**MEDICAL DATABASE SECURITY**

**Submitted in fulfilment of**

**INFORMATION AND SECURITY SYSTEM**

**RESEARCH PAPER-1**

**By**

**V RITHIK 19MIS1189**

**UNDER THE GUIDANCE OF**

**PROF RAJESH KANNAN**

**SECURITY PROBLEM**: Wireless Sensor Networks (WSN) is an emerging technology that has the potential to transform the way of human life. Healthcare applications are considered promising fields for Wireless Medical Sensor Network, where patient’s health can be monitored using Medical Sensors. Wireless Medical Sensor Networks (WMSNs) are the key enabling technology in healthcare applications that allows the data of a patient’s vital body parameters to be collected by wearable biosensors. Current WMSN healthcare research trends focus on patient reliable communication, patient mobility and energy-efficient routing. Wireless medical sensor networks are more vulnerable to eavesdropping, modification, impersonation and replaying attacks than the wired networks. So protection is an important task for patient data. Now a days there is a lot of transferring data in the present world where the security of data is tends to be very low, there is possibility of leaking data and patients details comes to risk where other organisation will try to threat them, and their life gone be at risk.

**SOLUTION:**

* + - To prevent the patient data from the inside attacks, this propose a new data collection technique, where a sensor splits the sensitive patient data into three components according to a random number generator based on hash function and sends them to three servers, respective, via secure channels.
    - To keep the privacy of the patient data in data access, proposed a new data access technique on the basis of the Paillier cryptosystem. The protocol allows the user (e.g., physician) to access the patient data without revealing it to any data server.
    - To preserve the privacy of the patient data in statistical analysis, proposed some new privacy-preserving statistical analysis protocols on the basis of the Paillier and ElGamal cryptosystems. These protocols allow the user (e.g., medical researcher) to perform statistical analysis on the patient data without compromising the patient data privacy.

**METHOD:**

In this usage of cryptosystems like Elgamal and paillier this can be shown and El\_Gamal is a public-key cryptosystem technique was designed by Dr. Taher Elgamal El\_Gamal depends on the one way function, means that the encryption and decryption are done in separate functions. The encryption process requires two modular exponentiations (extra time).

**Key generation**

* + - Generate a large random prime number (p)
    - Choose a generator number (a)
    - Choose an integer (x) less than (p-2) ,as secret number.
    - Compute (d) where
      * d= a**x** mod p
    - Determine the public key (p, a, d), and the private key (x)

**Encryption**

* + - Obtain the public key (p , a , d ) from
    - the receiver A.
    - Choose an integer k such that :
      * 1 < k < p-2
    - Represent the plaintext as an integer m where 0 < m < p-1
    - compute (y) as follows :
      * y = ak mod p
    - compute (z) as follows :
      * z = (dk \* m ) mod p
    - Find the ciphertext (C) as follows :
      * C= ( y , z )
    - The sender B send C to The receiver A .

**Decryption**

* Obtain the ciphertext (C) from B .
* compute (r) as follows :
  + r = yp-1-x mod p
* Recover the plaintext as follows:
  + m = ( r \* z ) mod p

**WHY ELGAMAL:**

In Elgamal encryption is provides security more than any other algorithm, is easy to use the operation can be simple while comparing to different methods. The main advantage of elgamal method isOne of the strength of ElGamal is its non-determinism-encrypting the same plaintext multiple times will result in different, ciphertexts, since a random k is chosen each time. El-Gamal encryption is used in the free GNU privacy Guard Software, recent versions of PGP , and other cryptosystems.

The Elgamal encryption is done by generation of keys using discrete algorithms. Encryption and decryption of algorithms use large computing process so that encryption results look like twice the size of the original size.