Security for Electronic Health Record Based on Attribute using Block-Chain Technology

Shilpa Patil[1]

[1]*Assistant Professor, Department of Bachelor of Computer Application(Women), Sharnbasva University Kalaburagi, Karnataka.*
Shilpa.pattil@gmail.com

ABSTRACT

Blockchain in medical care upgrades widely inclusive security of patient's clinical records, settle the issues and empowers secure interoperability between medical care associations. Issue with Today's Healthcare System is that there is a need to work on the interoperability and security of the present electronic wellbeing record the board framework that requires Blockchain-based arrangements. One more issue with the present framework is manual documentation. The solutions that Blockchain can offer to the healthcare industry by including the cryptography. The present system of hospital is completely manual, We want to automate the hospital healthcare system using Blockchain technology.

Many problems were identified during the survey to tackle it, 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. For securing data RSA algorithm and ABE algorithm are applied, Together both algorithm is applied which is the hybrid Blockchain. The Encrypted/Decrypted data provides high level security for healthcare system using Blockchain technology. The propose system is robust and efficient. Hence the work finds a good application for any hospital management.

Key words: Electronic Health, Attribute, Block-chain technology, RSA Algorithm

I. INTRODUCTION

Blockchain innovation was once produced for the digital currency Bitcoin and was first introduced in the Bitcoin whitepaper by Nakamoto in 2008. Since blockchain innovation showed up, it has been praised as another mechanical unrest actually like the development of the steam motor or the Internet as a result of its colossal impaction on society. In a 2015 World Economic Forum report, 58% of review respondents expected that 10% of worldwide Gross Domestic Product (GDP) will be applicable to the blockchain innovation through 2015. Blockchain is another innovation that guarantees a proficient, financially savvy, solid, and secure framework for managing and recording any exchange without the need of agent. As of now, various constraints have been put on sharing immense EHRs because of the threats to data security or spillage of private patient information during data exchange. A Blockchain is a kind of data base. To have the choice to appreciate Blockchain, it serves to at first get what an informational collection truly is. An informational collection is a variety of information that is taken care of electronically on a PC system. Data, or information, in data sets is ordinarily organized in table configuration to take into consideration simpler looking and separating for explicit data. Then, at that point there will not be any contrast between somebody utilizing a bookkeeping page to store data instead of an information base. Accounting pages are expected for one individual, or a little assembling of people, to store and access limited proportions of information. Alternately, an informational index is expected to house through and through greater proportions of information that can be gotten to, filtered, and controlled quickly and successfully by a significant number customers right away. As far as Blockchain in medical care, The Medical information ought to be moved by, and permitted to be used by information subjects other than emergency clinics.

II. LITERATURE SURVEY

The literature surveyed for this can be described in the following :

[1] Peng Jiang et al. In 2020, Discovered that 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. In 2019, 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. In 2018, Demonstrated an Interoperability in medical services has generally been engaged around information trade between business elements, for instance, unique clinic frameworks. Patient-focused interoperability, notwithstanding, 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. In 2018, Discovered a safe and adaptable information sharing is 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. In 2016, Developed a succor 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. In 2014, Demonstrated an EHR frameworks are expected as effectsly affecting the presentation of clinics, their execution is a perplexing endeavor. 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. In 2011, Discovered 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. In 2001, 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 endeavors. Here they proposed online clinical record frameworks could be created and utilized clinically.

SUMMARY: The study from the above work concentrates mainly on data transparency which is easily accessible to the users. The newly developed dashboard system that is made by using blockchain approach, is well designed which gives reminders to the medical authorities by accessing their medical data.

III. PROPOSED METHODOLOGY

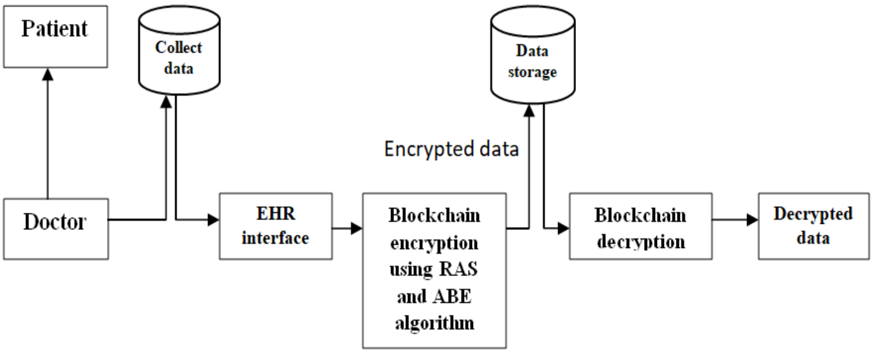


Fig1. System design for proposed methodology

In Fig 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:

1. **Patient:** Here the patient delivers the information to the doctor required for the appointment to be scheduled.
2. **Doctor:** The doctor stores the information received from the patient and assigns the particular appointment serially.
3. **Collect data:** Here, the data is collected by doctor and upload in the electronic health record interface.
4. **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.
5. **Blockchain encryption:** Here the encryption of the selected data takes place.
6. **Data storage:** After the encryption the produced encrypted data is stored in the location which we have selected so far while the encryption process.
7. **Blockchain decryption:** The data which is produced after the encryption process will further undergoes the decryption process.
8. **Decrypted data:** The data which undergoes decryption process, produces the decrypted data which can be used by the doctor as and when required.

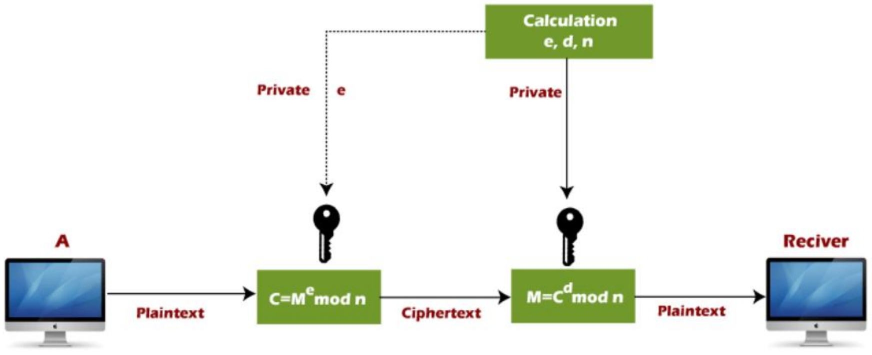
Here it is proposed that the data or the patient details which is to be stored maintains the security, since converting it to the cipher text by generating the keys:

- 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).

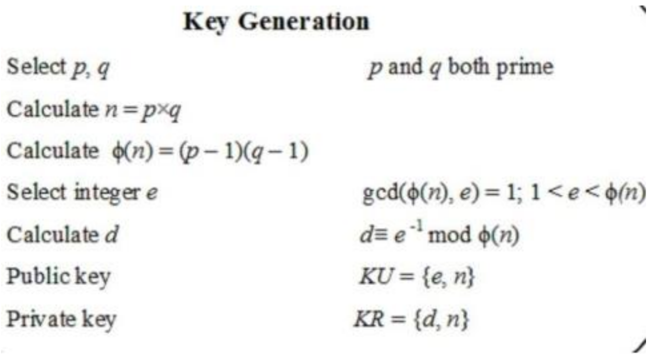
Private Blockchain: The private blockchain are planned mostly for single endeavor arrangements and they are utilized to oversee information trades happening between any people or various divisions. The security is one of the significant viewpoints considered because of which each individual member should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

The RSA algorithm :



RSA

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

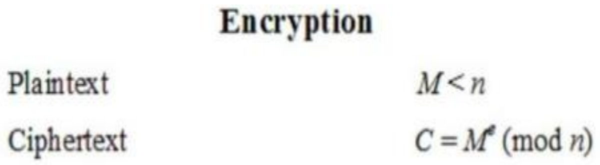
Select p, q	p and q both prime
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \bmod \phi(n)$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

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.

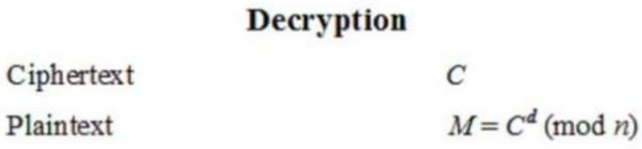
Encrypt: The encryption calculation takes as info the public boundaries, a message, and an entrance structure over the universe of qualities. The calculation will encode and create a code message with the end goal that solitary a client that has a bunch of characteristics that fulfills the entrance construction will actually want to unscramble the message. We will expect that the code text C certainly contains.



Encryption

Plaintext	$M < n$
Ciphertext	$C = M^e \pmod{n}$

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

Ciphertext	C
Plaintext	$M = C^d \pmod{n}$

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.

IV. RELATED WORK

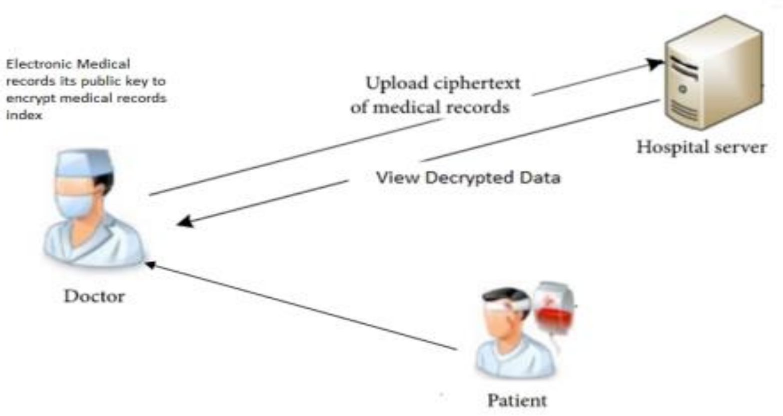

Electronic Medical records its public key to encrypt medical records index
Upload ciphertext of medical records
Hospital server
View Decrypted Data
Doctor
Patient

Fig 2. Pictorial representation of the methodological process which includes block chain technology

Here in Fig 2, 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 its required.

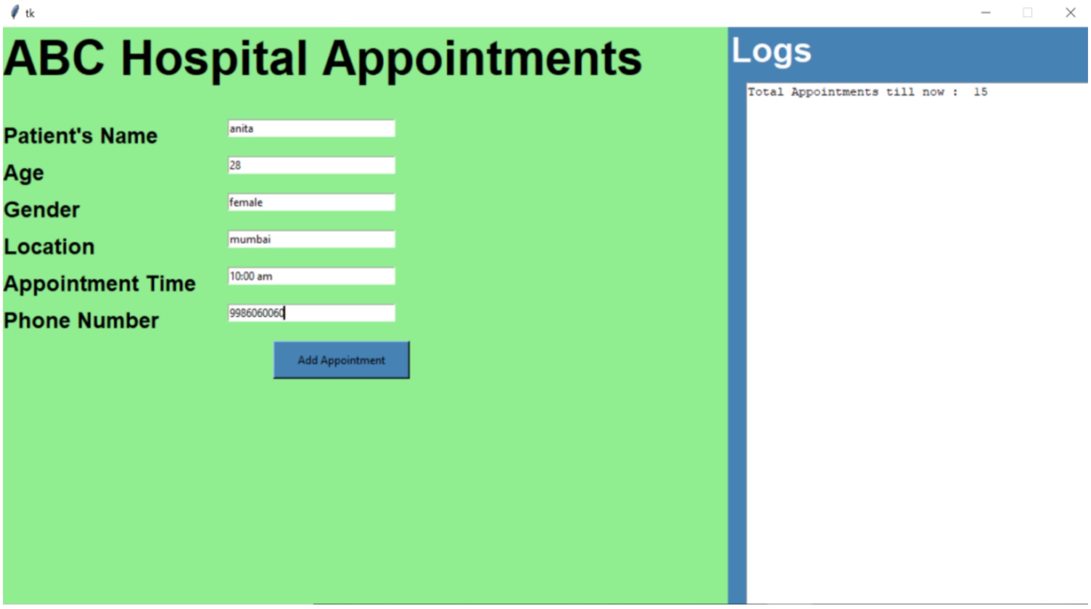
- **Patient**: Appointments of patients are registered and appointment number is assigned to each patient.
- **Doctor**: Access the patient record and enters the patient complaint and responses of the patient in the software.
- **Hospital Server**: Application accepts the details entered by the doctor 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.

The process initiates with representing the Sample patients information in Fig 3, As such it is a 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 in Fig 4, 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 in Fig 5, 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 as shown in Fig 6, is for the old user which have already been registered to enter the symptoms of the disease or diagnosis query form. The health record server in Fig 7, represents to choose the file for the further encryption process, where the keys are generated before the encryption process.The encryption process representing in Fig 8, 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 as shown in Fig 9, 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 is shown as in Fig 10, 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 shown in Fig 11, 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 depicted in Fig 12, 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.

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 specialists 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.

V. RESULTS AND DISCUSSION

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



ABC Hospital Appointments

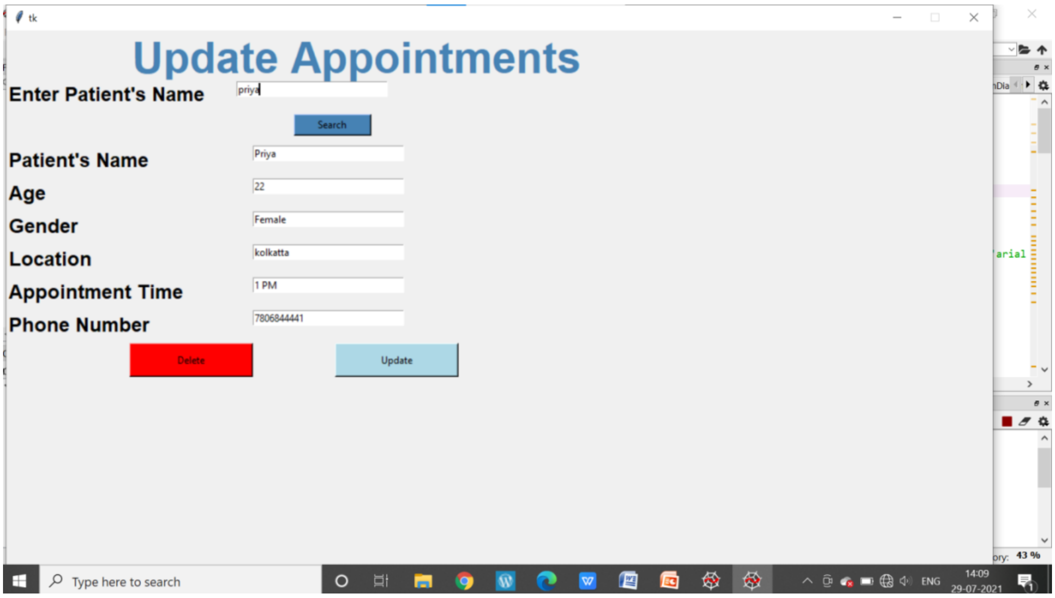
Patient's Name: anita
Age: 28
Gender: female
Location: mumbai
Appointment Time: 10:00 am
Phone Number: 9986060060

Logs

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

Fig 3. Patients appointment form

The above Fig 3, represents the patients 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.



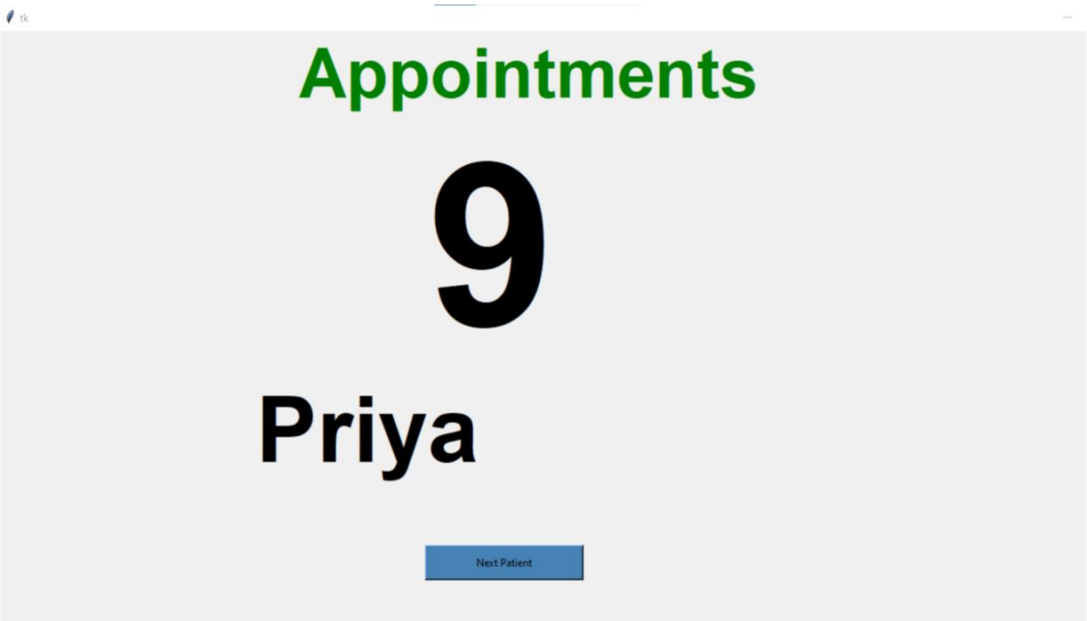
Update Appointments

Enter Patient's Name: priya

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

Fig 4. Patients details updating form

The Fig 4, 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

Fig 5. Displaying the patients appointment scheduled

Here in Fig 5, 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.

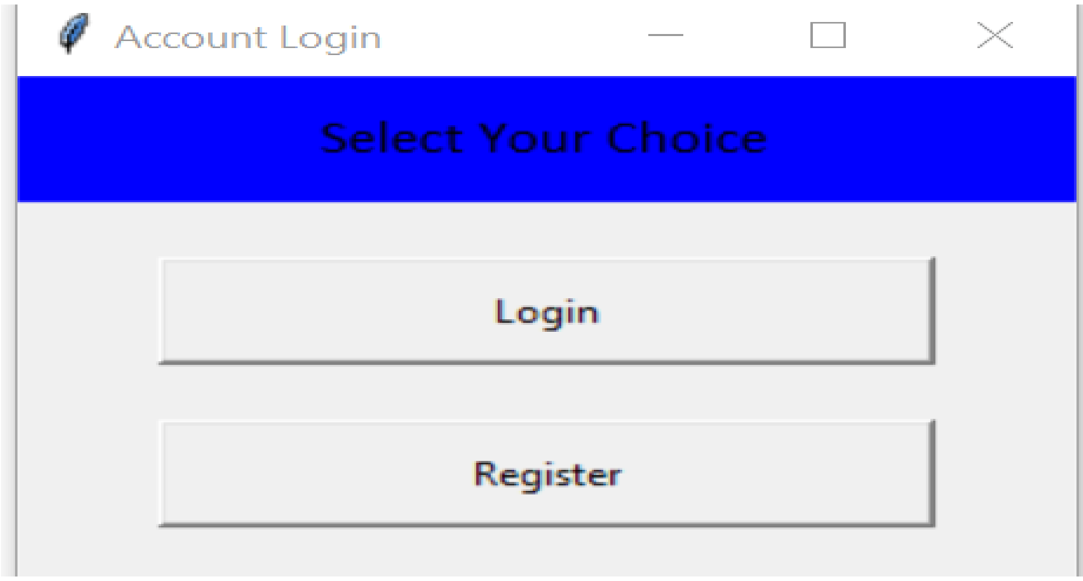
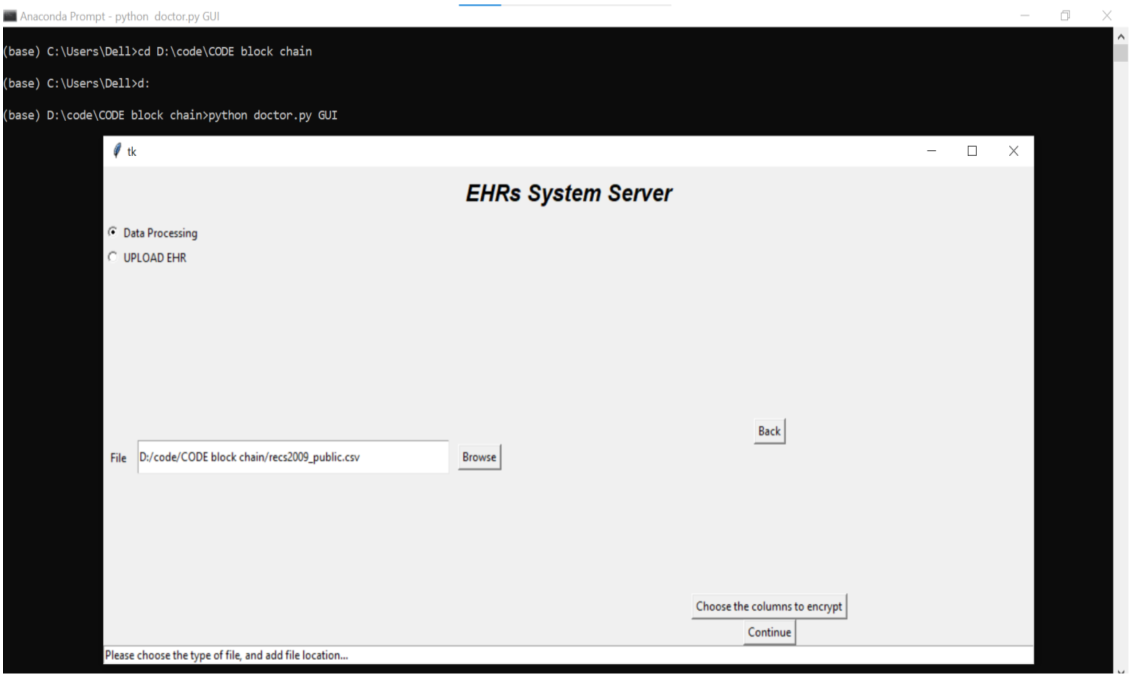


Fig 6. Registration/login page for user

In Fig 6, it 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

```
(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
```

tk

EHRs System Server

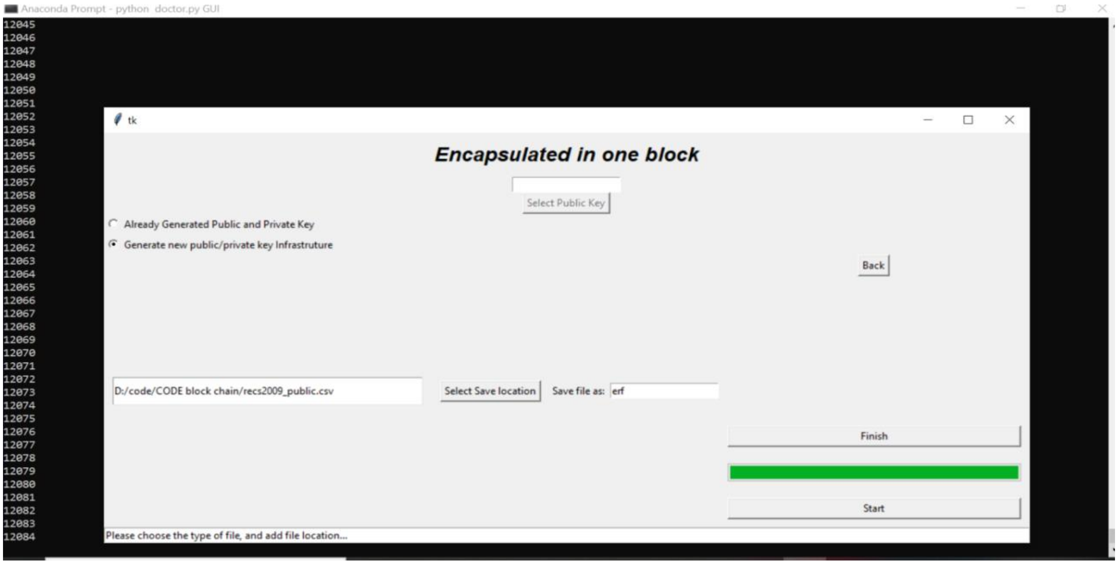
● Data Processing
○ UPLOAD EHR

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

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

Fig 7. Selecting the file that is to be encrypted

In Fig 7, represents the health record server to choose the file for the further encryption process.



Anaconda Prompt - python doctor.py GUI

```
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
```

tk

Encapsulated in one block

○ Already Generated Public and Private Key
● Generate new public/private key Infrastruture

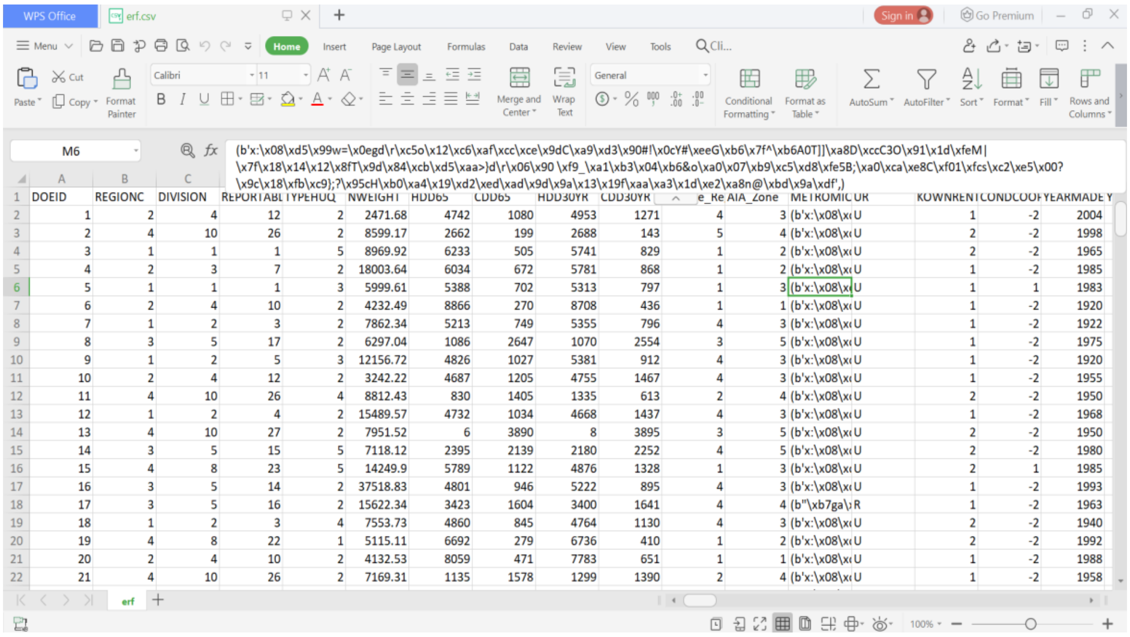
D:/code/CODE block chain/recs2009_public.csv

Save file as: erf

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

Fig 8. Selecting the column and location to store the encrypted file

In Fig 8, representing the encryption process to the particular chosen column from the data file for maintaining the data security of the patients health record through EHR interface with the similar storage for each block.



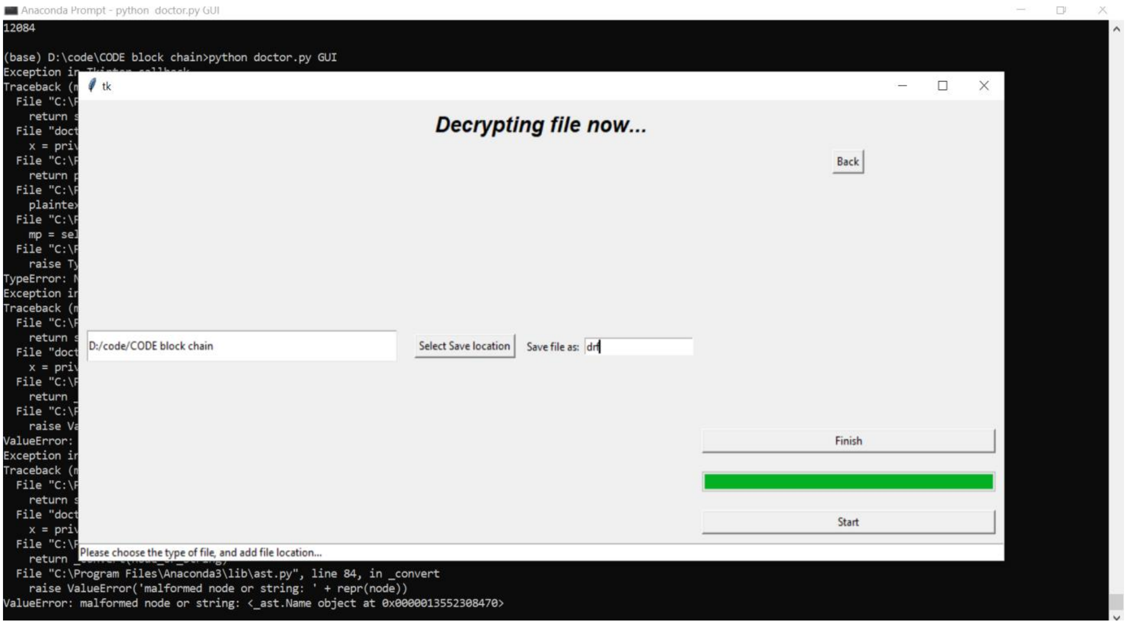
M6

fx (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',)

	A	B	C															
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	

Fig 9. Result after encrypting the particular column from data file

Here in Fig 9, it is displaying 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 (m
  File "C:\F
    return s
  File "doct
    x = priv
  File "C:\F
    return p
  File "C:\F
    plaintex
  File "C:\F
    mp = sel
  File "C:\F
    raise Ty
TypeError: N
Exception in
Traceback (m
  File "C:\F
    return s
  File "doct
    x = priv
  File "C:\F
    return _
  File "C:\F
    raise Va
ValueError:
Exception in
Traceback (m
  File "C:\F
    return s
  File "doct
    x = priv
  File "C:\F
    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>
```

Decrypting file now...

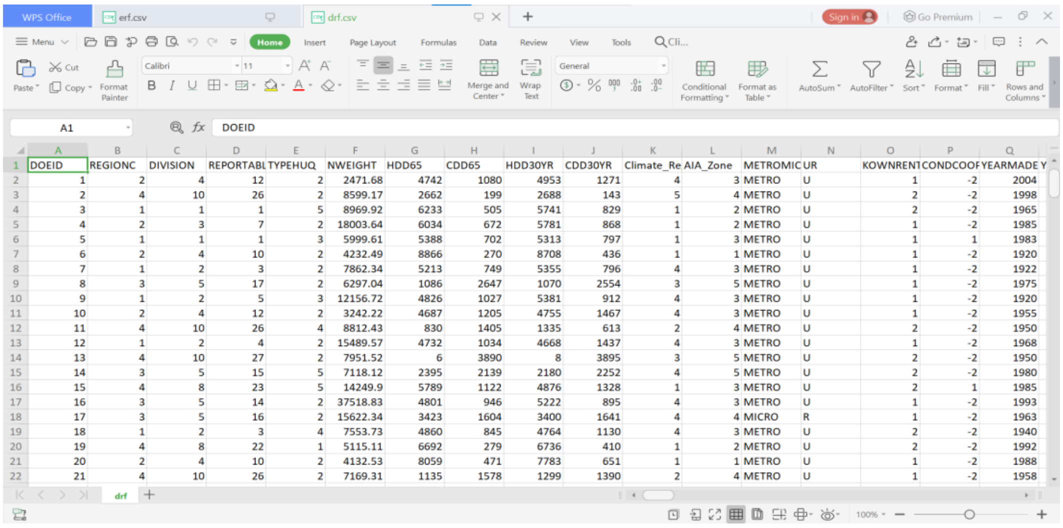
D:/code/CODE block chain

Save file as: dri

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

Fig10. Representing the decryption process

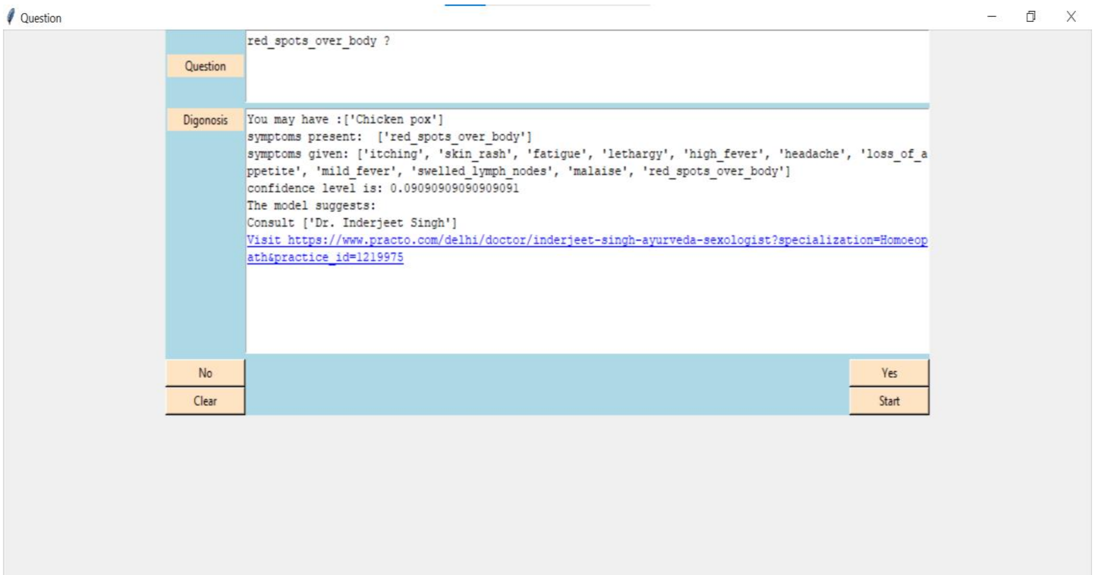
In Fig 10, its showing the decryption of the file or the particular column that is the METROMICRO column which is already encrypted, also the location should be selected for storing the decrypted file and before encryption were the eariler formed its own private key is used for decrypting the file.



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

Fig 11. Result after the decryption process

Here in Fig 11. shows the final outcome of 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.



```
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
```

Fig 12. Representing the patients Diagnosis

Here in the above Fig 12, depicting the query diagnosis form which 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.

VI. CONCLUSION

Ensuing to come up with a primer on Blockchain technology and a high level implementation guide for healthcare systems exploring the use of Blockchain technology. 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.

FUTURE SCOPE

Since on the trial run here we have designed it using tinker standalone application. Further in up-coming days we can even built this on web application for leveling up the performance.

REFERENCES

[1] P. Jiang[1], F. Guo[2], K. Liang[3], J. Lai[4] and Q. Wen[5], "Searchain: Blockchain-based private keyword search in decentralized storage", ***Future Generat. Comput. Syst.***, *Volume107*, June 2020, Pages 781-792.

[2] A. A. Siyal[1], A. Z. Junejo[2], M. Zawish[3], K. Ahmed[4], A. Khalil[5] and G. Soursou[6], “Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives,” **Cryptography**, vol. 3, no. 1, pp. 3, Jan. 2019.

[3] W. J. Gordon[1] and C. Catalini[2], “Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability,” **Comput. Struct. Biotechnol. J.**, vol. 16, pp. 224-230, Jan. 2018.

[4] P. Zhang[1], J. White[2], D. C. Schmidt[3], G. Lenz[4] and S. T. Rosenbloom[5], "FHIRChain: Applying blockchain to securely and scalably share clinical data", **Comput. Struct. Biotechnol. J.**, vol. 16, pp. 267-278, Jul. 2018.

[5] Y. Sakai[1], N. Attrapadung[2] and G. Hanaoka[3] ,“Attribute-based signatures for circuits from bilinear map” **. PKC**, pp. 283-300, 2016.

[6] A. Boonstra[1], A. Versluis[2] and J. F. J. Vos[3],“Implementing electronic health records in hospitals: A systematic literature review” **BMC Health Services Res.**, vol. 14, no. 1, Sep. 2014.

[7] T. Okamoto[1] and K. Takashima[2], "Efficient attribute-based signatures for non-monotone predicates in the standard model", **Proc. PKC**, pp. 35-52, 2011.

[8] K. D. Mandl[1], P. Szolovits[2] and I. S. Kohane[3], "Public standards and patients’ control: How to keep electronic medical records accessible but private", **BMJ**, vol. 322, pp. 283-287, Feb. 2001.