SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V11I12P136

Volume 11 Issue 12, 399-405, December 2024


*Original Article*

# An Effective Paillier Encryption for Health Data with Cloud Storage and Prediction Using RNN

R. Sahila Devi[1], Govinda Patil[2], D. Srinivasa Rao[3], Jitendra Choudhary[4], Sriram Gopalam[5], Priyanka Parmar[6]

[1]*Department of Computer Science and Engineering, Rohini College of Engineering and Technology, Palkulam, India.*
[2,4]*Department of Computer Science, Medi-Caps University, Indore, Madhya Pradesh, India.*
[3]*Department of Computer Science and Engineering, Medi-Caps University, Indore, Madhya Pradesh, India.*
[5]*Department of Computer Science, School of Distance Education, Andhra University, India.*
[6]*Department of Computer Applications, Medi-Caps University, Indore, Madhya Pradesh, India.*

[1]*Corresponding Author : r.sahiladevi@gmail.com*

Received: 20 October 2024 Revised: 21 November 2024 Accepted: 19 December 2024 Published: 31 December 2024

***Abstract -*** *An emerging technology in data analytics, Cloud Computing (CC) is used to store, retrieve, and distribute data in a dispersed setting. Both individuals and businesses save their data on cloud servers. However, data privacy and security have become a rising problem that limits the organization from employing cloud services. In order to overcome that problem, the Paillier encryption method is proposed to offer safety for healthcare cloud data. Creating a pair of keys offers a comparatively easier method to ward against attacks and safeguard data confidentiality. Following data selection, the Paillier methodology is used to encrypt the input. The encoded health data were then kept in cloud environments, where they provided better read-write storage operations. The Paillier method is used in the data decryption procedure to get the data from the cloud environment. A Recurrent Neural Network (RNN) classifier is employed in healthcare diagnosis to categorize and forecast a patient's ailment, after which the diagnosis is communicated to the patient and physician. The proposed work uses Python software, and a comparative analysis is conducted. An effective prediction using RNN showcases an accuracy of 96.4% with a better performance matrix. After classification, the outcomes are conveyed to patients and doctors for treatment.*

***Keywords -*** *Cloud computing, Healthcare data, Paillier method, RNN, Diagnosis.*

## 1. Introduction

Healthcare deals with various health services, from emergency care centers, intensive care clinics, restoration centers, speciality outpatient services and long-term care facilities. In medical services, treatment is a main concern, and it needs to be considered for the welfare of society [1, 2]. In order to protect patients, medical personnel are concentrating on enhancing the communications between specific patients and clinics [3, 4]. Every day, the growth of medical technology and fields like computed tomography and magnetic resonance imaging create enormous amounts of data, much of which is high dimensional and variable-rich. Healthcare providers, however, face significant challenges in managing, sharing, and processing the vast amounts of medical data that are now available [5, 6]. Because the healthcare cloud is straightforward to manage, CC has thus been used in the healthcare field for computing and storing healthcare data and delivers a safe and real-time solution for confidential health data records kept in the cloud. Along with vast storage resources for large Electronic Health Records (EHR) datasets, it also entails improved monitoring and analysis of data relevant to diagnosing and treating various diseases. However, upholding data security and privacy is CC technologies' most important difficulty [7-9]. People who are careless or malicious can endanger data security. Data encryption is the most crucial of several techniques that give data security. An integral part of cybersecurity architecture is data encryption and decryption. Thus, data security approaches are needed to safely and securely manage medical and health data in critical systems [10–13]. In [14], a modular encryption standard that is based on layered modeling of security methods is introduced. Improved performance and a supplementary qualitative security guarantee that measures are successful. Nevertheless, this method is designed for textual data encoding and decoding; the picture-directed data set has not yet been considered. In [15], a new lightweight cryptographic technique that may be used with secure CC apps is given for enhancing data security. It has a high degree of security and seems to have improved regarding security forces and cipher execution time measurements. The encryption/decryption algorithm is easy to use and very safe. For the cloud environment, the algorithm provides a simple and efficient structure. The algorithm only runs five rounds to optimize energy efficiency results. Nevertheless, each round needs four data bits to perform crypto mathematical calculations.

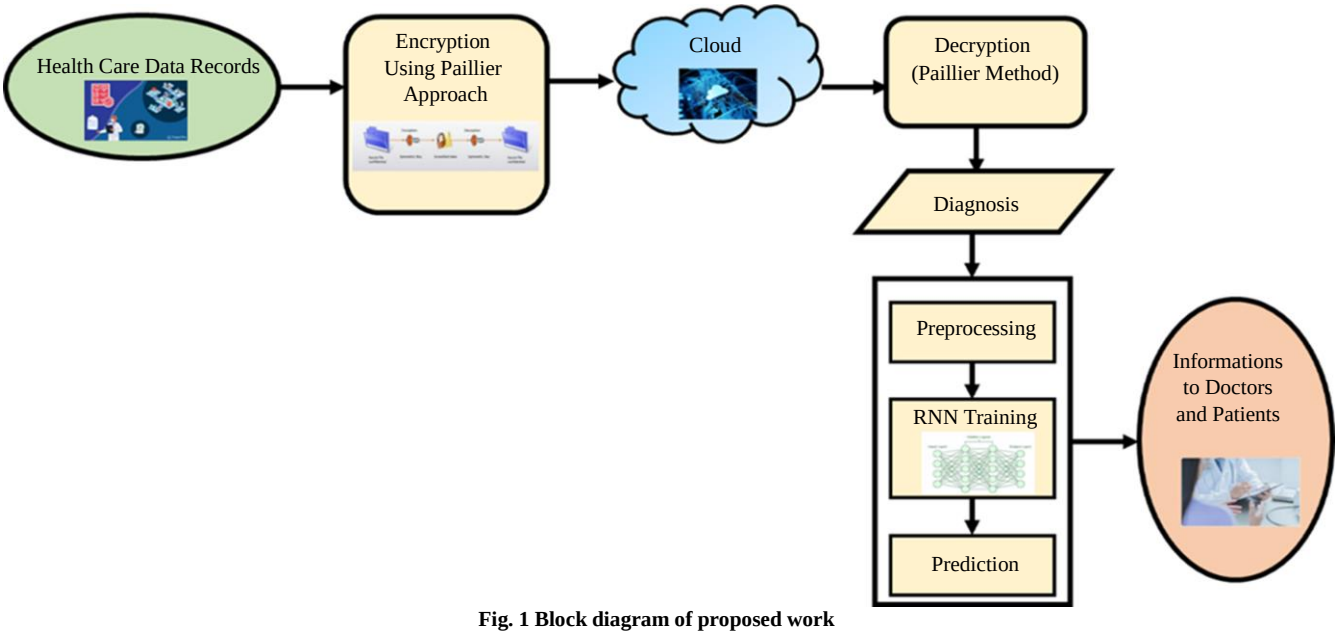


**Fig. 1 Block diagram of proposed work**

To secure large amounts of cloud data, [16] used triple data encryption standard. By increasing the size of standard keys for data encryption, the technique provides a relatively simpler way to protect data privacy and stop attacks. However, it required higher CPU and network usage. A modified version of the advanced encryption standard for CC data security is presented in [17], which added random disturbance information to enhance data security. The algorithm must be made relevant to encryption to ensure greater security and efficiency. However, the key length size is quite long, which makes the whole process slow and complex sometimes. Due to this, the proposed work implemented a paillier method to secure the health data stored in the cloud. For healthcare data analysis and disease diagnosis, many traditional techniques such as SVM [18], CNN [19] and DNN [20] are used in the medical field. However, managing, storing, and processing healthcare data is complicated for large healthcare datasets and extraordinary performance classifiers are needed for healthcare data processing. Therefore, this work proposes an RNN for classifying data in the healthcare field. The primary goals of this work are given below,

- To secure healthcare data with Cloud computing, a Paillier method is used for data encryption and decryption.
- Data pre-processing eliminates unwanted noise for medical diagnosis and corrects errors from healthcare input data.
- The RNN is used to categorize various diseases from healthcare data, and then the classified results are used to predict patients' diseases.

## 2. Proposed Methodology

Cloud computing, characterized by transferring computing services over the internet, has revolutionized how healthcare organizations save, manage and analyze data. However, there are several issues, including data security and privacy; private patient data must be shielded from hackers and unauthorized access. To overcome this issue, we propose a paillier encryption method that provides data security in the healthcare environment. Figure 1 depicts the block diagram of the proposed work.

The healthcare dataset is used as input in the initial input selection process. Patient characteristics, including name, age, month, gender, symptoms, and place, are included in the datasets. The Paillier approach encrypts the input after the data is selected. Then, the encrypted medical records are kept in cloud settings, which offer better support for read-write storage operations. The paillier method is used to decrypt data to get it from the cloud. The proposed Paillier method produced a pair of keys to prevent attacks and safeguard data privacy, offering a more straightforward method. Pre-processing is done on the decrypted cloud data for medical diagnostics to remove unnecessary noise from the healthcare data through data cleaning and filtering. Then, RNN is used to forecast a patient's disease for categorization purposes precisely, and both the patient and the physician are notified of the expected data.

### *2.1. Cloud Based Healthcare Data*

Security in cloud computing has grown in importance recently, especially when it comes to disease prediction and the storage of medical data. The healthcare industry creates significant amounts of data due to advancements in medical technology. Thus, these massive volumes of data are

handled, processed, and stored using CC technologies. However, data security and privacy are major difficulties that prevent companies from using cloud services. The Paillier encryption technique is proposed to solve this problem, offering massive data security in the Cloud context. The healthcare dataset is regarded as an input in the first step, data or input selection. 17 parameters: total name of the patient, sex, age, month, symptoms, location, disease, maximum heart rate attained, body mass index, past medical history, name of consultant, serum cholesterol, body weight, height, and type of employment are included in the dataset. The necessary data are chosen and considered for the encryption process based on the attributes of the patients.

### *2.2. Paillier Method for Protecting Healthcare Data*

The administrator first generates a mask for the patient's name, age, gender, previous history, specialist name, location, job type, and body weight before encrypting the data. The Paillier method is used for input encryption after the data has been selected.

#### *2.2.1. Data Encryption*

A security procedure called data encryption transforms plaintext data into inaccessible ciphertext to keep data safe between clouds. It is among the finest models for preserving data confidentiality and preserving cloud data, opposing cyberattacks, though it is in use or transit. The only people who will decrypt the ciphertext and access the data are those who possess the matching private key. Unauthorized users are prevented from accessing the data in this way. Sensitive data, known as Personal Health Records (PHR), is encrypted. This work uses a paillier method to encrypt the input data to secure healthcare data. One kind of key pair-based encryption is the Paillier approach. Each user will have a public and private key; only the corresponding private key will be needed to decrypt messages encrypted with a public key. One distinctive feature of Paillier is that they offer additive homomorphism, which implies that messages will be added to them during encryption, and they will correctly decrypt. The process of paillier encryption consists of three key phases. They are encryption, decryption, and key pair generation.

*Key Generation Process*

It is used for producing cryptography keys. A key is employed to encrypt and decrypt any data that has been encrypted or decrypted.

1. Choose two big prime numbers $p\ and\ q$ arbitrarily and autonomously of one another.
$$gcd = \big(pq, (p-1)(q-1)\big) = 1 \quad (1)$$
2. Compute $n = p * q$ and take $lcm$ and name it $\lambda$.
$$lcm = ((p-1)(q-1)) \quad (2)$$
3. Select a random integer $g$ where it fits to $Zn^2$.
4. The order of $g$ is a multiple of $n$ in $Z^*n^2$.
5. The key for the public is $(n, g)$.
6. The key to privacy is $(\lambda, \mu)$.

*Encryption Process*

The paillier encryption technique is employed to encode the data. A matching private key and public key are generated throughout an encryption process. They transferred it to the cloud server once it had been encrypted.

1. Let $m$ be an encrypted message where $0 \leq m < n$.
2. Choose random variable $r$ where $0 < r < n$ and $r$ belongs to $Z^*n^2$
3. Calculate ciphertext as
$$c = gm * rn\ mod n^2 \quad (3)$$

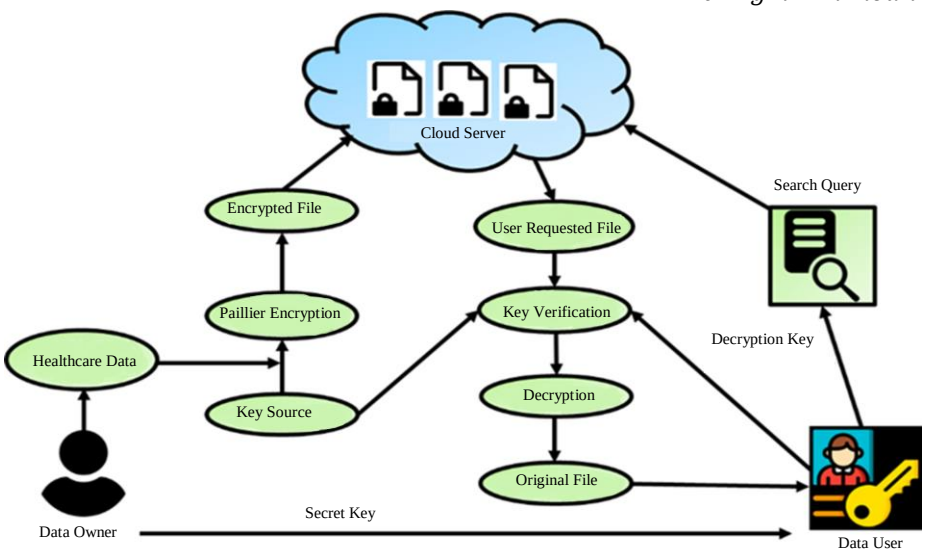


**Fig. 2 Architecture diagram for Paillier method**

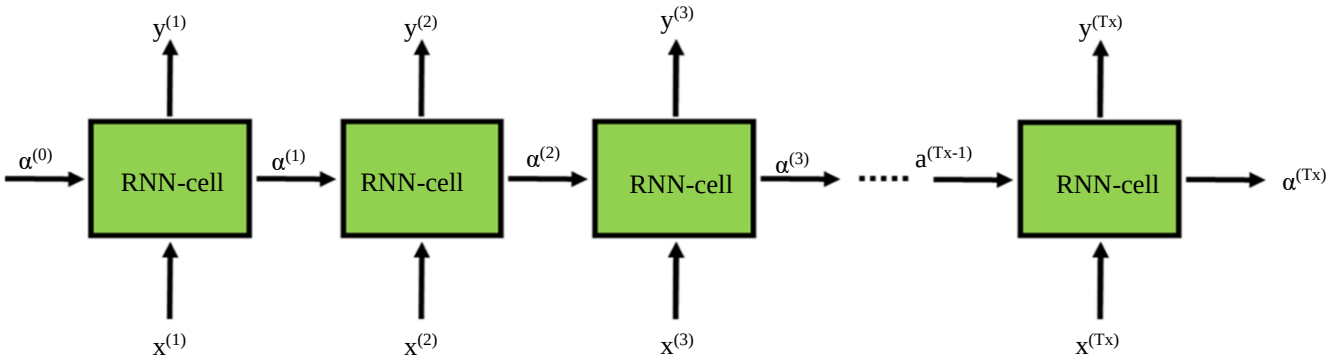


**Fig. 3 Simple RNN structure**

*Decryption Process*

The cloud-based encrypted data is retrieved during this process, and the public key decrypts it. The only person who accesses and decrypts data is the one who possesses the associated secret key to the message.

1. Let $c$ be the ciphertext to decrypt, where $c$ fits to $Z^* n^2$.
2. Calculate the plaintext message as

$$= L(c^{\lambda} mod\ n^2) \quad (4)$$

Figure 2 depicts the architecture diagram of the Paillier encryption method. Patients use the cloud environment to share their encrypted data during transmission, and the resultant ciphertext is kept in a cloud environment where only authorized users will access it, known as the cloud-stored cipher or encrypted data. Only the one with the message's matching secret key will access and decrypt the data. After encryption, the diagnostic process for the healthcare data is implemented utilizing the proposed RNN.

### *2.3. Disease Prediction*

After encryption, the following steps are used to detect patients' disease, and the classification results are communicated to the specialists for treatment.

*2.3.1. Data Preprocessing*

Pre-processing is utilized to remove the captured data from noises and analyze them efficiently. It gets two different kinds of information: (1) sensory data and (2) personal data. For optimal results, noise levels need to be lowered, and lost samples will be recovered when various event readings from sensors are captured. This component's job is to make sensor properties less dimensional. Furthermore, personal data about patients will be used to take additional necessary action. The RNN classifier receives the pre-processed data and divides it into two categories: normal data and data impacted by disease.

*2.3.2. Classification Using RNN*

After pre-processing, an effective classification algorithm, RNN, is utilized for healthcare data classification. An artificial neural network with directed loop connections between its units is called an RNN. RNNs are feed forward neural networks that include the concept of time into the conventional neural network paradigm by having edges that grow in tandem with neighboring time steps. RNNs and feed forward networks vary in that NNs lack conventional edge-to-edge loops. On the other hand, loops will be formed by repeating edges that connect consecutive time steps, including long loops that self-connect from a node. Equation (5) proves how nodes with recurrent edges at time $t$ obtain their input from the current data point $x^t$ and hidden node values $h^{t-1}$ in the network's preceding state. Equation (6) proves how values ht of hidden node at time t are used to calculate output $y^t$. Recursive connections to $y^t$ and beyond permit the $x^{t-1}$ input at time $t-1$ to impact output at time $t$.

$$h^t = \sigma(W^{hx} x^t + W^{hh} h^t + b_h) \quad (5)$$

$$y^t = sortmax(W^{hx} x^t + b_y \quad (6)$$

Here, $W^{hx}$ is the input in this case, and the buried layer uses standard weights. $W^{hh}$. Are the hidden layers and their recurring weights matrix in neighboring time steps? The vectors for the bias parameters are$b_h$ and $b_y$. Figure 3 shows an example of a basic RNN structure.

A feature of RNN designs is a cyclic connection, which allows modernizing the present state based on the input and states that have come before. The recurrent layers of the RNNs are made up of recurrent cells. Past states and feedback connections in the current input affect the states of the recurrent cells. Recurrent layers will be organized into several designs to generate several RNNs. Therefore, RNNs are distinguished by their network architecture and recurrent cell. RNN performance is determined by different cells and the connections inside them. These networks, which consist of standard recurrent units (sigma cells and tanh cells) and will be composed of entire RNNs or selective RNNs, have demonstrated extraordinary performance in certain scenarios. The RNN model's architecture is depicted in Figure 4.

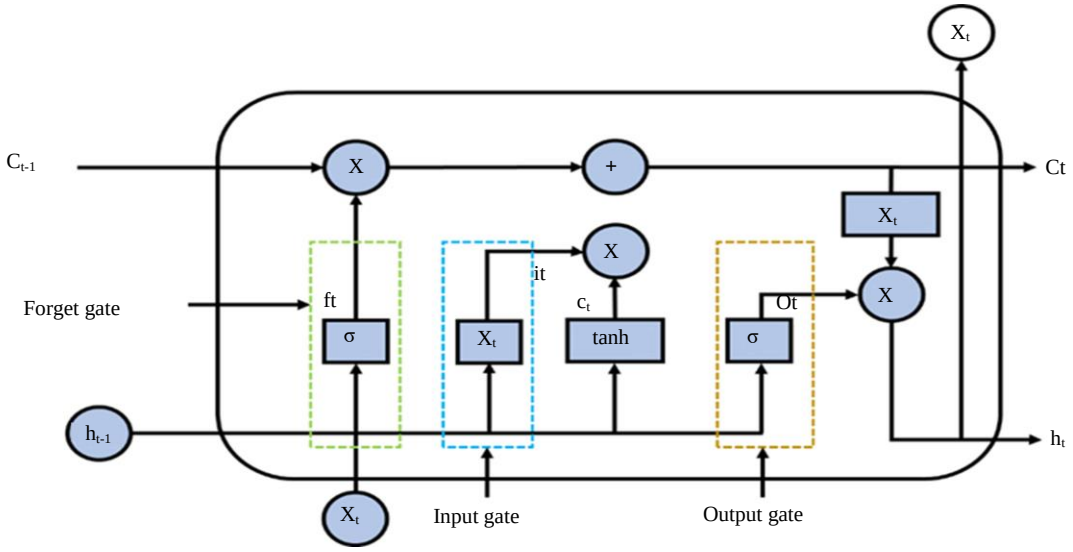


**Fig. 4 RNN's structure**

The RNN is useful for processing, categorizing, and predicting time-series data. The RNN categorizes the processed data into normal and disease contrived data. Finally, the classified patient data is used to predict the disease and then inform to the patients and patients.

## 3. Results and Discussion

A Paillier encryption method is proposed to offer safety for healthcare data in the cloud. The healthcare dataset is used as input in the initial input selection process. Following data selection, the Paillier methodology is employed to encrypt the input, and the encrypted healthcare data is then kept in cloud environments, where better read-write storage operations are provided. An RNN classifier is utilized in healthcare diagnosis to categorize and forecast a patient's ailment, after which the diagnosis is informed to the patient and physician. The proposed work is implemented in Python software, and a comparative analysis is performed using conventional methods.

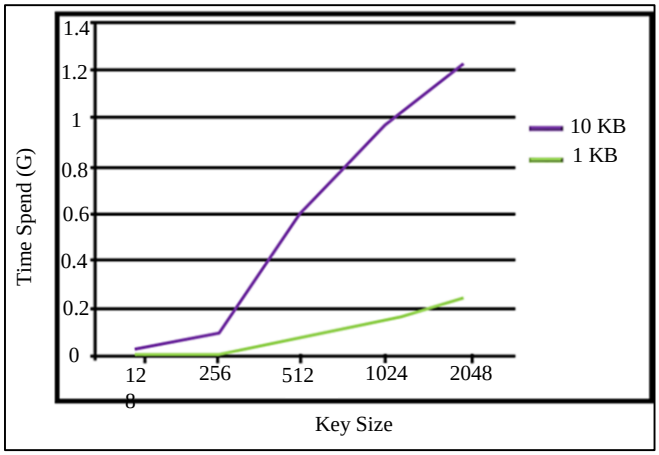


**Fig. 5 The average time encryption utilizing the Paillier method**

Figure 5 displays the difference in time required to encode 1 KB of data against 10 KB utilizing the paillier technique with diverse length keys. Figure 6 shows how the key size significantly impacts how long it takes to use the Paillier technique for decryption.

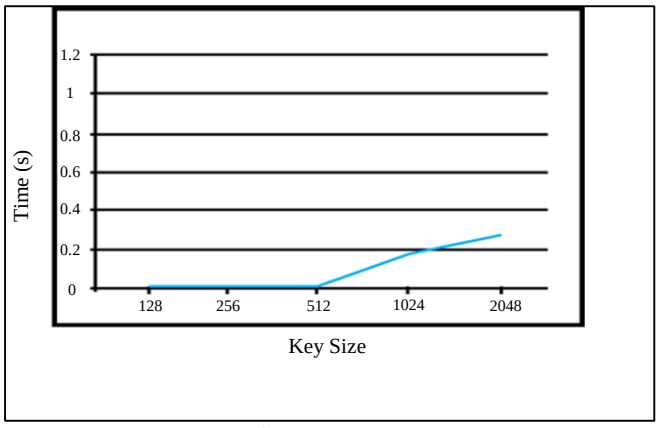


**Fig. 6 The average time for decryption utilizing Paillier method**

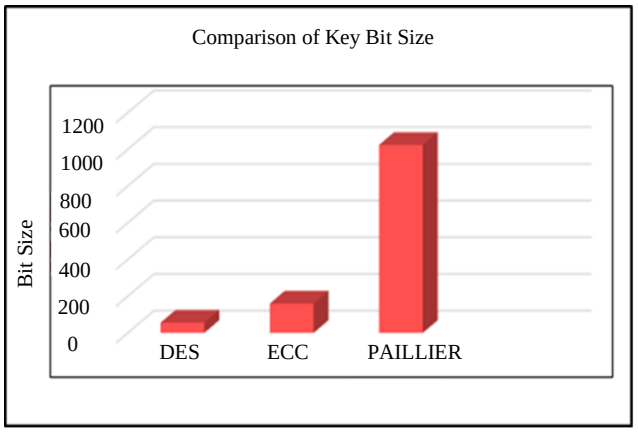


**Fig. 7 Comparison of key bit size**

Figure 7 compares key bit sizes for various methods like DES [21], ECC [22] and Paillier encryption method. The DES and ECC method have the lowest bit size, and the Paillier method has the highest bit size of 1024 bits.

Table 1 displays the comparison of encryption and decryption time. The paillier method has encryption and decryption times of 295 ms and 345 ms.

Figure 8 depicts the accuracy comparison for J48 [10], CNN [5], and RNN methods. Here, the CNN and RF have the lowest accuracy, and the proposed RNN achieves the highest accuracy of 96.4%.

Figure 9 highlights the comparison of sensitivity with DT [23], KNN [5] and RNN methods. The proposed RNN attains a better sensitivity of 95.4%, which is better than other methods.

**Table 1. Encryption and decryption time comparison**

| Method | Encryption (ms) | Decryption (ms) |
|---|---|---|
| **TDES [16]** | 350 | 480 |
| **Homomorphic Encryption [24]** | 410 | 500 |
| **Paillier** | 295 | 345 |

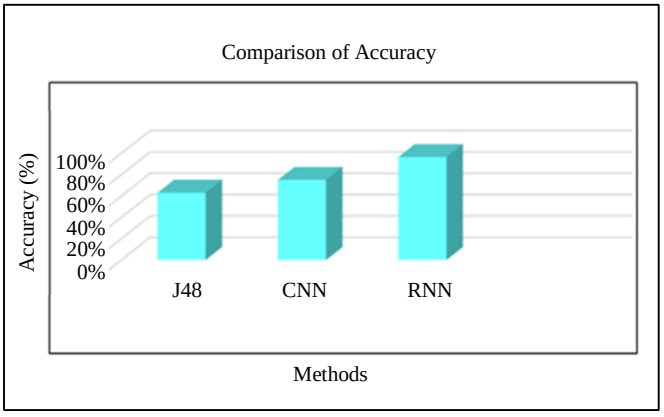


**Fig. 8 Comparison of accuracy**

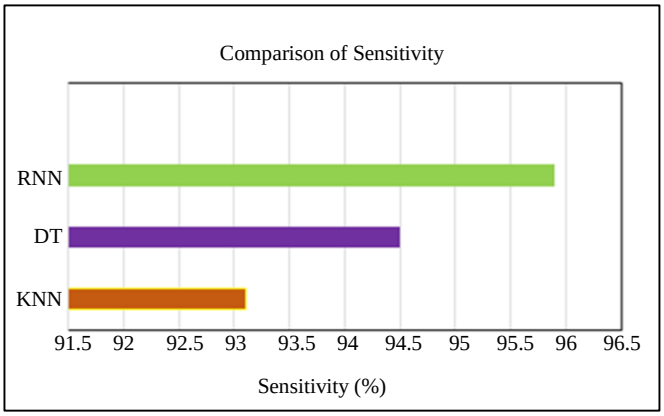


**Fig. 9 Comparison of sensitivity**

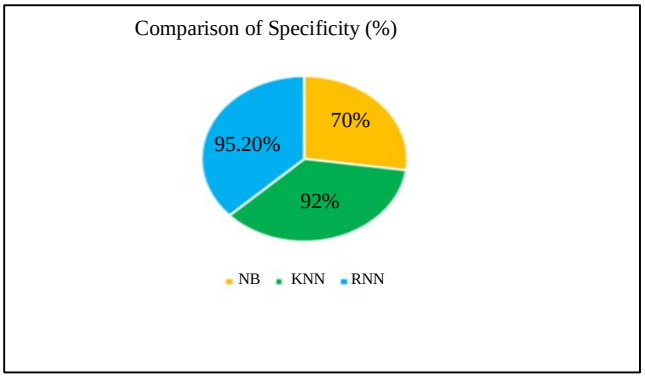


**Fig. 10 Comparison of specificity**

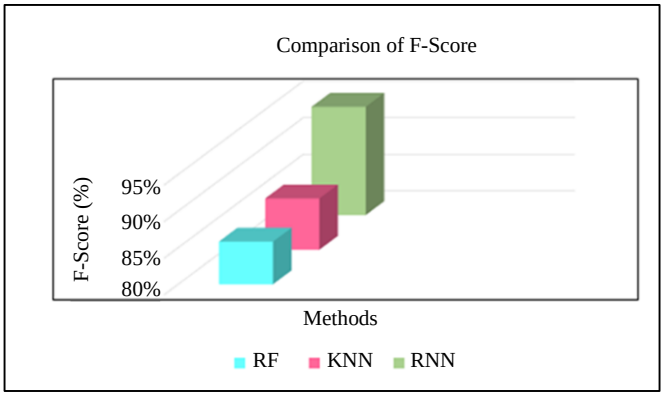


**Fig. 11 F-score's comparison**

Figure 10 compares specificity for NB [23], KNN [5] and RNN methods. The proposed RNN outperforms with a specificity of 95.2%. Figure 11 compares the F-score with some methods like KNN [5], RF [10] and RNN. The proposed RNN outperforms other approaches with an F-score of 94.8%.

## 4. Conclusion

The confidentiality and safety of data are difficult concerns that limit organizations from employing cloud services. Paillier encryption technique has been proposed to solve that problem, providing cloud data security through healthcare data. The first step in the input selection procedure is to use a healthcare dataset. Following data selection, the Paillier methodology is used to encrypt the input. The encoded health data were then stored in cloud environments, where they provided better read-write storage operations. The Paillier method applies data decryption to recover data from the cloud. Healthcare data in a cloud environment will be securely and privately managed using the paillier technique. RNN classifier is employed in healthcare diagnosis to categorize and forecast a patient's disease, after which the diagnosis is communicated to the patient and physician. The proposed work uses Python software, and a comparative analysis is conducted. In conclusion, the RNN designed for disease prediction yields the highest accuracy (96.4%), with a better performance matrix in the healthcare field.

## References


[1] Asad Abbas et al., "Blockchain-Assisted Secured Data Management Framework for Health Information Analysis Based on Internet of Medical Things," *Personal and ubiquitous computing*, vol. 28, no. 1, pp. 59-72, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[2] P. Blessed Prince, and S. P. Jeno Lovesum, "Privacy Enforced Access Control Model for Secured Data Handling in Cloud-Based Pervasive Health Care System," *SN Computer Science*, vol. 1, no. 5, pp. 239, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[3] G. Muneeswari et al., "Self-Diagnosis Platform Via IOT-based Privacy Preserving Medical Data," *Measurement: Sensors*, vol. 25, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] Lidia Ogiela, Marek R. Ogiela, and Hoon Ko, "Intelligent Data Management and Security in Cloud Computing," *Sensors*, vol. 20, no. 12, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[5] J. Deepika, C. Rajan, and T. Senthil, "Security and Privacy of Cloud-and IOT-Based Medical Image Diagnosis Using Fuzzy Convolutional Neural Network," *Computational Intelligence and Neuroscience*, pp. 1-17, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[6] Ali I. Siam et al., "Secure Health Monitoring Communication Systems Based on IOT and Cloud Computing for Medical Emergency Applications," *Computational Intelligence and Neuroscience*, vol. 2021, no. 1, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[7] P. Chinnasamy et al., "Efficient Data Security Using Hybrid Cryptography on Cloud Computing," *In Inventive Communication and Computational Technologies: Proceedings of ICICCT*, Springer, Singapore, pp. 537-547, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[8] Feras M. Awaysheh et al., "Security by Design for Big Data Frameworks over Cloud Computing," *IEEE Transactions on Engineering Management*, vol. 69, no. 6, pp. 3676-3693, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[9] Muhammad Tahir et al., "CryptoGA: a Cryptosystem Based on Genetic Algorithm for Cloud Data Security," *Cluster Computing*, vol. 24, no. 2, pp. 739-752, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[10] Samira Akhbarifar et al., "A Secure Remote Health Monitoring Model for Early Disease Diagnosis in Cloud-Based IOT Environment," *Personal and Ubiquitous Computing*, vol. 27, no. 3, pp. 697-713, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] M. Mehrtak et al., "Security Challenges and Solutions Using Healthcare Cloud Computing," *Journal of medicine and life*, vol. 14, no. 4, pp. 448, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[12] K. Suresha, and P. Vijaya Karthick, "Enhancing Data Security in Cloud Computing Using Threshold Cryptography Technique," *Advances in Cybernetics, Cognition, and Machine Learning for Communication Technologies*, pp. 231-242, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[13] Javad Pool et al., "Systematic Analysis of Failures in Protecting Personal Health Data: A Scoping Review," *International Journal of Information Management*, vol. 1, no. 74, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[14] Maryam Shabbir et al., "Enhancing Security of Health Information Using Modular Encryption Standard in Mobile Cloud Computing," *IEEE Access*, vol. 9, pp. 8820-8834, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[15] Fursan Thabit et al., "A New Lightweight Cryptographic Algorithm for Enhancing Data Security in Cloud Computing," *Global Transitions Proceedings*, vol. 2, no. 1, pp. 91-99, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[16] Mohan Naik Ramachandra et al., "An Efficient and Secure Big Data Storage in Cloud Environment by Using Triple Data Encryption Standard," *Big Data and Cognitive Computing*, vol. 6, no. 4, pp. 1-20, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[17] Lin Teng et al., "A Modified Advanced Encryption Standard for Data Security," *International Journal of Network Security*, vol. 22, no. 1, pp. 112-117, 2020. [Google Scholar] [Publisher Link]

[18] Alireza Souri et al., "A New Machine Learning-Based Healthcare Monitoring Model for Student's Condition Diagnosis in Internet of Things Environment," *Soft Computing*, vol. 24, no. 22, pp. 17111-17121, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[19] Ankita Anand et al., "An Efficient CNN-Based Deep Learning Model to Detect Malware Attacks (CNN-DMA) in 5G-IOT Healthcare Applications," *Sensors*, vol. 21, no. 19, pp.1-23, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[20] K.V. Praveen et al., "Deep Learning Based Intelligent and Sustainable Smart Healthcare Application in Cloud-Centric IOT," *Computers, Materials & Continua*, vol. 66, no. 2, pp. 1987-2003, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[21] Dhirendra K.R. Shukla, Vijay K.R. Dwivedi, and Munesh C. Trivedi, "Encryption Algorithm in Cloud Computing," *Materials Today: Proceedings*, vol. 37, pp. 1869-1875, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[22] Alabi Orobosade et al., "Cloud Application Security Using Hybrid Encryption," *Communications on Applied Electronics*, vol. 7, no. 33, pp. 25-31, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[23] Prabal Verma, Sandeep K. Sood, and Sheetal Kalra, "Cloud-Centric IoT Based Student Healthcare Monitoring Framework," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, no. 5, pp. 1293-1309, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[24] Greeshmanth Ch. Rupa, and Mohd Asif Shah, "Novel Secure Data Protection Scheme Using Martino Homomorphic Encryption," *Journal of Cloud Computing*, vol. 12, no. 1, 2023. [CrossRef] [Google Scholar] [Publisher Link]