SYSTEM ANALYSIS

EXISTING SYSTEM:

Electronic medical records, one of the sensitive data, are stored in public or private cloud service providers. Cloud systems provide security with firewall and intrusion detection systems, and these systems ensure privacy with access control and end-to-end encryption. However, while sending data to the cloud system, attackers can capture the data with the help of Man in the Middle attacks and vulnerabilities of the storage systems. The easy implementation of AES and Rivest-Shamir-Adleman encryption (RSA) is the motivation of the study. The query contents of the medical staff user role are encrypted with AES. These data are written and updated to the database as AES encrypted. In reading query, AES is decrypted and the requested data is displayed to the medical staff user role. In patient and researcher user roles EMRs are encrypted with RSA and signed with a private key. Then, the signed data transmitted to the user. The user who has a signature key can decrypt the signed EMR with the private key and the public key. Public and private keys are distributed to users with the key distributor system developed innovatively in the study.

DISADVANTAGES:

* Security level is low.
* Cloud is semi trusted.
* Key generation and maintenance process are difficult.

PROPOSED SYSTEM:

Cryptographic Systems can be divided into deterministic and probabilistic encryption scheme. Deterministic encryption scheme allows the plaintext is encrypted by using keys that always provide the same ciphertext, but the encryption process is repeated many times. In this scheme, every plaintext has one to one relationship with the keys and ciphertext otherwise it will produce more than one output of particular plaintext during the decryption process. Probabilistic Encryption Scheme shows the plaintext has different ciphertext with the different keys. The probabilistic encryption scheme is significantly secure than the deterministic encryption scheme because it makes difficult for a cryptanalyst to access any sensitive information regarding plaintext that is taken from ciphertext and corresponding key.

Elliptic Curve Cryptography ECC) is as well-known as public key cryptography, which normally has a pair of keys, a public key and a private key and a set of actions associated with the keys to complete the cryptographic operations. The most important advantage of ECC is the small key size. The operations of elliptic curve cryptography are explained over two predetermined fields: Prime field and Binary field. For cryptographic operations, the suitable field is selected with finitely massive number of points. The prime field operations choose a prime number and finitely large numbers of basic points are produced on the elliptic curve, such that the generated points are between 0 to Z. Consequently, we randomly pick one basic point Pr (R1,R2) for cryptographic operations and this point pleases the equation of the elliptic curve on a prime field, which is explained as,



α and β are the parameters that labeling the curve and u and v are the coordinate values of the generated points bp given in Eqn. (1). In order to randomly pick one basic point pr to carry out the cryptography, it is necessary to select a private key pvky, which arbitrarily select integers less than pvky and produce a public key puky = pvky \* pr. At this time, every updated file have detached private key pvky and public key puky. The private and public values are inserted and that decimal value is changed into the binary value. Next least important bit is selected, which DataStream is employed for the encryption of the updated motion parameters. Here we are including a firefly algorithm for finding a optimized primary key.

ADVANTAGES:

* Efficient securing of data in cloud.
* Key size is minimum.