Industrial Engineering Journal
ISSN: 0970-2555
Volume : 51, Issue 10, July-December: 2022

AI-POWERED ENCRYPTION AND DECRYPTION WITH NEURAL NETWORK ALGORITHMS

D. Siva Ranjan Das[1] , G. Archana Reddy[2]

[1] Assoc. Professor, Department of Computer Applications, Aurora's PG College (MBA), Uppal, Hyderabad
Email: sivaranjandas@yahoo.com

[2]Assistant Professor, Department of Computer Applications, Aurora's PG College (MBA), Uppal, Hyderabad
Email: archanareddy054@gmail.com

ABSTRACT

Cryptography is used to prevent the plain text of a cipher from being decrypted without the accompanying key. Security in network communication is of utmost importance. The two basic parts of cryptography—encryption and decryption—allow for the transmission of confidential and private data over unsecure networks. For the purpose of preventing misuse, data must be concealed from users who are not authorized. This is the core idea behind cryptography. If you employ strong cryptography, it is almost impossible to use brute force to break the algorithm or the key. Very long keys and encryption algorithms that are resistant to other types of attack are essential components of good cryptography. The neural net application represents the next level in good cryptography. Neural nets have applications in cryptography and can be quite helpful. The use of neural networks for this purpose is covered in this paper. In this study, plain text and keys will be used to train a neural network for encryption and decryption. This project also consists of an experimental demonstration.

Keywords: Neural Network Algorithms, Artificial Intelligence, Encryption, Decryption

1. INTRODUCTION

science and practice of information concealing. Data encryption and decryption are also involved. Additionally, it makes it possible to communicate data securely over unreliable networks. Decryption is the opposite of encryption, which is the process of applying a key to plain text to transform it into encrypted text. There are essentially two sorts of cryptography models: symmetric models and asymmetric models.

cryptography
Encryption and decryption are two methods used in the science of data concealment via insecure networks: encryption transforms plain text into cipher text, and decryption transforms cipher text back into plain text. Public Key encryption is a type of encryption that employs an asymmetric model [2]. Since everyone on the network is aware of the public key used here to encrypt plain text, it is sometimes referred to as a shared key [1]. In public key cryptography, decryption of cipher text is accomplished with a private key only; that is, only the recipient who possesses the corresponding private key can decrypt the message. A private key is a secret key that is kept secret from other users on the network and is only known to the corresponding users.

A cryptography system that uses the symmetric cryptography model is called private key cryptography. This uses a private secret key for encryption of plain text and the same secret key for decryption of ciphered material [5]. A shared secret key is one that is utilized in both encryption and decryption, like in this instance. The shared key that is being used here is exclusive to this session and is only shared with the sender and the recipient.

2.LITERATURE SURVEY AND RELATED WORK

There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications is that of cryptography. Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used .non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet. Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below. In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into cipher text, which will in turn (usually) be decrypted into usable plaintext.

Types of Cryptographic Algorithms :

There are several ways of classifying cryptographic algorithms. Here they will be categorized based on the number of keys that are employed for encryption and decryption. The three types of algorithms are:

Secret Key Cryptography –

With secret key cryptography, a single key is used for both encryption and decryption. As shown in the figure, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key (or rule set) to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption.

Public Key Encryption –

Public-key cryptography has been said to be the most significant new development in cryptography in the last 300-400 years. Modern PKC was first described publicly by Stanford University professor Martin Hellman and graduate student Whitfield in 1976. Their paper described a two-key crypto system in which two parties could engage in a secure communication over a non-secure communications channel without having to share a secret key. In PKC, one of the keys is designated the public key and may be advertised as widely as the owner wants. The other key is designated the private key and is never revealed to another party. It is straight forward to send messages under this scheme.

Hash Functions –

Hash functions, also called message digests and one-way encryption, are algorithms that, in

some sense, use no key. Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a digital fingerprint of a file's contents, often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords. Hash functions, then, provide a measure of the integrity of a file.

3 EXISTING SYSTEM

Cryptographic software is vulnerable to software based assaults (e.g., malware) since the associated cryptographic keys can be compromised in their entirety. To lessen the impact of repeated attacks on cryptographic software, we look into key-insulated symmetric key cryptography in this study. Our proof of-concept implementation in a Kernel-based Virtual Machine (KVM) environment shows that key insulated symmetric key cryptography is feasible.

4 PROPOSED WORK AND ALGORITHM

The ultimate goal is to make it possible for a coded message to be deciphered without the use of a Key. Encryption uses two main techniques: symmetric and asymmetric. In symmetric encryption, The encryption and decryption keys are shared by both parties. P stands for plain text, while K stands for the secret key used by the sender to construct C stands for encrypted, or cipher text, Artificial intelligence, machine learning, and deep learning all benefit from neural networks' ability to mimic the human brain's functioning. Deep learning methods rely on neural networks, often known as artificial neural networks (ANNs) or simulated neural networks (SNNs). Because they replicate the way biological neurons communicate with one another, their name and structure are derived from the human brain as well .The aim of this research is to develop an effective method to predict heart disease, in particular Coronary Artery Disease or Coronary Heart Disease, as accurately as possible.

Required steps can be summarized as follows:

1) Five datasets are combined to develop a larger and more reliable dataset.
2) Two selection techniques, Relief and LASSO, are utilised to extract the most relevant features based On rank values in medical references. This also helps todeal with over fitting and under fitting Problems of machine learning.
3) Additionally, various hybrid approaches, including Bagging and Boosting, are implemented to improve the testing rate and reduce the execution time.
4) The performance of the different models is Evaluated based on the overall results with All, Relief and LASSO selected features.

5 METHODOLOGIES

MODULES

DATA SET

This paper utilizes the data set provided by revolution analytics for the detection of the cardio vascular dataset from Kaggle. Dataset has 51149 legal transactions and 3312 fraudulent transactions. The dataset is divided as 60%, 20% and, 20% in the Train, Valid and Test set, respectively.

DATA PREPROCESSING

For efficient implementation of the classification algorithm, data preprocessing is performed before feature selection. Under-sampling is performed to make the dataset balanced to avoid the biasing of the classification algorithm towards the majority class. Feature Selection is implemented on a balanced dataset.

FEATURE SELECTION

Feature selection methods are used to remove unnecessary, irrelevant, and redundant attributes from a dataset that do not contribute to the accuracy of a predictive model or which might reduce the accuracy of the model. In this paper seven feature selection techniques namely Select-K-best, Feature Importance, Extra tress classifier, Person's correlation, Mutual Information, Step forward selection and Recursive feature elimination are used.

FEATURE IMPORTANCE

Feature importance is a class of techniques for assigning scores to input features to a predictive model that indicates the relative importance of each feature at the time of making a prediction. It reduces the number of input features. In this paper, feature importance is implemented using an extra tree classifier from the decision tree.

Extra Trees is similar to Random Forest, it builds multiple trees and splits nodes using random subsets of features, but unlike Random Forest, Extra Tree samples without replacement and nodes are split on random.

6 RESULTS AND DISCUSSION

Fig 1: HOME SCREEN

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 51, Issue 10, July-December: 2022

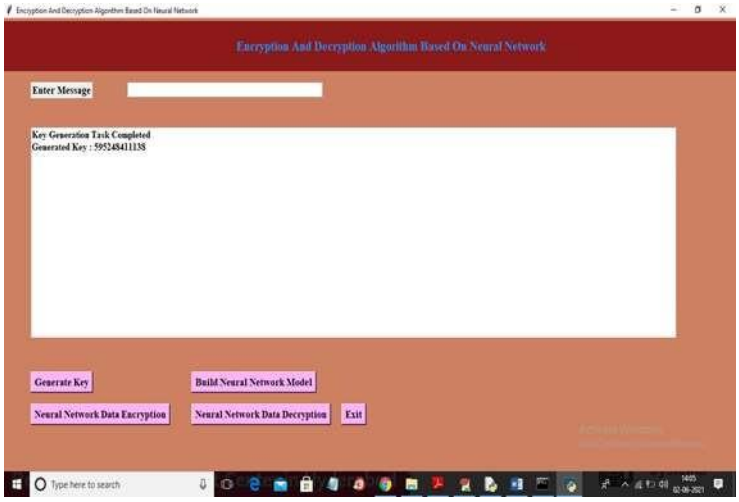

Fig 2: KEY GENERATED IN PAGE

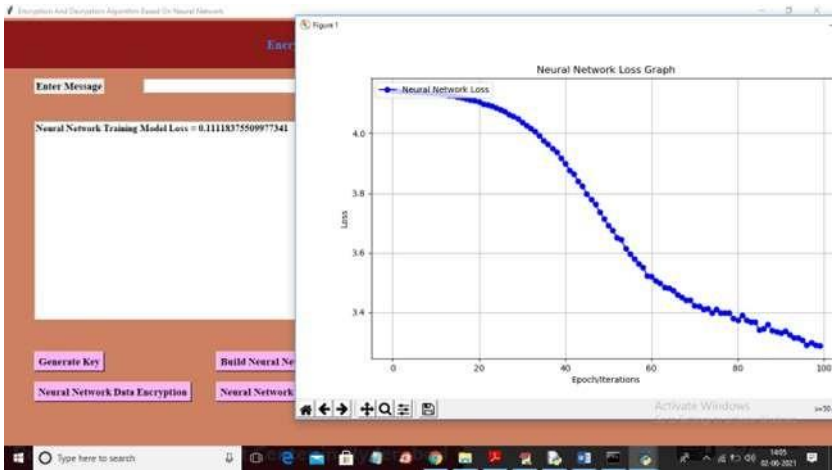

Fig 3: NEURAL NETWORK LOSS PAGE

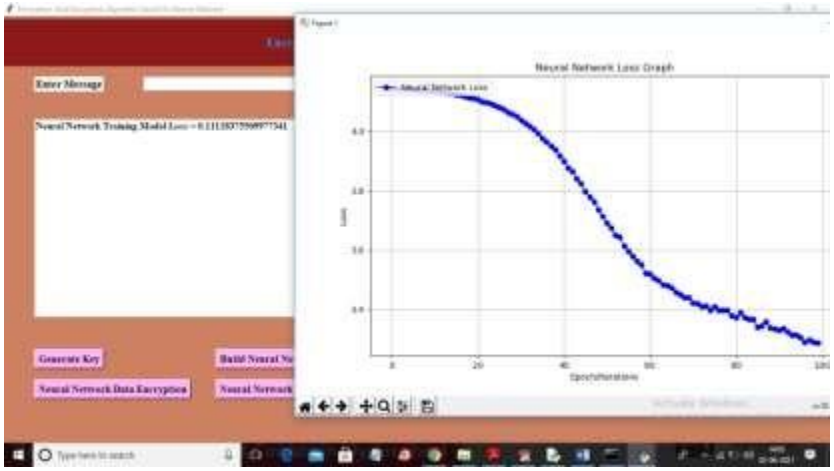

Fig 4: NEURAL ENCRYPTION OF DATA

Fig 5: NEURAL DECRYPTION OF DATA

7. CONCLUSION AND FUTURE SCOPE

The idea of applying neural networks to the realm of cryptography is expanding quickly. The literature has a variety of neuro-crypto algorithms that researchers have proposed. However, the majority of them are restricted to cryptanalysis and key creation. In the study project, plain text is encrypted into a form that is completely different from the previous one using an auto associative memory network. The technique boasts faster encryption and decryption speeds and is relatively easy to implement. Because the technique uses a symmetric key scheme, key leaks are a possibility. To get around this, communication should only be between trusted parties, or an authority figure should be employed to stop important leaks. Overall, the discussion has demonstrated that different classifiers' performances were adequate when compared to earlier research; yet, there are a few restrictions. For example, relying too much on Relief in this situation or using a certain feature selection technique to generate incredibly precise outcomes. Furthermore, a significant percentage of missing values in the dataset may be detrimental. Since we've shown how to solve the problem using the right techniques, if the missing value is quite large, other datasets used with this model also need to handle this problem. Additionally, even though our instruction

8 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.

[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.