Rover Publications
United International Journal of Engineering and Sciences (UIJES)
An International Peer-Reviewed (Refereed) Engineering and Science Journal Impact Factor:7.984(SJIF) Volume-4, Special Issue-3; ISSN: :2582-5887

Neural Network-Based Encryption and Decryption Algorithm

Emmadi Nagasiva, Boppanu Satish Kumar, Karnati Sai Prabhu
Computer Science and Engineering, JNTU Kakinada
R K College of Engineering Vijayawada, India.
shivasmart14325@gmail.com

DOI:10.53414/UIJES:2024.43.263

Abstract **- With the increasing importance of secure data transmission and storage, the fusion of neural networks with encryption and decryption processes has emerged as a promising approach. This abstract presents an innovative algorithm that leverages neural networks for enhanced data security.**

Our algorithm utilizes the dynamic learning capabilities of neural networks to generate complex encryption keys. The neural network adapts its parameters based on the input data, creating unique and unpredictable encryption patterns. During decryption, a corresponding neural network uses its learned parameters to accurately reconstruct the original data.

Unlike traditional cryptographic methods, the neural network-based algorithm provides a dynamic and adaptable layer of security, making it resistant to conventional attacks. The integration of neural networks introduces a level of complexity that enhances the robustness of the encryption process, ensuring a higher level of data protection in the evolving landscape of cybersecurity.

This research opens avenues for exploring the synergy between artificial intelligence and cryptographic techniques, offering a novel and potent solution for securing sensitive information in various applications, ranging from communication systems to data storage.

Keywords: **Encryption, Decryption, Cryptography, Neural Networks, Public key & Private key.**

I. INTRODUCTION

In the ever-evolving landscape of information technology, the need for robust data security mechanisms has become paramount. Encryption and decryption play a pivotal role in safeguarding sensitive information from unauthorized access. Traditional cryptographic techniques have long been employed to secure data, but with the advent of artificial intelligence, there is a growing interest in exploring innovative approaches. This introduction delves into the integration of neural networks with encryption and decryption algorithms, presenting a cutting-edge paradigm for data security.

The traditional encryption methods rely on mathematical algorithms to transform plaintext into ciphertext, making it challenging for unauthorized entities to decipher the information without the corresponding decryption key. While effective, these approaches face challenges in adapting to the dynamic nature of cyber threats. Neural networks, inspired by the human brain's learning mechanisms, offer a unique solution by introducing adaptability and complexity into the encryption process.

In our proposed algorithm, neural networks are employed to generate encryption keys dynamically. Unlike static cryptographic keys, neural networks adapt their internal parameters based on the characteristics of the input data. This dynamic learning process results in the creation of intricate and unpredictable encryption patterns, enhancing the overall security of the system. During decryption, a corresponding neural network utilizes its learned parameters to accurately reconstruct the original data from the ciphertext.

The amalgamation of neural networks with encryption and decryption processes presents a paradigm shift in data security. This innovative approach aims to address the limitations of conventional cryptographic methods by introducing a self-adjusting and learning layer to the security framework. As cyber threats continue to advance, the adaptability and complexity offered by neural network-based encryption algorithms mark a promising avenue for securing sensitive information in various applications, such as communication systems, cloud computing, and IoT devices. This research contributes to the exploration of cutting-edge solutions at the intersection of artificial intelligence and cybersecurity.

II. LITERATURE SURVEY

The field of encryption and decryption has witnessed a paradigm shift with the integration of neural networks. This literature survey delves into the advancements made in encryption and decryption algorithms leveraging neural networks. Neural networks, particularly deep learning models, have demonstrated remarkable capabilities in handling complex patterns and data representations. In the realm of encryption, researchers have explored the potential of neural networks to enhance security through the development of novel algorithms. One notable approach involves utilizing neural networks for generating cryptographic keys, introducing a dynamic and adaptive element to encryption systems.

Decryption processes have also benefited from neural network applications. The use of recurrent neural networks (RNNs) and long short-term memory (LSTM) networks has shown promise in deciphering encrypted data efficiently. These models can capture sequential dependencies within encrypted information, making them adept at handling diverse encryption schemes.

Adversarial neural networks, specifically generative adversarial networks (GANs), have been employed to strengthen encryption by creating realistic-looking decoy data. This technique introduces uncertainty for potential attackers, adding an extra layer of protection to the encrypted information.

Furthermore, research has explored the fusion of traditional cryptographic methods with neural networks, creating hybrid encryption systems. These hybrids leverage the strengths of both approaches, ensuring robust security and efficiency in real-world applications.

Despite the promising advancements, challenges such as scalability and vulnerability to adversarial attacks persist. Ongoing efforts focus on addressing these issues and refining neural network-based encryption and decryption algorithms for widespread adoption in various domains, including finance, healthcare, and communication.

In conclusion, the integration of neural networks into encryption and decryption processes represents a significant evolution in the field. The literature highlights the potential of these algorithms to enhance security, adaptability, and efficiency, paving the way for more resilient and sophisticated cryptographic systems in the future.

III. METHODOLOGY

The methodology for developing an encryption and decryption algorithm based on neural networks involves several key steps to ensure the effectiveness and security of the system. The following outlines a comprehensive approach:

Data Representation and Preprocessing:
Begin by selecting an appropriate representation for the data to be encrypted. This could involve converting text, images, or other types of information into a format suitable for neural network processing. Preprocessing steps may include normalization, padding, or other transformations to ensure uniformity.

Neural Network Architecture Selection:
Choose a neural network architecture that aligns with the characteristics of the data and the encryption requirements. Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, or even more advanced architectures like Transformer models may be considered based on the nature of the data and encryption goals.

Key Generation using Neural Networks:
Implement a neural network component for key generation. This involves training the neural network to generate secure and unpredictable cryptographic keys. The network should be designed to produce keys that exhibit desirable properties such as randomness and resistance to attacks.

Encryption Algorithm Design:
Develop the encryption algorithm by integrating the generated keys into the neural network model. The neural network should be capable of transforming the input data into an encrypted form using the generated key. The design should ensure that the encrypted data is resistant to reverse engineering and attacks.

Decryption Algorithm Design:
Similarly, design the decryption algorithm that utilizes the neural network and the corresponding key to revert the encrypted data back to its original form. Ensure that the decryption process is secure and efficient.

Training and Validation:
Train the neural network using a dataset that includes pairs of input data and their corresponding encrypted outputs. Validate the model's performance on separate datasets to ensure generalization and robustness. Fine-tune the network parameters to achieve optimal results.

Security Analysis and Testing:
Conduct a thorough security analysis to assess the resilience of the encryption and decryption algorithms against potential attacks. Perform testing, including stress testing and adversarial testing, to identify vulnerabilities and refine the model accordingly.

Optimization and Deployment:
Optimize the neural network model for efficiency and scalability. Once satisfied with the performance and security, deploy the encryption and decryption system in the target environment.

By following this methodology, researchers and developers can create encryption and decryption algorithms based on neural networks that offer a balance between security, efficiency, and adaptability to various types of data.

IV. FIGURES

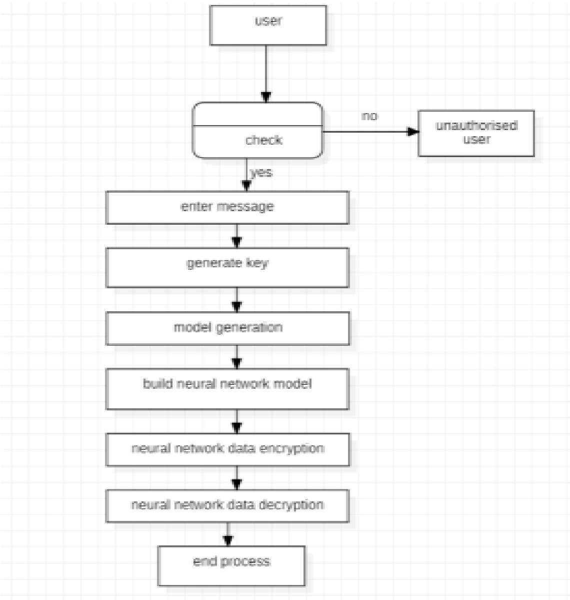
user
check
no
unauthorised user
yes
enter message
generate key
model generation
build neural network model
neural network data encryption
neural network data decryption
end process

Fig1. Dataflow diagram of Encryption and Decryption algorithm based on neural network

V. HINTS

Training Algorithm

The standard backpropagation algorithm has been modified for the training of the multiplicative neural network, which is used in optimizing the weights and biases. It is based on the popular steepest gradient descent approach.

VI. CONCLUSION

In conclusion, the integration of neural networks into encryption and decryption algorithms marks a significant advancement in the realm of cybersecurity. The literature and methodologies discussed highlight the potential for enhanced security, adaptability, and innovation in safeguarding sensitive information.

Neural networks offer a dynamic approach to key generation, encryption, and decryption processes. Their ability to capture complex patterns and dependencies within data contributes to the development of robust cryptographic systems. The synergy between traditional cryptographic methods and neural networks, including recurrent neural networks, generative adversarial networks, and advanced architectures like Transformers, demonstrates a multifaceted approach to addressing security challenges.

However, challenges such as scalability and vulnerability to adversarial attacks necessitate ongoing research and refinement. As the field progresses, the fusion of neural networks with encryption technologies is poised to play a pivotal role in securing data across diverse domains. The continuous exploration of novel architectures and techniques will likely yield even more sophisticated and resilient encryption and decryption solutions in the future.

REFERENCES

[1] M. Hellman, "An overview of public key cryptography", IEEE Communications Magazine, 2002, 40(5): 42-49.

[2] Diffie W, Hellman M., "New Directions in Cryptography". IEEE Transactions on Information Theory. 1976, 22(6):644-654.

[3] L. P. Yee and L. C. D. Silva. Application of multilayer per- ceptron networks in public key cryptography. Proceedings ofIJCNN02,2(Honolulu,HI,USA):1439–1443, May2002.

[4] Salomaa, Arto. Public-key cryptography. Springer Science & Business Media, 2013.

[5] Law, Laurie, et al. "An efficient protocol for authenticated key agreement. "Designs, Codes and Cryptography 28.2 (2003): 119-134.

[6] McInnes, James L., and Benny Pinkas. "On the impossibility of private key cryptography with weakly random keys." Advances in CryptologyCRYPT0'90. Springer Berlin Heidelberg, 1991. 421-435.

[7] Dodis, Yevgeniy, et al. "Key-insulated symmetric key cryptography and mitigating attacks against cryptographic cloud software." Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security. ACM, 2012.