Medical Image Cryptanalysis using Adaptive, Lightweight Neural Network based Algorithm for IoT based Secured Cloud Storage

M V Narayana, Ch Subba Lakshmi, Rishi Sayal
Guru Nanak Institutions Technical Campus
Hyderabad, India

***Abstract*—Currently available modern medical system generates large amounts of data, such as computerized patient data and digital medical pictures, which must be kept securely for future reference. Existing storage technologies are not capable of storing large amounts of data efficiently. It is a key and abrogating topic of specialized, social, and medical significance and a key and abrogating subject of general interest. The results of cars, purchasers, and Internet of Things industry-based and essential segments, sensors, and other daily objects are fused with a network of the Internet and solid information abilities that promise to alter the way we operate and live future. The suggested work demonstrates a symmetric-key lightweight technique for secure data transmission of images and text, which uses an image encryption system and a reversible data hiding system to demonstrate the program's implementation. On the other hand, cloud storage services can meet demand due to features such as flexibility and availability. Cloud computing is enabled by amazing internet innovation as well as cutting-edge electrical equipment. Even though medical images may be stored on the cloud, most cloud service providers only save client data in plain text. As part of their overall strategy, cloud users must take responsibility for protecting medical data. Because attackers' increasing computing power and creativity are opening up more and more areas in this mathematical form, most existing image encryption schemes are vulnerable to the plaintext attack of choice. This article presents an image encryption method inspired by an Adaptive IoT-based Hopfield Neural Network (AIHNN) that can resist other assaults while optimizing and improving the system through continuous learning and updating.**

***Keywords*—Cloud storage; IoT; medical image; neural network**

I. Introduction

There have been enormous improvements in Information Technology (IT) and analytics during the last several years. Cloud computing is one kind of technology that many businesses use for the hosting of their apps and data storage. Modern gadgets, which allow for digitalized data exchange, have established a new standard for transmitting information globally, regardless of the application. The information is shared with the public. There is a concern about the level of privacy and security that should be provided for people and confidential material [14]. Information sharing across different companies, particularly medical imaging system users, has increased in recent years, resulting in novel storage methods such as cloud edge [1]. Many online services, such as e-commerce, telemedicine, electronic payment access, and social networking sites are hosted on the cloud.

Storage as a Service (SAS) is by far the most frequently demanded service according to most Internet of Things (IoT) devices [2], and computing has reached a pinnacle in recent years. Data security in cloud storage is a joint responsibility of customers and service providers. Thus, issues related to medical data privacy, in particular, must be successfully handled via the use of suitable cryptographic standards. It is essential for patient safety to be able to offer information security for a medical image stored in a public and shared system such as the cloud. According to the cloud data security debate, cloud service providers are focusing on security measures for cloud infrastructure, hosts, and data. User data, on the other hand, is only accessible as plain text up to a certain point in time.

To address this issue, it is suggested that data be encrypted and stored utilizing encryption methods. The authors proposed a fully homomorphic encryption (FHE) technique to encrypt photos in cloud storage in order to guarantee image security, even for small-scale images, while the complexity increased even for small-scale images [13]. There are many encryption methods available, and they may be used to encode the text, images, and audio. Despite this, the security measure used for text transmission less performs when used for image transmission due to the intrinsic characteristics of images, including such mass data capacity, also has and strong association among the pixel data; as a result, a separate security system is presented by each type of multimedia data protection. Image security becomes more critical due to the difficulties in managing pictures as contrasted to text documents. As a bonus, pictures are used to convey the context of the majority of critical applications such as telemedicine and education and biometric verification and identification. Chaos-based picture encryption methods [9] have gained popularity due to their increased vital strength, which is achieved via key sensitivity. That perhaps the key has an actual value is the reason for the importance of the turmoil. According to chaos theory, the nature of chaos is entirely dependent on the original seeds.

According to cryptanalysts, chaos-based cryptographic protocols, on the other hand, are not resistant to the chosen plaintext attack. On the other hand, most contemporary cryptographic methods are susceptible to cryptanalysis, in which the attackers undermine the cryptosystem by using

known-plaintext and chosen-plaintext assaulting strategies. The reverse exclusive-OR procedure has been integrated into picture encryption because of its advantages, including reversibility and the ability to cause bitwise confusion. It is also possible to construct a stream cipher using this method. It does, however, allow for cryptanalysis via the use of a specific plaintext attack. In this paper, the homomorphic encryption method is discussed as superior encryption technology, emphasizing cloud data security. On the other hand, the homomorphic encryption method is susceptible to cryptanalysis, wherein security keys may be recovered with less than 8s [19].

According to the initial study, most current schemes are vulnerable to plaintext attacks because of their daily use of simple XOR-based propagation and continuous operation rounds. The number of activities may enhance the complexity, but the change in processing time is unneeded, resulting in a low throughput rate. The encryption method must be complicated to avoid cryptanalysis, particularly the selected plaintext attack, and that it is irreversible, self-adaptive, and parameter aware. As previously stated, neural-based encryption methods are the preferred option for meeting the criteria. An artificial neural network (ANN) is a set of predictive classification networks capable of performing multiple classifications and optimization operations in parallel while still including essential components known as neurons. Because of the self-learning and adaptable character of ANN, it may be used in conjunction with traditional methods to provide correct results. Furthermore, ANN may learn about its environment by using real-time and training data. As a consequence, neural networks are being used in a variety of applications, including data protection, predictive analytics, medical data classification, and civil structure analysis [6][7], with data security being the focus of this study.

A. Artificial Neural Networks and Cloud Computing

Artificial neurons should have been able to replicate the activity of actual neurons, according to the basic principle. As a result, it is characterized by erratic behavior. Because of the security concerns, cryptography applications [12] are attracted to the chaotic activity of neurons. According to the research, the ANN model may be expanded to describe complex reversible encoders as well. ANN may also be used in combination with a non-traditional image encryption technique. The ANN may be thought of as a nonlinear encoder that might replace the traditional diffusion method. Random indexes, in addition to dispersion, are needed to achieve the appropriate degree of confusion. To produce random indices, the neural network must also show recurrent activity, which is inevitable in the generation of pseudo-random sequences for picture encryption applications.

As a result, the recurring as a major component of this paper's proposed neural blended adaptive image encryption system, an adaptive IoT-based Hopfield neural network (ANN) is presented (NBAIE). The Adaptive IoT-based Hopfield neural network is an influence exerted based on human brain features [3]. It is a one-of-a-kind neural network model that is based on human mind features. It has a time-dependent behavior. In many respects, it varies from previous neural architectures. Other neural networks are ideally suited for classification and grouping tasks and other activities since they are made up of distinct hidden units that process the inputs.

In contrast, recurrent AIHNN contains hidden units that are linked. Time-dependent behavior is achieved by activating one of the hidden units at a certain point in time. It is helpful in applications dependent on the sequence of consecutive occurrences, like pseudo-random sequence generation, where the sequence of succeeding occurrences is essential. The following are the key differentiators of the algorithm suggested:

Because of its BPN's multi-layered architectural design and nonlinear activation device weight matrix, predicting the key is reduced.

Because distinguishing features of the image are used as input for the BPN, and the generated keys are much more highly adaptable to the input plain image than the primary image itself.

- Keys' behavior may be varied due to BPN's ability to self-learn.
- Because of its recurrent and chaotic behavior, AIHNN necessitates the use of crucial seeds which are similar to chaos, which is favourable to linear neural architectures including such BAM and BPN because the preliminary essential seed is larger in scale (size is much larger than basic image), reducing communication rate [20].
- Establishing a link between the authorized user and the public cloud computing environment Each image has its own key. As a consequence, unauthorized people will not be able to attack the image and key using a specific plaintext attack.
- Image specific pseudo-sequence creation, followed by dynamic ambiguity and diffusion, to achieve the desired effect.
- Medical picture repositories on the cloud may now have enhanced privacy protection.
- The weight matrix of the AIHNN may be modified for each picture, resulting in the creation of image-specific pseudo sequences using the algorithm.

As a result, the algorithm's prediction becomes more complicated due to the use of an Adaptive IoT-based Hopfield neural network, which is implemented in this scheme [16].

Further, this work is furnished such as in Section – II, describes about Internet of Things are discussed, in Section – III, the parallel research outcomes are analyzed and discussed for finding the bottlenecks of the current applications, in the Section – IV, the identified drawbacks and the proposed solutions are presented using The Proposed Adaptive Iot-Based Hopfield Neural Network (AIHNN), based on the mathematical models, the proposed algorithms are furnished and discussed, the obtained results from these two novel algorithms are furnished and realized, in the Section – V, and in the Section – VI, the final research conclusion is presented.

II. The Internet of Things (IoT)

The Internet of Things (IoT) is expected to provide social and financial benefits to emerging and developing countries soon. Incorporating Blockchain technology addresses supported agriculture, water quality utilization, human services, and ventures managing condition, among other things [5]. The Internet of Things (IoT) also promises to become a means of achieving the Sustainable Development Goals of the United Nations. It is not new for developed countries to be confronted with the enormous scope of Internet of Things problems [10]. The benefits of the Internet of Things must also be considered by the municipalities that are developing them.

More requirements and challenges in putting this concept into action in less-developed areas must be addressed, such as frameworks, marketplace. Enterprise motivating factors, specialist skills, and approach resources, among other things, because the connections between things, the environment, and the general public are becoming more dynamic [4]. The Internet of Things today ensures that we will live in a progressive, fully connected, dazzling world]. However, the tests and concerns regarding the Internet of Things should be examined. Moreover, it should be addressed to determine the possible benefits to individuals, communities, and businesses [17]. Finally, increasing the benefits of the Internet of Things while simultaneously reducing the security risks cannot be achieved by engaging in an unending debate that pits the affirmation of the Internet of Things against its flaws. It will pledge dedication and collaboration throughout the partner meetings to provide the most acceptable ways to the public in the future. The use of Internet of Things segments prompted a slew of legal questions and gave rise to previously unaddressed legal problems relating to the Internet of Things. The inquiries are massive in scope, and the rapid evolution of IoT technology concerns the ability of the associated approach, legal framework, and regulatory zones to be changed. In this group of problems, one would be the information stream which occurs when IoT devices collect information about people within their purview and transmit it to a different location with different data security rules to advance the treatment of the information. Another issue is that the data collected by IoT devices are susceptible to misuse, which results in unsatisfactory outcomes for the customers [11]. Other legal problems associated with the Internet of Things devices include disagreements between law enforcement agencies and standards-setting organizations, information pulverization, and legal obligations for non-required uses, security, and protection concerns. The Internet of Things is now accessible because we have information internet associations, which allows us to access it. The development of information and internet association may be traced back through history and across time. The time information is sent to the Internet facilitates the efficient delivery of information to the Internet. After that, the following section provides a brief historical overview of the information era [18-24].

This study aims to develop and evaluate lightweight and asymmetric block cipher-based cryptosystems that are suitable with MANET, IoT, and wireless communication devices to achieve data security while also maintaining quality control. The following are some possible discussion points on the work's goal. Prepare a design and simulation of a data security system that incorporates a block cipher, image processing, and reversible data concealing. To develop standard protocols that is interoperable with WSN, MANET, and the Internet of Things. Understanding and implementing the mathematical modeling of cryptographic algorithms is essential for success.

III. Parallel Works

When it comes to security, a lightweight authentication model for the Internet of Things (IoT) provides a high degree of protection against various assaults such as impersonation attacks, man-in-the-middle attacks, and unknown key sharing attacks in the E-health domain. Based on IoT-based E-health apps, the author proposed a safe, lightweight authentication method that is easy to implement. The suggested approach, based on the Internet of Things, offers authentication, an energy-efficient system, and computing for healthcare. Elliptic curve cryptography (ECC) is a concept that defines the characteristics of the suggested model, in addition to the individuals who offer healthcare and the patients. In general, the author's motivation is to design a lightweight security scheme based on ECC principles for E-health applications based on the IoT (IoT) [8. The author devised an authentication method based on the minor key, which offers a high degree of security for the system. They also developed a high-performance, lightweight security scheme for E-health applications based on the Internet of Things. The proposed security model is based on the RSA cryptographic algorithm. The algorithm for public-key cryptography is most widely used. In communication stacks, it is used to offer UDP/IPv6 networking to use less power and energy [8].

In [15], a protocol for robust and secure authentication in the Internet of Things systems was suggested to be efficient and safe. In order to ensure security, the proposed protocol uses a physical function that cannot be copied. The proposed protocol protects various attacks while being highly efficient in memory, computations, energy, and communication. An Internet of Things (IoT) mutual authentication mechanism was described by the author. The system is based on PUFs, which use a challenge-response mechanism to send authentication information [15]. Because the protocol offers secure authentication and creates a session key without the need for it, an IoT device does not need to store anything. The author demonstrated that the proposed protocol is highly efficient and provides security against a variety of attacks, including physical attacks, side-channel attacks, and cloning attacks, among others. One of the most important requirements for Internet-of-Things (IoT) systems is security while using as few resources as feasible. Because IoT devices are low-cost and simple, they are a great target for physical, side-channel, and cloning threats, among others. To solve the same issue, the developer developed an effective protocol for mutual authentication for Internet of Things devices.

IV. Proposed Adaptive IoT-based Hopfield Neural Network (AIHNN)

AIHNN features metastable states that are triggered by external input and a previously selected state. The chaotic behavior is provided by an ANN that is constructed with a minimal number of nodes, chosen node connections, and a

suitable asymmetric weighted route. The proposed work will be utilized for the AIHNN, which consists of eight nodes. It features an AIHNN architecture with eight nodes, and each node may be connected to any other node and any external input sources. It also has a link to itself. The starting state of the input nodes and external input, as well as other variables, influence the output of each node. The weighted route links every node in the network to every other node. As demonstrated in the previous section, Fig. 1 depicts a recurrent AIHNN that has been rebuilt into a chaotic architecture with eight nodes.

Each node in chaotic design is considered as an input/output node, resulting in a faster generation of the pseudo-random sequence than in traditional architecture. As a result, it is said to be an instance of hyperchaotic architecture. Because each node in this design is not connected to every other node and weights are modified using the Hebb rule in combination with the hyperbolic activation function, this architecture has several distinguishing features. Furthermore, AIHNN has been designed with a certain number of nodes and an appropriate asymmetric weighted path to produce the desired chaotic behavior in a controlled setting.

$$W_{ij} = \begin{bmatrix} \begin{bmatrix} w_{11} & w_{12} & w_{13} & w_{14} & w_{15} & w_{16} & w_{17} & w_{18} \\ w_{21} & w_{22} & w_{23} & w_{24} & w_{25} & w_{26} & w_{27} & w_{28} \\ w_{31} & w_{32} & w_{33} & w_{34} & w_{35} & w_{36} & w_{37} & w_{38} \\ w_{41} & w_{42} & w_{43} & w_{44} & w_{45} & w_{46} & w_{47} & w_{48} \end{bmatrix} \\ \begin{bmatrix} w_{51} & w_{52} & w_{53} & w_{54} & w_{55} & w_{56} & w_{57} & w_{58} \\ w_{61} & w_{62} & w_{63} & w_{64} & w_{65} & w_{66} & w_{67} & w_{68} \\ w_{71} & w_{72} & w_{73} & w_{74} & w_{75} & w_{76} & w_{77} & w_{78} \\ w_{81} & w_{82} & w_{83} & w_{84} & w_{85} & w_{86} & w_{87} & w_{88} \end{bmatrix} \end{bmatrix} \quad (1)$$

$$w_{ij} = \begin{cases} \sum_{m=1}^{M} d_i^m d_j^m & \text{if } i \neq j \\ 0 & \text{otherwise} \end{cases} \quad (2)$$

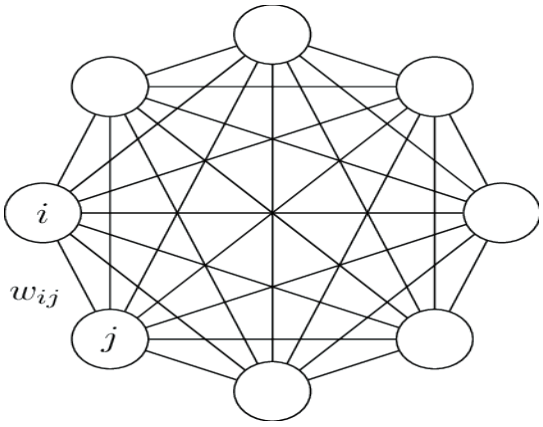

Fig. 1. Architecture of Hyperchaotic AIHNN with Eight Nodes.

Given that the selected Adaptive IoT-based Hopfield neural network has eight nodes, the weight matrix dimension is 8x8, equivalent to W11–W88 in the preceding example. The weight values in Equation 2 relate to the neural network strength acquired during training, which influences the accuracy of the produced result (rate of closeness among required and received output). The weight values are either integers or floating decimal numbers, depending on the activation function (identity or hyperbolic activation function). The following equation (2) and the following equation (3) are used to incrementally update each node (3). Each node in the preceding equation (2) receives a weighted signal from the other nodes, as well as external input and information from other nodes (Xi). The adjusted sigmoid transfer function is then computed using the revised Xi as shown in the equation:

- The architecture depicted in Fig. 1 produces cyclic random sequences by deriving the following equations: (2) and (3), where Cmax is the steady and Max.
- Cmax is the initial state.
- Wij is the mass function in both.

$$M_{\max} = \frac{n}{2\log(n)} \quad (3)$$

$$C_{\max} = \frac{n^2}{2\log(n)} \quad (4)$$

$$Q = \frac{n(n-1)}{2}\log_2(P) \quad (5)$$

Adoptive IoT based Hopfield Neural Network $(AIHNN)$

$$P_{\max} = M_{\max} + 1 \; and \; then$$

$$Q_{\max} = \frac{n(n-1)}{2}\log_2\left(M_{\max}+1\right) \quad (6)$$

This leads to:

$$\eta = \frac{n}{(n-1)\log(n)\log_2\left(\frac{n}{\log(n)}+1\right)}n \quad (7)$$

$$\approx \frac{1}{\log(n)\log_2\left(\frac{n}{\log(n)}\right)}n \quad (8)$$

V. Experimental Results and Discussion

Visual information that is not medical is referred to as Image data (I), and it serves as a carrier of Critical Medical Information (CMI). As shown in Fig. 2, a Secret Key (SK) is utilized by the Steganographic embedding function (SFE) to conceal CMI, and Stego data (SD) is produced as an output (by the device at the transmitting end DT).

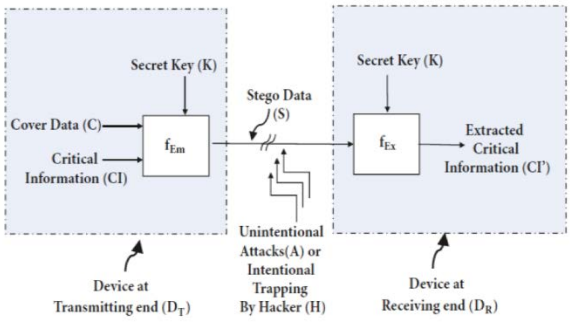

Fig. 2. Steps Involved in Reversible Hiding Algorithm.

The Steganographic extraction function (SFE) extracts CI using the precise Secret Key (K) provided by the user (as a device at receiving end DR). The stego data is CI is Extracted Critical Information, and the secrete key is the secrete key. Fig. 3 depicts a generalized hardware Steganographic data concealing device that is used in the industry. Crypto xStegoSystem is the name given to the proposed reversible data concealing system, intended for use in the implementation of a data hiding system and comprises cryptographic and Steganographic methods. The suggested approach is shown in the Fig. 3.

The central idea of the investigation may be broken down into the many shown in Fig. 3.

1) Ensure that low-complexity symmetrical key encryption is implemented on various platforms (JPEG-2000, JPEG, BMP, PNG, GIF).

2) Evaluation of the performance of the simulated method on user-defined and real-time imagery.

3) An investigation of incorrect key encryption.

4) Design and development of the Graphical User Interface for the proposed system.

5) An evaluation of the suggested system's execution time and memory allocation is performed.

6) The development of a reversible data-hiding system for picture and text multiple encryptions is underway.

7) Evaluation of the suggested system's AIHNN and MSE results as shown in Fig. 4 and Table I.

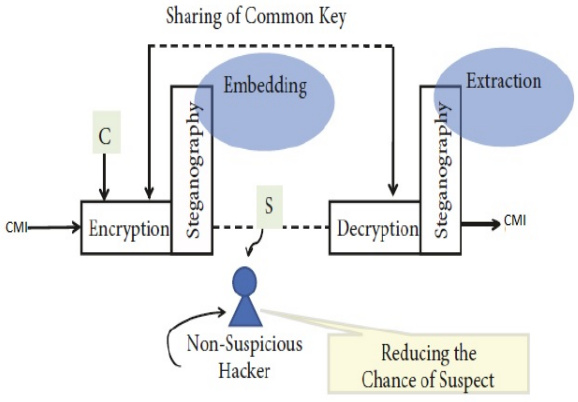

Fig. 3. Phases in Key Sharing in AIHNN Algorithm.

Algorithm 1: The overall process is explained as follows: -

1. Validate CI and store it in the Message Cache
2. Accept the LOOK-UP Table as an Embedding Key in Step 2. (K)
3. Parse the cover data in 8-byte chunks (C)
4. Compute the DWT of the first 8bytes of the cover data
5. Select a byte(Ym) at random from the Message Cache.
6. It was chosen using 3LSBs of the contents of the selected byte LOOK-UP Table.
7. Insert the chosen bit at DWT coefficient C3 to complete the operation.
8. Compute IDWT of 8bytes of cover data in order to get Stego information.
9. Repeat steps three within 8 for all of the bits in the Message Cache and all of the characters.

TABLE I. AIHNN ENCRYPTION AND DECRYPTION MSE

Type of Medical Image	ANN	MSE
BMP	70.543	0.0242
GIF	66.231	0.0242
JPEG	67.001	0.0231
JPEG-2000	71.643	0.0176
PNG	68.332	0.0209

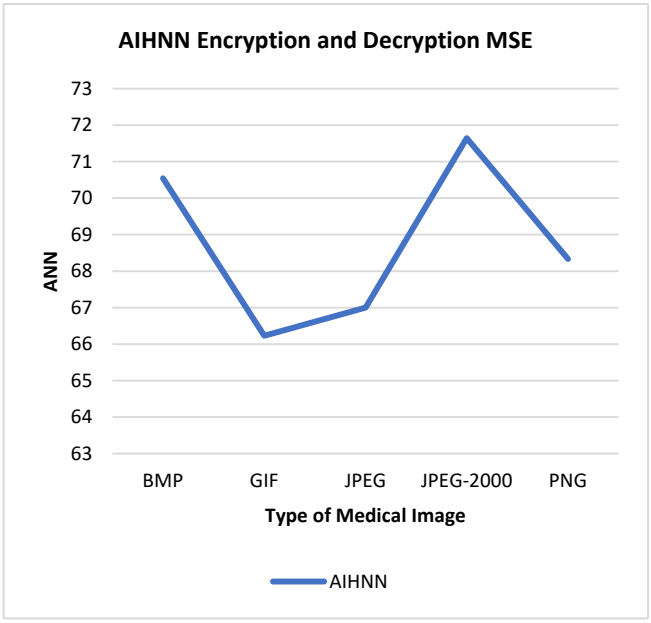

Fig. 4. AIHNN Encryption and Decryption MSE.

The method presented here is to create chaotic sequences using AIHNN rather than nonlinear equations that show chaotic behavior. The image-specific key is treated as a control parameter, and the bit of color is produced using the pseudo-code shown in Algorithm 2. Followed by the tested images and its testing results mentioned in Fig. 5, Fig. 6, Fig. 7 and Table II.

Algorithm -2: Random sequence generation using AIHNN and image specific key

Input: Multiplicative identity matrix (B) _(8×8), Sampling rate T_w, Random initiator h_(1×8)

Output: Nonlinear random sequence Ω

Step 1. Initialize

$$w_{ij} \leftarrow \left[\frac{w\ w}{2\sigma} - w; \Psi 2w3w0; 3w\phi w0; MW\ w \quad 0 \quad 0 \quad nw\right]$$
$$\leftarrow [1 \quad 0.5 \quad -5 \quad -1 \quad ; -0.37$$

Step 2. $2 \quad 3 \quad 0 \quad ; 3 \quad -13 \quad 1 \quad 0 \quad ; 100 \quad 0 \quad 0 \quad 1$

Update the w_{ij} with new σ, Ψ, ϕ

Get H(0) ← [h]^T

Step 3. For i.j 11 to do

$$f(H(r)) = \tanh H(r)$$
$$\mathrm{H}(r+1) = (1 - \mathrm{B}T_w)\mathrm{H}(r) + T_w w f(\mathrm{H}(r))$$
$$\mathrm{Dh} = |(\mathrm{H}(\mathrm{r}+1) - |\mathrm{H}(\mathrm{r}+1)|)|$$

Step 4. Until $\mathrm{r} \leq$ (Image size / 4) Initialize $\Omega \leftarrow \{\}$ for $\mathrm{f} \leftarrow 1$ to 16384

Step 5. for $\mathrm{i} \leftarrow 1$ to 4 $\Omega((4 \times (\mathrm{f} = 1)) + \mathrm{i}) = \mathrm{Dh(i)}$

Step 6. End

Step 7. End

Step 8. Return Ω

The encrypted medical image has also been stored in public cloud storage, and only authorized customers will be forced to access the clouds to get a ciphered image. The main image may only be accessed using the private key(s) that were assigned to it.

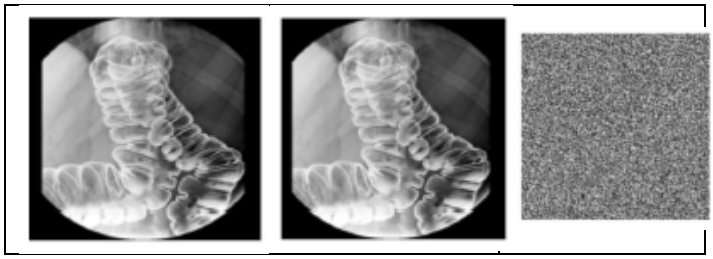

Fig. 5. Medical: (i) A Plain Image (Img); (ii) an Encrypted Image (EImg = E(Img); (iii) A Decrypted Picture (Img = D(EImg)).

In order to arrive at exclusive encrypted pictures for each medical image, the proposed AIHNN system changes the weight matrix for each medical image. The adaptive encoding aspect of the proposed work has resulted in an average entropy of 8.11, independent of the original medical pictures used in the analysis.

Healthcare terminology:

Keys are important to the functioning of encryption systems, and key sensitivity analysis is a helpful tool for evaluating the robustness of encryption methods. Analysis of key sensitivities. For the most part, encryption techniques utilise the same key for each image transmission. The proposed approach, on the other hand, offers an independent and adjustable key for each image based on image attributes. When the key is in double data type, it is feasible to reflect even minor changes in the image's properties.

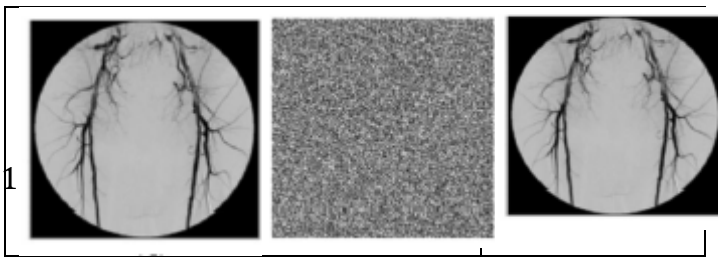

Fig. 6. (iv) Plain (MImg); (v) Encrypted (EImg = E(MImg); (vi) Decrypted (MImg = D(EImg)).

TABLE II. TEST IMAGES WITH ENTROPY

Test images	Global Entropy		Local entropy
	Original image	Encrypted image	No. of blocks =50 Block size: 88*88 Encrypted image
MI1	4.5	8.1245	8.1106
MI2	5	8.1263	8.1112
MI3	6.3	8.1272	8.1118
MI4	6.5	8.1287	8.1124
MI5	7.4	8.13005	8.1131
MI6	8.13	8.1314	8.1136
MI7	8.86	8.13275	8.1142
MI8	9.59	8.1341	8.1148
MI9	10.32	8.13545	8.1154
MI10	11.00	8.1368	8.1163

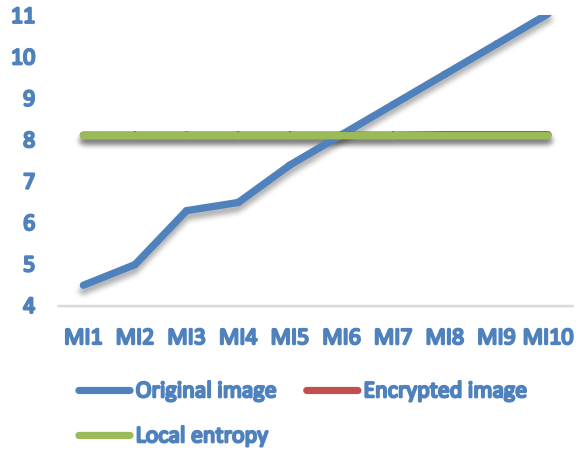

Fig. 7. Test Images with Entropy.

VI. CONCLUSION

The consolidation of computers, sensors, and systems to pass the report on and control devices have been around for a long time, but as significant technological and business trends advance, the "Internet of Things" is experiencing a new

phenomenon known as the "Internet of Things." A progressive, fully linked world is promised by the Internet of Things, connecting different things and their surroundings and between articles and people becoming increasingly securely connected over time. On a basic level, it has the potential to alter how people perceive what it means to be "on the web." Even the potential is significant, and there are many obstacles to overcome – primarily in the areas of security and protection, interoperability and scales, legal problems, and human rights issues, including emerging economies. Consequently, it is necessary to recognize and address its problems while maximizing its benefits and minimizing its risks. Answers for enhancing the optimal use of IoT while also minimizing the risks cannot be found by being involved in a heated debate that pits the benefits of IoT against the concerns of cybersecurity.

There are numerous obstacles to overcome when it comes to the Internet of Things, including intensity, data transmission capacity, flexibility, security, and protection. Predefined security arrangements at each tier are nevertheless vulnerable to security-related attacks, even though they have been strengthened. Because of their openness and multi-tenancy, cloud storage systems are susceptible to a wide range of security vulnerabilities. This suggested solution provides data security for data saved in cloud storage and data in various states such as underuse, rest, and transit, among others. Creating a secure medical picture archive on the cloud is the driving force behind this project. It is crucial to highlight that the Hopfield attractor is an important component of the surveillance system for medical images stored in the cloud, and its fitness is also validated using standard metrics. The proposed research utilized a Hopfield attractor to confuse pixels, followed by diffusion, and the findings demonstrated that the system was resistant to additional attacks.

REFERENCES

[1] Asadi S, Nilashi M, Husin ARC, Yadegaridehkordi E (2017) Customers perspectives on adoption of cloud computing in the banking sector. Inf Technol Manag 18:305–330.

[2] Dana Halabi, Salam Hamdan, “Enhance the security in smart home applications based on IoT-CoAP protocol.

[3] Domer B, Fest E, Lalit V, Smith IFC (2003) Combining dynamic relaxation method with artificial neural networks to enhance simulation of tensegrity structures. J Struct Eng 129:672–681. https://doi.org/10.1061/(ASCE)0733-9445(2003)129:5(672).

[4] Himanshu Gupta, GarimaVarshney, “A Security Framework for IoT devices against wireless threats, second international conference on telecommunication and networks, 2017.

[5] Jin HyeongJeon, Ki-Hyung Kim, "Blockchain-based data security-enhanced IOT server platform, IEEE ICOIN, 2018.

[6] Kohonen T (1988) An introduction to neural computing. Neural Netw 1:3–16. https://doi.org/10.1016/0893-6080(88)90020-2.

[7] Maria Almulhim, Noor Zaman, “Proposing secure and the lightweight authentication scheme for IoT based E-health applications” International conference on advance communication technology; 2018.

[8] Mourad Talbi and Med Salim Bouhlel, “Application of a Lightweight Encryption Algorithm to a Quantized Speech Image for Secure IoT”, Preprints.org; 2018. DOI: 10.20944/preprints201802.0096.v1.

[9] Muhammad NaveedAman, KeeChaing Chua, "A lightweight mutual authentication protocol for IOT system, 2017.

[10] MuhammetZekeriyaGunduz, Resul Das, “A comparison of cyber security-oriented testbeds for IOT based smart grids, IEEE 2016.

[11] Nithya C, Pethururaj C, Thenmozhi K, Amirtharajan R (2020) An advanced framework for highly secure and cloud-based storage of colour images. IET Image Process. https://doi.org/10.1049/iet-ipr. 2018.5654.

[12] Qin K (2017) On chaotic neural network design: a new framework. Neural Process Lett 45:243–261. https://doi.org/10.1007/ s11063-016-9525-y.

[13] Qin Z, Weng J, Cui Y, Ren K (2018) Privacy-preserving image processing in the cloud. IEEE Cloud Comput 5:48–57. https://doi. org/10.1109/MCC.2018.111121403.

[14] Shahzadi S, Iqbal M, Dagiuklas T, Qayyum ZU (2017) Multiaccess edge computing: open issues, challenges and future perspectives. J Cloud Comput. https://doi.org/10.1186/s13677-017- 0097-9.

[15] Singh A, Chatterjee K (2017) Cloud security issues and challenges: a survey. J Netw Comput Appl 79:88–115. https://doi.org/ 10.1016/j.jnca.2016.11.027.

[16] Tang H, Li H, Yan R (2010) Memory dynamics in attractor networks with saliency weights. Neural Comput 22:1899–1926. https://doi.org/10.1162/neco.2010.07-09-1050.

[17] Tao M, Ota K, Dong M (2017) Ontology-based data semantic management and application in IoT- and cloud-enabled Smart homes. Future Gener Comput Syst 76:528–539. https://doi.org/ 10.1016/j.future.2016.11.012.

[18] Dr. Ranga Swamy Sirisati, M Vishnu Vardhana Rao, S Dilli Babu, Dr. M.V.Narayana, “An Energy effecient PSO based Cloud Scheduling Strategy”, Lecture Notes in Networks and Systems book series (LNNS, volume 171) Springer, Singapore, Print ISBN 978-981-33-4542-3, Online ISBN 978-981-33-4543-0, DOI: https://doi.org/10.1007/978-981-33-4543-0_79, - pp: 749-760.

[19] Thomas Maurin, Laurent, George Caraiman, "IoT security assessment through the interfaces P-SCAN test bench platform, 2018 EDAA.

[20] Yu W, Cao J (2006) Cryptography based on delayed chaotic neural networks. Phys Lett Sect A Gen At Solid State Phys 356:333–338. https://doi.org/10.1016/j.physleta.2006.03.069.

[21] U Shivanna, NiladriShekar Dey, K Purnachand, M V Narayana, Govardhana Rao I, “A Comparative Study of Famous Image Compression Methods Based on Bits per Pixel: A Survey”, Journal Of Critical Reviews, VOL 7, ISSUE 18, 2020, pp.1094-1104, ISSN-2394-5125.

[22] M V Narayana, “Compression, Encryption, Watermarking & Steganography (CEWS) Technique for Image Steganography” International Journal of Latest Engineering and Management Research (IJLEMR), Volume 3, Issue 3, PP. 20-27, (March, 2018), e-ISSN: 2455-4847– UGC Indexed Journal- 48163.

[23] M V Narayana, U Shivanna “A Review on Region of Interest (ROI) based compression Techniques for Medical Images” International Journal of Management, Technology And Engineering, Volume 7, Issue IV, APRIL/2017 PP 51-56. ISSN NO : 2249-7455 (UGC Approved Journal).

[24] M V Narayana, U Shivanna “Local Features Based Image Matching Using Sift Algorithm” International Journal of Research, Volume 5, Issue 2, 2016 PP 51-55. ISSN NO : 2236-6124 (UGC Approved Journal).