LAUTECH Journal of Engineering and Technology 19 (1) 2025: 224-239
10.36108/laujet/5202.91.0112

An Enhanced Security Algorithm Using a Hybrid Data Encryption Technique for a Distributed Computing Environment (DCE)

[1*]Ayeni J. A., [2]Chidozie I. E, [3]Chidozie U. P. and [4]Adeniran O. T.

[1, 4]Department of Computer Sciences, Ajayi Crowther University, Oyo, Oyo State, Nigeria,
[2,3,] Department of Computer Science, Federal School of Survey. Oyo, Oyo State, Nigeria.

[1]ja.ayeni@acu.edu.ng ,[2] ifeanyievanschidozie@yahoo.com [3]promiseokoro99@gmail.com
[4]adeniranolajumoke2021@gmail.com

Article Info

Article history:

Received: Jan. 17, 2025
Revised: Apr. 08, 2025
Accepted: Apr. 10, 2025

Keywords:

Crypto, Keyword,
Cyber, Hybrid,
Neural,
Asymmetry, Symmetry

Corresponding Author:
ja.ayeni@acu.edu.ng

ABSTRACT

Cyberspace has witnessed a surge in different forms of attacks, with the user now at the losing end. The need to improve the performance of the crypto system has necessitated the urge to develop systems that are almost impenetrable to attackers and improve the level of confidentiality of data transmissions over the network, especially in Distributed Systems. A lot of research has recently been conducted on several neural net-based encryption techniques using single-layer or multilayer perceptron models. A hybrid combination of a conventional crypto system and Neural Crypto system has been discovered to be effective in curbing the incessant network data breaches. In this paper, a framework for the development of a hybrid data encryption system is presented. Some of the known techniques were analysed and the various steps for the development of the hybrid algorithm were presented. Finally, this work developed an algorithm for an enhanced crypto system with the combination of IDEA (International Data Encryption Algorithm and Artificial Feed Forward Neural Network (AFFNN) Algorithms. Performance evaluation tests indicated a higher performance level for the developed system (Hybrid) compared to the conventional system.

INTRODUCTION

Due to its revolutionary impact on the industry, distributed computing has continued to be one of the most significant developments in the computing world this century. The application of multiuser, multiprogramming, and multi-agent systems has expanded (Dominic *et al.*, 2021). A distributed computing approach shares the parts of a software system among multiple computers, or nodes. Even if the software components are spread across different computers that are situated in different locations, they function as a single system. The goal of doing this is to increase output and efficacy. The systems on different networked computers link and cooperate by sending messages to finish a given task. Distributed computing is a popular computing architecture in database and application design because it can improve performance, robustness, and scalability. Compared to monolithic computer environments, distributed systems are significantly more complicated and present some design, operation, and maintenance-related difficulties (Isak *et al.*,2021). Managing a large number of nodes in a heterogeneous or globally distributed environment creates numerous security challenges. A single weak link in a file system or larger distributed system network can expose the entire system to attack. From the above-stated risks, security in a DCE has assumed a worrisome level for organisations, especially the financial sector, where cases of internet fraud have remained at an alarming

level, and unauthorised access to sensitive data and information. Cyberspace has become one of the prominent targets for hackers and intruders. It is for this reason that an enhanced security algorithm using a hybrid data encryption technique for a Distributed Computing Environment (DCE) is being developed in this work.

LITERATURE REVIEW

Data Security and the WEB

The process of protecting digital information from unauthorized access, accidental loss, disclosure, alteration, manipulation, or corruption over its whole lifecycle—from creation to destruction—is known as data security. This approach must be used to safeguard an organization's data's availability, confidentiality, and integrity (CIA Triad).

Confidentiality is the preservation of information privacy; integrity is the assurance of information accuracy and comprehensiveness; and availability is the provision of access to authorized parties. Businesses that have any one of the three components of the CIA Rules, technologies, controls, and procedures for safeguarding data created, gathered, kept, received, and transmitted by an enterprise, are all necessary components of this kind of strategy. According to International Business Machines (IBM), data security is the process of preventing illegal access, corruption, or theft of digital information across its complete lifecycle. This idea includes all aspects of information security, such as physical security of hardware and storage devices, logical security of software programs, and administrative and access controls. It also contains the policies and processes of the company. The CIA triad serves as the foundation for a data security policy.

Types of Data Security

Researchers in this field have come up with solutions using various forms of algorithms to implement data security strategies. Some of these strategies are:

Encryption: By employing an algorithm to change regular text characters into an unintelligible format that can only be read by authorized people, encryption keys jumble data. File and database encryption solutions that use tokenization or encryption to conceal their contents safeguard sensitive volumes. Most systems additionally provide security key management functions. The CIA's "triad" encapsulates the fundamental concepts of information security. The following three information-related factors are the main emphasis of information security: Confidentiality, Integrity and Availability.

There are two types of encryption often implemented by organizations:

i. Encryption: Server-side vs. Client-side

Data security, secrecy, and integrity are the major objectives of encryption. The fact that the server-side encryption model encrypts only data stored on the server helps to distinguish it from the client-side encryption model.

ii. Encryption: Client-side

In contrast, client-side, or end-to-end, encryption encrypts user data transmission and limits the key's accessibility to the user's device. Users cannot view the conversations if not logged in, using a different device.

Data Erasure

Data erasure uses software to completely replace data on any storage device, making it more secure than standard data cleaning, proving the inability of the data recovery process.

Data Masking

By masking data, organizations can enable teams to create applications or train individuals using actual data. When necessary, it hides personally identifiable information (PII) to allow for

development in environments that comply with regulations. The objective is to protect the original data while offering a workable substitute in cases where the original data is not needed.

Data Resiliency

Resilience is the capacity of an organization to tolerate or bounce back from any kind of failure, including power outages, hardware malfunctions, and other occurrences that impact data availability (PDF, 256 KB). For instance, the cloud enables data resiliency because it allows data to be stored in multiple locations, with no location being better than the others as long as the data is not destroyed and the recovery process is simplified in the event of a location failure.

Access Control

One essential element of security is access control, which determines who can access particular files, applications, and resources and under what circumstances. Just as keys and pre-approved guest lists secure physical spaces, access control regulations do the same for digital spaces. Stated differently, they allow entry to the right persons while excluding the incorrect ones. The effectiveness of access control policies is largely dependent on methods like authorization and authentication, which allow organizations to confirm that users are who they claim to be and that their access levels are appropriate given the device, role, location, and many other contexts (Microsoft, 2023). One of the best ways to secure data, according to Sharon (2022), is to limit who has access to it.

Data Loss Prevention

Any business's security plan must include a Data Loss Prevention (DLP) system. It examines and keeps an eye out for anomalies and policy infractions in data. Data discovery, inventory, classification, and analysis of data in motion, rest, and use are just a few of its many capabilities (Sharon, 2022). Data loss can occur on any device that stores information. The permanent loss of data that is essential to the organization's continued operation is the main cause for concern, even if any loss of data or information, even a straightforward misplacement, is formally considered a loss (Menachem *et al.*, 2019).

CYBER SECURITY

Scholars and professionals in Cybersecurity have been defined in the field of data security in several novels and literary works. The International Telecommunications Union (ITU) defines cybersecurity as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets" under the CIA (confidentiality, availability, and integrity) objectives (Rossouw and Johan, 2013). Cybersecurity is defined as an activity or process that safeguards and/or defends information and systems against damage, unauthorized access, or theft by the National Initiative for Cybersecurity Careers and Studies. Protecting sensitive data and important systems from online assaults is known as Cybersecurity. Information technology (IT) security, also referred to as Cybersecurity measures, aims to stop threats to networked systems and applications, regardless of where they come from (Cains *et al.,* 2021). Cybersecurity, according to Kaspersky (2022), is the process of protecting networks, computers, servers, mobile devices, electronic systems, and data from hostile infiltration. It is frequently called electronic data security or information technology security. These definitions emphasize asset protection, but they ignore the human element of cybersecurity because they are primarily concerned with technology and

software. The goal of Cybersecurity measures, also known as information technology (IT) security, is to prevent attacks on networked systems and applications, no matter where they originate (Cains *et al.,* 2021).

Cybersecurity, according to Kaspersky in (Kaspersky, 2022), is the process of protecting networks, computers, servers, mobile devices, electronic systems, and data from hostile infiltration. It is frequently called electronic data security or information technology security. These definitions emphasize asset protection, but they ignore the human element of cybersecurity because they are primarily concerned with technology and software. As a result, practitioners and academic researchers working in the field of cybersecurity are unable to communicate effectively with one another (Cains *et al.,* 2021).

Fundamental Concepts of Cybersecurity

The outcomes of successful hacking assaults against commercially available Cybersecurity protection systems marketed as "secure" are condensed into a collection of ideas applicable to a wide range of protection planning scenarios. The ideas that explain why trust in those systems was misplaced give a framework for examining known exploits as well as evaluating suggested protective measures for identifying possible flaws (Kelce and Muge, 2014).

Overview of Types of Cybersecurity

Cybersecurity types are nothing more than methods for guarding against data theft or intrusion. Viruses and other harmful code are among the many hazards to data that affect computers and all kinds of portable devices daily. Using internet services is made easier by all of these gadgets. The purpose of these internet services is to greatly simplify end users' lives. Among these services are online shopping, online banking, and ticket booking, among others. Denial of Service (DoS), Hacking, Malware, Phishing, Spoofing, Ransomware, and Spamming are among the several forms of cyberattacks (Priya, 2022). Cybercrime is a type of organized crime focused on computers that can impact individuals who use devices connected to a network. Its primary goals are Monetary Gain and Information (stealing to sell). Hence, it is very important to protect these devices to prevent access by hackers and of course, there are tools such as anti-viruses and firewalls (Christof and Pelzi, 2010).

Cryptography

The science of secret writing to protect data privacy is known as cryptography. In contrast, the study or art of decrypting cryptosystems is known as cryptanalysis (Achivchauhan, 2023). Both terms are subcategories of the term "cryptology." "Crypto" means "secret" or "hidden," and cryptography is a crucial component of network security. Cryptography comes in two varieties: symmetric and asymmetric keys (Achivchauhan, 2023).

i. Symmetric Key Cryptography

It entails the use of a single secret key, as well as encryption and decryption methods that aid in the security of the message's contents. It is faster than asymmetric key cryptography. As the key must be sent from the sender to the recipient via a secure route, a key distribution problem develops (Priya, 2022).

ii. Asymmetric Key Cryptography

Asymmetric Key Cryptography employs both a public and a secret key is also referred to as public-key cryptography. It overcomes the key distribution problem because both sides use distinct keys for encryption/decryption. It is impractical to employ for mass message decryption since it is much slower than symmetric key cryptography.

Overview of Encryption and Encryption Algorithms

In cryptography, encryption is the process of converting plain text or information into ciphertext, which is information that only the intended recipient can decode. A cipher is the name given to the algorithm employed in the encryption process. It aids in preventing unwanted access to emails, private information, and client data. Additionally, it contributes to the security of communication networks. The data is concealed from prying eyes using encryption as depicted in Figure 1. This is the encoding method used to shield data from being viewed or altered by unauthorized parties. Data encryption's primary characteristics are (Soheila *et al*., 2015):

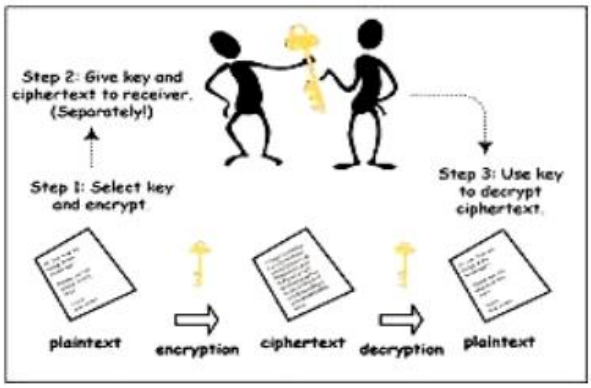

Figure 1: Schematic Representation of Cryptographic Algorithm (Soheila *et al*., 2015)

There are currently various alternatives for selecting and determining the most secure algorithm that matches our requirements. Some of the highly secure and unbreakable algorithms are (Soheila *et al*., 2015):

Triple DES

Triple DES is a block encryption algorithm designed to replace the earlier Data Encryption Standard (DES). Triple DES was created in 1956 to increase the key space without altering the algorithm after it was determined that DES's 56 key bits were insufficient to fend off brute force attacks. Despite having three 56-bit DES keys and a 168-bit key length, a meet-in-the-middle attack only provides effective protection for 112 bits. However, Triple DES suffers from sluggish software performance. Triple DES lends very easily to hardware implementation as shown in Figures 2, 3 and 4. However, AES (Advanced Encryption Standard) has proven to be more effective than Triple DES.

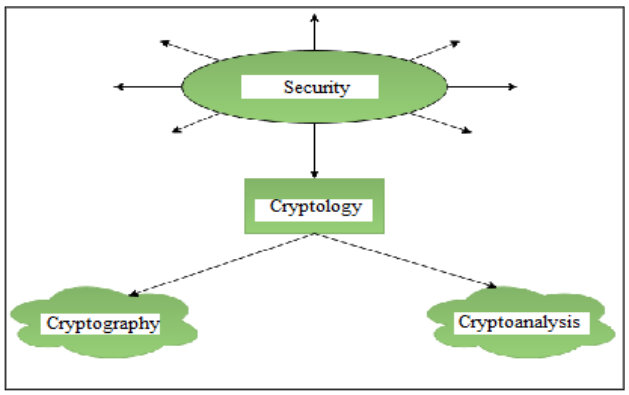

Figure 2: Depicts the Components of a Security System (Quasim, 2023)

RSA

The asymmetric key algorithm known as RSA bears the names of its creators, Rivest, Shamir, and Adleman. The method, called Prime Factorization when RSA is an asymmetric key algorithm named after its creators (Rivest, Shamir, and Adleman), is based on the fact that it is challenging to determine factors for large composite numbers.

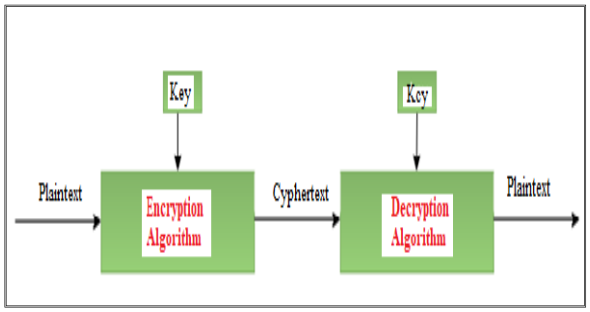

Figure 3: Symmetric Key Cryptography (Quasim, 2023).

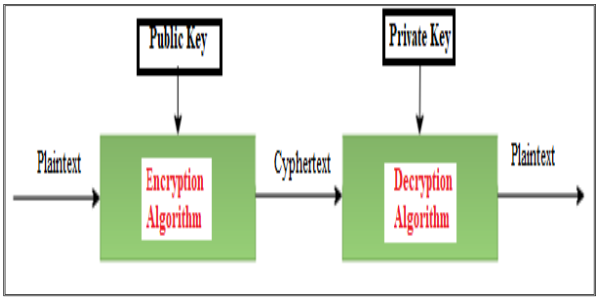

Figure 4: Asymmetric Key Cryptography. (Quasim, 2023)

The public key is used to convert plaintext to ciphertext, and the private key is used to convert ciphertext back to plaintext. The private key is kept confidential, but the public key is accessible to everyone. The private and public keys are stored separately. It is a more secure algorithm for data security as a result.

Twofish

The Blowfish method is succeeded by the Twofish algorithm. Bruce Schneier, Niels Ferguson, Chris Hall, Doug Whiting, David Wagner, and John Kesley were among those who developed it. They employ block ciphering. It is claimed to work well for both software operating on tiny processors, such as those found in smart cards, and hardware embedding. It uses a single 256-bit key. To achieve performance balance, it enables implementers to trade off encryption speed, key setup time, and code size. Twofish, created by Bruce Schneier's Counterpane Systems, is open source, unpatented, and license-free (Christof and Pelzi, 2010).

AES

The Advanced Encryption Standard, or AES, is a symmetric block cipher that is used to encrypt sensitive data from software and hardware. It was selected by the US government to safeguard sensitive data. Three 128-bit fixed block ciphers with keys of 128, 192, and 256 bits are available from AES. Key sizes are infinite, while block sizes are limited to 256 bits (Quasim, 2024). The AES algorithm uses a substitution-permutation network (SPN) rather than the Data Encryption Standard (DES) Feistel network.

IDEA

The International Data Encryption Algorithm (IDEA) is a symmetric-key block cipher that was first introduced in 1991 and is used in a wide range of applications, such as electronic voting systems, financial transactions, and secure communications. It was developed to provide safe encryption for digital data and uses a 64-bit block size and a 128-bit key size (Chritof and Pelzi, 2010). It uses a variety of mathematical techniques, including bit shifting, modular arithmetic, and exclusive OR (XOR) operations, to transform the plaintext into ciphertext. The cipher is meant to be extremely safe and impervious to several kinds of assaults, such as linear and differential cryptanalysis (Robbi *et al.*, 2017). IDEA's effective hardware and software implementation is one of its advantages. The algorithm uses very little memory and computing power and is comparatively fast. Because of this, it is frequently used in embedded devices and other applications with constrained resources (Zou *et al.*, 2008).

Overview of Artificial Neural Networks

Neural networks, sometimes referred to as Simulated Neural Networks (SNNs) or artificial neural networks (ANNs), are a branch of machine learning that serves as the basis for deep learning methods. They mimic the communication between organic neurons and are named and shaped like the human brain (Quasim, 2024). A machine learning tool called an artificial neural network (ANN), sometimes referred to as a neural network, was created to mimic the functioning of the human brain. Complex analysis techniques are needed to uncover the underlying causal relationships between one or more answers and a large collection of variables due to the data explosion in contemporary drug

development research. The increasing need for drug discovery modeling can be met by a variety of flexible approaches, including the ANN. The ANN is capable of describing intricate nonlinear relationships in contrast to conventional regression techniques. Along with being fast and extremely scalable with parallel processing, the ANN is also fault resilient (Harivans *et al.*, 2013).

3.5.1 Applications of ANN

To find a novel pattern, ANNs—nonlinear statistical models—show a complex link between inputs and outputs. Applications for artificial neural networks include medical diagnosis, machine translation, speech recognition, and picture recognition. The ability of ANN to learn from sample data sets is a major benefit. The most popular use of ANN is the approximation of random functions. With these technologies, it is possible to develop solutions that cost-effectively specify distribution. ANN can also provide an output result based on a subset of the data rather than the entire dataset. Because of their strong prediction skills, existing techniques for data analysis can be enhanced by using ANNs. Some applications that are in the proof-of-concept stage include medicine, electronic nose, security, and loan applications. Neural networks have already been employed more successfully than many humans in these applications (Debasish, 2023).

3.5.2 Artificial Neural Networks Architecture

An input layer, one or more hidden layers, and an output layer make up a node layer in an ANN. Every artificial neuron, or node, has a weight and threshold of its own and is connected to the other nodes. When a node's output reaches a specific level, it is activated and data is transferred to the network's next layer (Debasish, 2023). If this is not the case, no data is forwarded to the next tier of the network. A multitude of parameters and hyperparameters influence the performance of a neural network. These variables heavily influence the output of ANNs. Among them are weights, biases, learning rate, batch size, and other parameters. A transfer function is used to calculate the weighted sum of the inputs and the bias. The weighted sum is fed into an activation function to generate the output. Activation functions control whether or not a node fires. Only those who have been fired make it to the output layer, as shown in Figure 5. Depending on the purpose, numerous activation functions can be used. Some of the most frequently used activation functions in Artificial Neural Networks are Sigmoid, RELU, Softmax, Tanh, and others in (Debasish, 2023).

A neuron is essentially a node with multiple inputs and one output, whereas a neural network is composed of many interconnected neurons, as shown in Figure 5. To perform their functions, neural networks must first go through a 'learning phase,' during which they must learn to connect incoming and outgoing information. They then get to work, receiving input data and creating output signals based on the data that has accumulated (Harivans *et al.*, 2013).

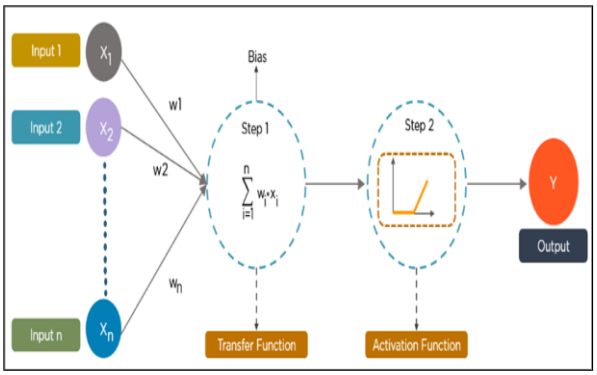

Figure 5: Diagrammatic Representation of the Architecture of ANN (Debasish, 2023)

The input node converts the information into numerical form. Each node is allocated a number, and the data signifies an activation value. The higher the number, the stronger the activation. The activation value is transmitted to the next node

based on the weights and the activation function (Bosem, 2023; Medium, 2023). Based on the transfer function (activation function), each node calculates and updates the weighted sum (Ayeni, 2022). It then goes through an activation process. This neuron alone performs this function. The neuron then decides whether or not to transmit the signal. The signal extension is dictated by the ANN's adjustment of the weights.

Feed Forward Neural Network

Artificial neural networks that do not develop loops are known as feed-forward neural networks. Because all input is simply sent forward, this sort of neural network is also known as a single-layer or multi-layer neural network. During data flow, input nodes receive data and send it to output nodes via hidden layers. There are no links in the network that may be utilized to relay information back from the output node (Turing, 2022). The following is how a feed-forward neural network approximates functions:

i. Classifiers are calculated by an algorithm employing the formula y = f* (x).

ii. As a result, input x is assigned to category y.

iii. The feed-forward model states that y = f (x).

During data flow, input nodes receive data, which travels via hidden layers and exits output nodes. There are no links in the network that may be utilized to send data back from the output node. Feed-forward neural networks serve as the basis for object detection in photos, as shown in the Google Photos app (Turing, 2022).

A gradient-based technique for training a feedforward neural network (FNN) is the back-propagation (BP) algorithm (García-Ródenas *et al.*, 2021). As a result of the simplified feedforward neural network, it appears as a single-layer perceptron. As inputs enter the layer, they are multiplied by weights. The weighted input values are then joined together to yield the sum. If the total of the values exceeds a specific threshold, which is normally set at zero, the output result is usually 1, whereas if it falls below the threshold, it is usually -1 (Turing, 2022).

ANN and Data Encryption

A crucial piece of technology for protecting data in computer systems is cryptography. It is the examination of encrypted communication channels that restricts a message's information access to the sender and the intended recipient alone (Rakhim *et al.,* 2020). Information security may be negatively impacted by cyberattacks. The importance of understanding cybersecurity is growing as the volume of data and internet traffic has both gone higher than before the advent of DS. One of the trickiest and most difficult topics for communication system development at the moment is establishing a sophisticated and reliable medium (Foo *et al.,* 2022; Marcin, 2019; Karthik *et al.,* 2019; Chen *et al.,* 2020). Chen proposed a model in (Chen *et al.,* 2020), which was analyzed in (Yang, 2009) using conventional techniques to decipher the cryptosystem's challenging secret.

Key Exchange Using ANN in Cryptography

The key exchange algorithm has numerous uses in cryptography. ANN can be used in Block Ciphers, Stream Ciphers, Bit Level, or Byte Level Encryption. The ANN approach can be utilized effectively to make the encryption process both difficult to crack and reliable. Common cryptographic attacks, such as known plain text assaults, Brute Force Attacks, and Differential assaults, may not be as simple in the context of data encryption employing Neural Networks (Arijit and Asoke, 2014). These common cryptographic attacks are:

a. **Cryptography plaintext attack:** In cryptography, plaintext is typically readable material that is normal before encryption into cyphertext or readable text after decryption, as shown in Figure 6:

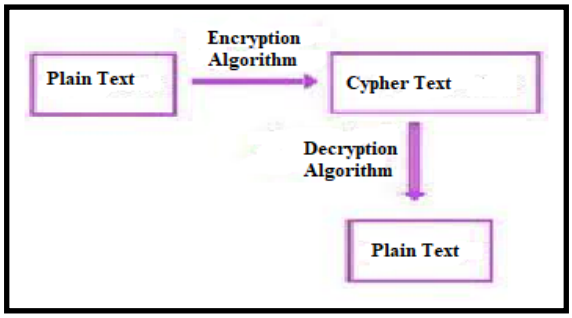

Figure 6. Schematic Representation of Plaintext Cryptography

b. A brute force attack is a type of hacking that employs trial and error to crack passwords, login credentials, and encryption keys. It is a simple yet dependable method for gaining unauthorized access to individual accounts as well as systems and networks of companies, as shown in Figure 7.

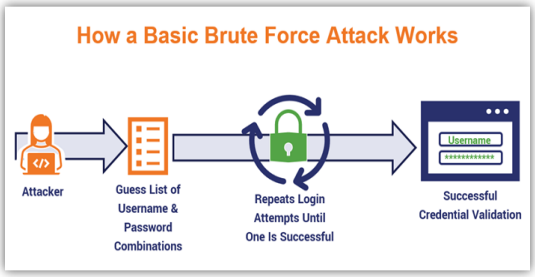

Figure 7: Schematic Representation of Brute Force attack as a type of hacking (Casey, 2021)

c. Differential assaults - To find the desired key or plaintext message, this attack compares variations in the input with variations in the encrypted output.

RELATED WORKS

Khaled *et al*. (2005) presented a Generalized Regression Neural Network (GRNN) encryption system that is fixed to the secret keys. Many training iterations were tested in the proposed system. The researchers also tested the system with different numbers of input data and hidden neurons. The obtained results were more accurate and had better performance than the traditional encryption methods.

The model is identical to the model presented by Nitin and Abhinav (2012). The demonstrated results showed that the two networks are safe and reliable, but as of now, without any results about promptitude. Murilo *et al*. (2018) protected communication with Adversarial Neural Cryptography (ANC) by using secure cryptography. The researchers showed that in the right circumstances, a perfectly secure cryptosystem can be improved and ameliorated by a neural network. In addition, the obtained results demonstrated that the original adversarial neural cryptography methodology is time-consuming to accomplish the goal. Moreover, the researchers showed a new CPA-ANC methodology (Chosen-Plaintext Attack) to enhance the function and the learned model. In the investigations, they used simple neural networks to improve and refine the learned model. The obtained results showed the dominant position of proposed CPA-ANC over the original ANC methodology, as in CPA-ANC, almost all the learned models were Neural Network-Based Cryptography: Learning perfectly secure cryptography to protect communication with Adversarial neural cryptography provided with primitive data to produce fake data. The fake data is then passed to the discriminator network. The researchers concluded that to force the solution into a formidable cryptosystem (Vasyl *et al.*, 2019), the adversary must be very strong. In this case, the standalone CPA-ANC methodology is not good enough to guarantee security (Vasyl *et al*., 2019); the key is to devise a very powerful adversarial capable of breaking cryptosystems. In their model,

the researchers showed that it was achievable. Shuying *et al*. (2022) proposed the creation of two pseudo-random sequences from a neural network and a complex network, respectively, to accomplish good encryption with high security performance. FIPS-142 and NIST tests are used to validate sequence complexity.

In the above related works presented, it could be stated that some of the weaknesses revolved around non-use of large ciphertext or keys which may increase the vulnerability level of such systems. The hybrid still involves use of key-exchange which exposes such systems to hacker's attack. Using a Neural Network-based cryptosystem with a larger number of plain-text/cipher-text pairs can reduce errors and attack to the barest minimum possible.

MATERIALS AND METHODS

The Hybrid Algorithm

In this section, the development of the hybrid encryption algorithm for a DSE with the combination of the traditional algorithm (IDEA) and feed-forward neural network (ANN) is presented. The process is split into two: The IDEA and the Artificial Feed Forward Neural Network (AFFNN) Algorithms. The goal is to achieve a fully secured data transmission system in a DSE based on two techniques;

The scenario could be explained thus: a user exchanging a file with another user from a machine using the traditional encryption program (IDEA) as depicted in Figure 8, resulting in a ciphertext depicted in Figure 8.

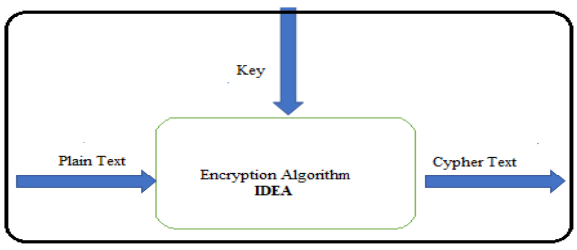

Figure 8: A traditional encryption process

The decryption of the encrypted message as (Cipher text), is depicted in Figure 9. A user communicating with another user from a machine using the FF neural network algorithm is depicted in Figure 10.

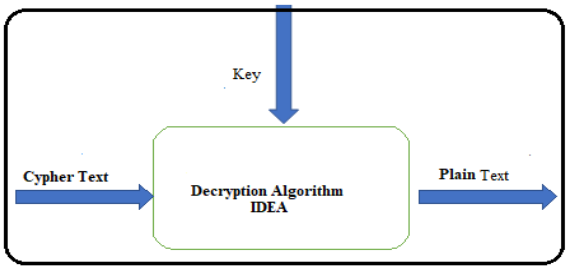

Figure 9: A traditional decryption process

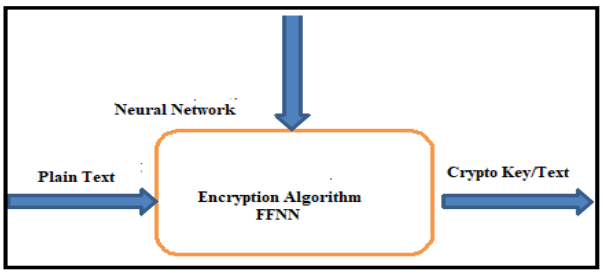

Figure 10: A Neural Network **Encryption** Process

The IDEA Encryption Algorithm

The first step entails the development of the IDEA encryption algorithm; a symmetric block cipher encryption of plain text to produce a cipher-key and ciphertext, which serves as input for the second step shown in Figure 9, decrypting to the plain text. The third step uses AFFNN to produce the key for the decryption process for the user.

The Tree Parity Machine Technique

The tree parity machine is a specific type of multi-layer feed-forward neural network. It is made up of K hidden neurons, KN input neurons, and one output neuron. The weights between the input and hidden neurons take the values from the binary inputs to the network. Each hidden neuron's output value is determined by adding up all of the input neurons' multiplications times these weights; if the scalar product is zero, the hidden neuron's output is mapped to -1 to guarantee a binary output value. The multiplication of all the values generated by the

hidden elements is the neural network's output. The system begins at synchronization, at which point each of the parties, A and B, utilizes a separate tree parity machine. The tree parity machines (Users A and B) are synchronized, as seen in Figure 11. Both tree parity machines' weights can be used as encryption or decryption keys by A and B once complete synchronization has been reached (Saswan, 2012). The algorithm is shown in Algorithms 1 and 2.

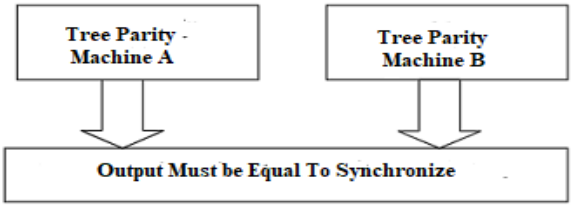

Figure 11. Two Tree parity machines (Saswan, 2012)

Algorithm 1: The Steps to Create Cyber Text and Cyber Key – IDEA

Set Array [64K] for the input text of 16 bits;
Init an array for the input text
Until End of Text; Loop
Set the length of key to 32 bits
(divide into 8 blocks of 4 bits each)
; key 32-bit length
Divide the Array into chunks of 4 bits each.
encrypts the chunks in 4 chunks of 4 bits each
; encryption
Algo_Encrypt (Nval) ; Call Function
Bitwise XOR: logical operation
Addition modulo (2^4)
Multiplication modulo (2^4) +1
End Inner Loop; Function encryption
set loop-count (4) each to produce 16 bits cyphertext
Update Key += Cypher-key
End Loop
Return Cypher, Key;
The returned key is passed to the FF function

Algorithm 2: The Feed Forward Neural Network (Multi-Layer)

The Input values from the **IDEA** function of **Algorithm 1**
Weight (W_i) values are randomly initialized
Until the full synchronization
RandomX:= Input vector X.
Func (Values hidden neurons)
Func (Values output neuron)
If TPM (1) equals TPM (2)
Repeat
else
Return (CypherKey = Value)
End.

The Techniques

Numerous types of cryptographic techniques are available for use. They all offer secure data transmission across network channels, guarantee authentication and confidentiality, and each has a different topology. The physical layer and security layer of the computer program must use all of these end-to-end encryption and decryption algorithms. Simultaneously, particular IP configurations and the protocol to be utilized for traffic transmission must be taken into account.

A. The Encryption Process involves User A sending a message of size (N) to User B to be encrypted. (example: file*size = 250KB*). The Hybrid algorithm processes the message; The IDEA generates the key and forwards it to the Feed Forward Neural Network (ANN) algorithm for processing. The FFNN generates an output that represents the new Key (unbreakable) between User A and User B, as shown in Figure 12. The final output text now contains the final Key to be sent to User B. The second phase is the decryption process by IDEA.

B. The Decryption Process

This process starts from the Crypto-Text using the key generated by the FFNN (ANN) between User B and User A to generate the Cypher-Text passed over to the IDEA algorithm of the developed system.

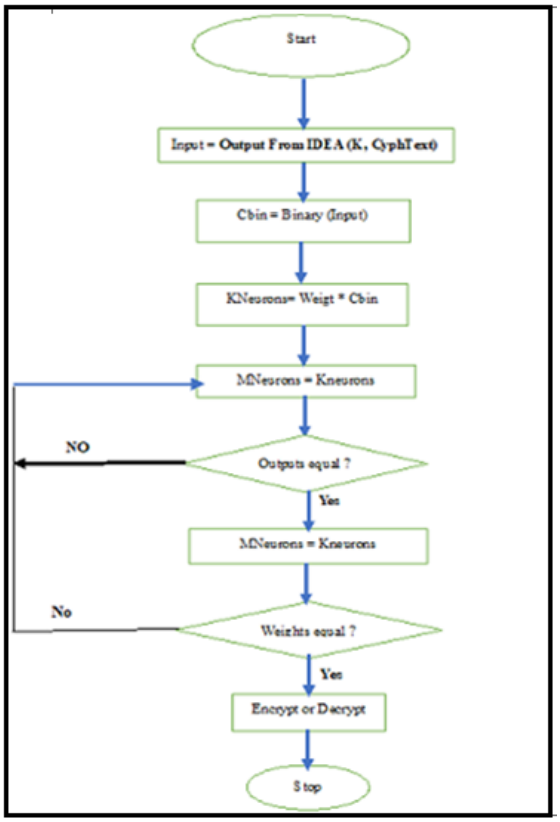

Figure 12: The flowchart of the Feed-Forward algorithm

PERFORMANCE EVALUATION METRICS

The performance metrics are encryption, Decryption time and throughput. Throughput = Sizeof (Plaintext) (KB) / Encryption time (msec.). Encryption algorithms have been experimented with using different data sizes. The steps are:

i. Encryption time – The amount of CPU time needed to convert plain text into a ciphertext is called the encryption time. (**eCT**) and measured in milliseconds.

ii. Decryption time - This is the amount of CPU time needed to extract plaintext from encrypted data (**dCT**) measured in milliseconds.

iii. Throughput - The throughput (**ThP**) of the encrypted algorithm is the total encrypted plaintext in kilobytes divided by the encryption time in milliseconds. This is also referred to as the encryption rate.

EXPERIMENTAL TEST AND RESULTS

i. Performance Test 1

There is no known Dataset for this type of research, as it has to do with the Cryptography of plain text exchange between users. Files of varying sizes were dynamically generated, i.e., (256, 800, 1024, 2054, 3078, 5032, and 8110 KB), and inputted into the developed Hybrid system and Conventional Non-Hybrid (IDEA) with the results harvested into a table as shown in Table 1. The comparative analysis of the results was carried out using the required metrics. The encryption time was plotted against the files of varying sizes as shown in Figure 13.

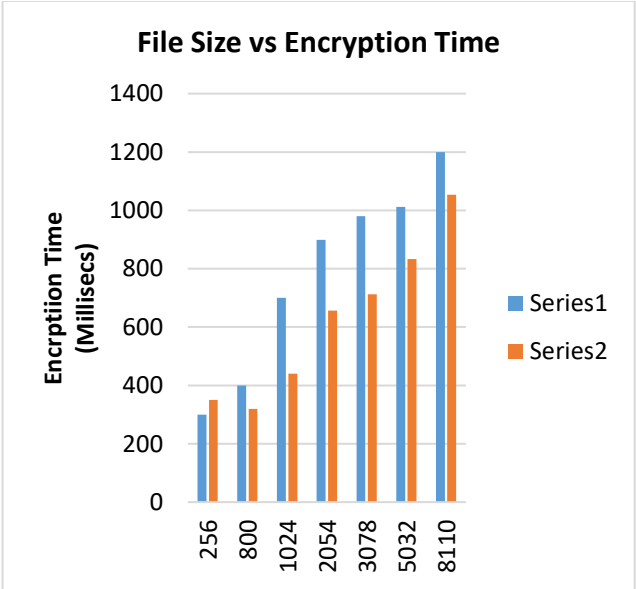

Figure 13: File Size Vs Encryption Time

ii. Performance Test 2.

The decrypted file is a binary file type, the result is the time taken to take it back to its original form (Plain-Text)

RESULTS

Table 1: Encryption Time (IDEA/Developed System)

File Size (KB)	IDEA (Msec)	DevSystem (Msec)
256	300	350
800	400	320
1024	700	440
2054	899	656
3078	980	712
5032	1012	833
8110	1200	1054

Table 2: Decryption Time (IDEA/Developed System)

File Size (KB)	IDEA (Msec)	DevSystem (Msec)
256	250	220
800	350	250
1024	500	340
2054	690	456
3078	780	602
5032	982	633
8110	1050	754

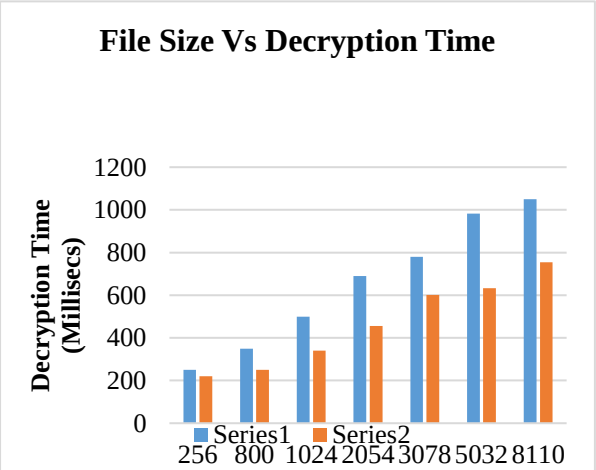

Figure 14: File Size Vs Decryption Time

DISCUSSION

The encryption Time plotted against the IDEA and the developed system indicated a higher performance level for the developed system compared to the conventional IDEA encryption algorithm, as shown in Figure 13. The first pass gave the advantage of the CPU time involved in the learning process of the FFNN (ANN) algorithm to the IDEA; thereafter, the subsequent passes removed the advantage from the IDEA and became more in processing the data. It could also be asserted that whereas the size of the file increases, the CPU time usage also increases with the conventional algorithm, while it decreases with the developed system.

The decryption Time of the IDEA and the developed system indicated a higher performance level for the developed system compared to the conventional IDEA decryption algorithm, as demonstrated in the result of the experiment. It is known that the Key for the decryption algorithm had already been generated and therefore put into use immediately. Therefore, it could also be asserted that whereas the size of the file increases, the CPU time usage also decreases with both algorithms, but considerably with the developed system.

The Throughput was computed as follows:

a. IDEA:

Total sum of File Size processed = 20354 (KB)

Total Processed Time = 5491 (Milliseconds)

ThP is: = 3.706793

b. Developed System

Total sum of File Size processed = 20354 (KB)

Total Processed Time = 4365 (Milliseconds)

ThP is = 4.663001 (Millisecs)

The Throughput of the developed system has a greater advantage over the conventional algorithm.

CONCLUSION

A Hybrid algorithm with the combination of the traditional IDEA encryption algorithm and Feed Forward Neural Network has been developed and presented. Based on the results of the performance analysis, the Hybrid system has demonstrated a higher performance level compared to the conventional algorithm (IDEA) because of the

combination and enhancement with the FFNN (algorithm).

REFERENCES

Ajit Rossouw von S. and Johan van N. (2013). From information security to cybersecurity. ELSEVIER. Science Direct. https://www. sciencedirect.com/science/article

Arijit G. and Asoke N. (2014). Cryptography Algorithms using Artificial Neural Network 2(11), November 2014. International Journal of Advanced Research in Computer Science and Management Studies

Ayeni J. A. (2022). Convolutional Neural Network (CNN): The architecture and applications. December 2022 Applied Journal of Physical Science 4(4):42-50 DOI: 10.31248/AJPS2022.085

Bosem A. (2023). https://editor.analyticsvidhya.com/uploads/94912bosem.png

Cains, M.G., Liberty F., Danica T., and Diane S H. (2021). Defining Cybersecurity and Cybersecurity Risk within a Multidisciplinary Context using Expert Elicitation. Available from: https://www.researchgate.net/publication/349347158_Defining_Cyber_Security_and_Cyber_Security_Risk_within_a_Multidisciplinary_Context_using_Expert_Elicitation [accessed Jul 26 2023].

Casey C. (2021). A Brute Force Attack Definition & Look at How Brute Force Works Available at: https://www.thesslstore.com/blog/brute-force-attack-definition-how-brute-force-works/ (Accessed 27 Jan 2024)

Chen L., Boyan P., Wenwen G. and Yuanqian L. (2020). "Plaintext attack on joint transform correlation encryption system by convolutional neural network", The School of Science, Hangzhou Dianzi University, Hangzhou Zhejiang 310018, China, 2020. Doi:https://doi.org/10.1364/OE.402958

Christof P. and Jan P. (2010). Understanding Cryptography: A Textbook for Students and Practitioners. Springer Edition. eBook.

Deb D., Kalita (2023). An Overview and Applications of Artificial Neural Networks https://www.analyticsvidhya.com/blog/2022/03/an-overview-and-applications-of-artificial-neural-networks-ann

Dominic L., Sukhpal G., Daria S. and Peter G. (2021). The evolution of distributed computing systems: from fundamental to new frontiers. Computing 103, 1859–1878 (2021). https://doi.org/10.1007/s00607-020-00900-y

Foo J. and Ng K.W. and Naveen P. (2022). Neural Network-Based Cryptography: A Primary Study on the Performances and Techniques. 10.2991/978-94-6463-094-7_6.. Proceedings of the International Conference on Computer, Information Technology and Intelligent Computing (CITIC 2022) (pp.68-78)

García-Ródenas, R., Linares, L.J. and López-Gómez, J.A. (2021). Memetic algorithms for training feedforward neural networks: an approach based on gravitational search algorithm. Neural Comput & Applic 33, 2561–2588. https://doi.org/10.1007/s00521-020-05131-y

Hariv Harivans P. S. , Shailendra M. and Shailendra M. (2013). Secure-International Data Encryption Algorithm. https://www.researchgate.net/publication/344299908_Secure/International_Data_Encryption_Algorithm/citations[Accessed 23 June 2024]

Isak S., Endrit M., Blend B. and Tonit B. (2021). Design of Modern Distributed Systems based on Microservices Architecture. International Journal of Advanced Computer Science and Applications. Vol. 12, No. 2, 2021 pgs. 153-159

Jiyun Y., Xiaofeng L., Wenwu Y., Kwok-wo W. and Jun W. (2009) "Cryptanalysis of a cryptographic scheme based on delayed chaotic neural networks", Choas, Solitons & Fractals, 40(2), 821–825, 2009. Doi: https://doi.org/10.1016/j.chaos.2007.08.029

Karthik N., Nalini R., Sharath P. and Shai H. (2019). "Towards Deep Neural Network Training on Encrypted Data". DOI: https://doi.org/10.1109/CVPRW.2019.00011

Kaspersky, E. (2022). Cybersecurity 101: The Fundamentals of Today's Threat Landscape Available at: https://media.kaspersky.com/us/pdf/cybersecurity101_ebook.pdf

Kelce W. and Muge A. K. (2014). Some Fundamental Cybersecurity Concepts https://www.researchgate.netpublication/260523812_Some_Fundamental_Cybersecurity_Concepts

Khaled M.G. N. and Hamid A. J. (2005). "Data Security Based on Neural Network", Task Quarterly 9.4 (2005): 409–414

Marcin N., (2019). "Error correction in quantum cryptography based on artificial neural networks", Quantum Information Processing (2019) 18:174, 2019

Medium (2023). https://editor.analyticsvidhya.com/uploads/49298learncplusplus.png

Menachem D., Sujata J. and Pandey R. (2019). Risk Mitigation Model for Data Loss: A Case Study Approach. Journal of Advanced Research in Dynamical and Control Systems. Available from:https://www.researchgate.net/publication/36254733_

Microsoft (2023). Access Control. https://www.microsoft.com/en-us/security business -Security-101/what-is-access-control

Murilo. C., Robson de Oliveira A., Fabio B., Luis J. G. V. and Tai H. (2018), " Learning perfectly secure cryptography to protect communication with Adversarial neural cryptography", MPBI, sensors 2018. DOI:https://doi.org/10.3390/s18051306

Nitin S. and Abhinav T. (2012). "An Empirical Investigation of Using ANN Based N-State Sequential Machine and Chaotic Neural Network in the Field of Cryptography", Global Journal of Computer Science and Technology Neural & Artificial Intelligence, Vol. 12, Issue.10, No 1,17–26, 2012

Priya P. (2022). Types of Cybersecurity. https://www.Educba.com/types-of-cyber--security/

Quasim M.H. (2024). Introduction to cryptography. In book: Computer Security, Al-Kunooze University College PublicationsAchivchauhan

Rakhim S. N.and Natalia V. S. (2020). "Application of the Neural Networks for Cryptographic Information Security", DOI: https://doi.org/10.1109/ITQMIS51053.2020.9322981

Risk_Mitigation_Model_for_Data_Loss_A_Case_Study_Aproach [accessed Jul 24 2023]

Robbi R. M., Mesran, M. S. and Andysah S. P. (2017). Data Security with International Data Encryption Algorithm. Journal Online Jaringan COT POLIPD(JOJAPS).

https://www.researchgate.net/publication/320519469_Data_Security_with_International_Data_Encryption_Algorithm

Sawsan S. A. (2012), Cryptography using artificial neural networks. Available from: https://www.researchgate.net/publication/346423923_cryptography_using_artificial_neural_network [accessed Feb 09, 2024].

Sharon, S. (2022). What is data security? The ultimate guide https://www.techtarget.com/searchsecurity/Data-security-guide-Everything-you-need to-know

Shuying W., Ling H. and Jun J. (2022). An image encryption scheme using a chaotic neural network and a network with multistable hyperchaos. Elsevier. https://www.sciencedirect.com/science/article/pii/S0030402622010336

Soheila O. A., Faroog, M. and .Amin B.. A. (2015). Comparison of Various Encryption Algorithms and Techniques for Improving Secure Data Communication. IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 1, Ver. III (Jan – Feb. 2015), PP 62-69 www.iosrjournals.org

Turing A. (2022). Understanding Feed Forward Neural Networks with Maths and Statistics.https://www.turing.com/kb /https://www.turing.com/kb/mathematical-formulation-of-feed-forward-neural-network

Vasyl Lytvyn, Roman Peleshchak, Ivan Paleshchak, Victoria Vysotska, "Information Encryption Based on the Synthesis of a Neural Network and AES Algorithm", 2019. DOI: https://doi.org/10.1109/AIACT.2019.8847896

Zou, J., Han, Y. and So, S.S. (2008). Overview of Artificial Neural Networks. In: Livingstone, D.J. (eds) Artificial Neural Networks. Methods in Molecular Biology™, vol 458. Humana Press. https://doi.org/10.1007/978-1-60327-101-1_2Humana Press. https://doi.org/10.1007/978-1-60327-101-1_2