities of utilizing ML in chaos-based encryption.

A. COMPLEXITY OF ML SOLUTIONS

Challenges: Wearable devices, in general, are resource-constrained devices that typically possess limited processing power and memory space. These limitations pose significant challenges when it comes to implementing complex ML algorithms on such computing devices. ML algorithms, particularly deep learning models, can be computationally intensive and require significant processing power and memory resources. The complexity and computational demands of ML algorithms can strain the capabilities of wearable devices.

Opportunities: Optimizing ML models to operate efficiently within the resource limitations of such devices is a research opportunity to explore. For example, it is possible to develop lightweight deep-learning models with reduced inference times for resource-constrained devices. Furthermore, the usage of compression methods such as low-rank factorization, parameter sharing, lossy weight encoding, and pruning can be useful in such a scenario. Additionally, for

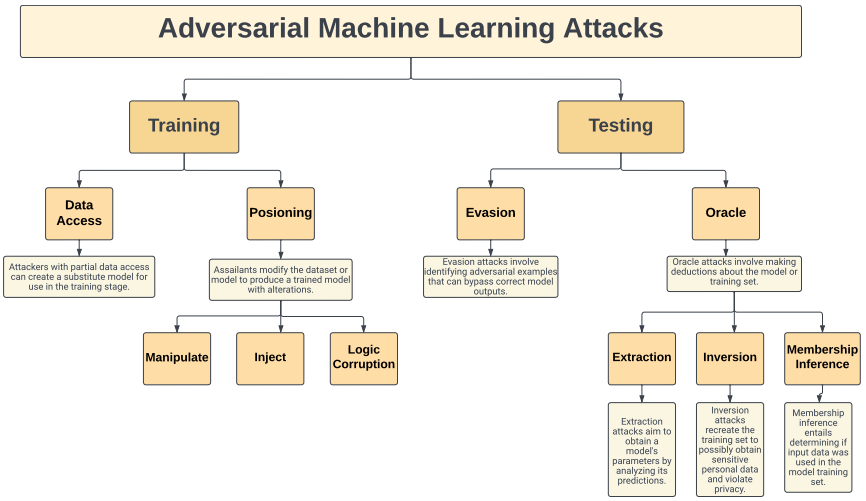


FIGURE 8. Characterization of adversarial machine learning attacks.

model optimization and compression of resource-constrained devices, game-theoretic techniques, swarm optimization, and genetic algorithms might be pursued. Overcoming these challenges is of utmost importance to unlocking the full potential of ML algorithms in wearable devices, enabling them to efficiently and securely support a wide range of critical applications, including healthcare monitoring, activity tracking, and personalized services.

B. AVAILABILITY OF TRAINING DATA

Challenges: The availability of training data poses an important challenge for ML models utilized in secure chaotic communication. Unsupervised models require a significant volume of high-quality training data to effectively capture the intricate dynamics and patterns within secure communication systems. However, obtaining a sufficient amount of reliable training data that accurately represents the complex and dynamic nature of chaotic signals can be difficult. When training data is limited or inadequate, it can negatively impact the performance and generalization capabilities of ML models, impeding their effectiveness in secure communication.

Opportunities: With the vast amount of data generated by the healthcare sector and the growing popularity of IoT devices, partnering with hospitals and wearable device companies can be a viable option for researchers to create and publish related real-world datasets with privacy protection. In addition, utilizing Generative Adversarial Network (GAN) systems to generate synthetic data while ensuring that the dataset is distributed in a representative manner can also be pursued.

C. ML PRIVACY CONCERNS

Challenges: Privacy concerns pose a significant challenge in the use of ML algorithms within wearable devices, as these algorithms rely on sensitive user data for accurate predictions. Wearable devices gather a vast array of personal health and activity information, encompassing heart rate, sleep patterns, location data, and more. Consequently, safeguarding the privacy and security of this sensitive user data becomes paramount. Therefore, it is important to safeguard the privacy and security of users' sensitive information.

Opportunities: To address privacy concerns, the ML models need to be designed and well-tuned according to robust privacy protection and enhancement mechanisms, including data anonymization, randomization, and secure encryption storage. In addition, the use of privacy-preserving ML techniques such as federated learning, distributed ML, and differential privacy to train models on decentralized data while upholding individual user privacy is another important direction to follow in order to prevent unauthorized access and data breaches.

D. REAL-TIME PROCESSING

Challenges: While ML has revolutionized various fields, it can have adverse effects on real-time processing applications. Real-time processing typically requires immediate and timely responses, which may be challenging to achieve with complex ML algorithms. ML models often involve computationally intensive operations, such as training large neural networks or performing extensive feature extraction, which can introduce significant processing delays. Moreover, the unpredictability and variability of ML algorithms can make it difficult to guarantee consistent real-time performance. Additionally, the need for continuous model updates and retraining can further complicate real-time processing, as it may require significant computational resources and disrupt the real-time workflow.

Opportunities: When integrating ML into real-time processing systems, careful consideration of the computational requirements, algorithmic complexity, and latency constraints is crucial to mitigate the adverse effects and

ensure efficient and reliable performance [87]. After such analysis, distributed computing can be researched using node-neighboring resources; in addition, finding solutions to the multilinearity problem, which arises when two or more independent variables are strongly associated with one another in a regression model, can also be a promising direction.

E. SECURITY VULNERABILITIES

Challenges: While ML algorithms can enhance performance, they also introduce security vulnerabilities in chaos-based communication systems. A significant concern is the side-channel leakage problem, where unintended information is unintentionally leaked through physical channels, such as power consumption or electromagnetic emissions. Adversarial attacks exploit these channels to compromise communication integrity, confidentiality, and privacy.

Opportunities: To secure ML-based chaos-based communication systems, a multi-layered proactive approach is required. Comprehensive threat assessments should identify vulnerabilities and analyze potential side-channel leakage sources. Techniques like adversarial training improve system resilience while exploring advanced encryption schemes and securing ML models can further enhance security.

VII. CONCLUSION AND FUTURE DIRECTIONS

In this paper, we highlighted the potential of ML algorithms in addressing reliability and security concerns in chaos-based encryption as a promising method for secure communication in resource-constrained devices such as wearable devices. We comprehensively explored ML techniques for understanding chaotic dynamical systems and improving signal synchronization. We gave more prominence to the in-depth exploration of the methodological aspects of machine learning. We also investigated state-of-the-art ML-assisted defenses and attacks on chaos-based encryption and reviewed the advantages and limitations of ML techniques in secure communication systems. We further expanded the applications to emerging areas like IoT, cloud computing, and wireless networks. By shedding light on the growing role of ML techniques in chaos-based encryption systems and their challenges and opportunities, this research laid a solid foundation for further advancements in intelligent, secure chaotic communication on wearable devices. It further provided valuable insights for researchers, developers, and practitioners to design more secure and robust chaos-based encryption schemes.

A. FUTURE SCOPE

As of the current state of research, there are notable gaps in the literature surrounding chaotic systems and their applications. Firstly, there is a need for more comprehensive studies that bridge the gap between theoretical chaotic models and practical applications. While theoretical advancements have been substantial, their seamless integration into real-world scenarios requires further exploration. A more profound grasp of the fundamental mechanisms that govern chaotic behavior in various systems is also crucial. This entails delving into the intricacies of chaotic phenomena in diverse domains such as engineering, cryptography, biology, and beyond. There is room for advancements in developing robust and efficient algorithms tailored for chaotic applications. Future research should also explore the potential interplay between chaos and emerging technologies like artificial intelligence and quantum computing. As we move forward, interdisciplinary collaboration between mathematicians, engineers, physicists, and other experts will play a pivotal role in realizing the complete potential of chaotic systems across a broad spectrum of applications. With concerted efforts, the future outlook for chaotic system applications appears promising, poised to revolutionize numerous fields and drive innovation in unforeseen ways.

REFERENCES

[1] (May 2020). *IDC's Global Datasphere Forecast Shows Continued Steady Growth in the Creation and Consumption of Data*. [Online]. Available: https://www.businesswire.com/news/home/20200508005025
[2] A. Hedayatipour and N. Mcfarlane, "Wearables for the next pandemic," *IEEE Access*, vol. 8, pp. 184457–184474, 2020.
[3] S. Mahfuz and F. Zulkernine, "A preliminary study on pattern reconstruction for optimal storage of wearable sensor data," 2023, *arXiv:2302.12972*.
[4] J. Monkiewicz, "Financial supervision in digital age: Innovations and data abundance," in *Digital Finance and the Future of the Global Financial System*. Evanston, IL, USA: Routledge, 2023, pp. 213–225.
[5] H. McCormick, "Addressing money laundering in the United States real estate sector," Univ. Kentucky, Lexington, KY, USA, Tech. Rep., 2023.
[6] (Sep. 2023). *RBC Capital Markets Navigating the Changing Face of Healthcare Episode*. [Online]. Available: https://www.rbccm.com/en/gib/healthcare/episode/thehealthcaredataexplosion
[7] G. Wiederrecht, S. Darwish, and A. Callaway. *RBC Capital Markets: Navigating the Changing Face of Healthcare Episode*. Accessed: Sep. 2023. [Online]. Available: https://www.rbccm.com/en/gib/healthcare/episode/thehealthcaredata
[8] J. Dey and R. Dutta, "Progress in multivariate cryptography: Systematic review, challenges, and research directions," *ACM Comput. Surv.*, vol. 55, no. 12, pp. 1–34, Dec. 2023.
[9] Y. Zhang, F. Wang, J. Chao, M. Xie, H. Liu, M. Pan, E. Kopperger, X. Liu, Q. Li, J. Shi, L. Wang, J. Hu, L. Wang, F. C. Simmel, and C. Fan, "DNA origami cryptography for secure communication," *Nature Commun.*, vol. 10, no. 1, p. 5469, Nov. 2019.
[10] S. Subramani and S. K. Svn, "Review of security methods based on classical cryptography and quantum cryptography," *Cybern. Syst.*, pp. 1–19, Jan. 2023.
[11] S. Ullah, J. Zheng, N. Din, M. T. Hussain, F. Ullah, and M. Yousaf, "Elliptic curve cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey," *Comput. Sci. Rev.*, vol. 47, Feb. 2023, Art. no. 100530.
[12] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, Nov. 1994, pp. 124–134.
[13] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, 2017.
[14] L. Chen, L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. A. Perlner, and D. Smith-Tone, *Report on Post-Quantum Cryptography*. document NISTIR 8105, vol. 12, U.S. Department of Commerce, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2016.
[15] D. Joseph, R. Misoczki, M. Manzano, J. Tricot, F. D. Pinuaga, O. Lacombe, S. Leichenauer, J. Hidary, P. Venables, and R. Hansen, "Transitioning organizations to post-quantum cryptography," *Nature*, vol. 605, no. 7909, pp. 237–243, May 2022.
[16] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehle, "CRYSTALS—Kyber: A CCA-secure module-lattice-based KEM," in *Proc. IEEE Eur. Symp. Secur. Privacy (EuroS&P)*, Apr. 2018, pp. 353–367.

[17] *Round 1 Submissions of Post-Quantum Cryptography*. Accessed: Mar. 25, 2023. [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-1-submissions

[18] K. Onuki, K. Cho, Y. Horio, and T. Miyano, "Secret-key exchange through synchronization of randomized chaotic oscillators aided by logistic hash function," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 69, no. 4, pp. 1655–1667, Apr. 2022.

[19] R. Vishwakarma, R. Monani, A. Hedayatipour, and A. Rezaei, "Reliable and secure memristor-based chaotic communication against eavesdroppers and untrusted foundries," *Discover Internet Things*, vol. 3, no. 1, p. 2, Mar. 2023.

[20] B. Tan et al., "Benchmarking at the frontier of hardware security: Lessons from logic locking," 2020, *arXiv:2006.06806*.

[21] O. A. Gonzales, G. Han, J. P. de Gyvez, and E. Sanchez-Sinencio, "Lorenz-based chaotic cryptosystem: A monolithic implementation," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 47, no. 8, pp. 1243–1247, Aug. 2000.

[22] S. Yu, J. Lü, W. K. S. Tang, and G. Chen, "A general multiscroll Lorenz system family and its realization via digital signal processors," *Chaos, Interdiscipl. J. Nonlinear Sci.*, vol. 16, no. 3, Sep. 2006, Art. no. 033126.

[23] D. Brown, A. Hedayatipour, M. B. Majumder, G. S. Rose, N. McFarlane, and D. Materassi, "Practical realisation of a return map immune Lorenz-based chaotic stream cipher in circuitry," *IET Comput. Digit. Techn.*, vol. 12, no. 6, pp. 297–305, Nov. 2018.

[24] A. S. Elwakil and M. P. Kennedy, "Construction of classes of circuit-independent chaotic oscillators using passive-only nonlinear devices," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 48, no. 3, pp. 289–307, Mar. 2001.

[25] S. Özoguz, A. S. Elwakil, and M. P. Kennedy, "Experimental verification of the butterfly attractor in a modified Lorenz system," *Int. J. Bifurcation Chaos*, vol. 12, no. 7, pp. 1627–1632, Jul. 2002.

[26] A. G. Radwan, A. M. Soliman, and A. El-Sedeek, "MOS realization of the modified Lorenz chaotic system," *Chaos, Solitons Fractals*, vol. 21, no. 3, pp. 553–561, Jul. 2004.

[27] Y.-L. Wu, C.-H. Yang, and C.-H. Wu, "Design of initial value control for modified Lorenz–Stenflo system," *Math. Problems Eng.*, vol. 2017, pp. 1–9, 2017.

[28] F. Zhang, R. Chen, and X. Chen, "Analysis of a generalized Lorenz–Stenflo equation," *Complexity*, vol. 2017, pp. 1–6, 2017.

[29] A. Farfan-Pelaez, E. Del-Moral-Hernandez, J. S. Navarro, and W. Van Noije, "A CMOS implementation of the sine-circle map," in *Proc. 48th Midwest Symp. Circuits Syst.*, Aug. 2005, pp. 1502–1505.

[30] S. Callegari, G. Setti, and P. J. Langlois, "A CMOS tailed tent map for the generation of uniformly distributed chaotic sequences," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, vol. 2, Jul. 1997, pp. 781–784.

[31] J. Lopez-Hernandez, A. Diaz-Mendez, R. Vazquez-Medina, and R. Alejos-Palomares, "Analog current-mode implementation of a logistic-map based chaos generator," in *Proc. 52nd IEEE Int. Midwest Symp. Circuits Syst.*, Aug. 2009, pp. 812–814.

[32] R. Anandkumar and R. Kalpana, "Analyzing of chaos based encryption with Lorenz and Henon map," in *Proc. 2nd Int. Conf. I-SMAC (IoT Social, Mobile, Anal. Cloud)*, Aug. 2018, pp. 204–208.

[33] B. Baruah and M. Saikia, "An FPGA implementation of chaos based image encryption and its performance analysis," *Int. J. Comput. Sci. Netw.*, vol. 5, no. 5, pp. 712–720, 2016.

[34] P. Dudek and V. D. Juncu, "Compact discrete-time chaos generator circuit," *Electron. Lett.*, vol. 39, no. 20, pp. 1431–1432, 2003.

[35] V. D. Juncu, M. Rafiei-Naeini, and P. Dudek, "Integrated circuit implementation of a compact discrete-time chaos generator," *Anal. Integr. Circuits Signal Process.*, vol. 46, no. 3, pp. 275–280, Mar. 2006.

[36] B. Kia, K. Mobley, and W. L. Ditto, "An integrated circuit design for a dynamics-based reconfigurable logic block," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 64, no. 6, pp. 715–719, Jun. 2017.

[37] Z. Hua, Y. Chen, H. Bao, and Y. Zhou, "Two-dimensional parametric polynomial chaotic system," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 7, pp. 4402–4414, Jul. 2022.

[38] A. Daoui, M. Yamni, H. Karmouni, M. Sayyouri, H. Qjidaa, M. Ahmad, and A. A. A. El-Latif, "Biomedical multimedia encryption by fractional-order Meixner polynomials map and quaternion fractional-order Meixner moments," *IEEE Access*, vol. 10, pp. 102599–102617, 2022.

[39] U. Erkan, A. Toktas, and Q. Lai, "2D hyperchaotic system based on Schaffer function for image encryption," *Expert Syst. Appl.*, vol. 213, Mar. 2023, Art. no. 119076.

[40] S. Li, Y. Liu, F. Ren, and Z. Yang, "Design of a high throughput pseudorandom number generator based on discrete hyper-chaotic system," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 70, no. 2, pp. 806–810, Feb. 2023.

[41] A. Hedayatipour, R. Monani, A. Rezaei, M. Aliasgari, and H. Sayadi, "A comprehensive analysis of chaos-based secure systems," in *Proc. 2nd Conf. Silicon Valley Cybersecurity Conf. (SVCC)*. San Jose, CA, USA: Springer, Dec. 2021, pp. 90–105.

[42] M. Zapateiro, Y. Vidal, and L. Acho, "A secure communication scheme based on chaotic duffing oscillators and frequency estimation for the transmission of binary-coded messages," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 4, pp. 991–1003, Apr. 2014.

[43] L. Xiong, Y.-J. Lu, Y.-F. Zhang, X.-G. Zhang, and P. Gupta, "Design and hardware implementation of a new chaotic secure communication technique," *PLoS ONE*, vol. 11, no. 8, Aug. 2016, Art. no. e0158348.

[44] A. J. A. El-Maksoud, A. A. A. El-Kader, B. G. Hassan, M. A. Abdelhamed, N. G. Rihan, M. F. Tolba, L. A. Said, A. G. Radwan, and M. F. Abu-Elyazeed, "FPGA implementation of fractional-order Chua's chaotic system," in *Proc. 7th Int. Conf. Modern Circuits Syst. Technol. (MOCAST)*, May 2018, pp. 1–4.

[45] T. Bonny, R. Al Debsi, S. Majzoub, and A. S. Elwakil, "Hardware optimized FPGA implementations of high-speed true random bit generators based on switching-type chaotic oscillators," *Circuits, Syst., Signal Process.*, vol. 38, no. 3, pp. 1342–1359, Mar. 2019.

[46] F. Wang, R. Wang, H. H. C. Iu, C. Liu, and T. Fernando, "A novel multi-shape chaotic attractor and its FPGA implementation," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 66, no. 12, pp. 2062–2066, Dec. 2019.

[47] T. Bonny, "Chaotic or hyper-chaotic oscillator? Numerical solution, circuit design, MATLAB HDL-coder implementation, VHDL code, security analysis, and FPGA realization," *Circuits, Syst., Signal Process.*, vol. 40, no. 3, pp. 1061–1088, Mar. 2021.

[48] O. A. Almatroud, V. K. Tamba, G. Grassi, and V.-T. Pham, "An oscillator without linear terms: Infinite equilibria, chaos, realization, and application," *Mathematics*, vol. 9, no. 24, p. 3315, Dec. 2021.

[49] L. Fortuna, M. Frasca, and M. G. Xibilia, *Chua's Circuit Implementations: Yesterday, Today and Tomorrow*, vol. 65. Cleveland, OH, USA: World Scientific, 2009.

[50] M. Kaur, A. A. Alzubi, D. Singh, V. Kumar, and H.-N. Lee, "Lightweight biomedical image encryption approach," *IEEE Access*, vol. 11, pp. 74048–74057, 2023.

[51] H. Chen, E. Bai, X. Jiang, and Y. Wu, "A fast image encryption algorithm based on improved 6-D hyper-chaotic system," *IEEE Access*, vol. 10, pp. 116031–116044, 2022.

[52] Y. Huang, L. Huang, Y. Wang, Y. Peng, and F. Yu, "Shape synchronization in driver-response of 4-D chaotic system and its application in image encryption," *IEEE Access*, vol. 8, pp. 135308–135319, 2020.

[53] Y. Luo, X. Ouyang, J. Liu, and L. Cao, "An image encryption method based on elliptic curve ElGamal encryption and chaotic systems," *IEEE Access*, vol. 7, pp. 38507–38522, 2019.

[54] M. Kaur, A. A. AlZubi, T. S. Walia, V. Yadav, N. Kumar, D. Singh, and H.-N. Lee, "EGCrypto: A low-complexity elliptic Galois cryptography model for secure data transmission in IoT," *IEEE Access*, vol. 11, pp. 90739–90748, 2023.

[55] X. Qian, Q. Yang, Q. Li, Q. Liu, Y. Wu, and W. Wang, "A novel color image encryption algorithm based on three-dimensional chaotic maps and reconstruction techniques," *IEEE Access*, vol. 9, pp. 61334–61345, 2021.

[56] O. S. Faragallah, A. Afifi, W. El-Shafai, H. S. El-Sayed, E. A. Naeem, M. A. Alzain, J. F. Al-Amri, B. Soh, and F. E. A. El-Samie, "Investigation of chaotic image encryption in spatial and FrFT domains for cybersecurity applications," *IEEE Access*, vol. 8, pp. 42491–42503, 2020.

[57] M. Hanif, R. A. Naqvi, S. Abbas, M. A. Khan, and N. Iqbal, "A novel and efficient 3D multiple images encryption scheme based on chaotic systems and swapping operations," *IEEE Access*, vol. 8, pp. 123536–123555, 2020.

[58] J. Zhang, L. Chen, B. Liu, B. Ouyang, Q. Xie, J. Zhu, W. Li, and Y. Meng, "3D adversarial attacks beyond point cloud," *Inf. Sci.*, vol. 633, pp. 491–503, Jul. 2023.

[59] M. I. Sobhy and A.-E.-R. Shehata, "Methods of attacking chaotic encryption and countermeasures," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, vol. 2, May 2001, pp. 1001–1004.

[60] R. Yeniçeri, S. Kilinç, and M. E. Yalçin, "Attack on a chaos-based random number generator using anticipating synchronization," *Int. J. Bifurcation Chaos*, vol. 25, no. 2, Feb. 2015, Art. no. 1550021.
[61] H. Fan, J. Jiang, C. Zhang, X. Wang, and Y.-C. Lai, "Long-term prediction of chaotic systems with machine learning," *Phys. Rev. Res.*, vol. 2, no. 1, Mar. 2020, Art. no. 012080.
[62] J. Pathak, A. Wikner, R. Fussell, S. Chandra, B. R. Hunt, M. Girvan, and E. Ott, "Hybrid forecasting of chaotic processes: Using machine learning in conjunction with a knowledge-based model," *Chaos, Interdiscipl. J. Nonlinear Sci.*, vol. 28, no. 4, Apr. 2018, Art. no. 041101.
[63] C. Zhang, J. Jiang, S.-X. Qu, and Y.-C. Lai, "Predicting phase and sensing phase coherence in chaotic systems with machine learning," *Chaos, Interdiscipl. J. Nonlinear Sci.*, vol. 30, no. 8, Aug. 2020, Art. no. 083114.
[64] F. Borra, A. Vulpiani, and M. Cencini, "Effective models and predictability of chaotic multiscale systems via machine learning," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 102, no. 5, Nov. 2020, Art. no. 052203.
[65] T. Weng, H. Yang, C. Gu, J. Zhang, and M. Small, "Synchronization of chaotic systems and their machine-learning models," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 99, no. 4, Apr. 2019, Art. no. 042203, doi: 10.1103/PhysRevE.99.042203.
[66] J. Pathak, Z. Lu, B. R. Hunt, M. Girvan, and E. Ott, "Using machine learning to replicate chaotic attractors and calculate Lyapunov exponents from data," *Chaos, Interdiscipl. J. Nonlinear Sci.*, vol. 27, no. 12, Dec. 2017, Art. no. 121102.
[67] T. Weng, H. Yang, J. Zhang, and M. Small, "Modeling chaotic systems: Dynamical equations vs machine learning approach," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 114, Nov. 2022, Art. no. 106452.
[68] J. Hwang, N. Hosseinzadeh, and A. Hedayatipour, "Enhancing continuous chaos communication using machine learning in resource-limited devices," in *Proc. IEEE 16th Dallas Circuits Syst. Conf. (DCAS)*, Apr. 2023, pp. 1–5.
[69] R. Popovici and R. Andonie, "Sensor signal clustering with self-organizing maps," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Jul. 2015, pp. 1–8.
[70] M.-P. Hosseini, A. Hosseini, and K. Ahi, "A review on machine learning for EEG signal processing in bioengineering," *IEEE Rev. Biomed. Eng.*, vol. 14, pp. 204–218, 2021.
[71] M.-P. Hosseini, T. X. Tran, D. Pompili, K. Elisevich, and H. Soltanian-Zadeh, "Deep learning with edge computing for localization of epileptogenicity using multimodal rs-fMRI and EEG big data," in *Proc. IEEE Int. Conf. Autonomic Comput. (ICAC)*, Jul. 2017, pp. 83–92.
[72] S. Jukić, D. kečo, and J. Kevrić, "Majority vote of ensemble machine learning methods for real-time epilepsy prediction applied on EEG pediatric data," *TEM J.*, vol. 7, no. 2, p. 313, 2018.
[73] T. Iwase, Y. Nozaki, M. Yoshikawa, and T. Kumaki, "Detection technique for hardware trojans using machine learning in frequency domain," in *Proc. IEEE 4th Global Conf. Consum. Electron. (GCCE)*, Oct. 2015, pp. 185–186.
[74] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," in *Proc. Int. Conf. I-SMAC (IoT Social, Mobile, Anal. Cloud) (I-SMAC)*, Feb. 2017, pp. 32–37.
[75] H. Landi. (Sep. 2021). *Fitbit, Apple User Data Exposed in Breach Impacting 61M Fitness Tracker Records*. [Online]. Available: https://www.fiercehealthcare.com/digital-health/fitbit-apple-user-data-exposed-breach-impacting-61m-fitness-tracker-records
[76] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2008, pp. 129–142.
[77] M. M. U. Rehman, H. Z. U. Rehman, and Z. H. Khan, "Cyber-attacks on medical implants: A case study of cardiac pacemaker vulnerability," *Int. J. Comput. Digit. Syst.*, vol. 9, no. 6, pp. 1229–1235, Nov. 2020.
[78] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *Proc. IEEE 13th Int. Conf. e-Health Netw., Appl. Services*, Jun. 2011, pp. 150–156.
[79] J. Radcliffe, "Hacking medical devices for fun and insulin: Breaking the human SCADA system," in *Proc. Black Hat Conf. Presentation Slides*, 2011, pp. 1–13.
[80] CR Formatted L. Pycroft, S. G. Boccard, S. L. F. Owen, J. F. Stein, J. J. Fitzgerald, A. L. Green, and T. Z. Aziz, "Brainjacking: Implant security issues in invasive neuromodulation," *World Neurosurg.*, vol. 92, pp. 454–462, Aug. 2016.
[81] V. Hassija, V. Chamola, B. C. Bajpai, Naren, and S. Zeadally, "Security issues in implantable medical devices: Fact or fiction?" *Sustain. Cities Soc.*, vol. 66, Mar. 2021, Art. no. 102552.
[82] R. Vishwakarma, R. Monani, A. Rezaei, H. Sayadi, M. Aliasgari, and A. Hedayatipour, "Attacks on continuous chaos communication and remedies for resource limited devices," in *Proc. 24th Int. Symp. Quality Electron. Design (ISQED)*, Apr. 2023, pp. 1–8.
[83] C. He, K. Ming, Y. Wang, and Z. J. Wang, "A deep learning based attack for the chaos-based image encryption," 2019, *arXiv:1907.12245*.
[84] F. Wang, J. Sang, C. Huang, B. Cai, H. Xiang, and N. Sang, "Applying deep learning to known-plaintext attack on chaotic image encryption schemes," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2022, pp. 3029–3033.
[85] X. Gao, M. Cheng, S. Li, and D. Zeng, "Unveil the time delay signature in delayed chaotic communication system via CNN," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–6.
[86] Y. Chen, R. Xin, M. Cheng, X. Gao, S. Li, W. Shao, L. Deng, M. Zhang, S. Fu, and D. Liu, "Unveil the time delay signature of optical chaos systems with a convolutional neural network," *Opt. Exp.*, vol. 28, no. 10, pp. 15221–15231, 2020.
[87] M. Vakili, M. Ghamsari, and M. Rezaei, "Performance analysis and comparison of machine and deep learning algorithms for IoT data classification," 2020, *arXiv:2001.09636*.

JINHA HWANG is currently pursuing the master's degree in computer science with California State University Long Beach (CSULB).

She is also a Machine Learning Researcher. With a strong background in computer engineering and media engineering, she brings a multidisciplinary approach to her work, exploring the intersection of artificial intelligence and hardware to develop innovative solutions that drive real-world impact. At CSULB, she is a Research Assistant on a project focused on hardware security with machine learning. In this project, she is proposing a mechanism that provides confidence and credibility measures for chaotic synchronization. Recently, she was a Speaker at the 16th IEEE Dallas Circuits and Systems Conference, where she presented her work on enhancing chaos communication using machine learning. Her research has also been published in several reputable publications, including IEEE, ACM, and KDD. Her research interests include machine learning spans several domains, including natural language processing, computer vision, and signal processing.

GAURI KALE received the B.E. degree in electronics engineering from the University of Mumbai, India, in 2019, and the M.S. degree in electrical engineering from California State University Long Beach (CSULB), Long Beach, in 2023.

She interned with the ASIC Team as a Digital IC Intern, in Summer 2022. She was a Student Researcher on a project focused on the implementation of 45nm technology on hardware security with CSULB. Her research interests include analog, mixed-signal design, VLSI design, and hardware security. She also received the Society of Women Engineer Graduate Scholarship, in Spring 2022, and the Thomas D. Jewett Endowed Award for Graduate Disability Research Scholarship, in Fall 2022, commending her remarkable research contributions in disability studies.

PERSIS PREMKUMAR PATEL received the bachelor's degree in information technology from SVBIT, Gandhinagar, India, in 2020, and the master's degree in computer science from California State University Long Beach (CSULB), Long Beach, in 2023. During her time at CSULB, she was also a Teaching Assistant for computer architecture. Subsequently, she was a Research Assistant, actively contributing to innovative projects. Since her graduation, she has been an Adept Application Developer with ADP. Her professional journey has been characterized by an ardent dedication to devising inventive software solutions that enhance user experiences. Demonstrating a profound interest in both software development and machine learning, she adeptly synthesizes her academic acumen and proactive exploration to seamlessly unite these spheres.

RAHUL VISHWAKARMA (Graduate Student Member, IEEE) received the Bachelor of Technology degree in computer science from the SRM Institute of Science and Technology, in 2009. He is currently pursuing the M.S. degree in computer science with California State University Long Beach, Long Beach. He was with Hewlett Packard Enterprise (HPE), where he designed reference architectures for ConvergedSystem for SAP HANA, and Dell Technologies, he drove solutions for data protection and assisted customers in safeguarding data with data domain (deduplication-based backup storage), while leveraging machine learning across the product stack. He holds 38 granted U.S. patents in the domains of machine learning, data storage, persistent memory, DNA storage, and blockchain. His current research interests include addressing bias, explainability, and the uncertainty quantification of machine learning models.

MEHRDAD ALIASGARI received the B.S. degree in electrical engineering from the Sharif University of Technology, and the M.S. and Ph.D. degrees in computer science and engineering from the University of Notre Dame.

After the Ph.D. degree, he joined as a Faculty Member of the Computer Engineering and Computer Science Department, in 2013. His research interests include computer security and applied cryptography. Particularly, he focuses on privacy-preserving computation and outsourcing, verifiable and secure outsourcing and storage of data, private biometric and genomic computation, and cloud security. His dissertation was titled ''Secure Computation and Outsourcing of Biometric Data.'' He developed the first efficient solution on secure multiparty floating point computation which has numerous applications in the field of secure computation and outsourcing. He teaches computer security and cryptography courses with California State University Long Beach.

AVA HEDAYATIPOUR (Member, IEEE) received the Ph.D. degree in electrical engineering from The University of Tennessee, Knoxville.

She joined the Department of Electrical Engineering, California State University Long Beach (CSULB), as an Assistant Professor, in Fall 2020. Her current research interests include analog integrated circuit designs, bio-implantable and biomedical devices, low-power and low-noise designs, microelectronics, mixed-signal VLSI designs, and hardware security. She was acknowledged as a rising star at the 2020 ISSCC Conference. She is also a recipient of a University of Tennessee Fellowship Award, in 2019, and the Outstanding Teaching Assistant Award, in 2018.

AMIN REZAEI (Member, IEEE) received the master's degrees in computer science from the University of Louisiana at Lafayette and in computer engineering from Shahid Beheshti University, and the Ph.D. degree in computer engineering from Northwestern University.

He joined the Department of Computer Engineering and Computer Science, California State University Long Beach, as an Assistant Professor, in Fall 2020. He has a dozen years of experience in hardware security and computer architecture and he has published 40 peer-reviewed scientific articles at flagship venues, such as DAC, ICCAD, DATE, and ASP-DAC. He has served on the technical program committees and the Session Chair of many major conferences in his area, including IPDPS, ICCAD, ASP-DAC, ICCD, and GLSVLSI. Furthermore, NSF has funded two of his grant proposals totaling half a million dollars towards CISE-MSI and CRII programs. He is also a recipient of an Academic Excellence Award from the University of Louisiana at Lafayette and Walter P. Murphy and Royal E. Cabell Fellowship Awards from Northwestern University.

HOSSEIN SAYADI (Member, IEEE) received the B.Sc. degree from the K. N. Toosi University of Technology, in 2012, the M.Sc. degree in computer engineering from the Sharif University of Technology, in 2014, and the Ph.D. degree in electrical and computer engineering from George Mason University, in 2019. He is currently an Assistant Professor with the Department of Computer Engineering and Computer Science, California State University Long Beach (CSULB), Long Beach, where he directs the Intelligent, Secure, and Energy-Efficient Computer Systems (iSEC) Laboratory. He is a two-time recipient of the Provost Doctoral Fellowship from George Mason University. His research interests mainly include hardware/architecture security, machine learning, cybersecurity, computer architecture, and cyber-physical systems, leading to over 65 peer-reviewed technical papers in prominent conferences and journals. Notably, his research endeavors have been supported by the National Science Foundation (NSF), resulting in multiple NSF grants, an Engineering Research Initiation (ERI) Award of $200K, and a CISE-Minority Serving Institutions (MSI) grant of $300K. He has served as the Guest Editor of two MDPI journals, such as *Sensors* and *Cryptography*, and a technical committee member of many international IEEE/ACM conferences. He also serves as the Technical Program Committee (TPC) Chair for the IEEE ISQED 2024 Conference.