JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

BES-256: A Hybrid Cryptographic Algorithm for secure ECG data transmission and classification using CNN.

Dr.S.Rajesh,
S.A.Aashish, R. Abishek Kanna, P. Ashwath
Department of Information Technology
Mepco Schlenk Engineering College
Sivakasi, Tamilnadu.

Abstract **- The proposed system suggests using cryptographic algorithms as an efficient means of access control in healthcare systems based on the Internet of Medical Things. One such algorithm is Blowfish, which generates a key value, and elliptic curve digital signature algorithm is used to encrypt the Blowfish key value. The resulting encrypted output is sent to the secure hash algorithm (SHA256) for a hashing process based on the cipher value, which enhances data integrity. By using high-security algorithms, confidentiality and availability are ensured, which protects sensitive information from implantable devices and strengthens healthcare systems by improving their services. The proposed scheme is shown to be more secure against various known attacks, such as router attacks, sensor attacks, and denial of service attacks. Through comprehensive experimental analysis and simulation results, it is clear that this proposed system has better resistance protocols for ensuring the safety of patients. In addition to that we use machine learning algorithms to detect the condition of the heart and also predicts the type of heart diseases if exists. Real time ECG data are collected with the help of AD8232 sensor and Arduino kit and is further encrypted and transmitted over a cloud server and ML Algorithms like CNN are performed over the decrypted data to classify the ECG data. The final report is shown to the patient as well as the doctor.**

I. INTRODUCTION

Internet of Things (IoT) offers with the mixture of both logical and bodily connection to web with the enhancement of present and new wi-fi applied sciences [1]. The special traits of IoT systems, such as dynamic, self-configuration, interoperability, self-adapting, and integration into facts networks, have made IoT collaborate with different clever applied sciences like synthetic intelligence, cloud com-putting, and Big information with IoT [2]. The first-rate advantages of IoT and its conceivable real-time purposes are predominantly in want for human usages in several domains such as industrial automation systems, clever domestic appliances, clever employer systems, clever fitness care systems, clever surveillance system, clever agricultural systems, clever surroundings recovery, and safety system.

Internet of Medical Things (IoMT) technological know-how approves the enhancement of provider satisfactory for patients, clinicians, pharmaceutical, and biomedical companies in a steady go with the flow to enhance efficiency, provider capability, and flexibility amongst clever de-vices. While these can reveal and observe their physique parameters on the structures they are linked to. The accumulated records can be dispatched to an administration unit/decision guide gadget to be processed in addition [5]. The filtered processing facts can then be used to allow the device to function self-action barring the want for human intervention.

The majority of superior computing functionalities assist tune the statistics from gadgets or transferring the important points safely to the scientific database. The normal computing methods are now and again of greater dangers in the case of attaching implantable sensors in the human physique [6]. Various assaults go in opposition to these implantable sensors. Because these sensors tune very touchy records and shop the small print immediately in the scientific database or the structures precise storage system [7], [8].

The phrase cryptography offers with safety and privacy problems in most real-time application. For example, trying out the photograph record with the patient' scientific facts is pretty straight-forward. Hence, forging would be viable by means of searching at it. Thus, unique clinical important points get faked very without problems [9], [10]. As we cross on to the digital world, this receives way tougher due to the fact in the digital world altering something is pretty convenient by means of intranet and IoT devices. To forestall the assaults from accomplishing implantable clinical devices, robust protection is enabled to grant confidentiality, integrity, and availability [11], [12].

II. RELATED WORK

The utilization of the Secure Hash Algorithm (SHA) in the proposed encryption scheme allows for the precise mapping of the seed key to the initial value of the chaotic system. This enhances the security of the encryption system by reducing the key space, making it more difficult for attackers to decrypt the data. It is worth noting that some encryption schemes use a single key to encrypt multiple images, which goes against the one-time pad strategy. However, this issue is addressed by the proposed Feedback Iterative Piece-Wise Linear Chaotic Mapping approach, which ensures that each image is encrypted using a unique key. (Sun & Chen, 2022) [1].

Public-key encryption with search functionality (PKE-SF) is a popular cryptographic approach that enables users to search encrypted data without requiring decryption. PKE-SF typically involves the use of primitives such as public-key encryption with keyword search (PKE-KS), public-key encryption with equality test

(PKE-ET), and plaintext-checkable encryption (PCE). Due to the vast array of PKE-SF schemes available, this survey provides a comprehensive analysis of these schemes from multiple perspectives to aid beginners and advanced researchers in gaining a better understanding of this complex area of study. (Xiong et al., 2022) [2].

An efficient RC6 HEVC PE technique that enables the secure encryption of sensitive video data bits while incurring minimal computational overhead. This technique is ideal for real-time applications as it enables fast encoding times and keeps a fixed HEVC bit rate. The proposed RC6 HEVC PE approach achieves these benefits by using the low computational complexity RC6 block cipher for encrypting selective video bins. Specifically, the RC6 HEVC PE encrypts the sign bit of the discrete cosine transform (DCT) coefficients, the suffixes of the remaining absolute values of DCT that are binarized using Exp-Gloom (EGk) order zero, the sign bits of motion vector difference (MVD), and the suffixes of MVD absolute values that are binarized using EGk order one. This approach offers an effective solution for video encryption that balances both security and computational efficiency. (Sallam et al., 2018) [3].

A novel approach for encrypting and decrypting medical images using a deep-learning-based image encryption and decryption network (DeepEDN). DeepEDN employs a cycle-generative adversarial network (Cycle-GAN) as the primary learning network to transform the medical image from its original domain to a target domain. (“DeepEDN: A Deep-Learning-Based Image Encryption and Decryption Network ...”) The target domain serves as the "hidden factors" that guide the learning model for achieving encryption. The encrypted image is then reconstructed using a reconstruction network to restore it to its original (plaintext) form, thus enabling image decryption. This approach offers a robust and effective solution for the encryption and decryption of medical images, which is critical for keeping patient privacy and confidentiality. (Ding et al., 2021) [4].

To evaluate the effectiveness of pseudorandom number generators (PRNGs), they must pass a set of statistical tests established by the National Institute of Standards and Technology (NIST). The NIST also advocates for the generation of random numbers using advanced encryption standard and triple data encryption standard algorithms with the counter mode of operation. However, it is worth noting that various block cipher algorithms (BCAs) and alternatives may produce even stronger PRNGs than those recommended by the NIST. Therefore, it is essential to carefully consider and evaluate the available options to select the most suitable PRNG for specific applications. (Aljohani et al., 2019) [5].

A novel technique for elliptic curve cryptography (ECC) that uses efficiently computable endomorphisms to enhance its performance and reduce computational overhead. This approach is particularly well-suited for hardware implementations, making it a perfect fit for Internet of Things (IoT) applications. The authors supply empirical evidence of the efficacy of their approach by implementing the ECC algorithm on an FPGA device and evaluating its performance. The outcomes show that the proposed method yields significant improvements in speed and power efficiency compared to traditional ECC methods, making it an attractive option for resource constrained IoT devices that require secure communication protocols. (Liu et al., 2017) [6].

III. PROPOSED HYBRID BES-256 MODEL

Encryption is one of the most important needs in healthcare as it helps in protecting the privacy of the patients. Encryption of patient data protects patient’s privacy by making the data unreadable to unauthorized individuals. In order to achieve this, the proposed system uses a hybrid encryption model which combines major cryptographic algorithms like Blowfish, ECDSA and SHA-256.

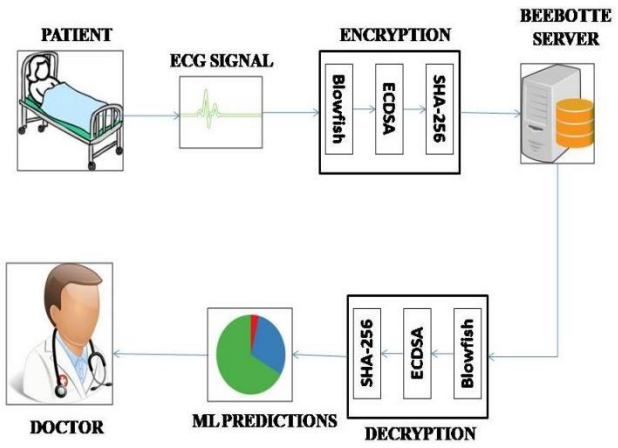

Fig.1. System Design

The System collects the patient’s real time data from the ECG sensor (AD-8232) and the data is encrypted using the proposed hybrid model.

At first key is generated using Blowfish algorithm and the key is encrypted along with the input data

A. BLOWFISH ALGORITHM

Blowfish is a symmetric-key block cipher which is widely used in applications such as secure communications, password protection, and digital signatures. The algorithm operates on 64-bit blocks of data and uses a variable-length key, which can range from 32 bits to 448 bits. The key is used to generate a series of subkeys, which are then used in a series of 16 rounds to encrypt the data.

ALGORITHM:

A. Key Expansion:

The key expansion process generates a series of subkeys from the user-supplied key. The key is first padded with null bytes to a multiple of 8 bytes, and then divided into 32-bit words. The subkeys are generated by applying the Blowfish encryption process to the initial state with the key schedule. The key schedule consists of 18 32-bit words, which are initialized using a constant hexadecimal value and the digits of pi.

The key expansion process is defined as follows:

1. Divide the key into 32-bit words.
2. Initialize the P-array and S-boxes with a fixed string and the digits of pi.
3. XOR each 32-bit word of the key with a corresponding word in the P-array

4. Repeatedly apply the Blowfish encryption process to the initial state with the key schedule to generate 18 32-bit subkeys.

B. Encryption:

The encryption process takes a 64-bit block of plaintext and transforms it into a 64-bit block of ciphertext. The plaintext is divided into two 32-bit halves, which are then transformed through a series of 16 rounds. Each round uses a 32-bit subkey generated during the key expansion phase.

The encryption process is defined as follows:

1. Divide the plaintext into two 32-bit halves, left and right.
2. Repeat the following process 16 times:
3. Apply the F function to the right half using the current subkey.
4. XOR the result with the left half
5. Swap the left and right halves.
6. XOR the final left and right halves with the 17th and 18th subkeys, respectively, to generate the cipher text.

The F function used in each round is defined as follows:

F(x) = ((S1[x >> 24] + S2[x >> 16 & 0xff]) XOR S3[x >> 8 & 0xff]) + S4[x & 0xff]

where:

x is a 32-bit input value

S1, S2, S3, and S4 are 32-bit substitution boxes, which are initialized during the key expansion phase.

The symbol >> represents a bitwise right shift and & represents a bitwise AND operation. The F function applies a series of substitution, permutation, modular addition, and XOR operations to the input value using the substitution boxes.

C. Decryption:

The decryption process is the reverse of the encryption process and also uses the 18 subkeys generated during the key expansion phase. The cipher text is divided into two 32-bit halves, which are then transformed through a series of 16 rounds. Each round uses a 32-bit subkey in reverse order.

The decryption process is defined as follows:

1. Divide the ciphertext into two 32-bit halves, left and right.
2. XOR the final left and right halves with the 17th and 18th subkeys, respectively
3. Repeat the following process 16 times:
4. Swap the left and right halves.
5. Apply the F function to the right half using the current subkey in reverse order.
6. XOR the result with the left half
7. Combine the final left and right halves to generate the plaintext.

Blowfish has several advantages over DES, including a larger key size, faster encryption and decryption, and a simpler algorithm. Overall, Blowfish is a widely used and respected encryption algorithm that provides a high level of security for a wide range of applications.

B. SHA-256

The SHA-256 (Secure Hash Algorithm 256-bit) is a cryptographic hash function that is widely utilized for its ability to generate a fixed-size output of 256 bits, irrespective of input size. It is known for its robust collision resistance and pre-image resistance, making it a popular choice for digital signatures, password storage, and data verification. This implies that it is computationally infeasible to find two distinct input messages that produce the same output hash value, or to find an input message that produces a given hash value, or to find two input messages that produce the same hash value. These properties make SHA-256 a suitable choice for various security applications.

ALGORITHM:

1. Pre-processing:

a. Given a message m of length L bits, append a single 1 bit to the end of the message.

b. Append k 0 bits, where k is the smallest non-negative integer such that L + 1 + k + 64 is a multiple of 512.

c. Append a 64-bit representation of the original message length in bits, with the most significant bit first.

2. Initialize hash values:

a. The initial hash values H0 to H7 are the first 32 bits of the fractional parts of the square roots of the first eight prime numbers, in hexadecimal notation:

H0 = 0x6a09e667

H1 = 0xbb67ae85

H2 = 0x3c6ef372

H3 = 0xa54ff53a

H4 = 0x510e527f

H5 = 0x9b05688c

H6 = 0x1f83d9ab

H7 = 0x5be0cd19

3. Process the message in 512-bit blocks:

a. Divide the message into 512-bit blocks M(1), M(2), ..., M(N).

b. For each block, perform the following operations:

i. Create a message schedule W(0), W(1), ..., W(63) from the block.

ii. Initialize working variables a, b, c, d, e, f, g, h to the current hash values H0 to H7.

iii. Perform 64 rounds of computation using the message schedule and working variables:

1. Compute the temporary values T1 and T2.

2. Update the working variables a, b, c, d, e, f, g, h.

iv. Update the hash values H0 to H7 with the working variables.

4. Compute the final hash value:

Concatenate the hash values H0 to H7 in the order H0, H1, H2, H3, H4, H5, H6, H7 to obtain a 256-bit hash value.

In summary, the SHA-256 cryptographic algorithm is a reliable and widely used hash function that provides strong security guarantees for many applications. Its simplicity, efficiency, and robustness against attacks make it a popular choice for digital signatures, password storage, and other security applications where data integrity is crucial.

C. ECDSA:

The Elliptic Curve Digital Signature Algorithm (ECDSA) is a widely used cryptographic algorithm for digital signatures. The use of elliptic curves in ECDSA provides several security benefits over other cryptographic algorithms. The shorter key lengths and faster computations make ECDSA more efficient than other public-key cryptographic algorithms. The one-way hash functions ensure that the message is not tampered with, and the signature cannot be reused for other messages.

ALGORITHM:

1. Choose a prime number p and an elliptic curve E_p(a,b) such that y^2 = x^3 + ax + b (mod p), where x, y, a, b ϵ GF(p).

2. Choose a base point G on the elliptic curve E_p(a,b) and compute its order n, i.e., nG = O where O is the identity element.

3. Choose a private key d ϵ [1, n-1] and compute the corresponding public key Q = dG.

4. To generate a signature for a message m, compute its hash value h(m) and let z be the leftmost n bits of h(m).

5. Choose a random integer k ϵ [1, n-1] and compute a curve point (x_1,y_1) = kG.

6. Calculate r = x_1 (mod n).

7. Calculate s = k^(-1)(z+rd) (mod n).

8. The signature for the message m is (r,s).

9. To verify the signature for a message m, compute its hash value h(m) and let z be the leftmost n bits of h(m).

10. Calculate u_1 = zs^(-1) (mod n) and u_2 = rs^(-1) (mod n).

11. Compute the curve point (x_1,y_1) = u_1G + u_2Q.

12. If r = x_1 (mod n), then the signature is valid; otherwise, it is invalid.

In ECDSA, the parameters p, a, b, G, and n are public, while the private key d and the random integer k used to generate the signature are kept secret. The security of ECDSA relies on the difficulty of solving the discrete logarithm problem on the elliptic curve used, where G is a generator point on the elliptic curve, n is the order of the curve, and hash is a one-way hash function. The signature is then sent along with the message to the recipient.

To verify the signature, the recipient calculates the hash of the message and uses the public key and the signature values to perform the verification. The recipient first calculates the inverse of s modulo n and then uses the values r, s, and the inverse of s to calculate a point on the curve. If the x-coordinate of the calculated point is equal to r, the signature is considered valid.

The use of elliptic curves in ECDSA provides several security benefits over other cryptographic algorithms. The shorter key lengths and faster computations make ECDSA more efficient than other public-key cryptographic algorithms. The one-way hash functions ensure that the message is not tampered with, and the signature cannot be reused for other messages.

ECDSA is widely used in digital certificates, secure electronic transactions, and secure communications. Its strong security guarantees, combined with its efficiency and versatility, make it a popular choice for many security applications.

D. CNN:

A Convolutional Neural Network (CNN) is a type of deep learning neural network designed for processing structured arrays of data such as images. CNNs are widely used in computer vision and have become the state of the art for many visual applications such as image classification. (“Convolutional Neural Network Definition | DeepAI”)

The architecture of a CNN is a multi-layered feed-forward neural network, made by stacking many hidden layers on top of each other in sequence. It is this sequential design that allows CNNs to learn hierarchical features. "The hidden layers are typically convolutional layers followed by activation layers, some of them followed by pooling layers." (“Convolutional Neural Network Definition | DeepAI”)

The power of a CNN comes from a special kind of layer called the convolutional layer. CNNs contain many convolutional layers stacked on top of each other, each one capable of recognizing more sophisticated shapes. With seven convolutional layers it is possible to classify the heartbeat as non-ectopic (N), supra ventricular ectopic (S), ventricular ectopic (V), fusion (F) and unknown beats (Q).

ALGORITHM:

Here is a more detailed overview of a CNN algorithm for classifying heartbeats from an ECG signal represented as an array:

1. **Preprocessing**: The ECG signal is preprocessed to remove noise and artifacts. This can be done using various techniques such as filtering, or wavelet transform.

2. **Segmentation**: The preprocessed ECG signal is divided into segments representing individual heartbeats. This can be done by detecting the R-peaks in the QRS complex of the ECG signal and using them to define the boundaries of each heartbeat segment.

3. **Feature extraction**: Each heartbeat segment is passed through a 1D-CNN model architecture based on three convolutional, max pooling and dense layers. The convolutional layers apply a set of filters to the input data to extract local features. The max pooling layers down sample the data to reduce its dimensionality. The dense layers combine the extracted features to make predictions.

4. **Classification**: The CNN model automatically extracts distinguishable nonlinear features from the ECG signals and automatically classifies them into different classes such as non-ectopic beats (Normal Beat), Supraventricular ectopic beats, Ventricular ectopic beats, Fusion Beats and Unknown Beats.

5.Output: The output of the CNN model is the classified heartbeat.

IV. EXPERIMENTAL RESULTS

The time vs size of input file graph is plotted below in fig3, which clearly shows that the proposed system is able to encrypt and decrypt data of larger file size in a shorter span of time.

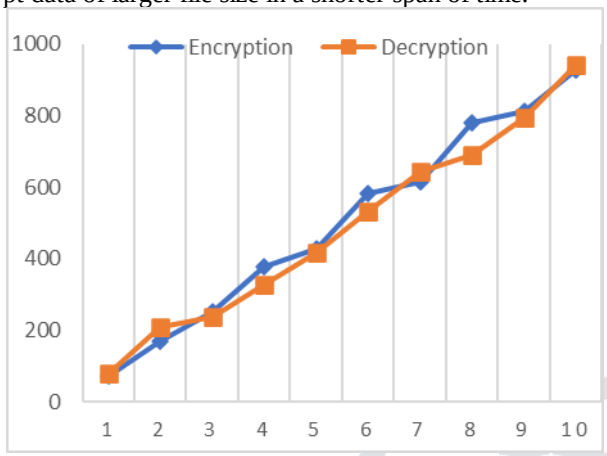

Fig 2. Encryption and Decryption time analysis for the BlowFish+SHA256+ECDSA Algorithm

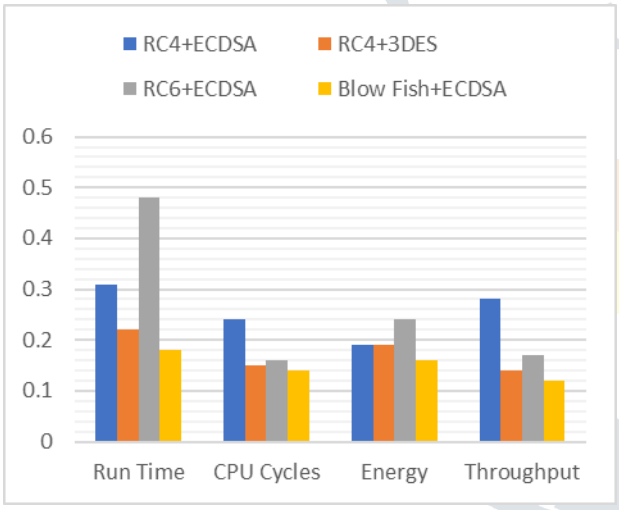

Fig 3. Performance analysis of RC4, RC2, RC6 types with blowfish.

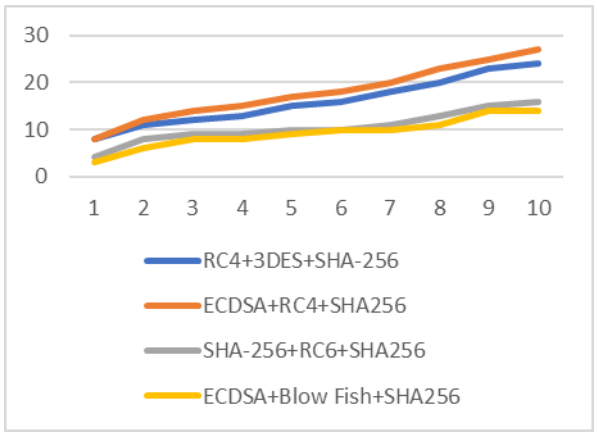

Fig 4. Encryption execution time comparison of RC variants with proposed model

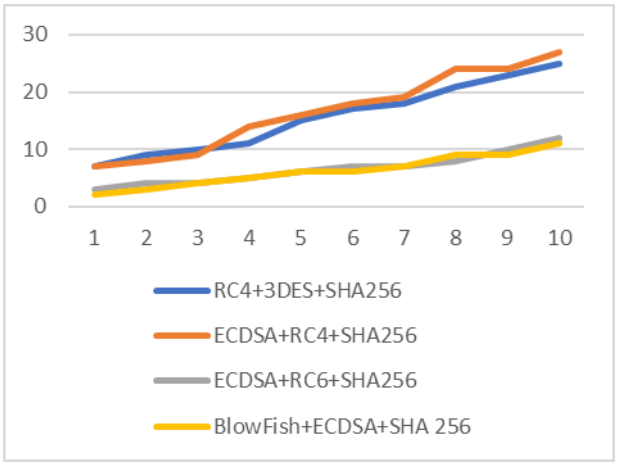

Fig 5. Decryption execution time comparison of RC variants with proposed model

This area will existing the statistical community performance and it's a range of parameters of fitness care offerings like encryption, decryption, and secret key timings with appreciate to metrics such as throughput, packet loss, time, and reminiscence speedup. We think about the MIT-BIH Arrhythmia Database [28] of ECE recordings from one subject. This will assist to test the security has been encoded or not. ECG consists of easy alerts which help to take a look at the coronary heart price is in everyday circumstance or not. For detecting and measuring the sign sensor will be attached to the human physique skin. The indicators are validated and saved in a storage system with the aid of a machine. Furthermore, these indicators are handed to the health practitioner for inspecting if the coronary heart charge is regular or abnormal based on the value. Based on the outcome, if the coronary heart charge is abnormal the affected person wishes to bear cure with proper care. The proposed work is evaluated the usage of python configuration with cryptographic standards. The mannequin makes use of 256-b key measurement and 256 block dimensions to check the overall performance evaluation of encryption and decryption ECG signals. The sampling frequency of the signal is one hundred twenty-five Hz and proven in Fig. 2. Fig.3 validates the protection of fitness care alerts for 10 input sample sorts which have been simulated between encryption and decryption for throughput as metric the use of proposed ECDSA, Blowfish and SHA256 protection algorithms. From this, the multi frequency signal facts are now not shared due to shared non-public and public keys. The community throughput is measured the usage of an enter file divided with the aid of a variety of devices wished for encryption (En) or decryption (De). The encrypted calculation is given in (9). Similarly, calculating the decryption technique is given in (10). Table I simulates the values for measuring the community throughput using structured secured algorithms. The kinds of RC4 procedure the ciphertext sign from the implantable clinical sensors the use of the frequency as measurement. The key enlargement of an algorithm will amplify a user-supplied key which fills in an accelerated array. For this experiment, we use a 32-b key size, 20 rounds, and sixteen block measurement that functionalize as a superior encryption trendy process. All the simulation has been carried out in an Intel processor with python as programming basics. The simulated effects are given in Table II. The run-time is the time taken to execute the ciphertext in the encryption and decryption process. The quantity of a number of cycles per every step is the execution of clock cycles. The energy price is calculated via multiplying the variety of cycles with key-value with the community ratio. Finally,

throughput is the number of statistics in pixel values ate up in the course of the ciphertext creation. Fig. 4 indicates the exceptional overall performance measures of RC6 variations and how Blowfish is properly in contrast with different existing methods. The under experimental effects show the throughput execution time with encryption and decryption. The consequences are tabulated in Tables III and IV. Throughput is calculated from the plaintext signal. From Figs. 5 and 6, the outcomes exhibit that the proposed work can be evaluated in fewer instances and efficiency. So, for fitness care evaluation purposes, the Blowfish algorithm key generation is used to generate the ECDSA signature key and later using SHA 256 hashing technique. We have described quick names for the comparative fashions as RC4 + 3DES + SHA-256 (Model-1), ECC+RC2+SHA-256(Model-2), ECDSA+RC4+SHA-256(Model-3), ECDSA+Blowfish+SHA-256 (Proposed model).

By using the proposed BES-256 algorithm we decrypted the data and then it passed to another convolutional neural network model where we have trained the model using the historical data of ECG signals of heartbeat which has the classification of 5 labels to classify it. The model is trained by applying the model by using max pooling and min pooling also applies with the activation function like SoftMax and relu.

Here, epoch is used to increase the accuracy score which consumes time but produces higher accuracy for the model. Our model gives the accuracy rate of about 78.27% with lower loss.

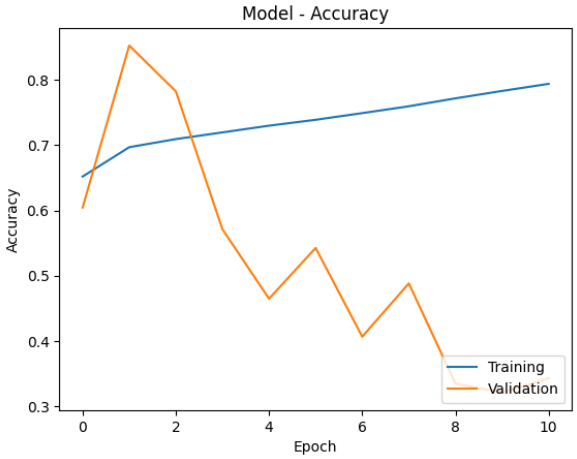

Fig 6. Convolution neural network model's accuracy vs epoch graph

In Fig 6. it clearly depicts that while training a model by increasing the epoch the accuracy is increased and the in the validation part also.

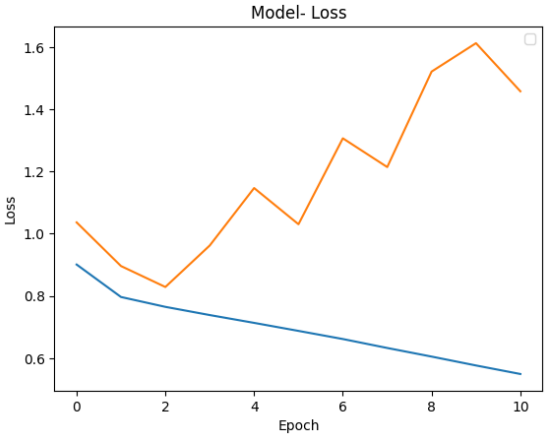

Fig 7. Convolution neural network model's loss vs epoch graph

In Fig 7. it says that while training a model by increasing the epoch the loss is reduced.

V. DISCUSSION

In latest situations still, many clever fitness care IoMT structures are affected with serious attacks, the use of unencrypted communication services, unprotected affected person data, and additionally placing week passwords. This proposed work makes use of cryptographic algorithms to enhance the protection layers of IoMT sensors, particularly from implantable units to put into effect sturdy safety and privacy. The protection mechanisms enabled in our work leverages the information captured from implantable sensors the use of information sharing non-public and public keys. The information obtained from implantable gadgets are entered into the nearby database earlier than transferring the small print into a scientific repository. The captured information is encrypted the usage of enormously authenticated signature and hashing secured keys. With this, stealing patients, data from a scientific database or unauthorized get right of entry will be denied by means of secured encryption mechanisms.

All the extraordinary sorts of provider layer gather statistics from the human physique via implantable units and transfer to a clinical repository. The protection and privateness prevention mechanisms make sure that the complete gadget is secured with cryptographic algorithms. Also, the statistical acquisition of a clever fitness care protection renovation device virtually affects the sensor electrocardiogram (ECG) patches and pulse oximeter. Hence, many different sensors are handy to extract the statistics captured by using the respective implantable devices. The ECG facts from the wearable sensor can assist to routinely ship the statistics of affected person situation in case of a coronary heart attack. These units will help in classifying the coronary heart recreation with the aid of checking the values and the indicators bought with the aid of the ECG.

Blowfish block cipher is one of the most modern and effective algorithms to encrypt information and alerts in an invulnerable and speedy manner in the fitness care sector. The block cipher takes the plaintext message and divides it into fixed-sized chunks referred to as blocks with the key parameter. Each block is represented with a set of bit strings as zeros and ones the use of constant size as sixty-four or 12 b. As a result, the Blowfish block cipher will encrypt when the sender sends the message and decrypted at the receiver aspect which manner one block at a time. The important blessings of Blowfish block cipher are excessive diffusion and immunity to tampering. There is a number encryption algorithm that has been used for binary and text-based messages. But these algorithms are challenging due to measurement and complicated operations in making use of for sign based totally input. For any sign based totally on encryption algorithm time, speed, error detection and compression are viewed as key vital factors.

To enhance the run-time overall performance of sign, enter selective encryption algorithm is applied. Also, to store the computation time of alerts and keep away from the sign compression fee exceptional password safety whilst presenting facts confidentiality. The proposed consequences confirmed that confidentiality upkeep will sequentially enhance the safety of fitness care services. In future, we will observe protection in inspecting the

troubles from patient's records and how docs can supply answer based totally on the overall performance finished with bettering extra safety alongside with neural community models.

Permutation-based operations such as whitening, and shifting, phrase permutation is used. The encryption evaluation will assist to consider and evaluate the visible degradation of input, an encrypted ratio of the facts size, speed, compression friendliness, and protection towards more than a few attacks. The indicators are represented as a rectangular array of pixel sign factors with a numeric value. The proposed safety constraints are in contrast with current models, which is given in Table V.

The safety and privateness of the proposed algorithm are compared the use of the following measures, such as confidentiality, authenticity, integrity, ownership, policy, and assault resistance. It has been determined from the evaluation that the proposed mannequin has the same opinion to all the safety constraints and help the sturdy framework in imparting the identification with fashionable algorithms in contrast to the present models. Because the ECDSA algorithm helps the core safety measures like integrity and possession whilst the different fashions are filed to provide. Hence, the fitness care storage database will shop all the integral data of sufferers earlier than sending it to a number of provider providers. Both the sender and receiver will be shared with a secured key to change the indispensable important points from the storage place. If the keys from each aspect are matched, the statistics is shared. In this way, the patient's important points are stored protected in a fairly secured manner.

VI. CONCLUSION

The implementation of smart healthcare services has led to the development of various hardware and software applications that aim to improve the quality of medical standards. However, a major challenge in this field is the processing of data from implantable devices, which contains sensitive patient information and is vulnerable to attacks. Therefore, it is crucial to ensure the security of patient data by implementing strong security measures. In this context, a study was conducted to enhance the security layers of implantable devices in smart healthcare systems using standard cryptographic algorithms such as Blowfish, ECDSA, and SHA256. These algorithms were utilized to encrypt the patient's medical details stored in the medical repository, which prevented unauthorized access and ensured data confidentiality. Public and private keys were utilized to control remote access with strong password protection, further strengthening the security measures. The results of the study demonstrated that implementing these security and privacy mechanisms significantly improved the confidentiality and protection of healthcare services. In the future, the study plans to further enhance the security measures and apply them in analyzing patient data to help doctors provide solutions based on the performance achieved with neural network models. In addition to this we used machine learning algorithms to know the health of the heart and predict the type of heart disease if exists. Overall, the proposed solution provides a promising approach to secure patient data, to know the health of the heart with that data and enhance the quality of healthcare services.

REFERENCES

[1] Sun, X., & Chen, Z. (2022). A Novel Chaotic Image Encryption Algorithm Based on Coordinate Descent and SHA-256. IEEE Access, 10, 114597–114611. https://doi.org/10.1109/access.2022.3217520

[2] Xiong, H., Yao, T., Wang, H., Feng, J., & Yu, S. (2022). A Survey of Public-Key Encryption With Search Functionality for Cloud-Assisted IoT. IEEE Internet of Things Journal, 9(1), 401–418. https://doi.org/10.1109/jiot.2021.3109440

[3] Sallam, A., Faragallah, O. S., & El-Rabaie, E. M. (2018). HEVC Selective Encryption Using RC6 Block Cipher Technique. IEEE Transactions on Multimedia, 20(7), 1636–1644. https://doi.org/10.1109/tmm.2017.2777470

[4] Ding, Y., Wu, G., Chen, D., Zhang, N., Gong, L., Cao, M., & Qin, Z. (2021). DeepEDN: A Deep-Learning-Based Image Encryption and Decryption Network for Internet of Medical Things. IEEE Internet of Things Journal, 8(3), 1504–1518. https://doi.org/10.1109/jiot.2020.3012452

[5] Aljohani, M. S., Ahmad, I., Basheri, M., & Alassafi, M. O. (2019). Performance Analysis of Cryptographic Pseudorandom Number Generators. IEEE Access, 7, 39794–39805. https://doi.org/10.1109/access.2019.2907079

[6] Z. Liu, J. Großschädl, Z. Hu, K. Järvinen, H. Wang and I. Verbauwhede, "Elliptic Curve Cryptography with Efficiently Computable Endomorphisms and Its Hardware Implementations for the Internet of Things," in IEEE Transactions on Computers, vol. 66, no. 5, pp. 773-785, 1 May 2017, doi: 10.1109/TC.2016.2623609.