Grenze International Journal of Engineering and Technology, January Issue

Securing Cyberspace: Innovations and Challenges in Computational Intelligence

Vijayalakshmi MM[1] and Dr. Vani Krishnaswamy[2]
[1]Research Scholar, School of Computer Science and Engineering, Reva University, Bengaluru, Karnataka.
Email: Email: vijayalakshmimm3@gmail.com
[2]Associate Professor, School of Computer Science and Engineering, Reva University, Bengaluru, Karnataka.
Email: vanikrishna.s@reva.edu.in

***Abstract*—Cybersecurity is of paramount importance in safeguarding computer networks, systems, and data from unauthorized access and malicious activities. As technology advances and digital infrastructure becomes more interconnected, the threat landscape evolves, leading to a surge in cyber-attacks. This surge has been fueled by accelerated digitization, increased reliance on digital infrastructure, and the proliferation of Internet-connected devices. Notably, the exponential growth in internet usage has led to a corresponding increase in cyber-attack incidents each year. To combat these threats, various counter-measures, including intrusion detection systems (IDSs), have been developed. In recent years, there has been a notable trend towards leveraging computational intelligence techniques, such as machine learning (ML), deep learning (DL), and data mining (DM), to bolster cybersecurity efforts. These techniques aim to enhance threat detection, understand attack patterns, and fortify defenses against evolving methodologies. However, challenges persist, including the mitigation of zero-day attacks and concerns about the security of ML techniques against adversarial attacks. Adversaries may exploit vulnerabilities in ML models, raising questions about their reliability and robustness in real-world cybersecurity scenarios. In this context, image encryption, neural network-based schemes, convolutional neural networks (CNNs), and deep learning-based adversarial learning schemes are widely deployed to ensure cybersecurity. These technologies play a crucial role in securing multimedia data and combating cyber threats in an increasingly interconnected digital landscape. This article presents a detailed literature review about existing methods to ensure the cybersecurity by utilizing, encryption neural cryptography and adversarial learning.**

***Index Terms*—Cybersecurity, Adversarial learning, cryptography.**

I. INTRODUCTION

Cybersecurity encompasses a range of technologies and methodologies aimed at safeguarding computer networks, programs, and data from unauthorized access, alterations, or harm. Defense mechanisms operate at various levels, including host, network, application, and data, employing tools such as “firewalls”, “antivirus software”, and intrusion detection systems (IDS). These tools work covertly to prevent attacks and identify security breaches. However, adversaries maintain an advantage, needing only to exploit one vulnerability in protected systems. With the proliferation of Internet-connected systems, cyber-attacks have grown in scale, complexity, and cost, particularly during the years 2019 and 2020. This expansion was driven by accelerated digitization and increased reliance on digital infrastructure. Symantec's report indicates a significant surge in

Grenze ID: 01.GIJET.11.1.309

malicious attempts, with over 60 million blocked in the second quarter of 2020 alone, representing a 74.6% increase from previous months [1].

The proliferation of technologies, from smartphones to expansive communication systems, has facilitated the emergence of a highly interconnected digital society and widespread internet usage. It is currently estimated that over 5 billion smart devices exist, along with 3 billion people using the internet worldwide. This interconnectedness is integral to various applications, including online banking, shopping, email correspondence, document sharing, critical information dissemination, video conferencing, and gaming, among others. Consequently, an immense volume of data, measured in terabytes per second, is generated, processed, exchanged, and stored.

Remarkably, it is believed that 90% of the world's data has been generated within the last two years alone. This exponential growth in internet usage has corresponded with an increase in cyber-attack incidents each year. A notable example is the 2015 breach of the United States Office of Personnel Management, which led to the theft of information from around 21.5 million government employees, including names, social security numbers, and addresses. In 2013, Yahoo, the email service provider, fell victim to a cyber-attack, affecting nearly 3 billion Yahoo email addresses. The WannaCry ransomware attack in 2017 encrypted device contents and demanded payment in Bitcoin. Additionally, a staggering US$7.4 million worth of cryptocurrencies was pilfered from the Ethereum app in 2017 within a mere 3-minute timeframe. Equifax, a prominent credit rating agency, disclosed in 2017 that their server had been breached, compromising the personal information of 150 million individuals. Furthermore, GitHub, a widely-used version control hosting service, experienced a massive Denial of Service (DoS) attack in 2018.

According to cybersecurity experts, the damage caused by cyber-attacks in 2017 alone may have amounted to approximately US$5 billion, with projections indicating a significant escalation in the future. For instance, it's anticipated that by 2021, the annual damage could soar to as much as US$6 trillion (source: hackmageddon.com). To combat these threats, a range of counter-measures has been developed, with one prominent category being intrusion detection systems (IDSs).

In recent years, there has been a notable trend towards leveraging computational intelligence techniques, including ML, DL, and DM, to bolster cybersecurity efforts. These advanced techniques aim to enhance the detection of cyber threats, improve the understanding of malicious samples and attack patterns, and fortify defenses against evolving attack methodologies. Despite the significant progress achieved in the application of computational intelligence techniques, there are lingering challenges that must be addressed, such as the mitigation of zero-day attacks, which exploit previously unknown vulnerabilities. Furthermore, there is a emergent apprehension regarding the security and susceptibility of ML model to various attacks. Adversaries may attempt to manipulate ML models through techniques like adversarial attacks, raising concerns about the reliability and robustness of these systems in real-world cybersecurity scenarios. Therefore, while computational intelligence has demonstrated promising results in bolstering cybersecurity, there is a pressing need for ongoing advancements and innovations to effectively combat the evolving threat landscape.

Due to advanced utilization of multimedia devices, the amount of multimedia data is increasing drastically therefore ensuring cybersecurity plays important role. In this context, image encryption, neural network or convolution neural network based schemes and deep learning based adversarial learning schemes are widely deployed to ensure the security for cybersecurity applications.

A. Research Questions

RQ 1: what are the current methods of Image encryption to ensure cybersecurity?
RQ 2: What is the role of neural network i.e. Machine Learning and Deep Learning based models for cybersecurity?
RQ 3: How is the adversarial learning beneficial for cybersecurity?
RQ 4: what is the impact of deep learning in various cybersecurity domains?

II. LITERATURE REVIEW

This section presents the detailed discussion on existing methods of image encryption, neural cryptography and adversarial learning based approaches for cyber security related applications.

A. Image Encryption for cybersecurity

Faragallah et al. [1] introduced an efficient color image cryptosystem based on RC6 with distinct encryption and decryption phases. The encryption process begins by decomposing the color plain-image into RGB components,

which are then segmented into 128-bit blocks and encrypted using RC6. These encrypted blocks are subsequently multiplexed to construct the final cipher-image. The decryption phase reverses this process.

Wu et al. [2] introduced a novel content-aware DNA computing system designed to encrypt medical images, thereby ensuring privacy and enhancing security in healthcare. The system comprises both sender and receiver components, each featuring identical structural designs performing opposite functions for encryption and decryption, respectively. The encryption process employs a random DNA encoding mechanism and a content-aware permutation and diffusion module. This DNA encoding utilizes a random rule selector to map medical image pixels to outputs, while the permutation module generates a sequence encoding pixel values and introducing redundancy among adjacent pixels Hasan et al. [3] discussed the formidable challenge of ensuring image security in the realm of medical imaging. However, traditional encryption techniques encounter limitations regarding data size, redundancy, and capacity, rendering them unsuitable for direct application to e-health data, especially during patient data transfer over open channels. Consequently, there is a heightened risk of compromising patient data privacy. In response to these challenges, researchers have proposed various image encryption techniques to mitigate security threats. Nevertheless, existing techniques still confront several application-specific security issues. Therefore, the paper introduces an efficient, lightweight encryption algorithm tailored for the healthcare industry. This proposed encryption technique employs two permutation techniques to enhance the security of medical images while addressing the aforementioned challenges. Faragallah et al. [4] introduced an optical ciphering framework utilizing Double Random Phase Encoding (DRPE) to ensure the secure and efficient transmission of 3D Videos. According to this approach, each frame of the video is converted into an optimal signal and later this technique encrypts the obtained signal by employing two kind of phase modulation across the time and frequency domains. Finally, a Charge Coupled Device digital camera is used to reconstruct the obtained frame data. Yasser et al. [5] proposed a novel hybrid encryption/decryption scheme tailored for application in e-healthcare, or the Internet of Healthcare Systems (IoHS), aimed at safeguarding medical images. This approach leverages chaotic maps based perturbation approach which is in both both rounds of confusion and diffusion to address the limitations of traditional chaos-based architectures. Specifically, the scheme utilizes new map parameters and chaotic sequences to regulate the permutation and diffusion properties, while the derived properties govern pixel shuffling and substitution operations. Alawida et al. [6] highlighted the challenge posed by image redundancy and therefore suggested to handle the spatial information during encryption. The main aim of this work to present image encryption approach based on chaotic maps. Subsequently, a novel encryption approach is developed by incorporating permutation operations.

Khan et al. [7] addressed the ongoing risk of disclosure and privacy breaches faced by images generated by sensors in the industrial IoT. In order to overcome this issue, a blockchain based scheme is developed where cryptographic pixel values are stored in blockchain to ensure the security for images.

Banu et al. [8] emphasized on encryption mechanisms to solve the security related issues and introduced an encryption method for medical images by employing chaotic attractors in the frequency domain. The proposed model utilizes integer wavelet transform for frequency domain integrated with deoxyribonucleic acid (DNA) sequence in spatial domain. Further, it uses chaotic 3D Lorenz attractor and logistic map to produce the pseudo-random keys used in encryption.

Rehman et al. [9] propose a novel approach called Key Substitution Encryption Process with Discrete Wavelet Transform (KSP-DWT) within their Image Encryption Technique (IET). Referred to as KSP-DWT-IET in their study, this method aims to balance security and efficiency. This approach uses key scheming technique to update the initial keys and follows a substation method to encrypt the images. Moreover, it also utilizes DWT for compression of frequency sub-bands to reduce the computational overhead.

Tewani et al. [10] introduced a novel method for image encryption grounded in chaos theory. They utilized logistic maps to generate a set of 24 keys employed in encrypting the image. The design of the method is characterized by simplicity and efficiency, relying on permutation, diffusion, and optimization techniques.

B. Neural Cryptography

Kadry et al. [11] focused on the importance of secure data transmission in wireless networks, particularly concerning machine learning-based IDS. To address the security and efficiency related challenges, a comprehensive solution integrating WCSO, QNN, and ECC is introduced in this work. The WOA is employed to select network data features crucial for intrusion detection accuracy. The optimized quantum network, incorporating WOA with feed-forward and backpropagation algorithms, aids in attack identification. Encryption of sensitive data is facilitated by the ECC algorithm, ensuring secure storage on servers and document security.

TABLE I. COMPARATIVE ANALYSIS OF IMAGE ENCRYPTION AND CYBERSECURITY RESEARCHES

Study	Main Focus	Approach/Technique	Advantages	Limitations/Challenges
Faragallah et al. [1]	Color image cryptosystem	RC6 with different modes of operation	Efficient encryption, high-quality metrics	Complexity in handling different modes of operation
Wu et al. [2]	Medical image encryption	Content-aware DNA computing system	Robust, enhances security, effective for wireless broadcasting	Complexity in DNA encoding and permutation
Hasan et al. [3]	Secure medical image encryption	Lightweight encryption algorithm	Efficient, suitable for e-health data	Limited by data size and capacity
Faragallah et al. [4]	3D video transmission	Double Random Phase Encoding (DRPE)	Secure, efficient transmission	Complexity in optical signal conversion
Yasser et al. [5]	Medical image encryption for e-healthcare	Hybrid encryption with chaotic maps	Improved permutation and diffusion, robust encryption	Complexity in chaotic map integration
Alawida et al. [6]	Digital image encryption	Enhanced chaotic map algorithm	High security, low time consumption	Implementation complexity
Khan et al. [7]	IIoT image security	Permissioned private blockchain	Eliminates third party, ensures privacy and security	Blockchain integration complexity
Banu et al. [8]	DICOM image encryption	Chaotic attractors with DNA sequence	High security, effective encryption	Complexity in chaotic and DNA integration
Rehman et al. [9]	Efficient image encryption	KSP-DWT encryption process	High security, low computational overheads	Single encryption round limitation
Tewani et al. [10]	Image encryption using chaos theory	Logistic maps	Simple, efficient, increased randomness	Dependency on logistic map keys

In scenarios where data owners store sensitive information on servers, documents are encrypted using ECC. Additionally, ECC optimization is utilized to determine the most effective key for encryption.

Wu et al. [12] presented a novel approach for resilience against known-plaintext and chosen-plaintext attacks in image cryptography systems, a novel approach is proposed leveraging adversarial neural cryptography in conjunction with SHA-256 controlled chaotic systems. According to this approach, the first phase performs training of GAN and later noise like intermediate image is utilized which goes under XOR operations to produce the logistic maps to obtain the final chaotic map of image.

Bakshi et al. [13] introduced RNN based model for privacy preserving task. The proposed model utilizes homomorphic encryption (HE) model. The RNN helps to ensure the consistent prediction on incoming sequential data.. To achieve this objective, this article addressed two primary challenges: the accumulation of noise during successive calculations and the incompatibility of HE with activation functions such as sigmoid, ReLU, and tanh.

Jia et al. [14] introduced a novel neural network approach inspired by text classification methods in natural language processing for detecting cryptographic function types. Their end-to-end model comprises two key modules: Instruction-2-vec and K-Max-CNN-Attention. The first module extracts assembly instruction "words" and converts them into continuous vectors. Subsequently, the next module encodes these instruction vectors to generate function representations. Finally, a softmax classifier is employed to predict the categories of the functions based on these representations.

Gupta et al. [15] aimed to securely share confidential information without any risk of exposure by introducing a secure method for sharing secret shares of an image between two parties, employing Shamir's scheme alongside neural cryptography. Neural cryptography, distinct from traditional number theory-based approaches, offers advantages such as reduced computation time and memory complexities. By leveraging neural cryptography, the authors seek to establish a common secret key between the parties, facilitating secure communication over a public channel while minimizing computational requirements. In this process, both parties receive matching input vectors, generate output bits, and undergo training based on these outputs. The dynamics of the neural networks and their weight vectors converge to a synchronized state with identical weights, effectively serving as a shared key between the parties.

El-Shafai et al. [16] focused on medical image cryptography by using Stacked Auto Encoder which is used to generate two different sets of chaotic random matrices. The first set is employed to create a comprehensive shuffling matrix, whereas, the second set generates independent sequences used to eliminate correlation between

the permuted encrypted medical image and the original one. Leveraging parallel SAE computations, the proposed system demonstrates robustness while significantly reducing runtime and complexity.

Jambhale et al. [17] addressed the growing volume of digital images in medical diagnosis, spanning X-rays, MRIs, CT scans, and photographs, which has led to increased vulnerability to cyber-attacks. To mitigate this risk and safeguard the privacy of medical diagnostic information, the authors propose a method integrating ANN for image steganography with the RSA cryptographic algorithm. This approach aims to enhance security measures while preserving the confidentiality of medical images.

Meftah et al. [18] discussed the importance for secure training and inference of ANN in the era of AI and machine learning as a service (MLaaS) by leveraging Fully Homomorphic Encryption (FHE). This article introduced DOReN, a novel approach aimed at improving the space-efficiency of evaluating DNN. Unlike prior works suffering from accuracy degradation and scalability issues, DOReN utilizes low-depth, batched neurons capable of simultaneously evaluating multiple quantized encrypted data.

Saharkhizan et al. [19] proposed deep learning based method to detect the cyber-attacks of IoT systems. Given the increasing targeting of IoT devices by cybercriminals, the authors integrate a set of LSTM modules into an ensemble of detectors to address the challenges posed by the scale and diversity of IoT deployment, as well as the fast-paced cyber threat landscape.

Hanafi et al. [20] discuss the looming threat posed by Quantum Computers to current cryptographic algorithms and the need for resilient systems in the face of such advancements. They introduce Adversarial Neural Cryptography as a potential solution in the Post Quantum Scenario, where Generative Adversarial Networks architecture is utilized. In this dynamic cryptography model, two Neural Networks aim to protect the communication channel while a third Neural Network attempts to compromise it, offering a promising approach to safeguarding data in the future quantum computing era.

TABLE II. COMPARATIVE ANALYSIS OF NEURAL CRYPTOGRAPHY BASED RESEARCHES

Study	Main Focus	Approach/Technique	Advantages	Limitations/Challenges
Kadry et al. [11]	Secure data transmission in wireless mesh networks	WCSO-based QNN and ECC	Accurate intrusion detection, secure data encryption	Complexity in integrating multiple algorithms
Hagras et al. [12]	Cybersecurity image encryption	APK-EC-DCNN and EC-DHKE	High-level security, robust encryption	Computational complexity, requires high-level cryptographic expertise
Bakshi et al. [13]	Privacy-preserving RNN-based inference	Homomorphic encryption	Preserves functionality of RNN, secure prediction on encrypted data	Noise increase between calculations, limitations of activation functions
Jia et al. [14]	Cryptographic function detection	Instruction-2-vec and K-Max-CNN-Attention	Effective classification, end-to-end model	Requires extensive training data, complexity in implementation
Gupta et al. [15]	Secure secret sharing of images	Shamir's scheme with neural cryptography	Less computation time, memory efficient	Synchronization complexity, potential vulnerabilities in public channels
El-Shafai et al. [16]	Medical image cryptosystem	Stacked Auto-Encoder (SAE) network	Robust, parallel computation reduces runtime	Complexity in hybrid implementation, dependency on chaotic matrices
Jambhale et al. [17]	Secure medical image transmission	Neural networks and RSA	Enhanced privacy and confidentiality, effective steganography	Computational overhead, complexity in combining techniques
Meftah et al. [18]	Secure training and inference with AI	Fully homomorphic encryption (FHE) and DOReN	Space-efficient, secure encrypted data processing	High computational complexity, potential accuracy degradation
Saharkhizan et al. [19]	IoT cyber-attack detection	LSTM-based ensemble detectors	Effective for large-scale IoT, adaptable to dynamic threats	Scalability issues, high resource requirement for LSTM ensemble
Hanafi et al. [20]	Post-quantum cryptography	Adversarial Neural Cryptography with GANs	Potential to withstand quantum computing attacks	Highly complex, requires advanced cryptographic and neural network knowledge

C. Adversarial Learning

Apruzzese et al. [21] introduced deep reinforcement learning based framework for botnet detection. This framework automatically generates realistic attack samples capable of evading detection and utilizes them to augment the training set for producing more robust detectors.

Farajzadeh-Zanjani et al. [22] introduced a novel framework called Adversarial Class-Imbalance Learning (ACIL) aimed at learning from skewed class distributions. This framework employs a generative adversarial approach with a unique loss function during training session. It iteratively adjusts the weights MLP layer to learn the distributions of both minority classes and majority classes (e.g., normal).

Alkhowaiter et al. [23] presented that existing adversarial attack models primarily target and exploit neural network structures. Leveraging this insight, authors introduced a hypothesis suggesting that classical machine learning models, may be immune to these attacks due to their non-reliance on neural network design. Experimental results support this hypothesis, leading to the development of an adversarial-aware deep learning system. This system combines a primary deep learning model with a classical machine learning model serving as a secondary verification system. While the secondary model may have lower accuracy, it effectively detects adversarial attacks without impacting the output accuracy.

In [24] authors proposed a methodology which mainly focus on employing generative adversarial networks (GAN) for multiclass classification for malware detection and classification. The findings reveal that the discriminator of the Adversarial Conditional GAN (AC-GAN) model generally performs competitively with the other machine learning methods considered.

Yu et al. [25] presented Sill-Rgan, a novel GAN tailored to enhance hyperspectral image (HSI) classification performance under varying lighting conditions. The Sill-Rgan model is specifically designed to map different light condition domains, thereby improving the robustness of sample classification and generating new virtual samples. In order to overcome the challenges, this approach leverages a deep proxy-based learning framework. The proposed model integrates the advanced GAN with multi-task networks to ensure the optimal stability and loss function optimization.

Liu et al. [26] developed an attention-guided global-local adversarial learning network for image fusion tasks. In first phase, the attention weights are used to generate the coarse fusion results and capture the important region from images. Later, an edge loss function is introduced along with that spatial feature transform layer is used to refine the fusion process. Similarly, a global local learning model is introduced to obtain the balance in pixel intensity distribution. Finally, a global-local discriminator is used to ensure the local patches in the fused images.

Shi et al. [27] addressed HIS classification networks to adversarial attacks by proposing an attack-invariant attention feature-based defense (AIAF-Defense) model. Traditional defense methods against adversarial examples often struggle with generalization to unknown attacks. To overcome this limitation, this model employs an encoder-decoder architecture to remove perturbations from HSI adversarial examples. Specifically, a feature-disentanglement network serves as the encoder to separate attack-invariant spectral-spatial features from attack-variant ones in the adversarial example, while a decoder reconstructs the original HSI example.

Liu et al. [28] introduced a novel approach for synthesizing magnetic resonance imaging (MRI) images across different imaging settings, addressing the challenge of missing images due to scanning time constraints or corruption. Leveraging GANs, the proposed method enables the synthesis of images with specific settings based on available MR images and multiscale features are extracted by encoding. These feature maps are then fused to generate target images under desired settings. To address the issue of blurred edges in GAN-generated images, gradient prior information is incorporated into the model to preserve high-frequency details such as tissue textures. Additionally, multiscale information is integrated into the adversarial learning process, enhancing the quality of synthesized images.

Sun et al. [29] reported that medical image data analysis plays a crucial role in diagnosis, treatment, and prognosis by identifying lesions. Traditional approaches rely on supervised learning with meticulously labeled data, which is labor-intensive and demands specialized expertise. In response, they introduced a novel medical image synthesis model termed Abnormal-to-Normal Translation Generative Adversarial Network (ANT-GAN). This model enables the generation of normal-looking medical images from abnormal counterparts without the necessity of paired training data.

Wang et al. [30] presented a novel active deep feature extraction scheme for classification of HSI data by combining informative and measurement techniques. Initially, an adversarial autoencoder is adapted followed by multi-variance and distributional distance measure to identify the valuable candidate during training process.

III. Issues and Challenges

A. Issues and Challenges in Image Encryption for Cybersecurity

The image encryption based approaches face several challenges which are categorized as complexity, security needs, data size and redundancy, multi-domain consideration, key management etc. Faragallah et al. [1] presented RC6 based color image encryption system. However, the complexity of handling multiple modes and

TABLE III. COMPARATIVE ANALYSIS OF ADVERSARIAL LEARNING BASED RESEARCHES

Study	Main Focus	Approach/Technique	Advantages	Limitations/Challenges
Apruzzese et al. [21]	Safeguarding botnet detectors from adversarial attacks	Deep reinforcement learning mechanisms, data augmentation	Enhanced robustness against attacks	Limited to botnet detection, may not generalize to other domains
Farajzadeh-Zanjani et al. [22]	Addressing class imbalance in learning tasks	Adversarial class-imbalance learning, GANs	Improved performance with imbalanced data	May be complex to implement and optimize
Alkhowaiter et al. [23]	Investigating vulnerability of deep learning models	Adversarial-aware deep learning system	Effective detection of adversarial attacks	Dependent on primary deep learning model
[24]	Malware detection using image-based classification	GANs, comparison with SVM, XGBoost, RBM	Enhanced detection accuracy with GANs	High spectral dimensionality and noise challenges
Yu et al. [25]	Improving hyperspectral image (HSI) classification	Sill-Rgan GAN model, deep proxy-based learning framework	Improved robustness under varying conditions	Specific to Mirai botnet, may not generalize
Liu et al. [26]	Fusing extreme exposure images with attention-guided global-local adversarial learning	Adversarial learning, edge loss function, attention-guided reconstruction	Enhanced image fusion quality	Dependent on encoder-decoder structure
Shi et al. [27]	Defending hyperspectral image (HSI) classification networks against adversarial attacks	Attack-invariant attention feature-based defense model, encoder-decoder architecture	Improved resilience against adversarial attacks	May require large datasets for effective training
Liu et al. [28]	Synthesizing magnetic resonance imaging (MRI) images across different settings	GANs, encoder-decoder architecture	Generation of realistic MRI images	Requires coordination among federated nodes
Sun et al. [29]	Generating normal-looking medical images from abnormal counterparts	Abnormal-to-Normal Translation GAN	Simplified generation of medical images	Dependent on quality of generated synthetic data

ensuring seamless integration into various systems can be a challenge. Balancing performance and security is crucial, as encryption should not significantly degrade system performance. Wu et al. [2] introduce a content-aware DNA computing system for medical image encryption, which adds complexity through DNA encoding and permutation modules. The challenge lies in maintaining robustness and effectiveness while managing the computational overhead, especially in real-time healthcare applications. Hasan et al. [3] highlight the difficulty of applying traditional encryption techniques to medical images due to data size limitations and redundancy. The challenge is to develop encryption methods that handle large, redundant medical images efficiently without compromising data confidentiality and integrity. Faragallah et al. [4] proposed an optical ciphering framework using DRPE for 3D video transmission, addressing the need for specialized encryption techniques in different media formats. The challenge is to create versatile encryption methods that can adapt to various application-specific requirements while ensuring high security. Yasser et al. [5] and Alawida et al. [6] explore chaotic maps and perturbation algorithms for image encryption. These methods face the challenge of optimizing chaotic maps for better security without increasing the computational burden. Ensuring that the chaos-based methods remain unpredictable yet computationally feasible is a significant challenge. Khan et al. [7] proposed a blockchain-based solution for securing images in the IIoT, addressing trust and third-party involvement issues. The challenge lies in integrating blockchain technology with image encryption efficiently, as blockchain can introduce latency and scalability issues. Banu et al. [8] use chaotic attractors and DNA sequences for DICOM image encryption across frequency and spatial domains. The challenge is in managing the complexity of multi-domain encryption processes and ensuring they work seamlessly together to provide robust security without excessive computational demands. Rehman et al. [9] develop a key substitution encryption process (KSP-DWT) to balance security and computational efficiency. The main challenge is achieving high security with minimal computational overhead, as high-security algorithms often require significant computational resources. Tewani et al. [10] use logistic maps to generate keys for image encryption, focusing on increased randomness. Managing and securing these keys, ensuring their randomness, and integrating them into the encryption process without compromising performance is a critical challenge.

B. Issues and challenges in Neural Cryptography related tasks

The field of image encryption and secure data transmission faces numerous issues and challenges that researchers are actively trying to address. Kadry et al. [11] proposed usage of WCSO combined with QNN and ECC for secure data transmission in wireless mesh networks. The main challenges here include maintaining computational efficiency despite potential attacks, accurately detecting these attacks, and optimizing ECC for key management to balance security and computational overhead. Similarly, Hagras et al. [12] suggest an authenticated public key elliptic curve-based approach using a DCNN for image encryption, facing challenges of computational complexity, ensuring high-level security and robustness through chaotic systems, and achieving a balance between robustness and fast encryption.

In the realm of privacy preservation in machine learning, Bakshi et al. [13] presented a privacy-preserving RNN-based inference system using homomorphic encryption, grappling with noise increase between calculations and enabling homomorphic encryption to function with common neural network activation functions. Jia et al. [14] addressed cryptographic function detection with a novel neural network incorporating Instruction-2-vec and K-Max-CNN-Attention, facing the challenges of accurate real-time classification and managing the transformation of assembly instructions into continuous vectors.

For secure secret sharing, Gupta et al. [15] introduced a mechanism using Shamir's scheme and neural cryptography, which involves minimizing computation time and memory complexities while ensuring synchronization between neural networks for reliable key generation. El-Shafai et al. [16] propose a medical image cryptosystem using Stacked Auto-Encoder (SAE) networks to generate chaotic random matrices, focusing on robustness, reduced runtime through parallel computations, and maintaining high ciphering performance.

Securing medical images also poses challenges, as Jambhale et al. [17] combine neural networks for image steganography with RSA cryptographic algorithms to ensure privacy and confidentiality of medical diagnostics while integrating steganography and cryptography effectively. Meftah et al. [18] explore fully homomorphic encryption (FHE) for secure training and inference of artificial neural networks, facing high computational complexity and scalability issues, as well as the need for space-efficiency and accuracy.

In the context of IoT device security, Saharkhizan et al. [19] designed an approach using LSTM modules for detecting cyber-attacks, addressing the scale and diversity of IoT deployments and the fast-paced cyber threat landscape. Finally, Hanafi et al. [20] discuss post-quantum cryptography with adversarial neural cryptography using Generative Adversarial Networks (GANs), focusing on developing methods resilient to quantum computing attacks and ensuring secure communication channels while defending against adversarial attacks.

These challenges highlight the continuous need for innovation and optimization in cybersecurity practices to balance performance, security, and computational efficiency across various applications.

C. Issues and challenges in Adversarial Learning

In the realm of cybersecurity, numerous issues and challenges arise as machine learning mechanisms become integral to defense strategies. Apruzzese et al. [21] addressed the escalating problem of adversarial evasion in supervised classifiers, noting that most countermeasures degrade performance when adversarial perturbations are absent and struggle with novel attack variants. Their proposed framework leverages deep reinforcement learning to protect botnet detectors by generating realistic attack samples for training augmented, more resilient detectors. Similarly, Farajzadeh-Zanjani et al. [22] introduce an ACIL scheme to address skewed class distributions, particularly in identifying cyber-attacks and physical faults within majority-normal data distributions. Alkhowaiter et al. [23] focussed on the vulnerability of deep learning models to adversarial attacks, suggesting a hybrid system where classical machine learning models serve as secondary verification to complement primary deep learning models. This approach aims to detect adversarial attacks without compromising primary model accuracy.

Yu et al. [25] presented Sill-Rgan, a GAN designed to improve hyperspectral image classification under varying lighting conditions. This model addresses challenges such as high spectral dimensionality and noise, enhancing classification robustness and generating new virtual samples. Shi et al. [27] propose an attack-invariant attention feature-based defense (AIAF-Defense) model for HSI classification to improve generalization against unknown adversarial attacks. This model uses an encoder-decoder structure to remove perturbations from adversarial examples, enhancing robustness. These studies collectively underscore the multifaceted challenges in cybersecurity, highlighting the need for innovative solutions to enhance robustness, efficiency, and security across various applications.

III. Conclusions

Cybersecurity remains a critical concern as technological advancements continue to shape our interconnected digital world. The proliferation of internet-connected devices and the exponential growth in internet usage have led to a corresponding increase in cyber-attack incidents, posing significant risks to computer networks, systems, and data. To address these challenges, a range of counter-measures, including intrusion detection systems, have been developed. In recent years, there has been a notable shift towards leveraging computational intelligence techniques, such as machine learning, deep learning, and data mining, to bolster cybersecurity efforts. These advanced techniques offer promising avenues for enhancing threat detection, understanding attack patterns, and strengthening defenses against evolving methodologies. However, ensuring security for wide range of applications remain a challenging task. Currently, Image encryption, neural network-based schemes, convolutional neural networks, and deep learning-based adversarial learning schemes play crucial roles in securing multimedia data and combating cyber threats. Overall, while significant progress has been made in bolstering cybersecurity through computational intelligence techniques, continued efforts and innovations are essential to effectively combat the evolving threat landscape and safeguard our digital infrastructure.

Acknowledgment

The authors wish to thank A, B, C. This work was supported in part by a grant from XYZ.

References

[1] O. S. Faragallah, W. El-Shafai, A. I. Sallam, I. Elashry, E. S. M. El-Rabaie, A. Afifi, et al., "Cybersecurity framework of hybrid watermarking and selective encryption for secure HEVC communication," J. Ambient Intell. Humaniz. Comput., pp. 1–25, 2022.

[2] Y. Wu, L. Zhang, S. Berretti, and S. Wan, "Medical image encryption by content-aware DNA computing for secure healthcare," IEEE Trans. Ind. Inform., vol. 19, no. 2, pp. 2089–2098, 2022.

[3] M. K. Hasan, S. Islam, R. Sulaiman, S. Khan, A. H. A. Hashim, S. Habib, et al., "Lightweight encryption technique to enhance medical image security on internet of medical things applications," IEEE Access, vol. 9, pp. 47731–47742, 2021.

[4] O. S. Faragallah, W. El-Shafai, A. Afifi, I. Elashry, M. A. AlZain, J. F. Al-Amri, et al., "Efficient three-dimensional video cybersecurity framework based on double random phase encoding," Intell. Autom. Soft Comput., vol. 28, no. 2, pp. 253–367, 2021.

[5] I. Yasser, A. T. Khalil, M. A. Mohamed, A. S. Samra, and F. Khalifa, "A robust chaos-based technique for medical image encryption," IEEE Access, vol. 10, pp. 244–257, 2021.

[6] M. Alawida, "A novel chaos-based permutation for image encryption," J. King Saud Univ. Comput. Inf. Sci., vol. 35, no. 6, p. 101595, 2023.

[7] P. W. Khan and Y. Byun, "A blockchain-based secure image encryption scheme for the industrial Internet of Things," Entropy, vol. 22, no. 2, p. 175, 2020.

[8] A. Banu S and R. Amirtharajan, "A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach," Med. Biol. Eng. Comput., vol. 58, pp. 1445–1458, 2020.

[9] M. U. Rehman, A. Shafique, K. H. Khan, and M. M. Hazzazi, "Efficient and secure image encryption using key substitution process with discrete wavelet transform," J. King Saud Univ. Comput. Inf. Sci., vol. 35, no. 7, p. 101613, 2023.

[10] R. Tewani, Y. Garg, J. S. Bagga, A. Singh, and R. Bhalsodia, "Image encryption using permutation–diffusion approach," in Advances in Data Sciences, Security and Applications: Proceedings of ICDSSA 2019, Springer, Singapore, 2020, pp. 363–373.

[11] H. Kadry, A. Farouk, E. A. Zanaty, and O. Reyad, "Intrusion detection model using optimized quantum neural network and elliptical curve cryptography for data security," Alex. Eng. J., vol. 71, pp. 491–500, 2023.

[12] J. Wu, W. Xia, G. Zhu, H. Liu, L. Ma, and J. Xiong, "Image encryption based on adversarial neural cryptography and SHA controlled chaos," J. Mod. Opt., vol. 68, no. 8, pp. 409–418, 2021.

[13] M. Bakshi and M. Last, "Cryptornn-privacy-preserving recurrent neural networks using homomorphic encryption," in Cyber Security Cryptography and Machine Learning: Fourth International Symposium, CSCML 2020, Be'er Sheva, Israel, July 2–3, 2020, Proceedings 4, Springer International Publishing, 2020, pp. 245–253.

[14] L. Jia, A. Zhou, P. Jia, L. Liu, Y. Wang, and L. Liu, "A neural network-based approach for cryptographic function detection in malware," IEEE Access, vol. 8, pp. 23506–23521, 2020.

[15] M. Gupta, M. Gupta, and M. Deshmukh, "Single secret image sharing scheme using neural cryptography," Multimed. Tools Appl., vol. 79, pp. 12183–12204, 2020.

[16] W. El-Shafai, F. Khallaf, E. S. M. El-Rabaie, and F. E. Abd El-Samie, "Proposed neural SAE-based medical image cryptography framework using deep extracted features for smart IoT healthcare applications," Neural Comput. Appl., vol. 34, no. 13, pp. 10629–10653, 2022.

[17] T. Jambhale and M. Sudha, “A privacy-preserving hybrid neural-crypto computing-based image steganography for medical images,” in Intelligent Data Communication Technologies and Internet of Things: Proceedings of ICICI 2020, Springer, Singapore, 2021, pp. 277–290.
[18] S. Meftah, B. H. M. Tan, C. F. Mun, K. M. M. Aung, B. Veeravalli, and V. Chandrasekhar, “Doren: toward efficient deep convolutional neural networks with fully homomorphic encryption,” IEEE Trans. Inf. Forensics Secur., vol. 16, pp. 3740–3752, 2021.
[19] M. Saharkhizan, A. Azmoodeh, A. Dehghantanha, K. K. R. Choo, and R. M. Parizi, “An ensemble of deep recurrent neural networks for detecting IoT cyber attacks using network traffic,” IEEE Internet Things J., vol. 7, no. 9, pp. 8852–8859, 2020.
[20] B. Hanafi, M. U. Bokhari, and I. Khan, “Enhancing Post-Quantum Cryptography with Adversarial Neural Cryptography,” in 2024 11th International Conference on Computing for Sustainable Global Development (INDIACom), IEEE, 2024, pp. 1706–1712.
[21] G. Apruzzese, M. Andreolini, M. Marchetti, A. Venturi, and M. Colajanni, “Deep reinforcement adversarial learning against botnet evasion attacks,” IEEE Trans. Netw. Serv. Manag., vol. 17, no. 4, pp. 1975–1987, 2020.
[22] M. Farajzadeh-Zanjani, E. Hallaji, R. Razavi-Far, and M. Saif, “Generative-adversarial class-imbalance learning for classifying cyber-attacks and faults-a cyber-physical power system,” IEEE Trans. Dependable Secure Comput., vol. 19, no. 6, pp. 4068–4081, 2021.
[23] M. Alkhowaiter, H. Kholidy, M. A. Alyami, A. Alghamdi, and C. Zou, “Adversarial-aware deep learning system based on a secondary classical machine learning verification approach,” Sensors, vol. 23, no. 14, p. 6287, 2023.
[24] H. Nguyen, F. Di Troia, G. Ishigaki, and M. Stamp, “Generative adversarial networks and image-based malware classification,” J. Comput. Virol. Hacking Tech., vol. 19, no. 4, pp. 579–595, 2023.
[25] Z. Yu and W. Cui, “Robust hyperspectral image classification using generative adversarial networks,” Inf. Sci., vol. 666, p. 120452, 2024.
[26] J. Liu, J. Shang, R. Liu, and X. Fan, “Attention-guided global-local adversarial learning for detail-preserving multi-exposure image fusion,” IEEE Trans. Circuits Syst. Video Technol., vol. 32, no. 8, pp. 5026–5040, 2022.
[27] C. Shi, Y. Liu, M. Zhao, C. M. Pun, and Q. Miao, “Attack-invariant attention feature for adversarial defense in hyperspectral image classification,” Pattern Recognit., vol. 145, p. 109955, 2024.
[28] X. Liu, A. Yu, X. Wei, Z. Pan, and J. Tang, “Multimodal MR image synthesis using gradient prior and adversarial learning,” IEEE J. Sel. Top. Signal Process., vol. 14, no. 6, pp. 1176–1188, 2020.
[29] L. Sun, J. Wang, Y. Huang, X. Ding, H. Greenspan, and J. Paisley, “An adversarial learning approach to medical image synthesis for lesion detection,” IEEE J. Biomed. Health Inform., vol. 24, no. 8, pp. 2303–2314, 2020.
[30] X. Wang, K. Tan, C. Pan, J. Ding, Z. Liu, and B. Han, “Active deep feature extraction for hyperspectral image classification based on adversarial learning,” IEEE Geosci. Remote Sens. Lett., vol. 19, pp. 1–5, 2022.