IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 08, Issue 9 (September. 2018), ||V (V) || PP 62-67

Preserving Electronic Health Data using Machine Learning Techniques and Cybersecurity Concerns

Iyyanki V Murali Krishna [1],Prisilla J[2]
[1]Former Professor and Director R&D JNTUH, Hyderabad, India,
[2] Research Scholar, Hyderabad, India,
Corresponding Author: Prisilla J

Abstract: Medical care data are huge with rich information and the records are increased within hours. Managing this heavy load of database with confidence and integrity is a major concern. In this study encryption and Convolution Neural Network has merged to give high security for accessing the patient data for medication. The finger print along with the face recognition of the authorized and authenticated doctors enhances the degree of security for the healthcare data. The cybersecurity awareness should be given to all the employees on a monthly basis and to train the newly joined staff. Regular backups and preserving the encrypted data are other concern to cope with ransomware attack.

Keywords: Authenticate, back-ups, encryption, ransomware

I. INTRODUCTION

Today's medical data has very rich information – it includes patient personal details, diagnosis information, doctor's identification and financial and health insurance information. Health care expenses are expensive and unavoidable. Hospital involves huge amount of patient details transmitted over the network, the medical devices are vulnerable to security breaches. The major reason why hospitals are targeted of cyberattacks is the fact that large and shared wireless networks. A hacker has more access to everything in the network. Attackers target patient records, research work and intellectual property as these are the most valuable data on the black market. The larger, the hospital more people are involved in the system and fall prey into the wrong hands.

Nowadays, many hospitals have focused on employing better surgeons, doctors, and staff and upgrading the medical technology, but have not realized the need for the cyber security. Security in health care is not just a one day work; rather it is the ongoing commitment of all the staff of the hospital with the organization working together for the improvement of the hospital. Most of the hospitals are unaware and are uncertain about the lack of security. People are the weakest link of security incidents result from human error not hackers such as phishing emails and spoofing. Artificial Intelligence in medical image analysis has proven beyond R & D and has undergone a significant amount of testing and evaluation by those in the health care field. Artificial Intelligence provides an opportunity for the hospitals to reach patients and provide health services. The key aim of the health system is for providing care for the new patients in the network through the use of machine learning and Artificial Intelligence applications. Artificial Intelligence enhances quality of care and improves patient outcomes.

CYBER SECURITY IN HEALTH CARE

In healthcare, hospital networks store all the health information of patient's database, evaluated by (machine learning algorithm) encryption method to provide better diagnosis. Machine learning / encryption is growing an impact on the effectiveness of cyberattack prevention. Gazing at the cyber security innovations for healthcare, technologies such as machine learning is assisting, medical institutions to improve their healthcare cyber security by automating network defenses and learning hacker behavior. Machine learning has proved to be an innovation for protecting clinical data stored on both on premise and in the cloud.

Cyberattacks on the hospital are launched for many reasons; few have fun in stealing the data whereas others deliberately destroy infrastructure. The key reason is to steal intellectual property or personal information for the financial gain and the hospital has lots of valuable information like social security number and health insurance number.

The awareness of cyber security and regular backups of the information can prevent ransom ware attacks.

The data security center makes sure the patient data and information is secure and safe, and the policies provide good practice guidance. Having the medical reports of the patients being stolen, a heavy price is paid by health care providers to cyber security complacency. The patients are the victims as they suffer the personal financial loss when the cyberattacks on the medical information in the health care. Few patients have been the victims of paying bills of others unwittingly.

Defense measures safeguard future patient revenue and healthcare who have entrusted providers with their medical and financial information [1].

II. THE FIELD STUDY

Alka Gangrade and Ravindra Patel suggest privacy-preserving classification rule mining, to build accurate classifiers without disclosing private information in the data. Secure Multiparty Computation (SMC) is one of the cryptographic methods for classification rule mining. The privacy-preserving C4.5 Decision tree classification algorithm on the union of their databases was implemented without missing any private information on the huge amount of databases [2].

Enn Tyugu, presents a brief analysis of artificial intelligences application in cyber defenses, increasing the intelligence of the defense systems enhances the cyber defense capabilities. The development of singularity technology led to 'Smarter-than-human-intelligence'. The intelligent method of IBM Watson was designed to prevent cyberattacks [3].

C.S.Kruse et al. proposes that health care center has huge valuable information and useful for the cyber criminals. The cyberattacks on health data would result in patient identity theft, medical fraud, and ability to illegally obtain controlled substances. The paper discusses about the HIPAA – (The Health Insurance Portability and Accountability Act) and the HITECH (Health Information Technology for Economic and Clinical Health Act) which requires healthcare entities to strengthen the practices of cyber security. The techniques like cyber security awareness of employees, software upgrade procedures and using virtual local area network (VLAN), using de-authentication were included as security breaching. Also ransomware was brought to light ensuring the protection of health data through regular backups [4].

Wang-Su-Jeon and Sang-Yong-Rhee, proposed a system which would enhance the quality of the fingerprints and classify them using VGGNet, a method of CNN. The preprocessing of a fingerprint is indispensable after comparing models. The classification of fingerprints is a fast matching [5].

III. DISCUSSIONS AND RESULTS

The work was carried out on windows 7, 64- bits using python 3.6. The data were collected from various hospitals and the doctors' finger prints were gathered for authentication reading. The fingerprints were maintained in a database, so that when the authenticated users wanted to access the decrypted database of the patients in the further medication, they can access without any difficulty. The thumb impression is verified and if it matches with the database then they can access the details of the patient otherwise the patient details will not made available to the unauthorized user. This research includes the face recognition of the authenticated user to access the patient details to have strong and secured databases. The thumb impression verification is carried out by Convolutional Neural Network (CNN).

THE HEALTHCARE ORGANIZATION SIZE

The health care industry includes very large health systems, single physician practices, public and private payers, research institutions, medical device and patient details. Most of the health care is still delivered by small practices in rural areas and hospitals do not have the information security resources to implement protections. The organizations do not possess the infrastructure to identify and track threats, lack the technical capability to analyze the threat data they receive. The organizations lack physical and logical access controls, consistent with best practices, and lack access to proper security training. Larger health care organizations extend information security and the risks and issues will continue to grow as the increase in complexity of attackers. The health care organizations of all sizes are targeted due to the interconnected nature of the industry and all organizations face resource constraints.

RISKS OF PATIENT DATA

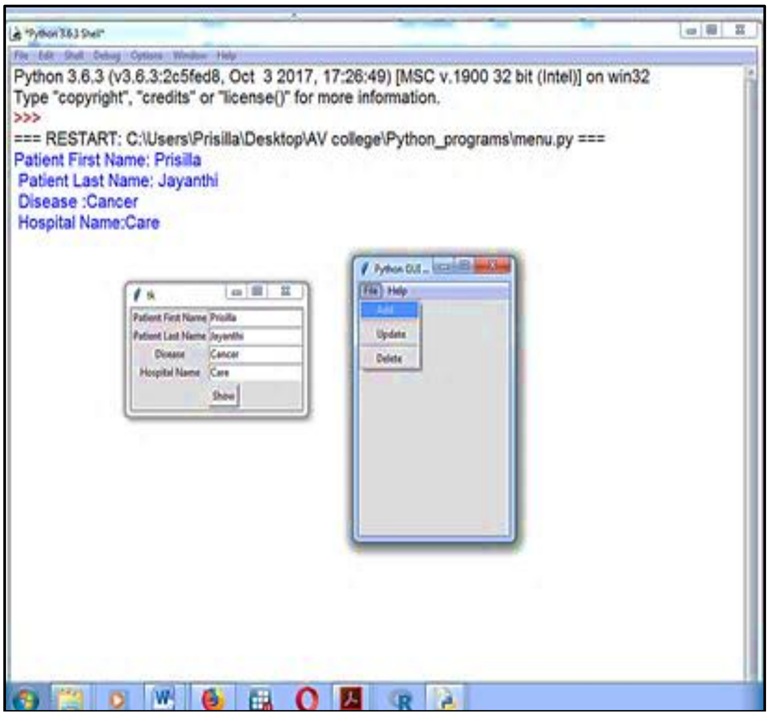
Health care data is one of the rare types of personal data that one can change and the value that may increase over time. Credit card numbers, phone numbers, and bank account numbers can be misused when personal data is lost. An unknown would steal a teenager's (student) medical history today, only to become valuable when the individual achieves a prominent role in public life. This difference in value is reflected in the price for medical records (vs. Credit card numbers). Few risks include the potential for fraud (e.g., prescription medicines, insurance, medi-care and medic-aid), brand damage, or stock manipulation based on vulnerabilities that are unknown to the public.

Hence, this patient data can be protected by taking preventive and protective measures in Information Security. The theft can happen in many ways one through networks and secondly on patient data. The cyber security education among the employee of the medical care and the one handling, entering the data be it a data entry operator, nurses, wardens or the duty doctors should an authorized person. An unauthorized person with or without knowledge may destroy the data intentionally. The trampling of data intentionally is very common now a days, data trampling is done for many reasons, the data stolen from health care can live a lifetime. The theft of patient data causes the unauthorized expose of illegal notification to the affected patients.

The most common attacks against medical care providers involves the use of ransomware, the patient records or complete database is hacked and locked unless a ransom amount is paid. For self- protection or for medical care protection one has to take regular backups and prevent such payment on attacks. As long as the data is with the medical care, the medical care need not worry about the ransomware attacks. A well –organized and repeated education of the cybersecurity among the staff and integration can help the medical care run smoothly. Otherwise, when a ransomware attack happens in a care center, then the complete work comes to halt that can be given medication to a patient, discharging a patient, billing a patient using health insurance, or doctors salaries or any other staff salaries can come to halt as the total data is stolen. No further work can be done unless the ransom amount (bitcoins) is paid. A great loss to the health care center and loss to the society, so handling such cases with necessary corrective actions and regular backups is needed.

PROTECTING PATIENT DATA

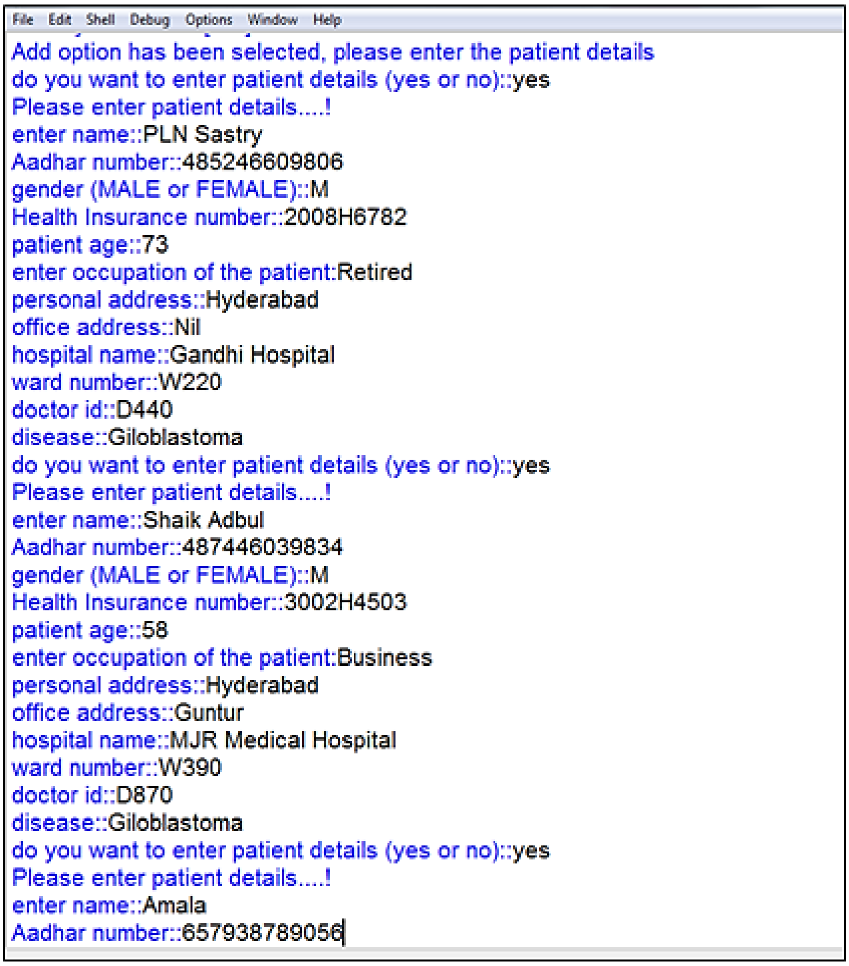
The patient data entered by data entry operator are shown in figure 2, should be encrypted as shown in figure 3 and can be decrypted only by the authorized person displayed in figure 4 with the key provided. The whole database should then be backed up regularly and maintain up to date with the reports. This backed up data in a hard device should be preserved, carefully such that only the concern authenticated user will know about it.



```
Python 3.6.3 (v3.6.3:2c5fed8, Oct  3 2017, 17:26:49) [MSC v.1900 32 bit (Intel)] on win32
Type "copyright", "credits" or "license()" for more information.
>>>
=== RESTART: C:\Users\Prisilla\Desktop\AV college\Python_programs\menu.py ===
Patient First Name: Prisilla
 Patient Last Name: Jayanthi
 Disease :Cancer
 Hospital Name:Care
```

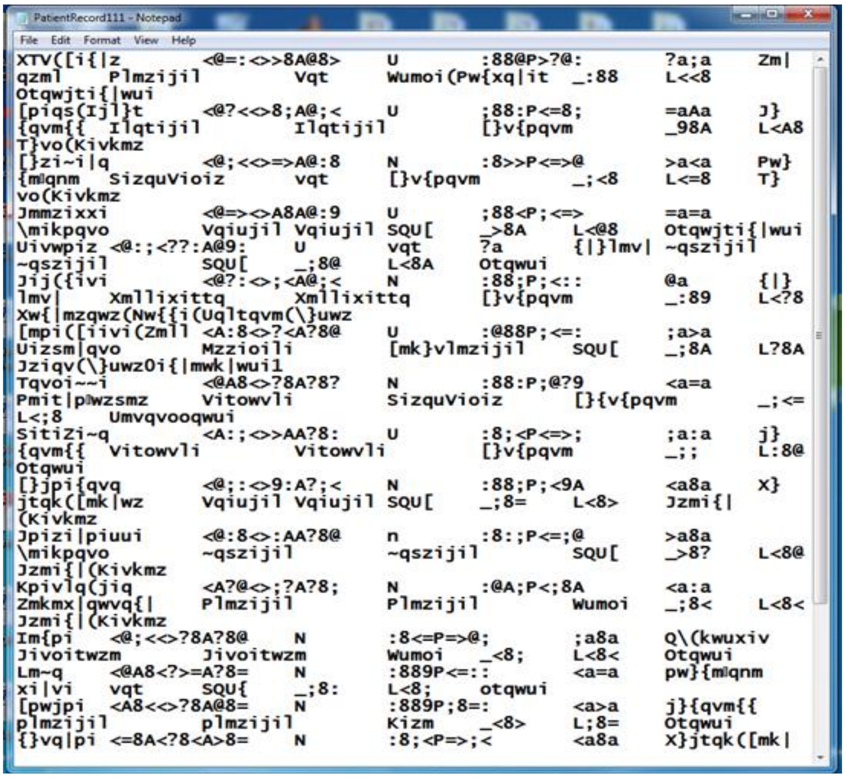
Patient First Name Prisilla
Patient Last Name Jayanthi
Disease Cancer
Hospital Name Care

Figure 1: Patient details Menu



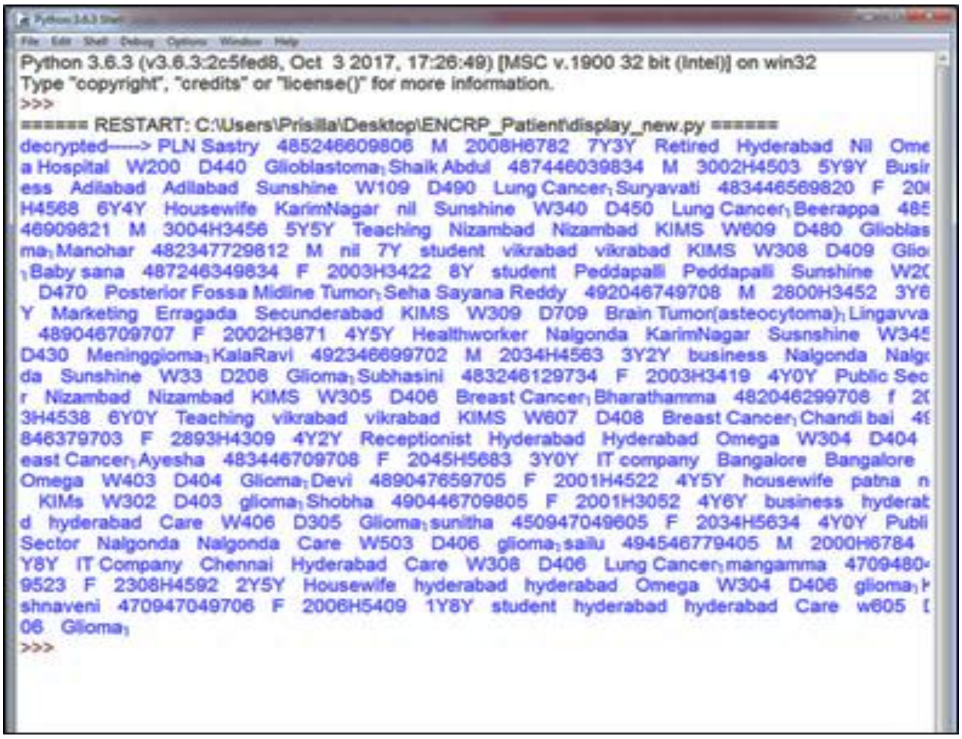
```
Add option has been selected, please enter the patient details
do you want to enter patient details (yes or no)::yes
Please enter patient details....!
enter name::PLN Sastry
Aadhar number::485246609806
gender (MALE or FEMALE)::M
Health Insurance number::2008H6782
patient age::73
enter occupation of the patient:Retired
personal address::Hyderabad
office address::Nil
hospital name::Gandhi Hospital
ward number::W220
doctor id::D440
disease::Giloblastoma
do you want to enter patient details (yes or no)::yes
Please enter patient details....!
enter name::Shaik Adbul
Aadhar number::487446039834
gender (MALE or FEMALE)::M
Health Insurance number::3002H4503
patient age::58
enter occupation of the patient:Business
personal address::Hyderabad
office address::Guntur
hospital name::MJR Medical Hospital
ward number::W390
doctor id::D870
disease::Giloblastoma
do you want to enter patient details (yes or no)::yes
Please enter patient details....!
enter name::Amala
Aadhar number::657938789056
```

Figure 2: Adding of patient details



```
XTV([i{|z        <@=:<>>8A@8>     U          :88@P>?@:         ?a;a     Zm|
qzml      Plmzijil          Vqt       Wumoi(Pw{xq|it  _:88      L<<8
Otqwjti{|wui
[piqs(Ijl}t      <@?<<>8;A@;<     U          ;88:P<=8;         =aAa     J}
{qvm{{  Ilqtijil          Ilqtijil           []v{pqvm          _98A     L<A8
T}vo(Kivkmz
[]zi~i|q         <@;<<>=>A@:8     N          :8>>P<=>@         >a<a     Pw}
{mqnm     SizquVioiz        vqt       []v{pqvm           _;<8      L<=8     T}
vo(Kivkmz
Jmmzixxi         <@=><>A8A@:9     U          ;88<P;<=>         =a=a
\mikpqvo         Vqiujil Vqiujil SQU[       _>8A      L<@8     Otqwjti{|wui
Uivwpiz <@:;<??:A@9:    U         vqt        ?a        {|}lmv| ~qszijil
~qszijil         SQU[      _;8@      L<8A       Otqwui
Jij({ivi         <@?:<>;<A@;<     N          :88;P;<::         @a       {|}
lmv|      Xmllixittq        Xmllixittq         []v{pqvm          _:89     L<?8
Xw{|mzqwz(Nw{{i(Uqltqvm(\}uwz
[mpi([iivi(Zmll <A:8<>?<A?8@     U          :@88P;<=:         ;a>a
Uizsm|qvo        Mzzioili          [mk}vlmzijil       SQU[      _;8A     L?8A
Jziqv(\}uwzOi{|mwk|wuil
Tqvoi~~i         <@A8<>?8A?8?     N          :88:P;@?9         <a=a
Pmit|pwzsmz      Vitowvli          SizquVioiz          []{v{pqvm          _;<=
L<;8      Umvqvooqwui
SitiZi~q         <A:;<>>AA?8:     U          :8;<P<=>;         ;a:a     j}
{qvm{{  Vitowvli          Vitowvli           []v{pqvm          _;;      L:8@
Otqwui
[]jpi{qvq        <@;:<>9:A?;<     N          :88;P;<9A         <a8a     X}
jtqk([mk|wz      Vqiujil Vqiujil SQU[       _;8=      L<8>     Jzmi{|
(Kivkmz
Jpizi|piuui      <@:8<>:AA?8@     n          :8:;P<=;@         >a8a
\mikpqvo         ~qszijil          ~qszijil           SQU[      _>8?     L<8@
Jzmi{|(Kivkmz
Kpivlq(jiq       <A?@<>;?A?8;     N          :@A;P<;8A         <a:a
Zmkmx|qwvq{|     Plmzijil          Plmzijil           Wumoi     _;8<     L<8<
Jzmi{|(Kivkmz
Im{pi    <@;<<>?8A?8@     N          :8<=P=>@;         ;a8a     Q\(kwuxiv
Jivoitwzm        Jivoitwzm          Wumoi     _<8;      L<8<     Otqwui
Lm~q     <@A8<?>=A?8=     N          :889P<=::         <a=a     pw}{mqnm
xi|vi    vqt       SQU{      _;8:      L<8;      otqwui
[pwjpi   <A8<<>?8A@8=     N          :889P;8=:         <a>a     j}{qvm{{
plmzijil         plmzijil           Kizm      _<8>      L;8=     Otqwui
{}vq|pi  <=8A<?8<A>8=     N          :8;<P=>;<         <a8a     X}jtqk([mk|
```

Figure 3: Encrypted Patient Data



```
Python 3.6.3 (v3.6.3:2c5fed8, Oct  3 2017, 17:26:49) [MSC v.1900 32 bit (Intel)] on win32
Type "copyright", "credits" or "license()" for more information.
>>>
====== RESTART: C:\Users\Prisilla\Desktop\ENCRP_Patient\display_new.py ======
decrypted-----> PLN Sastry  485246609806  M  2008H6782  7Y3Y  Retired  Hyderabad  Nil  Ome
a Hospital  W200  D440  Glioblastoma₁Shaik Abdul  487446039834  M  3002H4503  5Y9Y  Busir
ess  Adilabad  Adilabad  Sunshine  W109  D490  Lung Cancer₁Suryavati  483446569820  F  20
H4568  6Y4Y  Housewife  KarimNagar  nil  Sunshine  W340  D450  Lung Cancer₁Beerappa  485
46909821  M  3004H3456  5Y5Y  Teaching  Nizambad  Nizambad  KIMS  W609  D480  Glioblas
ma₁Manohar  482347729812  M  nil  7Y  student  vikrabad  vikrabad  KIMS  W308  D409  Glio
₁Baby sana  487246349834  F  2003H3422  8Y  student  Peddapalli  Peddapalli  Sunshine  W2C
  D470  Posterior Fossa Midline Tumor₁Seha Sayana Reddy  492046749708  M  2800H3452  3Y6
Y  Marketing  Erragada  Secunderabad  KIMS  W309  D709  Brain Tumor(asteocytoma)₁Lingavva
  489046709707  F  2002H3871  4Y5Y  Healthworker  Nalgonda  KarimNagar  Susnshine  W345
D430  Meninggioma₁KalaRavi  492346699702  M  2034H4563  3Y2Y  business  Nalgonda  Nalg
da  Sunshine  W33  D208  Glioma₁Subhasini  483246129734  F  2003H3419  4Y0Y  Public Sec
r  Nizambad  Nizambad  KIMS  W305  D406  Breast Cancer₁Bharathamma  482046299708  f  2C
3H4538  6Y0Y  Teaching  vikrabad  vikrabad  KIMS  W607  D408  Breast Cancer₁Chandi bai  4
846379703  F  2893H4309  4Y2Y  Receptionist  Hyderabad  Hyderabad  Omega  W304  D404
east Cancer₁Ayesha  483446709708  F  2045H5683  3Y0Y  IT company  Bangalore  Bangalore
Omega  W403  D404  Glioma₁Devi  489047659705  F  2001H4522  4Y5Y  housewife  patna  n
  KIMs  W302  D403  glioma₁Shobha  490446709805  F  2001H3052  4Y6Y  business  hyderat
d  hyderabad  Care  W406  D305  Glioma₁sunitha  450947049605  F  2034H5634  4Y0Y  Publi
Sector  Nalgonda  Nalgonda  Care  W503  D406  glioma₁sailu  494546779405  M  2000H6784
Y8Y  IT Company  Chennai  Hyderabad  Care  W308  D406  Lung Cancer₁mangamma  4709480
9523  F  2308H4592  2Y5Y  Housewife  hyderabad  hyderabad  Omega  W304  D406  glioma₁K
shnaveni  470947049706  F  2006H5409  1Y8Y  student  hyderabad  hyderabad  Care  w605  [
06  Glioma₁
>>>
```

Figure 4: Decrypted Patient Data

FACE RECOGNITION

Face recognition and eye detection provide yet another source of security. Signatures of any person can be manipulated or duplicated whereas retina of eye cannot be duplicated. Hence, face recognition provides in a long way, a security for accessing the electronic health database along with the finger print. In this study different doctors were approached to gather their information to maintain in the doctor database in healthcare. The software program helps us to identify the authenticated and authorized doctor following which the doctors can access the encrypted data. The following doctor’s face and finger prints are identified and shown in figure 5.

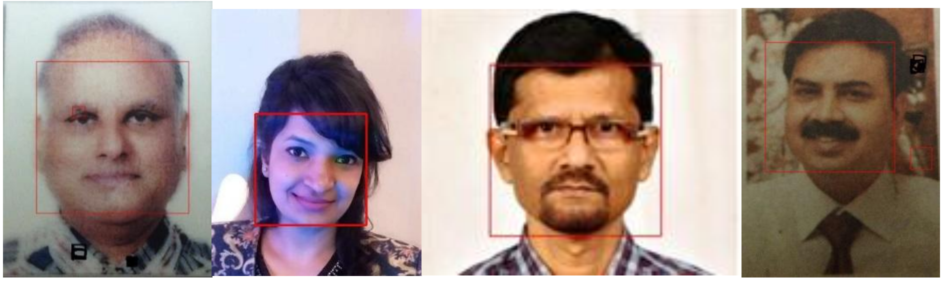


Figure 5: Red Square box indicates that the faces has been recognised

IV. CONCLUSIONS

The health care data is at risk without the knowledge of security. The electronic health data is vast increasing day to day, maintaining such data requires security measures. In this study, the raw patient data is encrypted and kept secured and is accessed by the authorized doctors.

ACKNOWLEDGEMENT

I am grateful to all the following doctors who helped me in carrying out the research work Dr. (Col) C.G. Wilson, Former Dean of Kamineni Hospital and presently working for Karunya Clinic, Grace Community Baptist Church, Secunderabad; Dr.Sadhna Aggarwal, AIIMS New Delhi; Dr. Prasad Behera, CARE Hospital, Hyderabad and Dr. Ch. Mohana Vamsy, Omega Hospital, Hyderabad.

CONFLICTS OF INTEREST

There are no conflicts of interest.

REFERENCES

[1]. "Health Care Industry cyber security task force", A Report on improving cyber security in the health care industry, June 2017.

[2]. Alka Gangrade and Ravindra Patel "Building Privacy-Preserving C4.5 Decision Tree Classifier on Multiparties", International Journal on Computer Science and Engineering Vol. 1(3), 2009, 199-205.

[3]. Enn Tyugu, "Artificial Intelligence in Cyber Defense", 3rd International Conference on Cyber Conflict C. Czosseck, 2011 by CCD COE Publications.

[4]. Clemens Scott Kruse, Benjamin Frederick, Taylor Jacobson and D. Kyle Monticone, "Cybersecurity in healthcare: A systematic review of modern threats and trends", Technology and Health Care 25 (2017) 1–10.

[5]. Wang-Su Jeonand Sang-Yong Rhee, "Fingerprint Pattern Classification Using Convolution Neural Network", International Journal of Fuzzy Logic and Intelligent Systems Vol. 17, No. 3, September 2017, pp. 170-176.

IOSR Journal of Engineering (IOSRJEN) is UGC approved Journal with Sl. No. 3240, Journal no. 48995.

Iyyanki V Murali Krishna " Preserving Electronic Health Data using Machine Learning Techniques and Cybersecurity Concerns" IOSR Journal of Engineering (IOSRJEN), vol. 08, no. 9, 2018, pp. 62-67.