A SURVEY ON CRYPTOGRAPHY FOR AUTHENTICATED COMMUNICATION OVER THE INTERNET USING OPTIMAL TECHNIQUES
Asst. Prof K. Vellaiammal, Computer Science, NPR Arts and Science College, Natham, Dindigul, TamilNadu, India.

ABSTRACT
In today situation, most of the communication over the internet and networks application requires the security and privacy of client sensitive information by storing data across single cloud storage providers, but these providers may be untrusted. Securities are Cryptography and steganography for image using lightweight encryption algorithm also known as secure internet of things algorithm. In cloud, splitting data into several chunks and storing parts of it on cloud in a manner using AES, DES and RC2 algorithm. RFID is a wireless technology for automatic identification and RFID data capture possible security attack and three different authentication algorithm of RFID based on ECC which is best method among them. Quantum computers would completely segregate more public key cryptosystems, including elliptic curve cryptosystems, Digital Signature Algorithm and Rivest Shamir Adleman. Benefit in terms of low cost and accessibility of data. Which fully satisfy the basic key factors of information security system which includes: Integrity, Authenticity, Confidentiality, availability and reliability.

Keywords: Cryptography, steganography, stego image, cipher image, Cloud, Encryption / Decryption Techniques, RFID, Reader, Tag, Backend Sever, Authentication, Security, ECC.

I. INTRODUCTION
Cryptography is the art and science which consists of two functions such as encryption and decryption. Whereas Encryption is the operation of transforming original image into the cipher image and decryption is just opposite operation of encryption. Cryptography is used to unauthorized access can be prevented. Steganography is a technique to hide information from attacker
A SURVEY ON CRYPTOGRAPHY FOR AUTHENTICATED COMMUNICATION OVER THE INTERNET USING OPTIMAL TECHNIQUES

which has a cover media into which the secret information is embedded. The embedding process produces a stego medium by replacing the information with data from hidden message.

There are 4 different types of steganography:
1. Text
2. Image
3. Audio
4. Video

- **Text Steganography** have a very small amount of redundant data, therefore they are very oftenly used.
- **Audio/Video Steganography** is very complex in use.
- **Image Steganography** is the most widely used for hiding process of data. It provides a secure and simple way to transfer the information over the internet.

It is categorized in various types:
- Transform Domain: It includes JPEG.
- Spread Spectrum: It includes patch work.
- Image Domain: It includes->LSB and MSB in BMP and LSB and MSB in JPG

Other techniques are (i) symmetric key based algorithm, sometimes known as conventional key algorithm and (ii) asymmetric key based algorithm, also known as public-key algorithm. In the cloud protected information prevented from malicious attacks. The cloud can be accessed through internet from anywhere. The users have to login to the cloud and provide details to access the data from database.

![Figure-1](image1.png)

Figure-1

On other hand security attack possible on RFID, its performance measurement, and three authentication methods or protocol.

![Figure-2](image2.png)

Figure-2

Security Attack on RFID

**Denial of Service (DOS):** In both of wireless and wired communication, Once attackers control a large number of fake readers and tags, they can make the data connection to abuse computational resources, and even use up the resources and network bandwidth. [3]

**Eavesdropping:** The communication between the tag and the reader can be eavesdropped, because the radio frequency channel is not secure communication channel. [3]

**User privacy:** The attacker can trace the user location with the tag identifier, when the output of the tag such as the tag identifier is unchangeable. [3]

**Replay attack:** The attacker obtains messages between the reader and the tag by
eavesdropping and reuses the message in order to impersonate a legitimate reader. [3]

**Spoofing attack:** The attacker impersonates a reader, sends a query to a tag, and then obtains the response of the tag. When the legitimate reader queries the tag, the attacker will send the obtained response to reader in order to impersonate the tag. [3]

**Cloning attack:** An attacker can build a cloned tag which will be interpreted by the reader as the legitimate tag, due to the fact that most tags are not tamper-proof. [3]

**Performance**

RFID schemes cannot use computationally intensive cryptographic algorithms for privacy and security because tight tag cost requirements make tag-side resources (such as processing power and storage) scarce. [3]

- **Capacity minimization:** The volume of data stored in a tag should be minimized because of the limited size of tag memory.
- **Computation minimization:** Tag-side computations should be minimized because of the very limited power available to a tag.
- **Communication compression:** The volume of data that each tag can transmit per second is limited by the bandwidth available for RFID tags. [3]
- **Scalability:** The server should be able to handle growing amounts of work in a large tag population. It should be able to identify multiple tags using the same radio channel. [3]

Performing an exhaustive search to identify individual tags could be difficult when the tag population is large. [3]

A transition to post-quantum cryptography is very unlikely to be just a simple “drop-in” replacement for current public-key cryptographic algorithms. Developing, standardizing, and deploying new post-quantum cryptosystems will require significant time and effort.

**II. LITERATURE SURVEY**

2. a. **Review on Image Encryption and Decryption technique using AES Algorithm**

The Advanced Encryption Standard (AES) algorithm is a symmetric block cipher that processes image which is of blocks size 128 bits using three different cipher key sizes of lengths 128, 192 or 256 bits. Based on the key size length used, the number of execution rounds of the algorithm is 10, 12 or 14 respectively. The proposed system consists of block size of 128 bits and key size of 256 bits. The algorithm is applied for both image encryption and decryption. As the key size is of 256 bits it will take 14 rounds.

b. **SIT: A Lightweight Encryption Algorithm for Secure Internet of Things**

The IoT is composed of many small devices such as RFIDs which remain unattended for extended times, it is easier for the adversary to access the data stored in the memory. Some well-known block cipher including AES, 3-Way, Grasshopper PRESENT, SAFER, SHARK, and Square use Substitution-Permutation (SP) network. Several alternating rounds of substitution and transposition satisfy the Shannon’s confusion and diffusion properties that ensure that the cipher text is changed in a pseudo random manner.


Encryption techniques such as AES, 3DES, Blowfish and DES. DES key size is too small as compare to other techniques. 3DES is slower than other block cipher methods and has poor performance. AES algorithm was considered to be the best algorithm than that of blowfish algorithm. The adjacent pixels
A SURVEY ON CRYPTOGRAPHY FOR AUTHENTICATED COMMUNICATION OVER THE INTERNET USING OPTIMAL TECHNIQUES

in an image have close relation which cannot be easily removed by AES algorithm.

d. A review on Image encryption techniques

Traditional encryption techniques like DES, AES or IDEA etc. for providing high security to the data that may be textual or image form.

3. Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key.

Symmetric key ciphers are implemented as either block ciphers or stream ciphers. A block cipher enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a stream cipher. The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are blocking cipher designs.

Asymmetric Key Cryptography:

Public-key algorithms are most often based on the computational complexity of "hard" problems, often from number theory.

Data Encryption Standard:

DES is the archetypal block cipher—an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another ciphertext bit string of the same length.

The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits. The key is nominally stored or transmitted as 8 bytes, each with odd parity.

Before the main rounds, the block is divided into two 32-bit halves and processed alternately; this criss-crossing is known as the Feistel scheme. The Feistel structure ensures that decryption and encryption are very similar processes—the only difference is that the sub keys are applied in the reverse order when decrypting.

For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

A. Byte Substitution (Sub Bytes)

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

B. Shiftrows

Each of the four rows of the matrix is shifted to the left. Any entries that “fall off” are re-inserted on the right side of row. Shift is carried out as follows –

i. First row is not shifted.

ii. Second row is shifted one (byte) position to the left.

iii. Third row is shifted two positions to the left.

iv. Fourth row is shifted three positions to the left.

v. The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

C. MixColumns

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the
four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

D. Addroundkey

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

E. Decryption Process

Each round consists of the four processes conducted in the reverse order –

- Add round key
- Mix columns
- Shift rows
- Byte substitution

RC-2 Encryption Algorithm:

In cryptography, RC2 (also known as ARC2) is a symmetric-key block cipher designed by Ron Rivest in 1987. "RC" stands for "Ron's Code" or "Rivest Cipher"; other ciphers designed by Rivest include RC4, RC5, and RC6. The development of RC2 was sponsored by Lotus, who were seeking a custom cipher that, after evaluation by the NSA, could be exported as part of their Lotus Notes software. The NSA suggested a couple of changes, which Rivest incorporated. After further negotiations, the cipher was approved for export in 1989.

ECC based algorithms would be the best choice for RFID system due to their small size key and efficient computation. So, ECC is very attractive for small devices like RFID with limited computational capacity, memory and low bandwidth network.

a) A secure ECC based RFID authentication protocol with ID verifier

This algorithm provide Mutual authentication, confidentiality, forward security, scalability. This algorithm resisting replay attack, tag masquerade attack, server spoofing attack, location attack, cloning attack [3].To implement this schema successfully a powerful server device needed [3].

b) Cryptanalysis and improvement of an efficient mutual authentication RFID scheme based on elliptic curve cryptography

Farash’s schema has proof against mutual authentication, tag privacy. Computational cost of Frash’s schema is same as Chou’s schema [8].The total computation of schema is very high.

c) Elliptic Curve Cryptography Based Mutual Authentication Protocol for Low Computational Capacity RFID Systems - Performance Analysis by Simulations

While in use of 160 bit elliptic curve might be very big and required high computational capacity and strong back-end sever [9].This paper have implementation in OMNET ++. Godor’s schema is acceptable for every attack except DOS. This schema also proves that computational time for 112 bit and 160 bit are almost near.
A SURVEY ON CRYPTOGRAPHY FOR AUTHENTICATED COMMUNICATION OVER THE INTERNET USING OPTIMAL TECHNIQUES

Comparison

<table>
<thead>
<tr>
<th>Attacks</th>
<th>Liao’s</th>
<th>Farash’s</th>
<th>Gedor’s</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mutual authentication</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Scalability</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>DOS</td>
<td>-</td>
<td>-</td>
<td>No</td>
</tr>
<tr>
<td>Cloning</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Server spoofing</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Replay</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
</tr>
</tbody>
</table>

Comparison factor

<table>
<thead>
<tr>
<th>Computational time</th>
<th>Liao’s</th>
<th>Farash’s</th>
<th>Gedor’s</th>
</tr>
</thead>
<tbody>
<tr>
<td>.32 sec</td>
<td>Not measured</td>
<td>.1006 (160bit)</td>
<td></td>
</tr>
</tbody>
</table>

4. The SHA-3 and AES candidates in consideration of the following factors:

- The requirements for public-key encryption and digital signatures are more complicated;
- The current scientific understanding of the power of quantum computers is far from comprehensive; and,
- Some of the candidate post-quantum cryptosystems may have completely different design attributes and mathematical foundations, so that a direct comparison of candidates would be difficult or impossible.

<table>
<thead>
<tr>
<th>Cryptographic Algorithm</th>
<th>Type</th>
<th>Purpose</th>
<th>Impact from large-scale quantum computer</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>Symmetric key</td>
<td>Encryption</td>
<td>Larger key sized needed</td>
</tr>
<tr>
<td>SHA-2, SHA-3</td>
<td>-</td>
<td>Hash functions</td>
<td>Larger output needed</td>
</tr>
<tr>
<td>RSA</td>
<td>Public key</td>
<td>Signatures, key establishment</td>
<td>No longer secure</td>
</tr>
<tr>
<td>ECDSA, ECDH (Elliptic Curve Cryptography)</td>
<td>Public key</td>
<td>Signatures, key exchange</td>
<td>No longer secure</td>
</tr>
<tr>
<td>DSA (Finite Field Cryptography)</td>
<td>Public key</td>
<td>Signatures, key exchange</td>
<td>No longer secure</td>
</tr>
</tbody>
</table>

Figure-5

1. In this paper, learned that encryption and decryption both are combined on cryptography and formed a new technique which is effective but needs additional operating requirements. Every technique has its own advantages or disadvantages according to the way of its working.

III. CONCLUSION

Cryptography and Steganography are technique provide higher security to data. The use of the Secure Internet of Thing algorithm and LSB gives a way to secure the information from unauthorized user and provide better PSNR value. LSB to hide encrypted image into stego image, which provides the new attract to the image steganography. It is very difficult to recover the hidden image for an unauthorized user without knowing the bits of the frames. The technique of elliptic curve cryptography encryption to protect data files in the cloud. The ECC Encryption algorithm used for encryption is another advantage to improve the performance during encryption and decryption process.

In the conclusion of three are ECC based on authentication schema; all are proved more efficient against simple PKI, simple HASH, AES and RSA. All three have more computational time to perform authentication and needed high capacity back-end sever. So in future some pre-computational method can implement with ECC. The process of post quantum cryptography standardization-resistant counterparts to existing standards, including digital signature schemes specified in Federal Information Processing Standards (FIPS) 186 and key establishment schemes specified in NIST Special Publications (SPs) 800-56 A and B. Finally I conclude that the proposed technique is effective for secret data and image communication.

Asst. Prof K. Vellaiammal
IV. REFERENCES

[1].http://www.google.com