SECURITY FOR ELECTRONIC HEALTH RECORD BASED ON ATTRIBUTE USING BLOCK-CHAIN TECHNOLOGY

Dr. Suvarna Nandyal*[1], Sanjana S Nazare[2]

[1]Professor at Department of Computer Science, PDA College of Engineering, Kalaburagi, Karnataka, India
[2]PG student at Department of Computer Science, PDA College of Engineering, Kalaburagi, Karnataka, India

---***---

Abstract - *Hospitals, rather than patients, have complete authority over Electronic Health Records (EHRs) of the patients, making the process of obtaining medical consultation from any other hospitals a troublesome job. An attribute-based signature technique having more than one authority is offered in order to ensure the authenticity of EHRs encoded in block chain. A patient recommends a response based on the attribute while giving no details besides the proof that he has verified to it. Moreover, various parties without a credible solitary or central authority creates and disseminates the patient's public or private keys, avoiding the lockup issue and conforming to the blockchain's distributed data storage method. Therefore the authority of managing the EHRs of the patients will be in their own control rather than hospital authorities. The RSA algorithm and Attribute Based Encryption algorithm (ABE algorithm) methods are used here. In this work patients details with few attributes such as Name, location, Contact, Age etc are considered. This convention prevents collusion threats by corrupted authorities through exchanging the secret pseudorandom function seeds amongst them. For securing data RSA algorithm and ABE algorithm is applied together forming a hybrid block chain. The Encrypted/Decrypted data provides high level security for healthcare system using Hybrid Blockchain technology compared to client-server network used in World Wide Web for the purpose of running database. The application of block chain technology together with RSA and ABE algorithms can be used in hospitals for maintaining the EHRs of the patients securely.*

***Key Words*: Attribute based encryption (ABE), RSA algorithm, Electronic health records (EHR) interface, Hybrid block chain, public and private keys.**

1. INTRODUCTION

Blockchain is a novel form of innovation to be an efficient, cost-effective, dependable, and secure system for performing and documenting transactions without the requirement of a middle person. Due to sheer threats to information protection or the leakage of personal data of patients through data transmission, several limitations have traditionally been imposed on exchanging big EHRs. A database or block chain is a sort of digital ledger. Database content is usually organized in the style of table to make browsing and sorting for precise data easier. Hence there will be no distinction between databases versus storing data in a spreadsheet. The purpose of spreadsheets is to reserve and retrieve minimal quantity of data for a single user or a small group of people. On the other hand a database is built to keep far bigger volumes of data which can be collected, processed, and altered by multiple users at the same time. Health records are required to be maintained by the authorized users only other than hospitals when it comes to block chain in healthcare. Patient-centered interconnectivity varies from traditional hospital interoperability in this regard. Lot of difficulties arise from hospital system integration like data standards, security, and privacy in addition to technology-related issues such as governance, incentives, scalability and speed. Hybrid block chain technology is used which incorporates components of private as well as public block chain. Hybrid block chain is created by combining the RSA algorithm and Attribute-based encryption algorithm. Medical records maintained in such a manner will assist in development of a smart healthcare system.

2. LITERATURE SURVEY

[1] Peng Jiang et al in 2020 discovered the *Search chain*, a blockchain-based keyword search system. It empowers absent pursuit over an approved watchword set in the decentralized stockpiling. They have applied oblivious keyword search (OKS) and ordered multi marks (OMS) to introduce a Search chain convention, which accomplishes absent distributed recovery with request saving exchange.

[2] A. A. Siyal et al. developed a fundamental outline of Blockchain innovation, trailed by a clinical application (Med Blocks). This innovation is utilized in the application, which means to work on the proficiency of the clinical calling. The objective of this examination is to show how this innovation has colossal guarantee and how it will significantly change how data is transmitted, communicated, and secured.

[3] W. J. Gordon et al. demonstrated interoperability in medical services has generally been engaged around information trade between business elements, for instance, unique clinic frameworks. Patient-focused interoperability carries with it new difficulties and necessities around security and protection, innovation, impetuses, and administration that should be addressed for this kind of information sharing to prevail at scale.

[4] P. Zhang et al. discovered a safe and adaptable information sharing fundamental for collaborative clinical dynamic. Applied blockchain innovation to clinical

information partaking with regards to specialized prerequisites characterized in the "Shared Nationwide Interoperability Roadmap" from the Office of the National Coordinator for Health Information Technology (ONC).

[5] Y. Sakai et al. offered succour to wide class of predicates, like the class of subjective circuits, with pragmatic productivity from a straightforward supposition, since these three viewpoints decide the value of the plan. They have utilized a trait based mark plot which permits us to utilize a discretionary circuit as the predicate with down to earth proficiency from the symmetric outer Diffie-Hellman supposition.

[6] A. Boonstra et al. proposed the EHR frameworks that are expected to affect the presentation of clinics; their execution is a perplexing endeavour. This orderly survey uncovers purposes behind this intricacy and presents a system of 19 intercessions that can assist with beating average issues in EHR execution. This structure can work as a source of perspective for implementers in creating powerful EHR execution techniques for medical clinics.

[7] T. Okamoto et al. presented a completely secure (versatile predicate remarkable and private) attribute based signature (ABS) conspire in the standard model. The security of the proposed ABS conspire is demonstrated under standard suspicions, the decisional linear (DLIN) supposition and the presence of collision resistant (CR) hash capacities.

[8] K. D. Mandl et al. developed a patient's clinical records are by and large divided across numerous treatment locales, representing a deterrent to clinical consideration, exploration, and general wellbeing endeavours. Here they proposed online clinical record frameworks could be created and utilized clinically.

3. PROPOSED METHODOLOGY

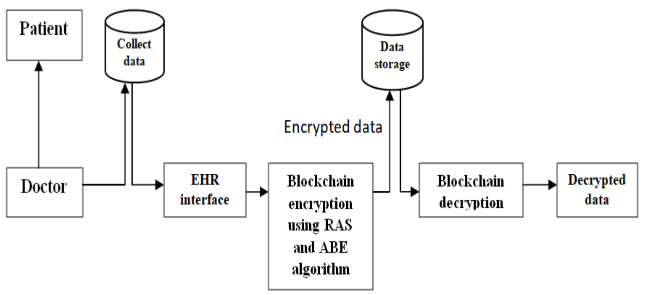


Figure 1.System design for proposed methodology

In [Figure 1], the doctor gains patients information which is to be stored, then for the privacy and security purpose that is encrypted and secured through the electronic health record, also while encrypting data its private key and public key is generated. Further when it is required the data is decrypted and used. The system design contains the following:

- **Patient:** Here the patient delivers the information to the doctor required for the appointment to be scheduled.
- **Doctor:** The doctor stores the information received from the patient and assigns the particular appointment serially.
- **Collect data:** Here, the data is collected by doctor and upload in the electronic health record interface.
- **EHR interface:** The data collected is uploaded then have to choose the particular column or part to encrypt it and location to store it after encryption.
- **Blockchain encryption:** Here the encryption of the selected data takes place.
- **Data storage:** After the encryption the produced encrypted data is stored in the location which we have selected so far while the encryption process.
- **Blockchain decryption:** The data which is produced after the encryption process will further undergoes the decryption process.
- **Decrypted data:** The data which undergoes decryption process, produces the decrypted data which can be used by the doctor as and when required.

Here it is proposed that the data or the patient details which is to be stored maintains the security, since converting it to the cipher text by generating the keys:

- Public key
- Private key

These keys are generated using the RSA algorithm (Rivest-shamir-adleman algorithm) and for the encryption process and decryption process, attribute based encryption algorithm (ABE algorithm).Using cryptography, a system for patient experiences from admission to discharge with healthcare trends has been developed. Cryptography is necessary for the chosen problem statement as it dynamically deals with uncommon or abnormal conditions/challenges. To encrypt or decrypt the data anaconda prompt is used to reach the electronic health record system servers.

- Public Blockchain: Public Blockchain offer a totally computational model where each part can see the Blockchain material and partake in the agreement cycle (for example Bitcoin and Ethereum).
- Private Blockchain: The private blockchain are planned mostly for single endeavor arrangements

and they are utilized to oversee information trades happening between any people or various divisions. The security is one of the significant viewpoints considered because of which each individual member should get the organization together with authorization gave and will be viewed as a real client.

The RSA algorithm

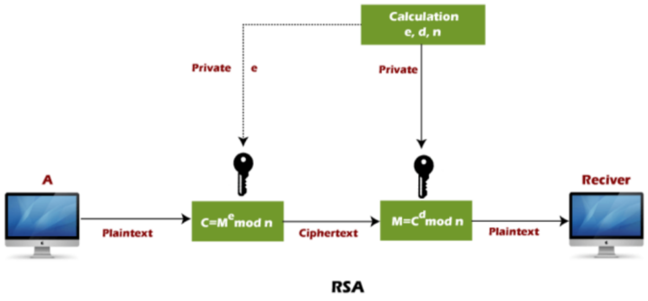


Figure 2.Representing RSA algorithm

[Figure 2] The RSA (Rivest–Shamir–Adleman) is a computation used by current PCs to encode and decode messages. The RSA computation is a set-up of cryptographic estimations that are used for unequivocal security organizations or purposes.

Key Generation

Select p, q	p and q both prime	
Calculate n= p x q		
Calculate	$\emptyset(n)$	
Select integer e	gcd	$(\emptyset(n), e) = 1$
Calculate d	e^{-1} mod	
Public key	KU = {e, n}	
Private Key	KR = {d, n}	

Attribute based Encryption algorithm

We have a few phases for the encryption and decryption measure:

- **Setup:** The arrangement calculation takes no info other than the understood security boundary.
- **Encrypt:** The encryption calculation takes as info the public boundaries, a message, and an entrance structure over the universe of qualities. The calculation will encode and create a code message with the end goal that solitary a client that has a bunch of characteristics that fulfills the entrance construction will actually want to unscramble the message. We will expect that the code text C certainly contains.

Encryption

Plain text	$M<n$
Cipher text	$C = M^e \pmod n$

- **Decrypt:** The decryption calculation takes as information the public boundaries, a code text, which contains an entrance strategy, and a private key, which is a private key for a bunch of characteristics. Assuming the arrangement of characteristics fulfills the entrance structure; the calculation will decode the code message and return a message.

Decryption

Cipher text	C
Plain text	$M = C^d \pmod n$

Blockchain innovation helps with the administration of electronic wellbeing records. An extraordinary key framework is allocated to every element in the framework. The information is encoded with a key, taking into consideration a safer and effective stockpiling strategy. There is no special case for anybody, including patients, to have a brief confirmation. This is on the grounds that each piece of information that is kept creates its own public and hidden keys. Something else, the information can be manufactured or changed by outsiders. The organization of wellbeing information, which may be improved by the possibility to incorporate heterogeneous frameworks and lift the precision of Electronic Health Records (EHRs), ought to be the accentuation of medical care change.

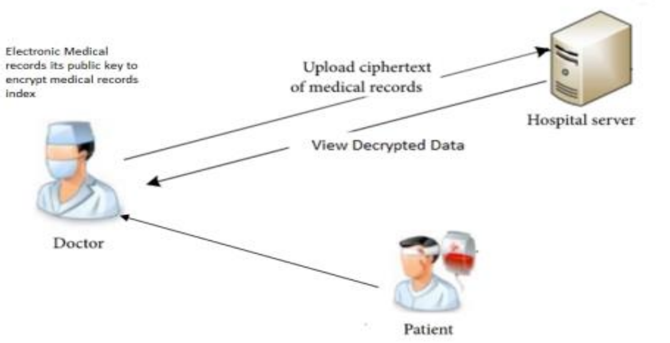

Electronic Medical records its public key to encrypt medical records index
Upload ciphertext of medical records
Hospital server
View Decrypted Data
Doctor
Patient

Figure 3.Pictorial representation of the methodological process which includes block chain technology

Here in [Figure 3] the patient details are collected by doctor and it is encrypted, then stored in server. The doctor can decrypt and view the data back when it is required.

- **Patient**: Appointments of patients are registered and appointment number is assigned to each patient.
- **Doctor**: Access the patient record and enters the patient complaint and responses of the patient in the software.
- **Hospital Server**: Application accepts the details entered by the doctor and generates a public n private key and converts pain data to encrypted cipher text and uploads to the hospital server. All the encrypted data can be decrypted by the authorized person and can view back the decrypted records.

4. IMPLEMENTATION

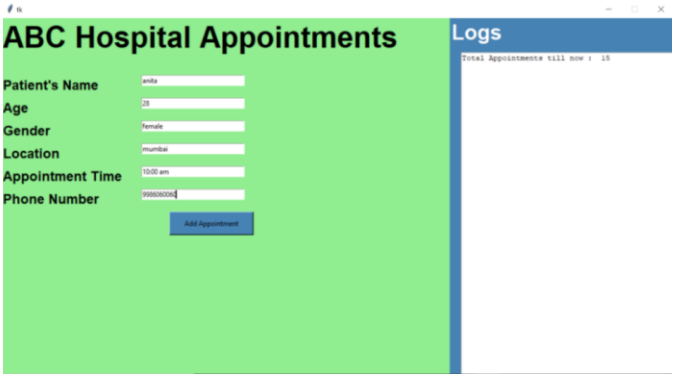
The process initiates with representing the sample patients information. As such it is an informative setup that is to be stored in the hospital records for the appointments noted in the particular date and time of the patient. Then the update page for the appointments represents which are stored and required some changes such as addition of data or deletion of some data that can be processed through it. Later it displays all the scheduled appointments which are stored in the hospital records serially with its particular serial number, name and along with the vocal voice behind.

The registration for new user and login is for the old users which have already been registered to enter the symptoms of the disease or diagnosis query form. The health record server represents to choose the file for the further encryption process, where the keys are generated before the encryption process. The encryption process representing in [Figure 9], to the particular chosen column from the data file for maintaining the data security of the patient's health record through EHR interface with the similar storage for each block. Then it displays the result or output.

After encrypting the particular chosen column that is METROMICRO column from the selected data set and its own public key and private key is formed each time before the encryption process. Here for encryption public key is used which is generated. The decryption of the file or the particular column that is the METROMICRO column which is already encrypted, also the location should be selected for storing the decrypted file and before encryption were the earlier formed its own private key is used for decrypting the file. The final outcome is the decryption process for the selected file and column, here that is METROMICRO column to which the decryption is applied with the private key which is generated before encryption process. The data which is decrypted will be remained unchanged as the data which was before encrypting that data. Further the query diagnosis form includes the questions related to some kind of disease, also the confidence level of it and suggests the particular doctor for it. It also consists of the link where one can find details about that doctor, if need can scheduled an appointment.

5. RESULTS AND DISCUSSION

The exploratory outcomes and previews are been clarified with figures in the accompanying.



ABC Hospital Appointments

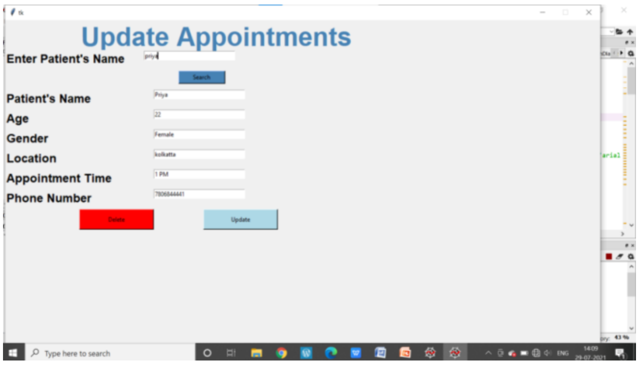
Patient's Name anita
Age 28
Gender female
Location mumbai
Appointment Time 10:00 am
Phone Number 9986060060

Logs

```
Total Appointments till now :  15
```

Figure 4.Patient's appointment form

[Figure 4] represents the patient's information as such it is a virtual setup that is to be stored in the hospital records for the appointments noted in the particular date and time of the patient.



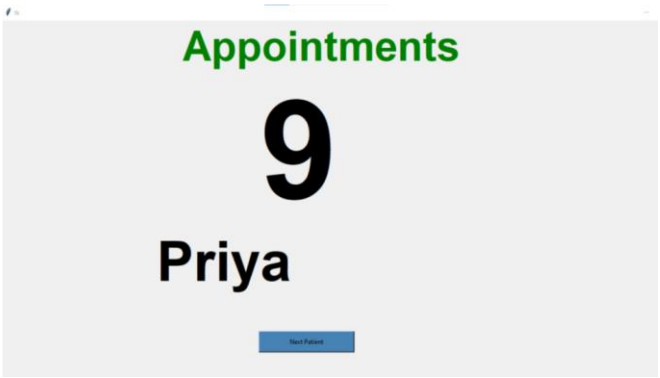
Update Appointments

Enter Patient's Name priya

Patient's Name Priya
Age 22
Gender Female
Location kolkatta
Appointment Time 1 PM
Phone Number 7806844441

Figure 5.Patient details update form

[Figure 5] represents the update page for the appointments which are stored and required some changes such as addition of data or deletion of some data that can be processed through it.



Appointments

9

Priya

Figure 6.Appointment Schedule

All the scheduled appointments are stored in the hospital records serially with its particular serial number, name and along with the vocal voice behind [Figure 6].

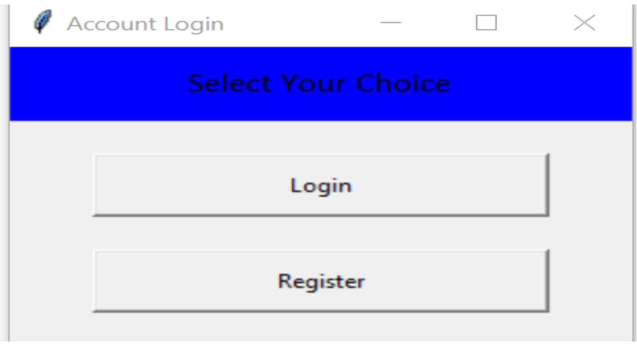
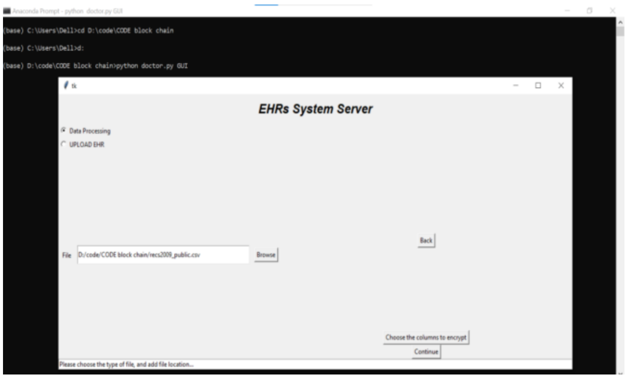


Figure 7.Registration/login page for users

[Figure 7] depicts the registration for new user and login for the old user which have already been registered to enter the symptoms of the disease or diagnosis query form.


Anaconda Prompt - python doctor.py GUI
tk
EHRs System Server
● Data Processing
○ UPLOAD EHR
Back
Browse
Choose the columns to encrypt
Continue

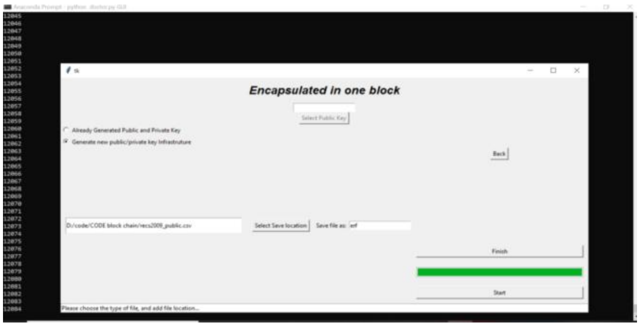
```
(base) C:\Users\Dell>cd D:\code\CODE block chain

(base) C:\Users\Dell>d:

(base) D:\code\CODE block chain>python doctor.py GUI
```

File: D:/code/CODE block chain/recs2009_public.csv

Please choose the type of file, and add file location...

Figure 8.Selecting the file to be encrypted

The health record server provides to select the file for further encryption process [Figure 8].


Anaconda Prompt - python doctor.py GUI
tk
Encapsulated in one block
Select Public Key
○ Already Generated Public and Private Key
● Generate new public/private key Infrastruture
Back
Select Save location
Finish
Start

```
12045
12046
12047
12048
12049
12050
12051
12052
12053
12054
12055
12056
12057
12058
12059
12060
12061
12062
12063
12064
12065
12066
12067
12068
12069
12070
12071
12072
12073
12074
12075
12076
12077
12078
12079
12080
12081
12082
12083
12084
```

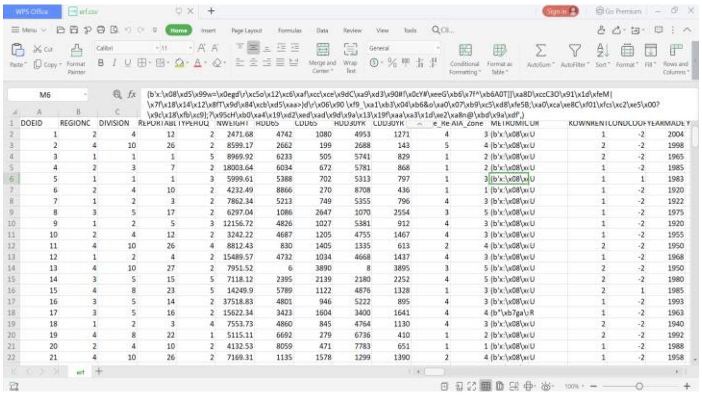
D:/code/CODE block chain/recs2009_public.csv

Save file as: erf

Please choose the type of file, and add file location...

Figure 9.Selecting the column and location to store the encrypted file

[Figure 9] represents the encryption process to the particular chosen column from the data file for maintaining the data security of the patient's health record through EHR interface with the similar storage for each block.



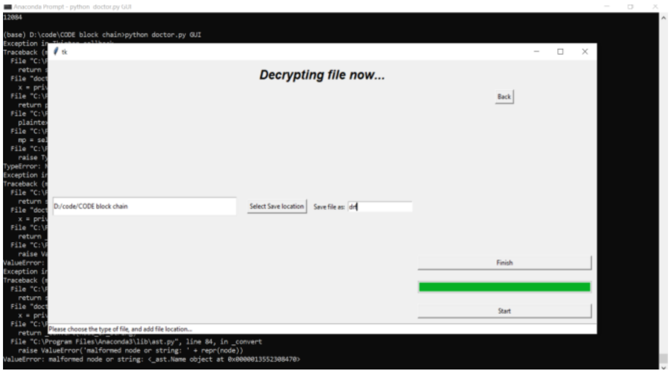
M6

```
(b'x:\x08\xd5\x99w=\x0egd'\r\xc5o\x12\xc6\xaf\xcc\xce\x9dC\xa9\xd3\x90#!\x0cY#\xeeG\xb6\x7f^\xb6A0T]]'\xa8D\xccC3O\x91\x1d\xfeM|
\x7f\x18\x14\x12\x8fT\x9d\x84\xcb\xd5\xaa>|d\r\x06\x90 \xf9_\xa1\xb3\x04\xb6&o\xa0\x07\xb9\xc5\xd8\xfe5B;\xa0\xca\xe8C\xf01\xfcs\xc2\xe5\x00?
\x9c\x18\xfb\xc9];?\x95cH\xb0\xa4\x19\xd2\xed\xad\x9d\x9a\x13\x19f\xaa\xa3\x1d\xe2\xa8n@\xbd\x9a\xdf',)
```

1	DOEID	REGIONC	DIVISION	REPORTABL	TYPEHUQ	NWEIGHT	HDD65	CDD65	HDD30YR	CDD30YR	e_Re	AIA_Zone	METROMIC	UR	KOWNRENT	CONDCOOF	YEARMADE Y
2	1	2	4	12	2	2471.68	4742	1080	4953	1271	4	3	(b'x:\x08\x	U	1	-2	2004
3	2	4	10	26	2	8599.17	2662	199	2688	143	5	4	(b'x:\x08\x	U	2	-2	1998
4	3	1	1	1	5	8969.92	6233	505	5741	829	1	2	(b'x:\x08\x	U	2	-2	1965
5	4	2	3	7	2	18003.64	6034	672	5781	868	1	2	(b'x:\x08\x	U	1	-2	1985
6	5	1	1	1	3	5999.61	5388	702	5313	797	1	3	(b'x:\x08\x	U	1	1	1983
7	6	2	4	10	2	4232.49	8866	270	8708	436	1	1	(b'x:\x08\x	U	1	-2	1920
8	7	1	2	3	2	7862.34	5213	749	5355	796	4	3	(b'x:\x08\x	U	1	-2	1922
9	8	3	5	17	2	6297.04	1086	2647	1070	2554	3	5	(b'x:\x08\x	U	1	-2	1975
10	9	1	2	5	3	12156.72	4826	1027	5381	912	4	3	(b'x:\x08\x	U	1	-2	1920
11	10	2	4	12	2	3242.22	4687	1205	4755	1467	4	3	(b'x:\x08\x	U	1	-2	1955
12	11	4	10	26	4	8812.43	830	1405	1335	613	2	4	(b'x:\x08\x	U	2	-2	1950
13	12	1	2	4	2	15489.57	4732	1034	4668	1437	4	3	(b'x:\x08\x	U	1	-2	1968
14	13	4	10	27	2	7951.52	6	3890	8	3895	3	5	(b'x:\x08\x	U	2	-2	1950
15	14	3	5	15	5	7118.12	2395	2139	2180	2252	4	5	(b'x:\x08\x	U	2	-2	1980
16	15	4	8	23	5	14249.9	5789	1122	4876	1328	1	3	(b'x:\x08\x	U	2	1	1985
17	16	3	5	14	2	37518.83	4801	946	5222	895	4	3	(b'x:\x08\x	U	1	-2	1993
18	17	3	5	16	2	15622.34	3423	1604	3400	1641	4	4	(b"\xb7ga\	R	1	-2	1963
19	18	1	2	3	4	7553.73	4860	845	4764	1130	4	3	(b'x:\x08\x	U	2	-2	1940
20	19	4	8	22	1	5115.11	6692	279	6736	410	1	2	(b'x:\x08\x	U	2	-2	1992
21	20	2	4	10	2	4132.53	8059	471	7783	651	1	1	(b'x:\x08\x	U	1	-2	1988
22	21	4	10	26	2	7169.31	1135	1578	1299	1390	2	4	(b'x:\x08\x	U	1	-2	1958

Figure 10.Result after encrypting the particular column from data file

[Figure 10] displays the result or output after encrypting the particular chosen column that is METROMICRO column from the selected data set and its own public key and private key is formed each time before the encryption process.



```
12084

(base) D:\code\CODE block chain>python doctor.py GUI
Exception in
Traceback (
  File "C:\
    return
  File "doc
    x = pri
  File "C:\
    return
  File "C:\
    plainte
  File "C:\
    mp = se
  File "C:\
    raise T
TypeError:
Exception in
Traceback (
  File "C:\
    return
  File "doc
    x = pri
  File "C:\
    return
  File "C:\
    raise V
ValueError:
Exception in
Traceback (
  File "C:\
    return
  File "doc
    x = pri
  File "C:\
    return
  File "C:\Program Files\Anaconda3\lib\ast.py", line 84, in _convert
    raise ValueError('malformed node or string: ' + repr(node))
ValueError: malformed node or string: <_ast.Name object at 0x0000013552308470>
```

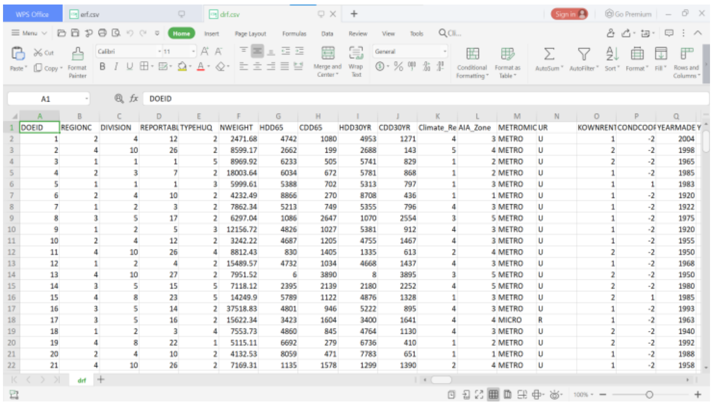
D:/code/CODE block chain

Save file as: drf

Please choose the type of file, and add file location...

Figure 11.Representing the decryption process

[Figure 11] shows the decryption of the file or the particular column that is the METROMICRO column which is already encrypted, also the location should be selected for storing the decrypted file and before encryption were the earlier formed its own private key is used for decrypting the file.

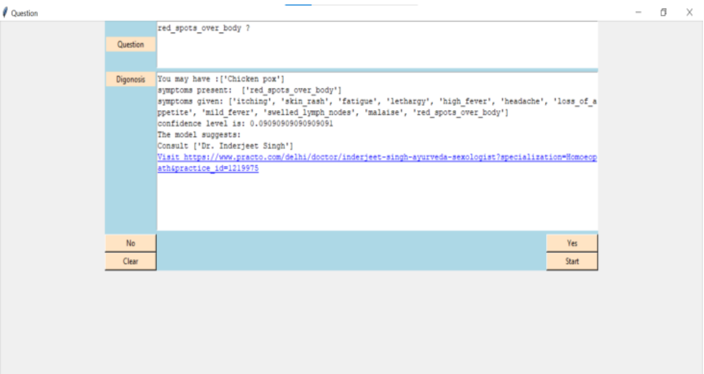


A1 DOEID

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	DOEID	REGIONC	DIVISION	REPORTABL	TYPEHUQ	NWEIGHT	HDD65	CDD65	HDD30YR	CDD30YR	Climate_Re	AIA_Zone	METROMIC	UR	KOWNRENT	CONDCOOF	YEARMADE Y
2	1	2	4	12	2	2471.68	4742	1080	4953	1271	4	3	METRO	U	1	-2	2004
3	2	4	10	26	2	8599.17	2662	199	2688	143	5	4	METRO	U	2	-2	1998
4	3	1	1	1	5	8969.92	6233	505	5741	829	1	2	METRO	U	2	-2	1965
5	4	2	3	7	2	18003.64	6034	672	5781	868	1	2	METRO	U	1	-2	1985
6	5	1	1	1	3	5999.61	5388	702	5313	797	1	3	METRO	U	1	1	1983
7	6	2	4	10	2	4232.49	8866	270	8708	436	1	1	METRO	U	1	-2	1920
8	7	1	2	3	2	7862.34	5213	749	5355	796	4	3	METRO	U	1	-2	1922
9	8	3	5	17	2	6297.04	1086	2647	1070	2554	3	5	METRO	U	1	-2	1975
10	9	1	2	5	3	12156.72	4826	1027	5381	912	4	3	METRO	U	1	-2	1920
11	10	2	4	12	2	3242.22	4687	1205	4755	1467	4	3	METRO	U	1	-2	1955
12	11	4	10	26	4	8812.43	830	1405	1335	613	2	4	METRO	U	2	-2	1950
13	12	1	2	4	2	15489.57	4732	1034	4668	1437	4	3	METRO	U	1	-2	1968
14	13	4	10	27	2	7951.52	6	3890	8	3895	3	5	METRO	U	2	-2	1950
15	14	3	5	15	5	7118.12	2395	2139	2180	2252	4	5	METRO	U	2	-2	1980
16	15	4	8	23	5	14249.9	5789	1122	4876	1328	1	3	METRO	U	2	1	1985
17	16	3	5	14	2	37518.83	4801	946	5222	895	4	3	METRO	U	1	-2	1993
18	17	3	5	16	2	15622.34	3423	1604	3400	1641	4	4	MICRO	R	1	-2	1963
19	18	1	2	3	4	7553.73	4860	845	4764	1130	4	3	METRO	U	2	-2	1940
20	19	4	8	22	1	5115.11	6692	279	6736	410	1	2	METRO	U	2	-2	1992
21	20	2	4	10	2	4132.53	8059	471	7783	651	1	1	METRO	U	1	-2	1988
22	21	4	10	26	2	7169.31	1135	1578	1299	1390	2	4	METRO	U	1	-2	1958

Figure 12.Results after decryption

[Figure 12] shows the final outcome of the decryption process. The data which is decrypted will be remained unchanged as the data which was before encrypting that data.



```
red_spots_over_body ?
```

```
You may have :['Chicken pox']
symptoms present:  ['red_spots_over_body']
symptoms given: ['itching', 'skin_rash', 'fatigue', 'lethargy', 'high_fever', 'headache', 'loss_of_a
ppetite', 'mild_fever', 'swelled_lymph_nodes', 'malaise', 'red_spots_over_body']
confidence level is: 0.09090909090909091
The model suggests:
Consult ['Dr. Inderjeet Singh']
Visit https://www.practo.com/delhi/doctor/inderjeet-singh-ayurveda-sexologist?specialization=Homoeop
ath&practice_id=1219975
```

Figure 13.Representing the patient's diagnosis

Query diagnosis form [Figure 13] includes the questions related to some kind of disease, also the confidence level of it and suggests the particular doctor for it. It also consists of the link where one can find details about that doctor, if need can scheduled an appointment.

6. CONCLUSION

A primer on blockchain technology and a high-level implementation guide for healthcare institutions interested in using blockchain technology have been developed. We have proposed a smart healthcare model through Hybrid Blockchain which is a combination of algorithms i.e., RSA algorithm and the Attribute based encryption algorithm. Our study revealed that RSA is a promising approach for the uniform data storage by generating the unique key system for the uniform data storage and Attribute based encryption algorithm for the encryption and decryption process for maintaining the data security. We believe that the proposed method may help clinicians in managing the healthcare systems in a better and effective way.

7. FUTURE SCOPE

For data trade, character affirmation, and verification, Blockchain innovation empowers huge scope interoperability among medical care suppliers, patients, and specialists. Moreover, Blockchain might be utilized to follow specialist therapy to stay away from clinical contentions, making it simpler for clinical organizations to pick excellent specialists and for patients to choose the appropriate medical services experts. Further in up-coming days we can even built this on web application for levelling up the performance.

REFERENCES

[1] P. Jiang1, F. Guo2, K. Liang3, J. Lai4 and Q. Wen5, "Searchain: Blockchain-based private keyword search in decentralized storage", ***Future Generat. Comput. Syst.***, Volume107, June 2020, Pages 781-792.

[2] A. A. Siyal1, A. Z. Junejo2, M. Zawish3, K. Ahmed4, A. Khalil5 and G. Soursou6, "Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives," **Cryptography**, vol. 3, no. 1, pp. 3, Jan. 2019.

[3] W. J. Gordon1 and C. Catalini2, "Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability," **Comput. Struct. Biotechnol. J.**, vol. 16, pp. 224-230, Jan. 2018.

[4] P. Zhang1, J. White2, D. C. Schmidt3, G. Lenz4 and S. T. Rosenbloom5, "FHIRChain: Applying blockchain to securely and scalably share clinical data", **Comput. Struct. Biotechnol. J.**, vol. 16, pp. 267-278, Jul. 2018.

[5] Y. Sakai1, N. Attrapadung2 and G. Hanaoka3,"Attribute-based signatures for circuits from bilinear map" **. PKC**, pp. 283-300, 2016.

[6] A. Boonstra1, A. Versluis2 and J. F. J. Vos3,"Implementing electronic health records in hospitals: A systematic literature review" **BMC Health Services Res.**, vol. 14, no. 1, Sep. 2014.

[7] T. Okamoto1 and K. Takashima2, "Efficient attribute-based signatures for non-monotone predicates in the standard model", **Proc. PKC**, pp. 35-52, 2011.

[8] K. D. Mandl1, P. Szolovits2 and I. S. Kohane3, "Public standards and patients' control: How to keep electronic medical records accessible but private", **BMJ**, vol. 322, pp. 283-287, Feb. 2001.