Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 11, November : 2023

ENCRYPTION AND DECRYPTION ALGORITHM BASED ON NEURAL NETWORK

Dr. K.N.S. LAKSHMI Professor, Department of Computer Science & Engineering, , Sanketika Vidhya Parishad Engineering College, P.M. Palem Vishakhapatnam, Andharapradesh : mnslakshmi.vvit@gmail.com@gmail.com

JAGADEESH AMPOLU M.Tech Scholar, Department of Computer Science & Engineering, Sanketika Vidhya Parishad Engineering College, P.M. Palem,, Vishakhapatnam, Andharapradesh Email Id: jagadeesh.ampolu1@gmail.com

ABSTRACT

In order to prevent a cipher's plain text from being decoded without the corresponding key, cryptography is used. In network communication, security is a top priority. Encryption and decryption are the two main components of cryptography, which makes it possible to transfer private and secret information through an insecure network. Data must be hidden from unauthenticated users so that they cannot misuse it. This is the fundamental principle of cryptography. It is nearly impossible to break the algorithm or the key using brute force if you use good cryptography. Good cryptography relies on extremely long keys and encryption algorithms that are resistant to other forms of attack Good cryptography's next step is represented by the neural net application. When it comes to cryptography, neural networks can be a useful tool. This paper discusses using neural networks for this purpose. Using neural networks to encrypt and decrypt, the neural network will be trained with keys and plain text in this study. An experimental demonstration is also included in this project.

KEYWORDS:- cryptography, neural networks, encrypt, decrypt

1 INTRODUCTION

Cryptography is derived from the Greek word kryptos which means hidden or secret. It is a technique for safe communication in the presence of unsecure third party. It is a science and practice of hiding information and it is a combination of both mathematics and computer science branch. It involves both encryption and decryption of data. And it enables to send the data securely over the insecure network. Encryption is applying key on plain text to convert it into cipher text and decryption is the reverse process of encryption. Cryptography model is of basically two types one is symmetric model and asymmetric model.

CRYPTOGRAPHY It is a science of hiding the important data while it travel's in the unsecure network and it involves encryption to convert plain text into cipher text and decryption to convert the cipher text into the plain text.

Public Key Cryptography: It is a cryptography system where asymmetric cryptography model is used [2]. In this for encryption of plain text public key is used and public key is known by all the users in the network that is why it is called as shared key [1]. Decryption of cipher text in public key cryptography is done using private key only which means if receiver is having the respective private key then only the receiver can decrypt the message Private Key is a secret key which is only known to the respective users and is hidden from others in the network.

Private Key Cryptography: It is a cryptography system where symmetric cryptography model is used. In this for encryption of plain text secret key is used which is private key and for decryption of cipher text also here same secret key is used [5]. As here in both the cases of encryption and decryption similar key is used so it is called shared secret key. Shared key used here is unique key for a session and is only disclosed to the sender and the receiver

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.

2.1 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.

2.2 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.

2.3 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 utilized to extract the most relevant features based On rank values in

medical references. This also helps to deal 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.

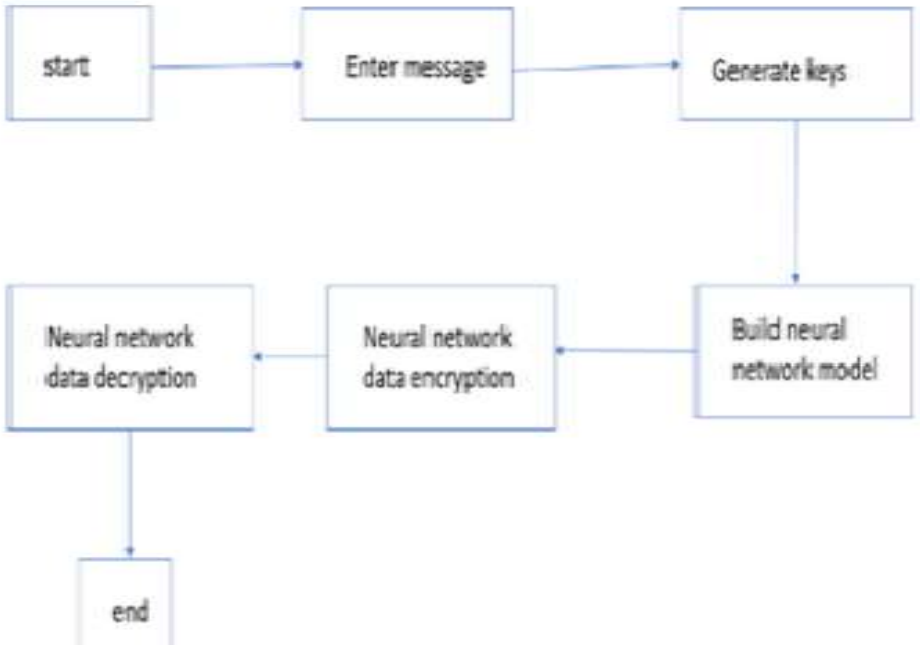

FIG 1:- PROPOSED MODEL FOR ENCRYPTION AND DECRYPTION

4.1 Algorithm:-

There are three network architectures:

1. Single Layer feed forward networks – In this layer, the input layer consist of source node that results the output in the form of neuron. It is feed forward type ofnetwork.
2. Multilayer feed forward networks – It only adds an extra layer known as hidden layer. Because of this hidden layer higher level of statistic is obtained.
3. Recurrent Network – This network contains at least one feedback loop. In this loop, output of a neuron is fed back into its own input which increases learning capability. And it also increases performance.

4.2 BACKPROPAGATION

There are so many restrictions in single layer feed forward network. So we use backpropagation to reduce the errors. The errors for the units of the hidden layer are determined by back-propagating the errors of the units of the output layer. This method is Backpropagation learning rule. It canalso be considered as generalization of delta rule for multilayer function.

An Artificial Neural Network (ANN) is an information processing paradigm that is inspired by the waybiological nervous systems, such as the brain, process information. The key element of this paradigm is the structure of the information processing system. It is composed of a large number of highly interconnected processing elements (neurones) working in unison tosolve specific problems. ANNs, like people, learn by example. An ANN is configured for a specific application, such as pattern recognition or data classification, through a learning process. Learning in biological systems involves adjustments to the

synaptic connections that exist between the neurones. This is trueof ANNs as well.

2Generalized Delta Rule –

This formula computes δ's for all units in the network. This generalized delta rule is for feed-forward network of non- linear units.

There are three types of cryptographic schemes used to accomplish these goals:

$$\delta_h^p = \mathcal{F}'(s_h^p) \sum_{o=1}^{N_o} \delta_o^p w_{ho}.$$

1. Secret key cryptography –

With secret key cryptography, a single key is used for bothencryption 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 ruleset) to decryptthe message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption.

2. Public-key cryptography –

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.

3. 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 thefile has not been altered by an intruder or virus. Hash functions are also commonly employed by many operatingsystems to encrypt passwords. Hash functions, then, provide a measure of the integrity of a file.

DESIGN OF THE PROPOSED ANN-BASED ENCRYPTION SYSTEM

Every practical encryption system consists of fourfundamental parts (Garfinger 1998), see Figure 3:

- The message that you wish to encrypt (called the *plain text*).
- The message after it is encrypted (called the *ciphertext*).
- The encryption algorithm.

The key (or keys), which is used by encryptionalgorithm

In this paper, we conducted an experimental study withusing neural network in cryptography. Thus, it means

- to design the topology of the neural network;
- to design the method of training algorithm of theneural network;
- to design the training set for training.

We successfully used neural networks as an encryption and decryption algorithm in cryptography. Parametersof both adapted neural networks were then included intocryptography keys. We used multilayer neural networks,which were adapted by backpropagation. Topology of each neural network is based on their training sets (see Table 1). In the encryption process, the input message isdivided into 6-bit data sets and also 6-bit sets are produced after the encryption process. Thus, both systems were designed as follows: 6 units on the input

layer and 6 output units. There is no predeterminednumber of units in the hidden layer, but we also used 6 units. Both networks were trained on binary representations of symbols. In each training set, chains of numbers of the plain text are equivalent to binary values of their ASCII code, chains of letters of the plain text are equivalent to their binary value, which are 96 less than their ASCII code, each chain of some punctuation symbol of the plain text is equivalent to a binary value of ASCII code of space (e.g. 32), and chains of others chars of the plain text are equivalent to zero. Then, the cipher text is a random chain of 6 bits.

The security for all encryption and decryption systemsis based on a cryptographic key. The SIMPLE systems use a single key for both encryption and decryption. Thegood systems use two keys. A message encrypted with one key can be decrypted only with the other key. If we use the neural network as encryption and also decryption algorithm, their keys have adapted neuralnetworks´ parameters; which are their topologies (architecture) and their configurations (weight values onconnections in the given order). Generally, each key is written as follow:

[*Input, Hidden, Output, Weights coming from the input units, Weights coming from the hidden units*]

where

Input is the number of input units; *Hidden* is the number of hidden units;*Output* is the number of output units;

Weights coming from the input units are weightvalues coming from the input units to hidden units in a predefined order;

Weights coming from the hidden units are weightvalues coming from the hidden units to output units in a predefined order

Parameter values of both ANNs in our experimentalstudy are the following:

- each input layer consists of 6 nodes, whichrepresents the 6-bit blocks;
- each hidden layer consists of 6 nodes;
- each output layer consists of 6 nodes, used to definethe decrypted output message;
- fully connected networks;
- a sigmoid activate function;
- a learning rate equals 0,3.

5 METHODOLOGIES

5.1 MODULES

5.1.1 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.

5.1.2 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.

5.1.3 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

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 11, November : 2023

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.

5.1.4 **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

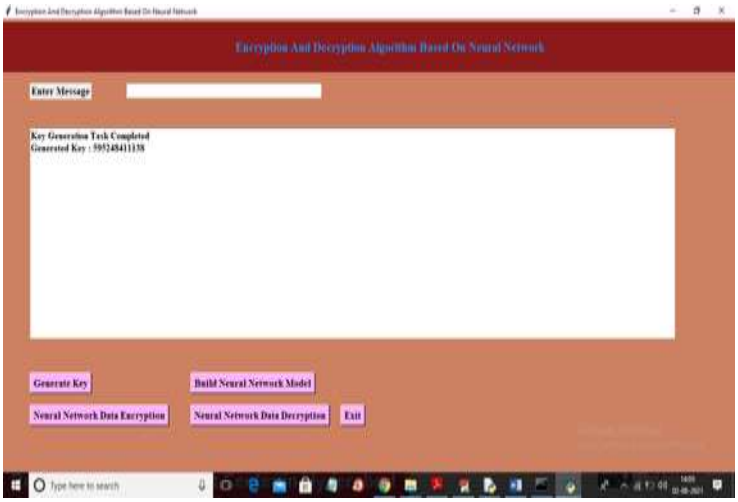

Fig 2: KEY GENERATED IN PAGE

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 11, November : 2023

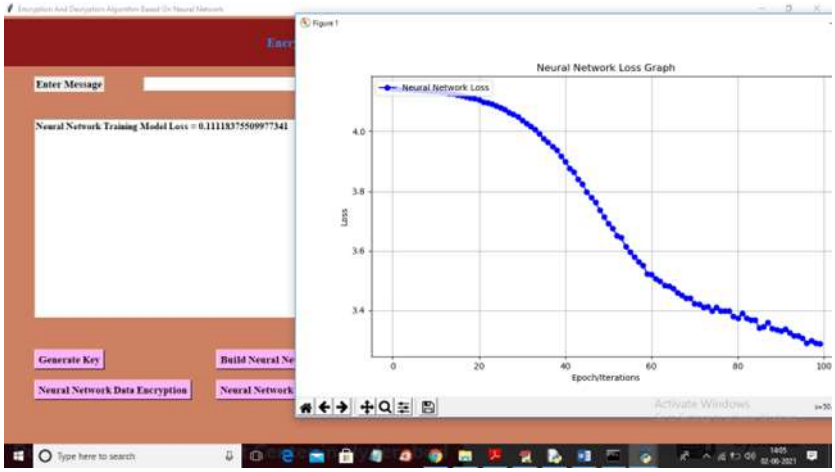

Fig 3: NEURAL NETWORK LOSS PAGE

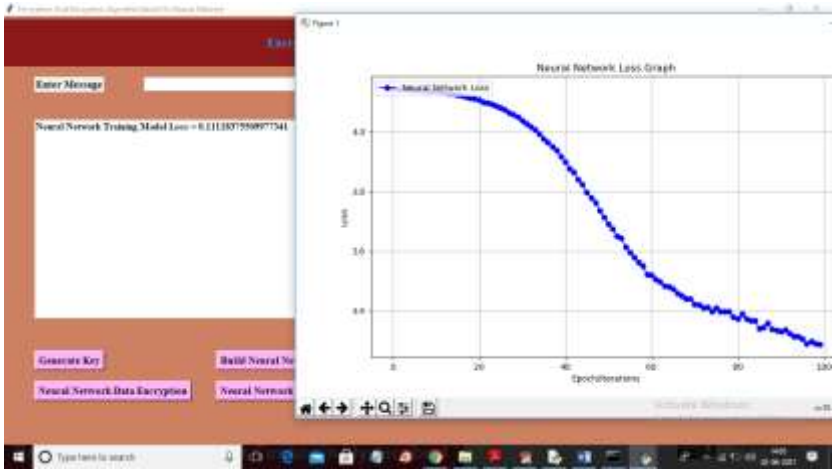

Fig 4: NEURAL ENCRYPTION OF DATA

Fig 5: NEURAL DECRYPTION OF DATA

7.CONCLUSION AND FUTURE SCOPE

The concept of using neural networks in the field of cryptography is growing at a rapid pace. Various neuro-crypto algorithms proposed by researchers are available in literature. But most of them are limited to the key generation and cryptanalysis. In the research work auto associative memory network is utilized to encrypt the plain text into the form which is totally independent from the previous one. The algorithm is pretty simple to implement and has faster encryption and decryption speed. The algorithm is following the symmetric key system which makes it vulnerable to leakage of key. To overcome this, only trusted parties should be involved in communication or a trusted third party can be used as an authority to prevent the key leakage.

The overall discussion has shown that the performance of Different classifiers were good enough in comparison to Previous studies, however, there are indeed few limitations, Such as, the dependency on a specific Feature Selection Technique, for instance more reliance on Relief in this case To produce highly accurate results. Additionally, high level Of missing values in the dataset can have an adverse effect? We have demonstrated how to address the issue through the Proper methods and therefore other dataset when used with This model, must also take care of this issue if the missing Value is quite significant. Furthermore, though our training

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.