MACHINE LEARNING BASED ENCRYPTION AND DECRYPTION USING NEURAL NETWORK

SK MEHARUNNISA, Scholar, Department of CSE, NIMRA COLLEGE OF ENGINEERING AND TECHNOLOGY, Andhra Pradesh., India.

Dr.G.MINNI, M.Tech.,Ph.D, Professor & HOD, Department of CSE, NIMRA COLLEGE OF ENGINEERING AND TECHNOLOGY, Andhra Pradesh., India.

ABSTRACT: The primary aim of data security is to protect the data during transmission. Information like financial, payment data, intellectual property, and sensitive personal information should be protected by mediators. Cryptography is a method used to transmit the data securely. Cryptography involves two techniques encryption and decryption; it basically enables to send sensitive and confidential data over the unsecure network. Cryptography is a method of protecting information and communications through the use of codes, So that only those for whom the information is intended can read and process it.

INTRODUCTION

To perform efficient searches, the cloud uses verification keys to maintain privacy protection or meet authentication requirements and provide equivalent proof of encrypted documents based on tokens.

Cryptography is derived from the Greek word kryptos which means hidden or secret. It is 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. Any organization can gain this benefit by paying or renting usage. Storage, servers and applications belong to the cloud computing area and are prerequisites for on-demand access. Therefore, unlike traditional methods of building data centers, hardware, applications and applications can be executed in a secure way before concentrating on building / transmitting business solutions. Cloud computing eliminates the need for expensive data centers and management because cloud vendors provide, manage and monitor the health and accessibility of the framework. Registering a cloud is an event on the network that allows administrators to provide versatility, quality of service (QoS) and, in most cases, to ensure custom on-demand and low-cost computing infrastructure. These infrastructures can be simple and access in a universal way. Cloud computing is a model used to authorize expedient, on-demand network admission to a public pool of configurable computing value (such as systems, servers, storage, function, or management). These resources can be managed by negligible or cloud Service-fast configuration and release The term "cloud" for vendor interaction is built from the network and its schematic representation is cloud. It refers to various specific types of services or submission that have been communicated in Internet cloud, and in many cases the devices used to get these products and applications require no special applications.

PROPOSED METHOD

Cryptographic Systems can be divided into deterministic and probabilistic encryption scheme. Deterministic encryption scheme allows the plaintext is encrypted by using keys that always provide the same ciphertext, but the encryption process is repeated many times. In this scheme, every plaintext has one to one relationship with the keys and ciphertext otherwise it will produce more than one output of particular plaintext during the decryption process. Probabilistic Encryption Scheme shows the plaintext has different ciphertext with the different keys. The probabilistic encryption scheme is significantly secure than the deterministic encryption scheme because it makes difficult for a cryptanalyst to access any sensitive information regarding plaintext that is taken from ciphertext and corresponding key. Furthermore, the cryptographic algorithms can be further divided into two main categories like keyless cryptosystem and key-based cryptosystem as shown in Fig. 1. In the keyless cryptosystem, the relationship between the plaintext and ciphertext having a different version of the message is exclusively depend on the encryption algorithm [8]. The keyless cryptosystem is generally less secure than key-based systems because anyone can gain access to the algorithm will be able to decrypt every message that was encoded using keyless cryptosystem such as Caesar cipher [9]. The key based cryptosystem can be further categories into symmetric key (secret key) encryption and asymmetric key (public key) encryption based on the type of security keys utilized for the encryption or decryption process.

LITERATURE SURVEY

MyoZaw et.al (2019) a database is a collection of organized data. Although there are various types of technologies (such as encryption and electronic signature) that can be used to protect data during cross-site transmission. Data protection refers to the common procedures used to defender safeguard data or data management software against illegal use or threats or malicious occurrences. In this article, we create 6 different ways to store and retrieve data information in a safe and efficient way in a more secure way. Discretion, integrity or accessibility (also known as three-in-one CIA) are models designed to guide information intelligence policies. There are many encryption technologies available, and ECC is one of the most powerful. Users want to store or request data, and users need to be verified. The verified user will receive the key of the main generator, and then the data must be encrypted or decrypted into database. Each key is stored in a large generator or retrieved from the key generator. Use 256-bit AES for high-level extraction, column-level theft, and component level analysis in database. The next 2 methods are to use 521-bit ECC encryption and signalling to encrypt high-level encryption or high-level encryption in the field using 256-bit AES encryption keys. The last technique is safest method in this article. This method uses AES and ECC encryption for component-level encryption to ensure confidentiality and uses ECC signatures for each component in database to ensure authenticity. In addition to translating data at interruptions, it is also significant to ensure that personal data is converted during network traffic to prevent database signatures. The advantage of the element level is difficult to attack, because attacker key will lose only one element. Loss requires thousands of keys to manage.

Learning rule for associative memory inrecurrent neural networks

We present a new learning rule for interlayer connections in neural networks. The rule is based on Hebbian learning principles and is derived from information theoretic considerations. A simple network trained using the rule is shown to have associative memory like properties. The network acts by building connections between correlated data points ,under constraints.

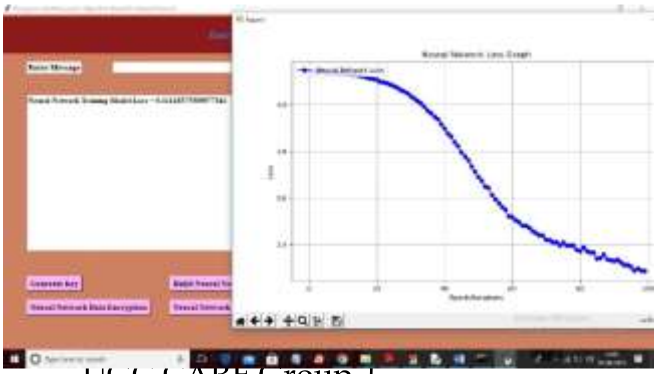
Key-insulated symmetric key cryptography and mitigating attacks against cryptographic cloud software

Software-based attacks (e.g., malware) pose a big threat to cryptographic software because they can compromise the associated cryptographic keys in their entirety. To illustrate the feasibility of key-insulated symmetric key cryptography, we also report a proof-of-concept implementation in the Kernel-based Virtual Machine (KVM) environment.

EXISTING SYSTEM

Homomorphic encryption solves security problems by storing data on third party systems (e.g., cloud or unreliable computers, service providers, etc.). The most important category of homomorphic encryption is complete homomorphic encryption. It allows unlimited operation of data in encrypted form, and the system exits cipher text space. This article provides basic information about homomorphic encryption and its various categories, namely homomorphic encryption, homomorphic encryption and full homomorphic encryption. Its main features are complete homomorphic encryption and the study of complete homomorphic encryption schemes. These tables use lattices, integers, error analysis and elliptic curve cryptography.

SCREEN SHOTS


Enter Message
Generate Key
Build Neural Network Model
Neural Network Data Encryption
Neural Network Data Decryption
Neural Network Loss Graph
Loss

CONCLUSION

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 in dependent 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.

Enter Message
Generate Key
Build Neural Network Model
Neural Network Data Encryption
Neural Network Data Decryption
Exit

Key Generation Task Completed
Generated Key : [illegible]

FUTURE SCOPE:

Lattice cryptography and other post-quantum possibilities differ from current standards in crucial ways. But they all rely on mathematical asymmetry. The security of many current cryptography systems is based on multiplication and factoring: Any computer can quickly multiply two numbers, but it could take centuries to factor a cryptographically.

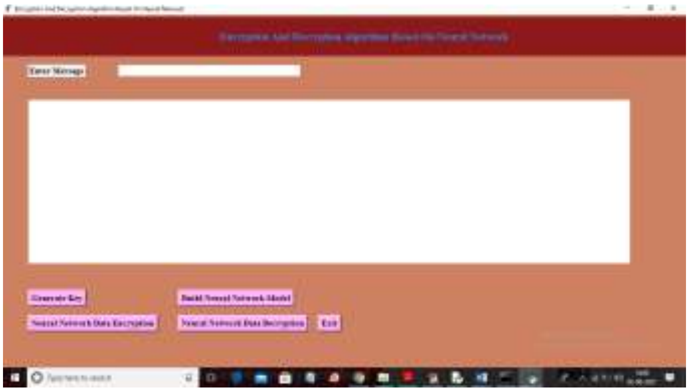
REFERENCES

[1] L.P.YeeandL.C.D.Silva.Applicationo fmultilayerper-ceptronnetworksinpublickeycryptography .ProceedingsofIJCNN02,2(Honolulu,HI, USA):1439–1443,May2002.

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

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

[4] McInnes, James L., and Benny Pinkas. "On the impossibility of private key cryptographywithweaklyrandomkeys."A dvancesinCryptologyCRYPT0'90.SpringerBerlinHeidelberg,1991.421-435.


Encryption And Decryption Algorithm Based On Neural Network
Enter Message
Generate Key
Build Neural Network Model
Neural Network Data Encryption
Neural Network Data Decryption
Exit

[5] Dodis,Yevgeniy,etal."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.

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

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

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

[9] Nakano,Kaoru."Associatron-

amodel of associative memory. "Systems, Manand Cybernetics, IEEE Transactions on 3(1972):380-388.

[10] Amari, S-I. "Neural theory of association and concept formation." Biological cybernetics26.3(1977):175-185.

[11] Wang, Guofeng, and YinhuCui. "Online tool wear monitoring based on auto associative neural network. "Journal of Intelligent Manufacturing 24.6(2013):1085-1094.

[12] 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.7,991,714.2Aug.2021.