ISSN XXXX XXXX © 2018 IJESC

Research Article Volume 8 Issue No.5

Privacy Protection in E-Healthcare System

Shanthi K.Guru[1], Shrutika Waghmode[2], Aroosha Rao[3], Monali Deshmukh[4], Mayuri Pawar[5]
Assistant Professor[1], BE Student[2, 3, 4, 5]
Department of Computer Engineering
D. Y. Patil College of Engineering, Akurdi, Pune, India

Abstract:
Healthcare applications are considered as promising fields for wireless networks, where patients can be monitored using wireless medical networks (WMNs). Current WMN healthcare research trends focus on patient reliable communication, patient mobility, and energy efficient routing, as a few examples. However, deploying new technologies in healthcare applications without considering security makes patient privacy vulnerable. Moreover, the physiological data of an individual are highly sensitive. Therefore, security is a paramount requirement of healthcare applications, especially in the case of patient privacy if the patient has an embarrassing disease. This project discusses the security and privacy issues in healthcare application using WMNs. We highlight some popular healthcare projects using wireless medical networks and discuss their security issues. The existing systems solutions can simply protect the patient data during transmission and storage but they are still prone to data loss. Therefore we are proposing an approach to prevent this by using multiple data servers to store patient data. The main contribution of this paper is to provider Security to the data store using encryption and distribution of data in multiple data servers.

Keywords: Patient data privacy, distribution of data, encryption, decryption.

I. INTRODUCTION

Several research groups and projects have started to develop health monitoring using wireless sensor networks. Wireless (i.e. online) healthcare application offers a number of challenges, like, reliable transmission of data, secured data transmission, nodes mobility, detection of event delivery of data in time, power management, etc. Deploying new technologies in healthcare applications without considering security often makes patient privacy vulnerable. For instance, the patient's physiological vital signals are very sensitive so the leakage of the patient's diseased data could make the patient embarrassed. Sometimes revealing disease information can be embarrassing. To prevent the patient data from the unauthorized person, we propose a new data collection protocol, where the sensitive patient data is distributed into three components and sends them to three servers, respective, via secure channels. To keep the privacy of the patient data in data access, we propose a new data access protocol on the basis of cryptosystem. The protocol allows the user (e.g. doctor) to access the patient data without revealing it to any data server. To preserve the privacy of the patient data in statistical analysis, we propose some new privacy-preserving statistical analysis protocol on the basis of cryptosystems. These protocols allow the user (e.g., medical researcher) to perform statistical analysis on the patient data without compromising the patient data privacy.

II. BASIC CONCEPT

Computers have improved the accuracy, speed and reliability of many of the administrative and technical tasks traditionally involved in patient care besides improving the service offered to patients. This has changed the workload of health professionals, allowing them to spend more time on the human aspects of patient care. Management Information Systems (MIS) are information systems, typically computer based, that are used within an organization. An information system is comprised of all the components that collect, manipulate and disseminate data or information. It usually includes hardware, software, people, communication systems such as telephone lines and the data itself. The activities involved include inputting data, processing of data into information, storage of data and information and the production of outputs such as management reports. The introduction of computerized systems in hospitals has changed the working practices. Patient data is stored on computer systems, which can then be used to manage patient lists, appointment bookings and issuing of prescriptions. This is usually faster, more reliable and more accurate than performing these tasks manually. Therefore, computerized systems are money saving and reduce the workload of clerical staff. This project has been developed using Java, JSP and SQL Server.

Related Work:

User Classes and Characteristics

[1] Educational level:

Users should be comfortable with the English language.

[2] Experience:

Users should have prior information regarding the online healthcare system.

[3] Skills:

Users should have basic knowledge and should be comfortable using general purpose applications on computers.

The Operating Environment used to develop this system are Java, JSP, MySQL

JAVA:

Java is a programming language expressly designed for use in the distributed environment of the Internet. Java is used to create full applications that may run on a single computer or be distributed among servers and clients in a network. It can also be used to build a small application module or applet for use as part of a Web page. Applets make it possible for a Web page user to interact with the page. It is used to build application module for use as a part of Web page and provides interaction between the pages.

JSP:

JavaServer Pages (JSP) is a **technology** that helps software developers create dynamically generated web pages based on

HTML, XML, or other document types. Released in 1999 by Sun Microsystems, JSP is similar to PHP and ASP, but it uses the Java programming language. JSP is based on Servlet. In fact, we shall see later that a JSP page is internally translated into a Java servlet. We shall also explain later that "*Servlet isHTML inside Java*", while "*JSP is Java inside HTML*". A JSP page consists of HTML tags and JSP tags. The jsp pages are easier to maintain than servlet because we can separate designing and development. It provides some additional features such as Expression Language, Custom Tag etc.

SQL:

Essentially, Structured Query Language (SQL) is used to retrieve data or otherwise interface with a relational database. As a standard going back to the 1970s, SQL is a popular way to get information out of relational database systems. The SQL language is written to comb the contents of tables in a conventional database. SQL is widely used in business and in other types of database administration. It is the default tool for "operating" on the conventional database, to alter tabled data, retrieve data or otherwise manipulate an existing data set.

Distributed DBMS:

A database that consists of two or more data files located at different sites on a computer network. Because the database is distributed, different users can access it without interfering with one another. However, the *DBMS* must periodically synchronize the scattered databases to make sure that they all have consistent data. In designing a distributed database, you must decide which portion of the database is to be stored where. One technique used to break up the database into logical units called fragments. Fragmentation information is stored in a distributed data catalogue which the processing computer uses to process a user's request.

Cryptosystem:

Cryptosystem takes sole responsibility to deliver the message to the authorized receiver only. It protects information from any leakage by protecting with encrypted codes. In cryptography, a cryptosystem is a suite of cryptographic algorithms needed to implement a particular security service, most commonly for achieving confidentiality (encryption). Typically, a cryptosystem consists of three algorithms: one for key generation, one for encryption, and one for decryption. The term *cipher* (sometimes *cypher*) is often used to refer to a pair of algorithms, one for encryption and one for decryption. Therefore, the term *cryptosystem* is most often used when the key generation algorithm is important. For this reason, the term *cryptosystem* is commonly used to refer to public key techniques; however both "cipher" and "cryptosystem" are used for symmetric key techniques.

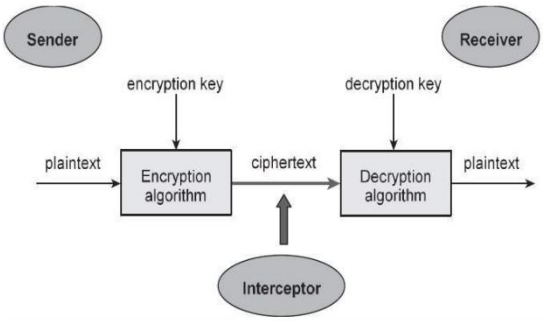

Figure.1. Basic working of cryptosystem

III. LITERATURE REVIEW:

In this paper [1],The use of AES in security purpose is described. The demand for protection raised, if the confidentiality of the information is of very high value. Security is very essential to avoid the unauthorized disclosure or alteration of the information. Due to the advance change in technologies nowadays, a number of multimedia data is being created and transmitted, leaving our own data vulnerable to be edited, modified and duplicated. Digital documents are therefore being faced by innumerable threats as they are very easy to copy and distribute. Cryptography is an art of secret writing, which authenticates data and important messages as well as protects the systems from valid attacks. One of the best existing security algorithms to provide data security is Advanced Encryption Standard (AES). It comprises of encryption and decryption process each related with a key which is supposed to be kept secret. In this paper the software Xilinx ISE 13.1 project navigator is used for the purpose of synthesis and simulation of AES algorithm. In this paper [2],They mentioned that due to the vast development of information technology, it is very necessary to protect the sensitive information via encryption which is becoming more and more important in daily life. One of the best symmetric security algorithms to provide security for data is advanced encryption standard (AES). AES has the advantage of being implemented in both hardware and software. AES is a non-Feistel cipher that encrypts and decrypts a data block of 128 bits. It uses 10, 12, or 14 rounds in algorithm and the key size, can be 128, 192, or 256 bits depending on the number of rounds. In this paper the software Xilinx ISE project navigator is used for synthesis and simulation for encryption. In this paper [3] ,they have explained that with the large growth of important data on cloud, cloud security is obtaining a lot of vital than even before. The cloud information and services reside in massively as might be accessed all over. The expansion of the cloud users has sadly been accompanied with a growth in malicious activity within the cloud. More and more vulnerabilities are discovered and nearly daily, new security advisories are revealed. Countless users are surfing the Cloud for varied purposes, so they have extremely safe and protected services. The long run of cloud, particularly in increasing the range of applications, involves a way deeper degree of privacy and authentication. We tend to propose a straightforward information protection model wherever information is encrypted exploitation Advanced secret writing common place (AES) before it's launched within the cloud, so making certain information confidentiality and security. This paper [4] presents a design of data encryption and decryption in a network using RSA algorithm. RSA algorithm that will convert the information to a form not understandable (encrypted) by the intruder therefore protecting unauthorized users from having access to the information even if they are able to break into the system. It is an asymmetric cryptographic algorithm. A user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but while decryption of message authorized person used their private key.

There are some drawbacks in this [4] paper :

1.Algorithm can slow in case where large data needsmto be encrypted by the same computer.

2.The RSA encryption and decryption algorithm need a lot of calculation and the speed is slowly, compared with the symmetric cryptographic algorithm thousands of times slower.

3. Complexity of the key creation. Because of the RSA algorithm is limited by the prime and efficiency of generating primes is relatively low, so it is difficult to achieve a secret once. In this [5] paper they have explained different encryption algorithms. Encryption is one of the principal means to

guarantee security of sensitive information. Encryption algorithm performs various substitutions and transformations on the plaintext and transforms it into cipher text. Many encryption algorithms are widely available and used information security. Encryption algorithm are classified into two groups: Symmetric key and Asymmetric key encryption. RSA: It is one of the best known public key cryptosystems for key exchange or digital signatures or encryption of blocks of data. It is an asymmetric (public key) cryptosystem based on number theory, which is a block cipher system. It uses variable size key. RSA operations can be decomposed in three broad steps- key generation, encryption and decryption.

DES:DES is publicly available cryptographic system. The Data Encryption Standard (DES) is a block Cipher which is designed to encrypt and Although the input key for DES is 64 bits long, the actual key used by DES is only 56 bits in length. The algorithm goes through 16 iterations that interlace blocks of plaintext with values obtained from the key.
3-DES: Data Encryption Standard (DES) uses a 56-bit key and is not deemed sufficient to encrypt sensitive data. 3-DES simply extends the key size of DES by applying the algorithm three times in succession with three different keys. The combined key size is thus 168 bits (3 times 56).In 3-DES the 3-times iteration is applied to increase the encryption level and average time.
AES: AES algorithm can support any combination of data (128 bits) and key length of 128, 192, and 256 bits. The algorithm is referred to as AES-128, AES-192, or AES-256, depending on the key length. AES system goes through 10 rounds for I28-bit keys, 12 rounds for I92-bit keys, and 14 rounds for 256-bit keys in order to deliver final cipher-text or to retrieve the original plain-text.
RSA: In RSA when the small values of p & q are selected for the designing of key then the encryption process becomes too weak and one can be able to decrypt the data by using random probability theory and side channel attacks. On the other hand if large p & q lengths are selected then it consumes more time and the performance gets degraded in comparison with DES. Further, the algorithm also requires of similar lengths for p & q, practically this is very tough conditions to satisfy.

Existing System:-

In the traditional system, there was only a single database through which the user could extract and store data. In such circumstance, if the hacker gets hold of this database he could damage the entire data system. The users were unable to detect the alterations done and would use the wrong data unknowingly. This can lead to many problems.

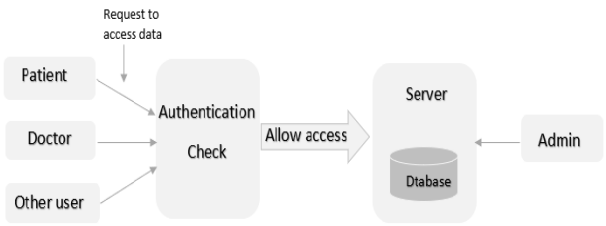

Figure.2.Flow of an existing system

In the existing system, to improve the system security replicas are made of a single database. This helps in maintaining backup in case of node failure also increases the level of security. If one server is hacked we need to detect the attack and take immediate action of switching off that server and redirecting the requests to other servers. It makes sure that integrity is maintained and only reliable data is provided to the user.

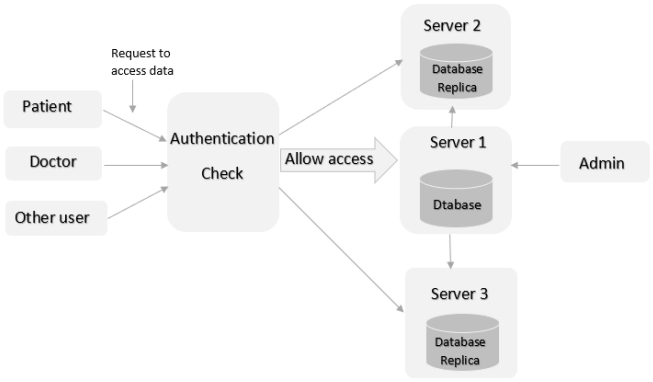

Figure. 3. Flow of an existing system

Proposed System:-
Even when the replicas help in providing backup they are not efficient in providing high security. If one server is hacked entire system can fall. So we use distribution of database into different servers. A user who needs data will send a request and data will be collected from all the servers and then returned to the user. If a single server is attacked not entire data is leaked. Also backup is provided by the administrator.

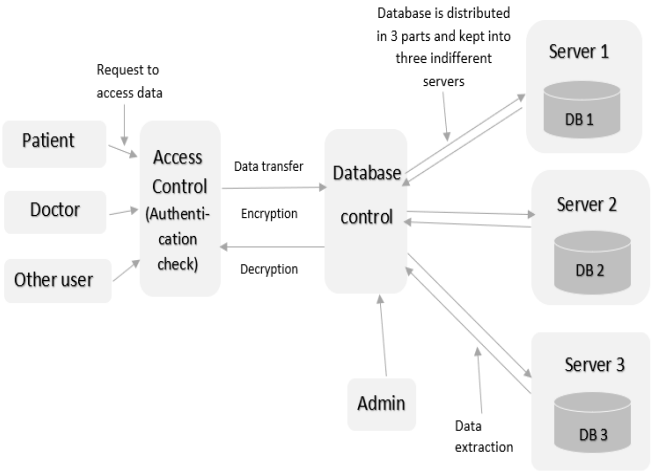

Figure. 4. Example of proposed system
The System will have all in one features like Format Independent, Load balancing, Audible Operator, User Friendly environment, Space utilization, Security Mechanism, Time utilization

Cryptography:
Cryptography is the science and study of methods of protecting data in computer and communication systems from unauthorised disclosure and modification. Classification into two cryptosystems, private-key cryptosystem and public-key cryptosystem. Boyh are based on complex mathematical algorithms and are controlled by keys.

Security goals:

1. Confidentiality or Privacy: Service is used to save the information content of all persons except that told them to get acquainted with them.
2. Data integrity: This service is used to save the information of change (delete or add or modify) by person unauthorised to do so.

3. Proof of identity (Authentication): This service is used to prove the identity of the data handling (authorized).
4. Non-repudiation: This service is used to prevent a person from denial todo something.

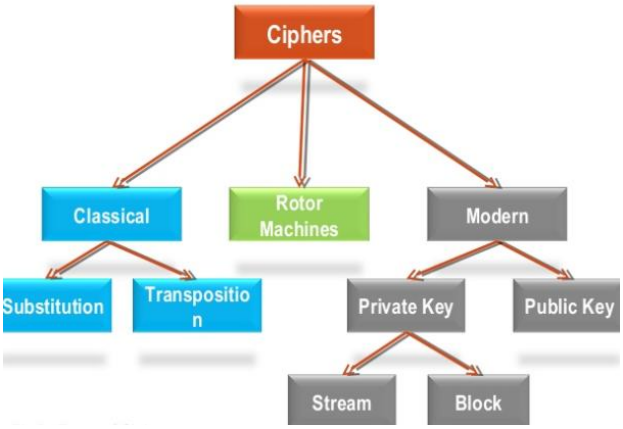

Figure.5. Types of cyphers

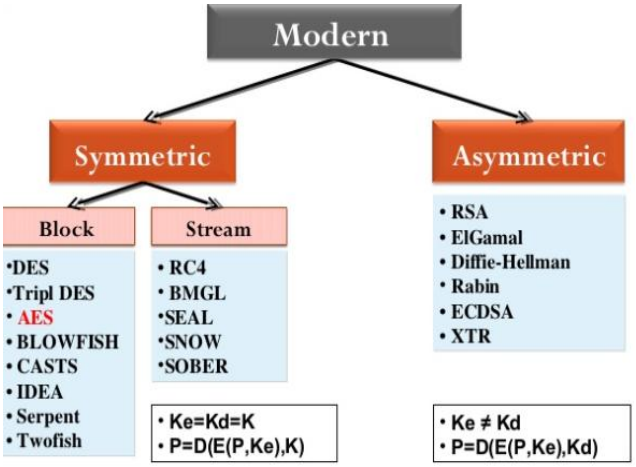

Figure.6.Types of modern cyphers

Symmetric Encryption:
An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message. Symmetric-key systems are simpler and faster. Symmetric-key cryptography is sometimes called secret-key cryptography. The most popular symmetric-key system is the Data Encryption Standard (DES).

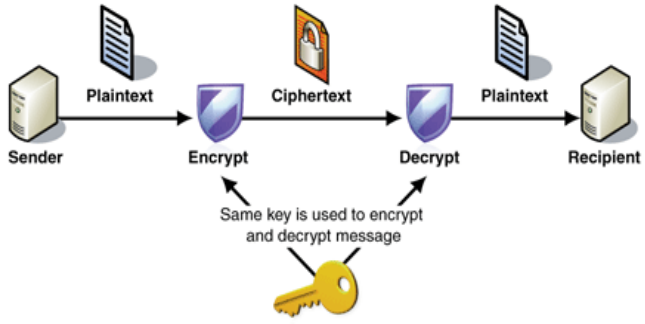

Figure.7.Structure of Asymmetric Encryption

Asymmetric Encryption: Public-key encryption is a cryptographic systemthat uses two keys -*a* public key known to everyone and a private or secretkey known only to the recipient of the message. An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them.

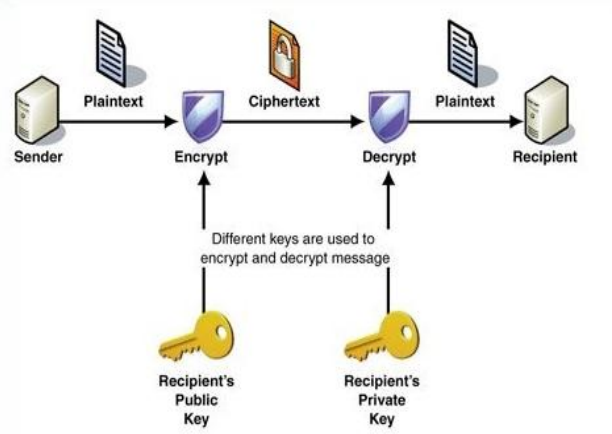

Figure. 8. Structure of Asymmetric Encryption

Advanced Encryption Standard (AES):
AES is an encryption standardpublished by the National Institute of Standards and Technology(NIST) in December 2001. It has been accepted word wibe as a desirable algorithm to encrypt sensitive data. It is a block cypher which operates on a block size of 128 bits for both encryption as well as decryption. It has keys of size 128/192/256 bits. The criteria defined by NIST for selecting AES into three areas :

1. Security
2. Cost
3. Implementation

AES is designed to have:

- Resistance against known attacks
- Speed and code compactness on many CPUs
- Design simplicity

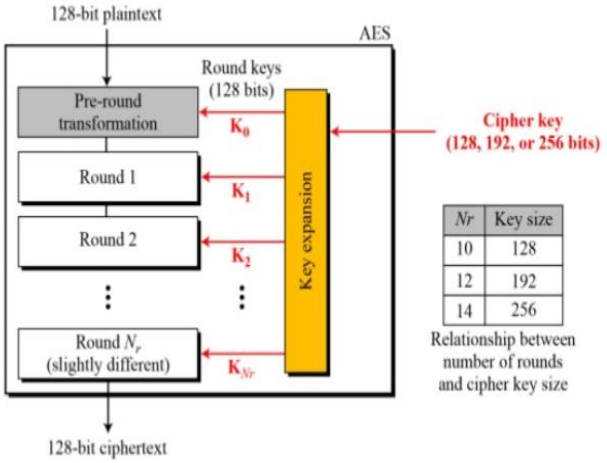

Figure. 9. general design of AES encryption cipher

AES structure:
The number of rounds performed by algorithm strictly depends on the size of key.
The following table gives overview of no. of rounds performed with the input of varying key length :

Key size (in bits) ***Rounds***
128.....10
192.....12
256.....14

The larger the number of keys, the more secure will be the data. The time taken by s/w to encrypt will increase with no. of rounds.

It has 10/12/14 rounds in which **e**ach round performs same 4 operations.

1. Byte substitution (1 S-box used on every byte)
2. Shift Row (permute bytes between groups/columns)
3. Mix Columns (subs using matrix multiply of groups)
4. Add Round Key (XOR state with key material)

Final round is little different because it removes the mix column step.

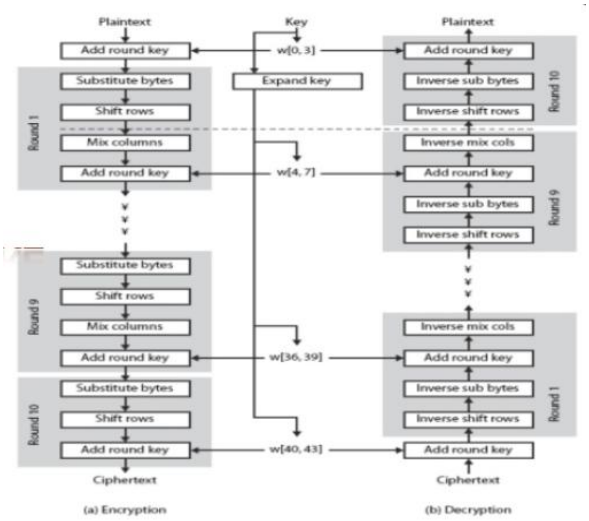

Figure.10. ciphers and inverse ciphers of the original design

```
Cipher (InBlock [16], OutBlock[16], w[0 … 43])
{
   BlockToState (InBlock, S)

   S ← AddRoundKey (S, w[0…3])
   for (round = 1 to 10)
   {
      S ← SubBytes (S)
      S ← ShiftRows (S)
      if (round ≠ 10)  S ← MixColumns (S)
      S ← AddRoundKey (S, w[4 × round, 4 × round + 3])
   }

   StateToBlock (S, OutBlock);
}
```

Figure. 11. Pseudo code for the cipher in the original design

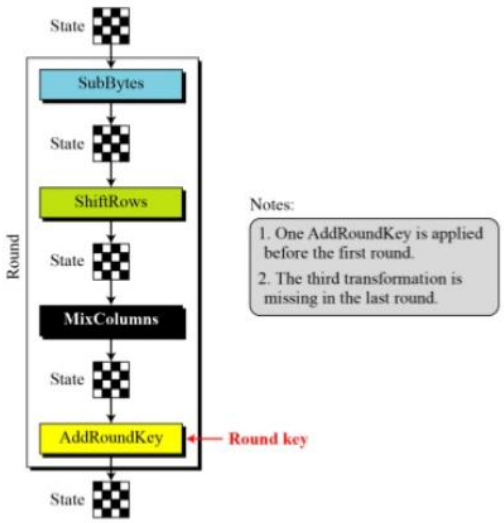

Figure.12. Structure of each round at the encryotion site

Key expanded into array of 32-bit words. 4 different stages are used as shown which has a simple structure. Only add round key use key. Decryption uses a key in reverse order.

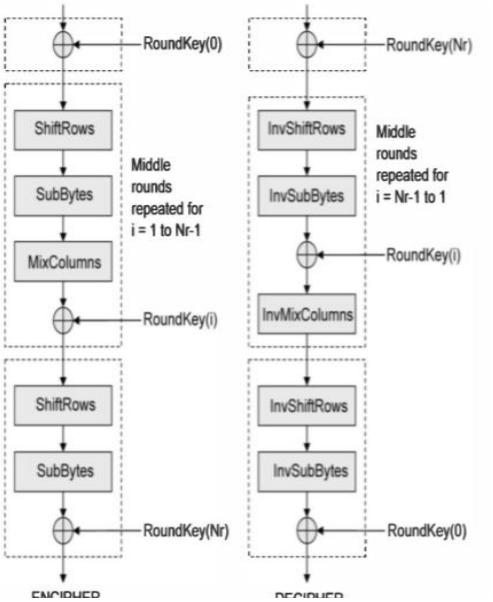

Figure. 13. AES basic process flow

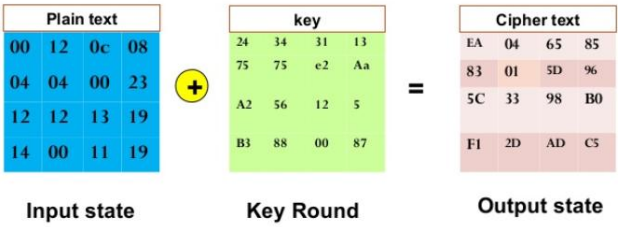

Figure.14. initial XOR key

Transformations:

To provide security, AES uses four types of yransformations:

Byte SubstitutionTranformation:

- Each byte of block is replaced by its substitute in an s-box.
- S-box constructed using defined transformation of values in GF
- Each byte of state is replaced by byte indexed by row & column.

Example- byte {95} is replaced by byte in row 9, column 5 which has value {2A}

- It is designed to be resistant to all known attacks

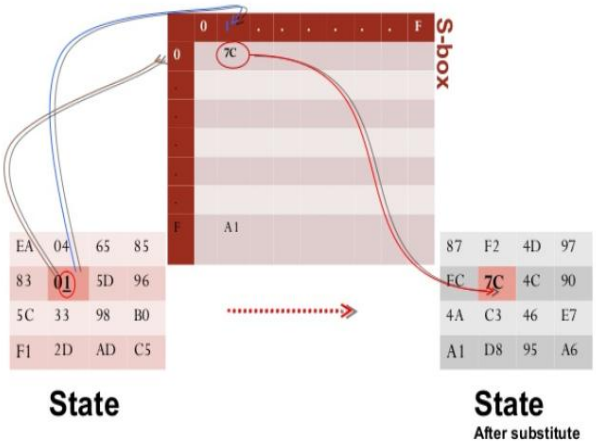

Figure.15. Substitution transformation

x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Figure.16. S-box

x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

Figure.17. Inverse s-box

ShiftRow Transformation:

Each row of the state is shifted cyclically a certain number of steps.

- 1st row is unchanged
- 2nd row does 1 byte circular shift to left
- 3rd row does 2 byte circular shift to left
- 4th row does 3 byte circular shift to left

Decrypt inverts using shift to right. Science state is processed by columns, this step permutes bytes between the columns

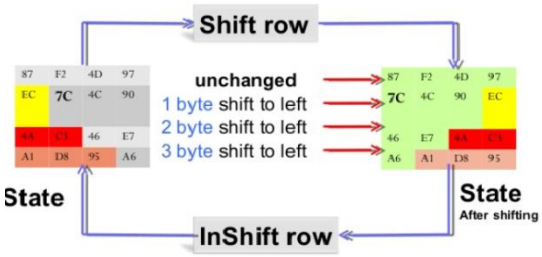

Figure.18. Shift rows

MixColumns Transformation:

In this step the block is multiplied with a fixed matrix. The multiplication in GaloisField. Each byte is replaced by a value dependent on all 4 bytes in a column. Effectively a matrix multiplication in GF(2^8) using prime poly m(x)= $x^8 + x^4 + x^3 + x + 1$

Decryption requires use of inverse matrix with large coefficients, hence a little harder.

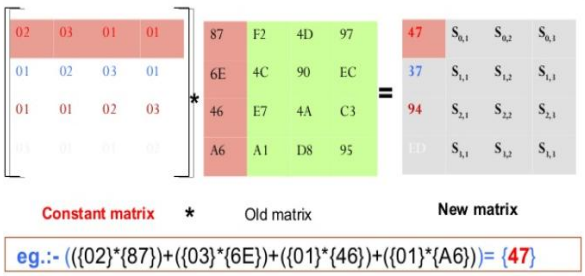

Figure.19. Mix column transformation

MixColumns (S)

```
{
    for (c = 0 to 3)
        mixcolumn (s_c)
}
mixcolumn (col)
{
    CopyColumn (col, t)                    // t is a temporary column
    col_0 ← (0x02) • t_0 ⊕ (0x03 • t_1) ⊕ t_2 ⊕ t_3
    col_1 ← t_0 ⊕ (0x02) • t_1 ⊕ (0x03) • t_2 ⊕ t_3
    col_2 ← t_0 ⊕ t_1 ⊕ (0x02) • t_2 ⊕ (0x03) • t_3
    col_3 ← (0x03 • t_0) ⊕ t_1 ⊕ t_2 ⊕ (0x02) • t_3
}
```

Figure.20. Pseudo code for mix column transformation

Add round key:

It is XOR state with 128-bits of the round key. In this step each byte is XOR-ed with corresponding element of key's matrix. Once this step is done the keys are no longer available for this step. Using the same key will weaken then algorithm.

To overcome this problem keys are expanded.

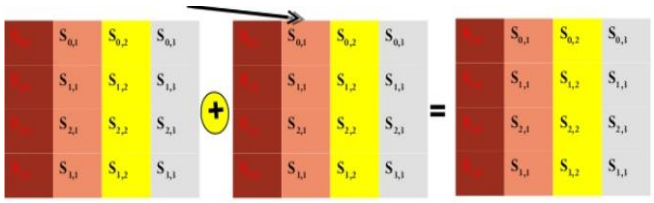

Figure. 21. Add round key

Pseudo code for add round key

```
AddRoundKey (S)
{
    for (c = 0 to 3)
        s_c ← s_c ⊕ w_round + 4c
}
```

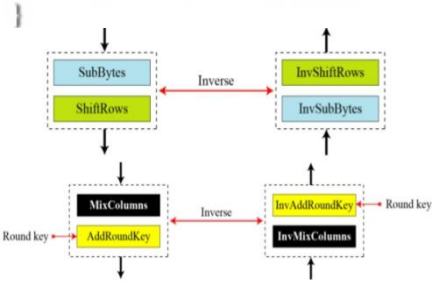

Figure.22. Invertibility of sub-bytes and shift-row combination

Key Expansion:

To create round key for each round, AES uses a key expansion process. If the number rounds is N_r, the key expansion routine creates N_r + 1128-bit round key from one single 128-bit cipher key.

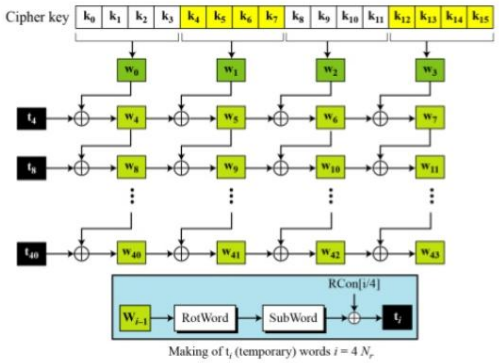

Figure.23. Key expansion in AES 128

Round	Constant (RCon)	Round	Constant (RCon)
1	$(\underline{01}\ 00\ 00\ 00)_{16}$	6	$(\underline{20}\ 00\ 00\ 00)_{16}$
2	$(\underline{02}\ 00\ 00\ 00)_{16}$	7	$(\underline{40}\ 00\ 00\ 00)_{16}$
3	$(\underline{04}\ 00\ 00\ 00)_{16}$	8	$(\underline{80}\ 00\ 00\ 00)_{16}$
4	$(\underline{08}\ 00\ 00\ 00)_{16}$	9	$(\underline{1B}\ 00\ 00\ 00)_{16}$
5	$(\underline{10}\ 00\ 00\ 00)_{16}$	10	$(\underline{36}\ 00\ 00\ 00)_{16}$

Figure.24. RCon constants

Round	Input State	Output State	Round Key
Pre-round	00 12 0C 08	24 26 3D 1B	24 34 31 13
	04 04 00 23	71 71 E2 89	75 75 E2 AA
	12 12 13 19	B0 44 01 4D	A2 56 12 54
	14 00 11 19	A7 88 11 9E	B3 88 00 87
1	24 26 3D 1B	6C 44 13 BD	89 BD 8C 9F
	71 71 E2 89	B1 9E 46 35	55 20 C2 68
	B0 44 01 4D	C5 B5 F3 02	B5 E3 F1 A5
	A7 88 11 9E	5D 87 FC 8C	CE 46 46 C1
2	6C 44 13 BD	1A 90 15 B2	CE 73 FF 60
	B1 9E 46 35	66 09 1D FC	53 73 B1 D9
	C5 B5 F3 02	20 55 5A B2	CD 2E DF 7A
	5D 87 FC 8C	2B CB 8C 3C	15 53 15 D4
3	1A 90 15 B2	F6 7D A2 B0	FF 8C 73 13
	66 09 1D FC	1B 61 B4 B8	89 FA 4B 92
	20 55 5A B2	67 09 C9 45	85 AB 74 0E
	2B CB 8C 3C	4A 5C 51 09	C5 96 83 57
4	F6 7D A2 B0	CA E5 48 BB	B8 34 47 54
	1B 61 B4 B8	D8 42 AF 71	22 D8 93 01
	67 09 C9 45	D1 BA 98 2D	DE 75 01 0F
	4A 5C 51 09	4E 60 9E DF	B8 2E AD FA
5	CA E5 48 BB	90 35 13 60	D4 E0 A7 F3
	D8 42 AF 71	2C FB 82 3A	54 8C 1F 1E
	D1 BA 98 2D	9E FC 61 ED	F3 86 87 88
	4E 60 9E DF	49 39 CB 47	98 B6 1B E1
6	90 35 13 60	18 0A B9 B5	86 66 C1 32
	2C FB 82 3A	64 68 6A FB	90 1C 03 1D
	9E FC 61 ED	5A EF D7 79	0B 8D 0A 82
	49 39 CB 47	8E B2 10 4D	95 23 38 D9
7	18 0A B9 B5	01 63 F1 96	62 04 C5 F7
	64 68 6A FB	55 24 3A 62	83 9F 9C 81
	5A EF D7 79	F4 8A DE 4D	3E B3 B9 3B
	8E B2 10 4D	CC BA 88 03	B6 95 AD 74
8	01 63 F1 96	2A 34 D8 46	EE EA 2F D8
	55 24 3A 62	2D 6B A2 D6	61 FE 62 E3
	F4 8A DE 4D	51 64 CF 5A	AC 1F A6 9D
	CC BA 88 03	87 A8 F8 28	DE 4B E6 92
9	2A 34 D8 46	0A D9 F1 3C	E4 0E 21 F9
	2D 6B A2 D6	95 63 9F 35	3F C1 A3 40
	51 64 CF 5A	2A 80 29 00	E3 FC 5A C7
	87 A8 F8 28	16 76 09 77	BF F4 12 80
10	0A D9 F1 3C	BC E0 55 E6	DB D5 F4 0D
	95 63 9F 35	02 E3 0D F1	F9 38 9B DB
	2A 80 29 00	8B B1 6D 82	2E D2 88 4F
	16 76 09 77	D3 95 F8 41	26 D2 C0 40

Figure.25. Example of encryption

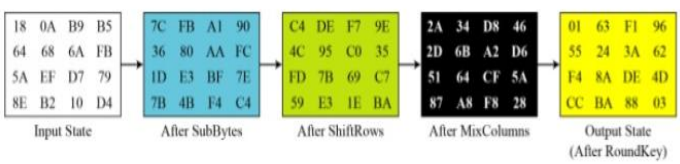

Figure.26. States in single round

AES features:

The selection process for this new symmetric key algorithm was fully open to public scrutiny and comment; this ensured a thorough, transparent analysis of the designs submitted**.** NIST specified the new advanced encryption standard algorithm must be a block cipher capable of handling 128 bit blocks, using keys sized at 128, 192, and 256 bits; other criteria for being chosen as the next advanced encryption standard algorithm included:

- **Security:** Competing algorithms were to be judged on their ability to resist attack, as compared to other submitted ciphers, though security strength was to be considered the most important factor in the competition.
- **Cost:** Intended to be released under a global, nonexclusive and royalty-free basis, the candidate algorithms were to be evaluated on computational and memory efficiency.
- **Implementation:** Algorithmand implementation characteristics to beevaluated included the flexibility of the algorithm; suitability of the algorithm to be implemented in hardware or software; and overall, relative simplicity of implementation.

Distribution

Input is given to the encryption module that is responsible for encrypting the data. Once the data gets encrypted it is further passed to the Distribution module in the encrypted format. The Distribution system is responsible for distributing the data into parts so that if the attacker gets access to one of the system, he can access only the amount of data that is stored in that Database. The rest of the data remains safe. The retrieval process is quite the opposite, the data is collected from different Databases and merged together before retrieval. The user may not know that the data is being gathered from different Databases. Once the data gets merged, it is then shown to the User.

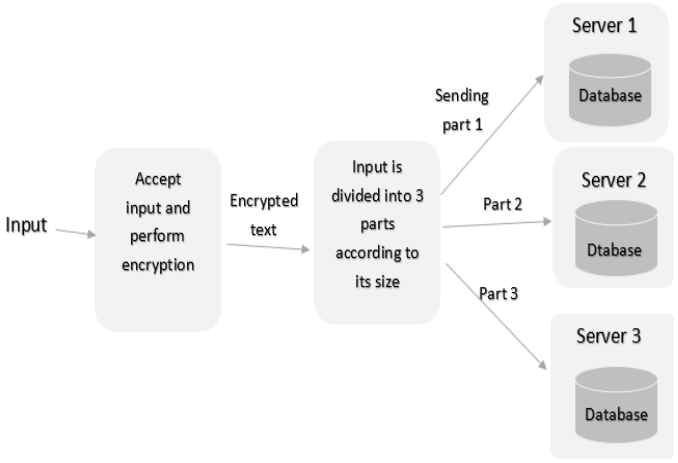

Figure.27. Data distribution

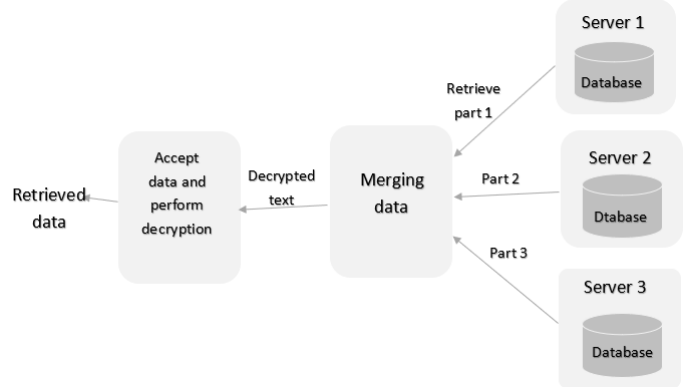

Figure.28. Data merging

IV. CONCLUSIONS

This survey describes the design of our proposed system. Our approach will be specially designed to handle a number of records of patientswhere security mechanism,splitting and concatenation operations are performed on database. The security will be provided to the data by encrypting and distributing it while transferring data to the appropriate server.

V. REFERENCES

[1]. Design and Simulation of AES Algorithm for Cryptography Radhika D. Bajaj ,Dr. U.M. Gokhale

[2].AES algorithm for encryption Radhika D. Bajaj, Dr. U.M. Gokhale

[3]. Securing Data in Cloud Using AES Algorithm Prasoon Raghav, Rahul Kumar, Rajat Parashar

[4].Data Encryption & Decryption Using RSA Algorithm in a Network Environment Nentawe Y. Goshwe.

[5].A study of Encryption Algorithms(RSA, DES, 3DES and AES) for Information Security Gurpreet Singh,Supriya

[6].Data Encryption and Decryption Using RSA Algorithm in a Network Environment Nentawe Y. Goshwe.

[7].Implementation of Advanced Encryption Standard Algorithm with Key Length of 256 Bits for Preventing Data Loss in an Organization Isaac Kofi Nti , Eric Gymfi and Owusu Nyarko

[8].AES Proposal: Rijndael Joan Daemen, Vincent Rijmen

[9].Designand Development of Online Hospital Management Information System Harpreet Kuri, Dinesh Grover

[10].Implementing an integrated computerized patient record system: Towards an evidence-based information system implementation practice in healthcare, AMIA 2008 Rahimi B., Moberg A., Timpka T., Vimarlund V