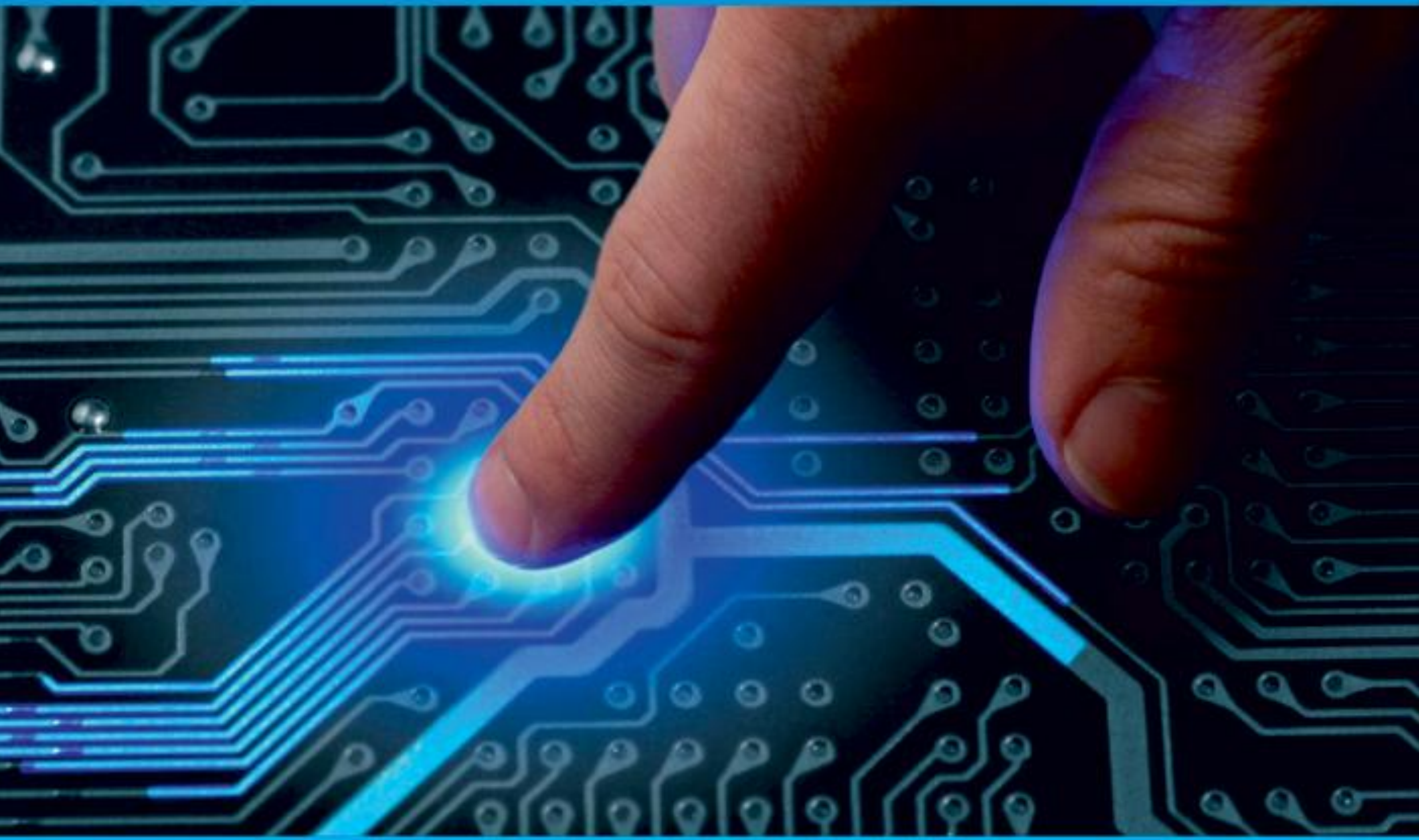
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 7, July 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

A Multiobjective Privacy Preservation Model Using Modified Whale Optimization

Muthulakshmi.K, Krishnaveni.R, Akshaya.V, Durga.B, Akshaya Gowri.C

Professor, Dept. of I.T., Panimalar Engineering College, Poonamallee, Chennai, India

UG Student, Dept. of I.T., Panimalar Engineering College, Poonamallee, Chennai, India

UG Student, Dept. of I.T., Panimalar Engineering College, Poonamallee, Chennai, India

UG Student, Dept. of I.T., Panimalar Engineering College, Poonamallee, Chennai, India

UG Student, Dept. of I.T., Panimalar Engineering College, Poonamallee, Chennai, India

ABSTRACT: This project focuses on safely securing the patient's medical records,using two fish encryption algorithm, modified whale optimization and convolution neutral network methods.Here the medical records are encrypted by two fish encryption algorithm employing a key generated by modified whale optimization algorithm and disease classification is completed by the Random forest classification algorithm.

KEYWORDS: IDE-Integrated development environment, Random Forest algorithm,Twofish encryption algorithm, modified whale optimization algorithm

I. Introduction

The broad application of artificial intelligence techniques in medicine is currently hindered by limited dataset availability for algorithm training and validation, due to the absence of standardized electronic medic al records, and strict legal and ethical requirements to protect patient privacy. In medical imaging, harmonized data exchange formats such as Digital Imaging and Communication in Medicine and electronic data storage are the standard, partially addressingthe first issue, but the requirements for privacy preservation are equally strict. To prevent patient privacy compromise while promoting scientific research on large datasets that aims to improve patient care, the implementationoftechnicalsolutionsto simultaneously address the demands for data protection and utilization is mandatory. In this project the medical data is from the patient which is encrypted with the two fish encryption algorithm and stored in the cloud server, the data from the cloud is decrypted with the help of key from modified whale optimization and then the decrypted data are classified with the Random forest algorithm,classification will determine whether the person has heart disease or not.

II. Related work

* Sandeep Pirbhulal et al The name of the paper Sandeep Pirubhlal et al was published within the year 2017. the most objective of this paper is to guard medical information from external threats.This research aims to guard medical information from external threats with the consumption of less possible resources of lowpowered medical devices. Here, the MLbased biometric security framework is proposed during which features are extracted from Electrocardiogram (ECG) signals for the training phase.
* Alfon et al The paper Alfon et al was published within the year 2018 .The main objective of this paper is to process the study of patient's health condition and knowledge using Deep Learning algorithms.To affect increasing volume of medical data, deep learning is incorporated into IoMT, which provides radical innovations in medical image processing, disease diagnosing, medical big data analysis and pathbreaking medical applications.
* MohamedElhoseny et al The paper Mohamed Elhoseny et al was published within the year 2019.The main objective of this paper is to supply a hybrid security model for securing the diagnostic text data in medical images and is made employing a combination of Advanced Encryption Standard, Rivest Shamir, and Adleman algorithms.
* Deshmukh The paper Deshmukh was published within the year 2017.The main objective of this paper is to style cloud security within the EHR for Indian healthcare services. It suggests the frame work for storing the health records by using double data storage strategy and authorized by key control scheme. Allows patients and physicians to access the health records.

* An et al The paper An et al was published within the year 2015.The main objective of this paper is to supply an adaptive quality of service (QoS) computation for medical processing in intelligent healthcare applications. Provides service through mobile by sending the patient coronary failure sign on to the doctor using remote protocol.

III. PROPOSED ALGORITHM

The present system makes use of two fish encryption algorithm modified whale optimization algorithm and convolution neural network (classification algorithm) that helps in encrypting the info , selecting the simplest optimal key required for encryption and classifying the patient data.Random forest algorithm examines the patient's report and classifies the health condition. The performance of the suggested method is set in terms of accuracy, time and memory utilization.

IV. MODULE DESCRIPTION

A. MODIFIED WHALE OPTIMIZATION

Used to determine/generate the optimized key from a cluster of dataset.

In order to find the best key it under goes the following stages:

1. ***Encircling prey***- It recognizes the location of the best search agent(key) and encircles them and tries to update their positions towards the best search agent.
2. ***Bubble net attacking method-***

- ***Shrinking encircling mechanism:*** Minimizes/shrinks the range of the search agent to the best search agent's position and encircles them.
- ***Spiral updating position:*** The search agent searches for the key within the shrinking circle, similar to the humpback whales that swim around the prey within the shrinking circle in a spiral-shaped path simultaneously

3. ***Search for prey***-we randomly choose a search agent instead of the best search agent.At each and every iteration the search agents update their positions thus, obtaining the best search agent (key) so far.

B. TWO FISH ALGORITHM

The Two fish may be a sort of block cipher that creates use of a key size of 128, 192 or 256 bits and a plaintext of 128 bits. The two words on the left are used as input to the g functions after the rotation by 8 bits of 1 of them and it consists of 4 byte wide key dependent sboxes, followed by a linear mixing step supported the MDS matrix.The results of two g functions are combined using pseudo Hadamard transform (PHT), by adding two keywords .One of the words on the proper is rotated by bit then both of them are XOR ed in to the result on the left.The left and right halves are swapped for subsequent round. After 16 rounds, the swap of the last round is reserved, and therefore the four words are XOR ed with four more key words to procedure the cipher text.

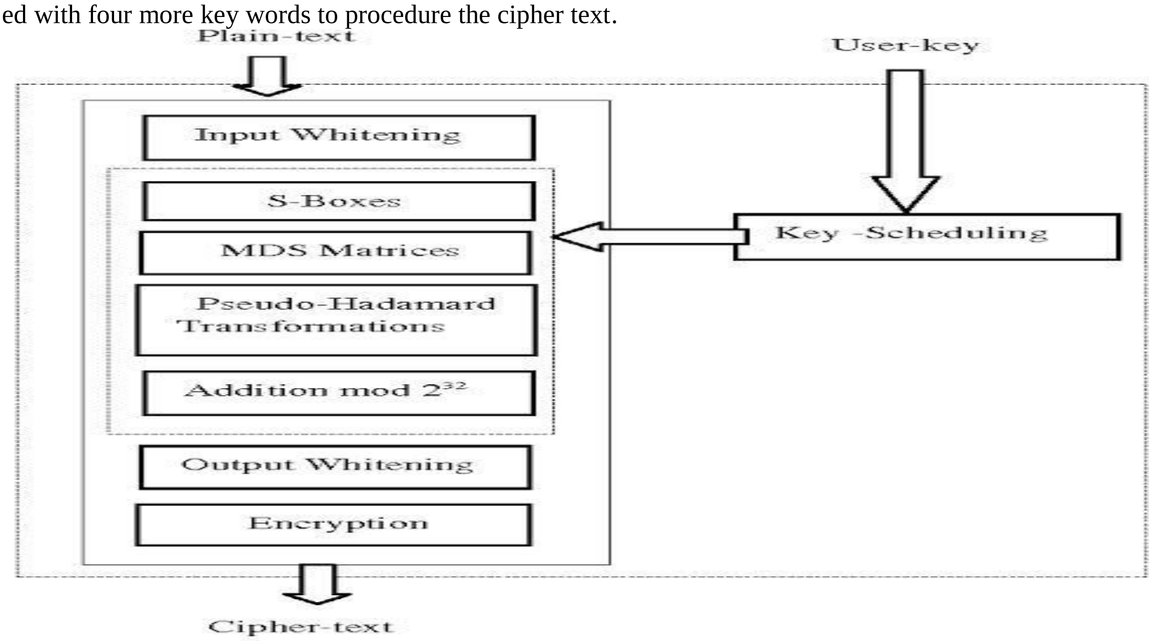


Fig.1. Two fish encryption algorithm

C. RANDOM FOREST:

Random Forest is a powerful and versatile **supervised machine learning algorithm** made up of decision trees Random Forest is used for both classification and regression. Here we used Random Forest algorithm to classify whether the person have heart disease or not.The train and test data are taken from the input dataset and random forest classifier performs best when n estimator is 120 , Seaborn and pyplot used for plotting confusion matrix and we write the target and prediction output in a csv file.

V. RESULTS

There are 4 modules,Encrypt,decrypt,upload and classification.On selecting the Encrypt button, choose a medical dataset/medical data file, click encrypt option. The medical dataset will be encrypted. Using the upload button, upload the encrypted file to the database.On selecting the Decrypt button, choose a medical dataset/medical data file that is already encrypted, and select the decrypt option. The medical dataset will be decrypted. Using the classification button, the dataset willbe classified based on the disease and its attributes.

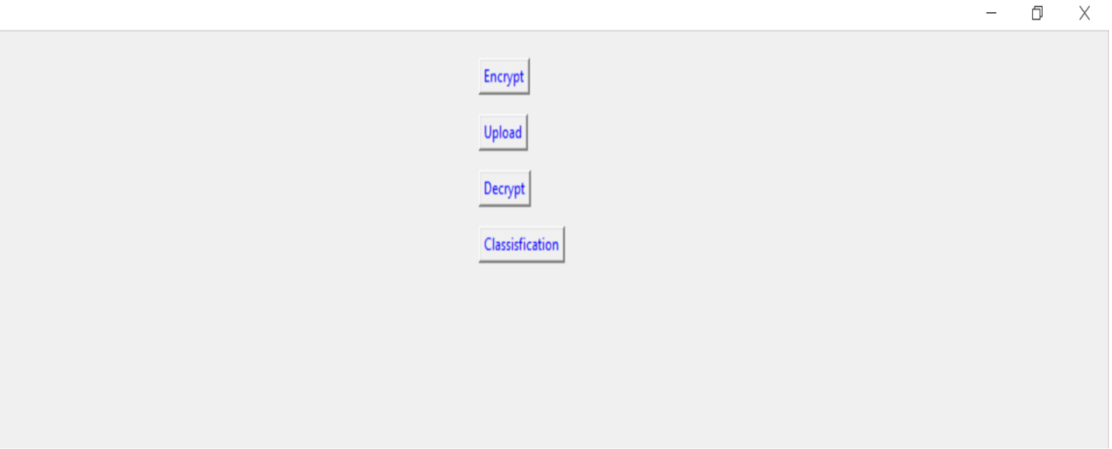
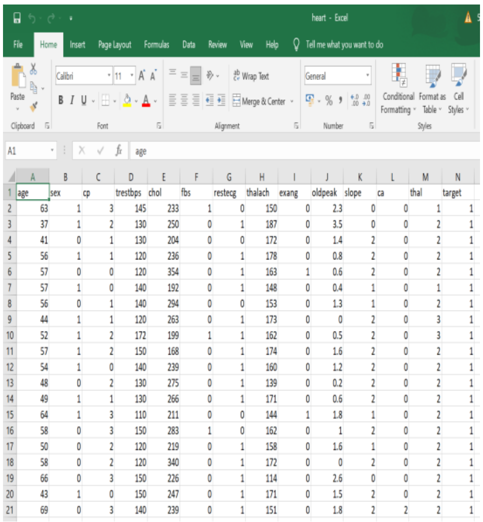
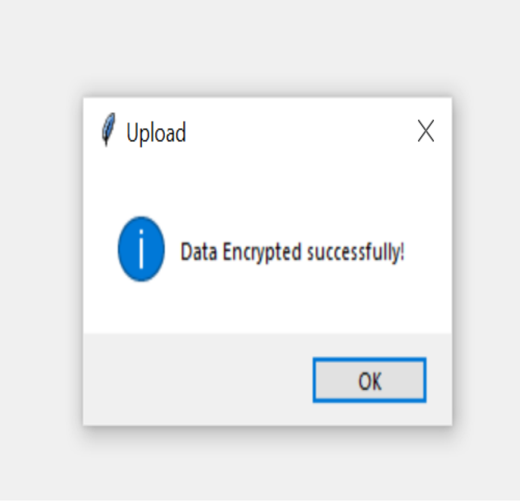


Fig.2. Main page



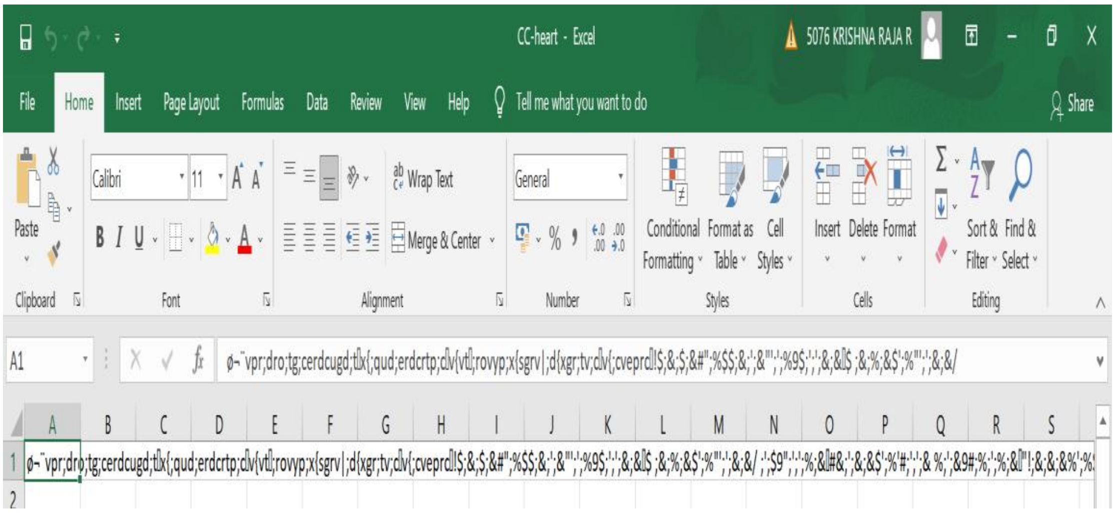
	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	age	sex	cp	trestbps	chol	fbs	restecg	thalach	exang	oldpeak	slope	ca	thal	target
2	63	1	3	145	233	1	0	150	0	2.3	0	0	1	1
3	37	1	2	130	250	0	1	187	0	3.5	0	0	2	1
4	41	0	1	130	204	0	0	172	0	1.4	2	0	2	1
5	56	1	1	120	236	0	1	178	0	0.8	2	0	2	1
6	57	0	0	120	354	0	1	163	1	0.6	2	0	2	1
7	57	1	0	140	192	0	1	148	0	0.4	1	0	1	1
8	56	0	1	140	294	0	0	153	0	1.3	1	0	2	1
9	44	1	1	120	263	0	1	173	0	0	2	0	3	1
10	52	1	2	172	199	1	1	162	0	0.5	2	0	3	1
11	57	1	2	150	168	0	1	174	0	1.6	2	0	2	1
12	54	1	0	140	239	0	1	160	0	1.2	2	0	2	1
13	48	0	2	130	275	0	1	139	0	0.2	2	0	2	1
14	49	1	1	130	266	0	1	171	0	0.6	2	0	2	1
15	64	1	3	110	211	0	0	144	1	1.8	1	0	2	1
16	58	0	3	150	283	1	0	162	0	1	2	0	2	1
17	50	0	2	120	219	0	1	158	0	1.6	1	0	2	1
18	58	0	2	120	340	0	1	172	0	0	2	0	2	1
19	66	0	3	150	226	0	1	114	0	2.6	0	0	2	1
20	43	1	0	150	247	0	1	171	0	1.5	2	0	2	1
21	69	0	3	140	239	0	1	151	0	1.8	2	2	2	1

Fig.3. Input dataset



Data Encrypted successfully!

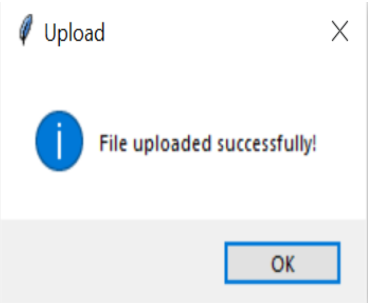
Fig .4. Encryption Pop Up



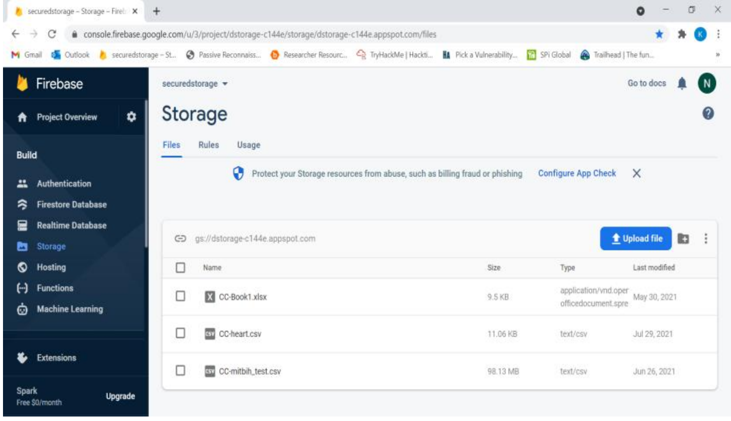
```
ø¬¨vpr;dro;tg;cerdcugd;tl̈x{;qud;erdcrtp;clv{vt;rovyp;x{sgrv|;d{xgr;tv;clv{;cveprcl!$;&;$;&#";%$$;&;';&"';';%9$;';';&;&l$ ;&;%;&$';%"';';&;&/
```

```
ø¬¨vpr;dro;tg;cerdcugd;tl̈x{;qud;erdcrtp;clv{vt;rovyp;x{sgrv|;d{xgr;tv;clv{;cveprcl!$;&;$;&#";%$$;&;';&"';';%9$;';';&;&l$ ;&;%;&$';%"';';&;&/ ;';$9";';';%;&l#&;';&;&$';%'#;';';& %;';&9#;%;';%;&l"!;&;&;&%';%
```

Fig 5 Encrypted Data



File uploaded successfully!



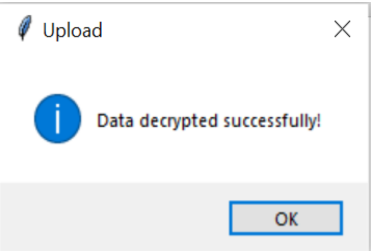
Protect your Storage resources from abuse, such as billing fraud or phishing

gs://dstorage-c144e.appspot.com

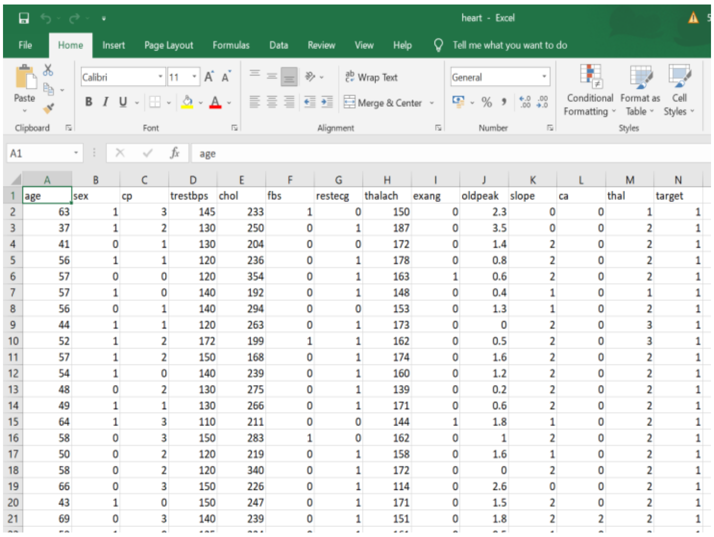
Name	Size	Type	Last modified
CC-Book1.xlsx	9.5 KB	application/vnd.oper officedocument.spre	May 30, 2021
CC-heart.csv	11.06 KB	text/csv	Jul 29, 2021
CC-mitbih_test.csv	98.13 MB	text/csv	Jun 26, 2021

Fig 6 File Upload pop up

Fig 7 Firebase Storage



Data decrypted successfully!



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	age	sex	cp	trestbps	chol	fbs	restecg	thalach	exang	oldpeak	slope	ca	thal	target
2	63	1	3	145	233	1	0	150	0	2.3	0	0	1	1
3	37	1	2	130	250	0	1	187	0	3.5	0	0	2	1
4	41	0	1	130	204	0	0	172	0	1.4	2	0	2	1
5	56	1	1	120	236	0	1	178	0	0.8	2	0	2	1
6	57	0	0	120	354	0	1	163	1	0.6	2	0	2	1
7	57	1	0	140	192	0	1	148	0	0.4	1	0	1	1
8	56	0	1	140	294	0	0	153	0	1.3	1	0	2	1
9	44	1	1	120	263	0	1	173	0	0	2	0	3	1
10	52	1	2	172	199	1	1	162	0	0.5	2	0	3	1
11	57	1	2	150	168	0	1	174	0	1.6	2	0	2	1
12	54	1	0	140	239	0	1	160	0	1.2	2	0	2	1
13	48	0	2	130	275	0	1	139	0	0.2	2	0	2	1
14	49	1	1	130	266	0	1	171	0	0.6	2	0	2	1
15	64	1	3	110	211	0	0	144	1	1.8	1	0	2	1
16	58	0	3	150	283	1	0	162	0	1	2	0	2	1
17	50	0	2	120	219	0	1	158	0	1.6	1	0	2	1
18	58	0	2	120	340	0	1	172	0	0	2	0	2	1
19	66	0	3	150	226	0	1	114	0	2.6	0	0	2	1
20	43	1	0	150	247	0	1	171	0	1.5	2	0	2	1
21	69	0	3	140	239	0	1	151	0	1.8	2	2	2	1

Fig 8 Decryption Pop Up

Fig 9 Original Data After Decryption

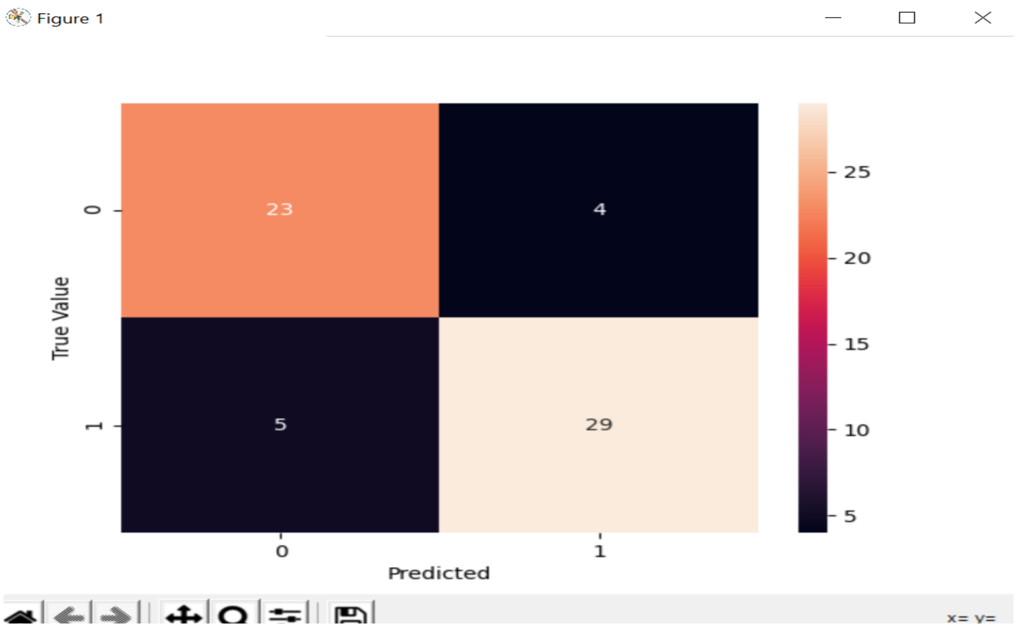
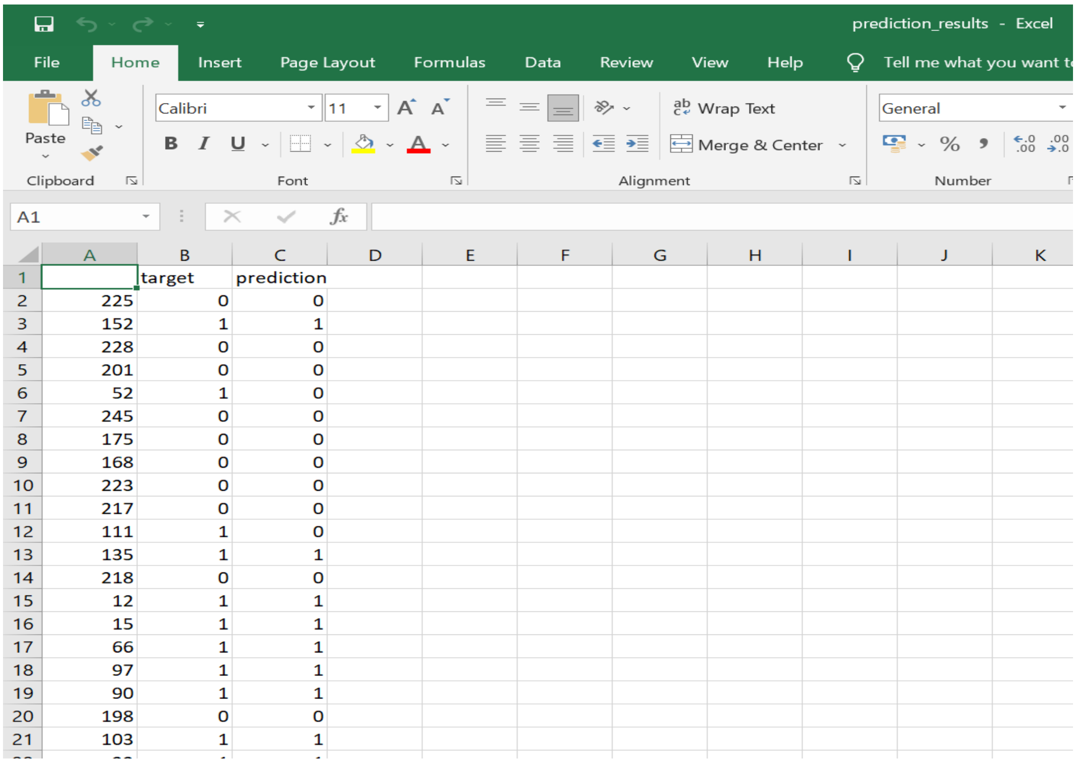


Fig 10 Confusion Matrix



	A	B	C
1		target	prediction
2	225	0	0
3	152	1	1
4	228	0	0
5	201	0	0
6	52	1	0
7	245	0	0
8	175	0	0
9	168	0	0
10	223	0	0
11	217	0	0
12	111	1	0
13	135	1	1
14	218	0	0
15	12	1	1
16	15	1	1
17	66	1	1
18	97	1	1
19	90	1	1
20	198	0	0
21	103	1	1

Fig 11 Classification Output

VI. Conclusion

Hence the proposed system uses Modified Whale Optimization algorithm to seek out the optimal key, twofish encryption algorithm to encrypt the medical records,and Random Forest algorithm, to classify the medical records and store the info securely in cloud. This encrypted are often retrieved within the decrypted format using the optimal key thus securing the patient’s medical data.

REFERENCES

1. Masdari M, ValiKardan S, Shahi Z, Azar SI (2016) Towards workflow scheduling in cloud computing: a comprehensive analysis.
2. Deshmukh P (2017) Design of cloud security within the EHR for Indian healthcare services. J King Saud Univ-Comput Inform Sci 29(3):281–287
3. ElGazzar R, Hustad E, Olsen DH (2016) Understanding cloud computing adoption issues: a Delphi study approach. J SystSoftw 118:64–84
4. Aldeen YAAS, Salleh M, Aljeroudi Y (2016) An innovative privacy preserving technique for incremental datasets on cloud Page 1 computing. J Biomed Informat 62:107–116
5. Ali O, Shrestha A, Soar J, Wamba SF (2018) Cloud computingenabled healthcare opportunities, issues, and applications: a scientific review. Int J Inform Manag 43:146–158
6. Jin Y, Liu Y, Si W (2020) Editorial for the special issue on Intelligent agent distributed signal processing for IoT. J Ambient Intell Hum Comput 11:447– 449.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details