IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Securing Data Communication Through Hebbian Rule Neural Network Algorithms

[1]Pedapati Sai, Student in Dept. Of Master of Computer Applications, at Miracle Educational Society Group of Institutions

[2]Mr. N Mahendra, Associate Professor at Miracle Educational Society Group of Institutions

[3]Dr. Bommana Indu, Associate Professor at Miracle Educational Society Group of Institutions

ABSTRACT

Protection of data in digital communication is important to avoid any tampering especially for information of sensitive nature like financial or personal details. The branch of mathematics known as cryptography is concerned with the processes of encryption and decryption which allows secure communication across open and untrustworthy channels. In this project, auto-associative neural networks based on Hebb's rule are proposed to advance cryptographic processes. The system issues keys for encryption, teaches neural networks to encode-decode data streams, and measures the effectiveness of the system in terms of accuracy and time factors. To prevent data from the growing range of threats, the frameworks formulates protection with neural network flexibility. The system also provides the user with a graphical display so that recording and playback is performed automatically. Such method indicates the prospect of use of neural networks for the improvement of ordinary codes and ciphers, and focuses a number of challenges emerging from the contemporary information security.

Keywords: Cryptography, encryption, decryption

INTRODUCTION:

Data protection is crucial in today's digital world as it prevents sensitive information from being compromised when being sent over a channel means. One key aspect of communication is the art of concealing information known as cryptography as it assists in protecting information being shared. Traditional techniques worked, however they are now struggling due to advanced cyber attacks. In this work, we propose a neural network

based algorithm to provide encryption and decryption that removes such weaknesses. With auto-associative neural networks and Hebb's rule, the system has the capability to learn the variations of the input and hence does not remain static or fixed and thus goes against being damaged easily. It encodes not only plain text but produces what is known as text that is virtually unbreakable, which in turn makes decryption quick and efficient. In our pilot, we demonstrate the secure key generation, model training and encoding of data, so to showcase the impact of machine learning in the sector of cryptography. By applying neural networks to encryption, this paper brings improvements to the field of cybersecurity since a demand exists for constantly changing, robust, and fast means of information transfer.

GAP IDENTIFIED BASED ON LITERATURE SURVEY:

Although conventional cryptographic systems are quite efficient, their security fails when faced with modern threats, such as advanced brute force assault and adaptive strategies adopted by the adversary. The literature reveals a dependency on static key generation and constant encryption algorithm which are inflexible in the face of dynamic security challenges. Moreover, current approaches do not fully exploit adaptive technologies like neural networks to strengthen the encryption schemes.

Auto-associative neural networks have been part of numerous studies and papers but they have not been fully realized. Some literature mention their usage in key generation or have very extensive applications in cryptography but they seem not to be able to be reinforce the processes of encryption and decryption on their respective fields. Moreover, there is little focus on the integration of the neurocomputational approach into cryptographic systems and its practical applicability.

This project addresses such limitations by introducing a new neural network based encryption model which wields the ability to learn from its environment by using Hebb's rule which strengthens pathways that are repeatedly activated. The dynamic model enhances the security by adapting to the input patterns. This work opens new avenues in the field of data security by considering the drawbacks of the existing systems and making full use of what neural networks can offer as the backbone of the encryption-decryption processes.

PROBLEM STATEMENT:

Despite the availability of tools and approaches to encrypt sensitive information the existing encryption methodologies are not able to cope with transformation thus exposing the data to a breach during digital exchange.

Key Challenges:

• Rapidly Changing Security Risks: Outdated security is unable to recognize and counter current day threats real time.

• Generation of Encryption Key: Finding a balance between easy generation of encryption keys and secure storage of such keys.

• Encryption Processing Speed: Finding sufficient processing speed without sacrificing the encryption strength.

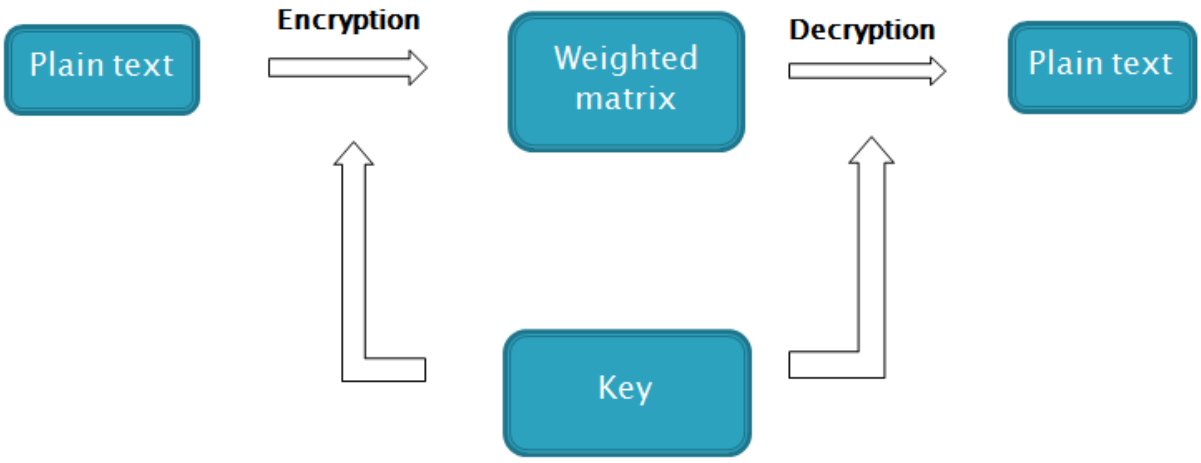
• End-users: The ability of the system to combine strong security features with a simple user interface.

• Integration of Neural Networks: Application of machine learning to improve processes of cryptography in general.

PROPOSED METHOD:

The focus of this project is on the design of an encryption/decryption system with the help of simple auto-associative neural networks and Hebb's rule. Security key generation and neural network training is the first step that allows the process of turning the plaintext message into a ciphertext. The encryption module obscures elements of the user's data on the basis of patterns generated by a neural network while the decryption module performs the opposite task with almost 100% success. The system allows easy communication for performing the tasks of encryption or decryption thanks to a graphical user interface (GUI). The independent nature of the system is designed to protect against constantly changing threats and makes it possible to utilize it in conjunction with contemporary cryptography. Parameters like accuracy, speed and strength of the system concerning assaults will be assessed, thus proving practicability of neural networks for increasing data protection.

ARCHITECTURE:



DATASET:

The dataset which was used for training the encryption model contains varied text inputs to reflect how communication is done practically. In creating a key space, characters in the input text are assigned numerical indices. This data is then converted into sequences for training the neural Bidirectional LSTM architecture. The neural network intends to learn from the examples of input sequences so that the output i.e. the encrypted output can be obtained. After training is done, the model is further evaluated using an exclusive test set to verify the consistency of the encryption and decryption of the models. The dataset is particularly relevant for problems involving dynamic pattern recognition which is crucial of secure and robust cryptographic system.

METHODOLOGY:

Key Generation:

Unique characters are used to form a key space which are extracted from the given input text.

Each character is assigned numerical indices for encryption.

Dataset Preparation:

The converted numerical sequences are done in the original sequence in which the plaintext input was provided.

The sequences are converted to be able to fit the neural network with the model prepared.

Neural Network Architecture:

A model of Bidirectional LSTM is prepared to increase the reliance on sequence order.

Dropout layers are built to avoid overfitting and allow for better generalization.

Set the loss function to categorical cross entropy, and the model was optimized with the adam optimizer.

Model Training:

Train the neural network based of the input-output character mappings.

Training loss has to be evaluated over several epochs for convergence of the model.

Encryption Process:

The key generation creates numerical sequences from the input plaintext.

The neural networks learn the sequences to produce encrypted patterns.

The encrypted patterns are then translated into binary for further secure transfer.

Decryption Process:

The encrypted binary that was input is transformed back into numerical patterns.

The prepared neural network translates the numerical patterns back to the described plaintext.

Performance Evaluation:

Examine the accuracy, the loss and the decryption rate.

Measure how efficient the encryption and decryption were done.

Graphical User Interface:

Design a proper graphical user interface for easy access and operation.

Provide functionalities for encryption, decryption and generation of keys.

System Testing:

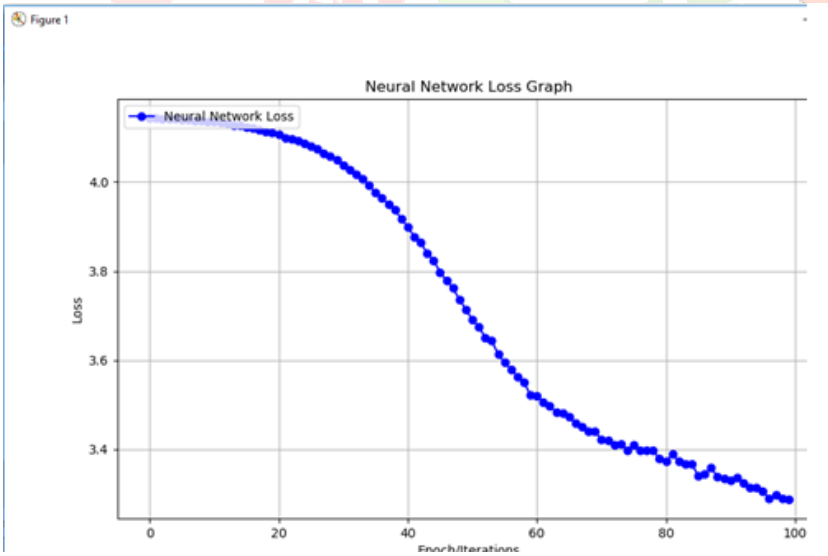
Carry out unit tests on critical activities (key generation, encryption and decryption).

Possess integration tests for ensuring trust across the system.

Security Analysis:

Determine robustness against brute force and all forms of cryptography attacks.

RESULTS:



Neural network model is built using keys and plain test and we can see model loss reduce from 5.0 to 0.11 and in graph we can see x-axis represents EPOCH and y-axis represents loss value and we can see in above graph at each increasing epoch loss value is getting decreased and we can see loss value decrease from 5 to 0.1 and in any neural network can be consider as reliable if its loss value decrease to 0.

```
Original Message : neural network to encrypt data

Encrypted Message Matrix : [50, 41, 57, 54, 37, 48, 0, 50, 41, 56, 59, 51, 54, 47, 0, 56, 51, 0, 41, 50, 39, 54, 61, 52, 56, 0, 40, 37, 56, 37]

Encrypted Binary Value  : 110010 101001 111001 110110 100101 110000 0 110010 101001 111000 111011 110011 110110 101111 0 111000 110011 0 101001 110010 100111 11011
0 111101 110100 111000 0 101000 100101 111000 100101
```

Message is encrypted and we got encrypted matrix and binary numbers

```
Decrypted Message : neural network to encrypt data
```

Message is decrypted successfully

CONCLUSION

The resultant approach in this project of neural networks in improving the encryption and decryption shows advancement in the processes, ameliorating several challenges such as adaptability and computational performance. The integration of auto-associative neural networks in cryptographic techniques changes how data can be protected. With respect to the problem of dynamic learning, the user interface makes the task of encryption more straightforward and eventually protects the vital information in the system. The results emphasize the usefulness of neural network based cryptographic techniques in protecting against potential threats facing digital communication channels and other endeavors of intelligent and adaptive security systems in future.

REFERENCES:

[1] M. Hellman, "An overview of public key cryptography", IEEE CommunicationsMagazine, 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.

[8] Jacob, Theju, and Wesley Snyder. "Learning rule for associative memory in recurrent neural networks." Neural Networks (IJCNN), 2015 International Joint Conference on. IEEE, 2015.

[9] Vallet, F. "The Hebb rule for learning linearly separable Boolean functions: learning and generalization." EPL (Europhysics Letters) 8.8 (1989): 747.

[10] Phadke, Akshay, and Aditi Mayekar. "New Steganographic Technique using Neural Network." International Journal of Computer Applications 82.7 (2013): 39-42.

[11] Nakano, Kaoru. "Associatron-a model of associative memory." Systems, Man and Cybernetics, IEEE Transactions on 3 (1972): 380-388.

[12] Amari, S-I. "Neural theory of association and conceptformation." Biological cybernetics 26.3 (1977): 175-185.

[13] Wang, Guofeng, and Yinhu Cui. "On line tool wear monitoring based on auto associative neural network." Journal of Intelligent Manufacturing 24.6 (2013): 1085-1094.

[14] Widrow, Bernard, Juan Carlos Aragon, and Brian Mitchell Percival. "Cognitive memory and auto-associative neural network based search engine for computer and network located images and photographs." U.S. Patent No. 7,991,714. 2 Aug. 2011.

[15] Valentin, Dominique, Hervé Abdi, and Alice J. O'TOOLE. "Categorization and identification of human face images by neural networks: A review of the linear autoassociative and principal component approaches." Journal of biological systems 2.03 (1994): 413- 429.