**LITERATURE SURVEY**

1. IoT Security-Cryptography and Steganography Techniques

The elliptic Galois cryptography protocol is presented as a means to encrypt data and prevent its unauthorized disclosure or modification while in transit. In addition to the secure cryp- tographic technique, The XOR steganography matrix method is implemented. Using these strategies, the secret information is embedded in the cover photo. Similarly, this makes use ofan optimization algorithm called Adaptive Firefly to pick the best possible cover blocks from within the image. Using this method, the secret message in an image will remain secure during network transfer[9].

1. A Novel image encryption technique

Four levels of security are discussed. The first level - Conformal Mapping is applied to the secret image to change the image angles(shapes). Second level incorporates Encoding techniques, where the image obtained from 1st level is set for encryption and decryption using the RSA method. In the Third level – LSB hiding method is used to hide the secret message inside the cover image. In the Fourth level compression of the final steganographic image is generated using GZIP tool[10].

1. Securing IoT Data Using Steganography

This paper employs a steganographic technique for hiding data in an Internet of Things cover signal. After completing this procedure, a stenography signal is produced and transmit- ted via the Internet of Things. Signal-to-noise (SNR) ratiosare improved with the use of low-frequency components of audio cover signals like speech and music as opposed to high- frequency components. Due to its higher energy, it proves to be an effective data-embedding medium. Signal spectra are used to reduce the interference introduced by secret information and improve the quality of the stenographic signal. The attenuation of 13 dB compared to the original signal spectrum is theresult of this attenuation. We used a multi-key combinationto satisfy the steganography system’s needs for embedding data against intentional removal attempts, including statistical undetectability, steganography signal quality[11],

1. Data security - Digital Signatures

A digital signature is a kind of signature, that is been used to sign in documents digitally[12]. This method is used in this paper. An electronic signature is like a signature is used to confirm the authenticity of the user i.e., the identity of the signatory who sent the information.In this paper, The digital signature key generation is based on based on RSA is discussed. First signature keys are created and RSA key pair is generated, withequation

ed ≡ 1 mod θ (N )

where N - the product of two random unique and large prime numbers, e and d belongs to integers, θ is used to determine

Euler’s totient function. where N and e consist of the sender’s public key, and the sender’s secret key is contained in d. To sign a message, m, the sender computes a signature equal to the equation

σ ≡ md modN

. To verify the value, in the receiver side, the receiver validates this with the mentioned equation

e ≡ m mod N

. A trapdoor permutation is a family of permutations. This method is easy to compute in the forward direction whereas computing is difficult in the reverse direction. Trapdoor permu- tations can be used for a digital signature where calculations are done in the reverse direction where the secret key is required for signing process[13].