**Report**

on

**Information-Security**
**(Assignment 2)**
**Connected Systems and Devices**
**(DA614A)**

**Submitted**

by

**Prakriti Dhang**
**Annwesh Mukherjee**
**Lakshmidas Gurukkalkandy**
**Manaswini Kolluru**

**Supervisor**

**Majid Ashouri Mousaabadi**


Department of Computer Science,
Faculty of Technology and Society
Malmö University
Malmö, Sweden

## I. Intoduction

This assignment is to extend the functionality of our client application to cryptographic approach. The client-server system, includes one server application running on the axis camera and one client application running on your desktop computer. The main functionality of this system is to protect unauthorized access to the images that are transferred over the, possible unsafe, network.

We all know that computers are running on multiple programs, mulitple services running on those machines. And, so if we get a packet, or information than just on specific machine, we need more information from point A to point B. So, TCP and IP are two separate protocols. TCP is responsible for getting correct service to the correct program and it has good gaurantee delivery. So, if we now couple a machine's IP address with so called port number and port number is how a specific service, or utility, or program identified on a machine. When a program wants to send a data, TCP helps to break the data into chunks and communicates with those packets to the computer's network software. It takes data and wraps the information around it. This assignment is an extension of the functionality of our client-server application using cryptographic approach.

Cryptography [1] is one of the practice and study of techniques for secure communication in the presence of third parties attackers. Cryptography is the process of encryption and deryption of messages that are sent from sender to receiver. Basically, encryption is the process of converting plain text to cipher text, whereas, decryption is the process of converting cipher text to plain text. Encryption and decryption of messages can be done through many algorithms.We used RSA [2] and XOR for encrypting and decrypting.

## II. Requirements for the application

- Encrypting the Frequency and Resolution in the Client
- Decrypting the Frequency in the server
- Encrypt the captured image at the server.
- Decrypt the Images in the client

## III. UML diagrams of our model

### A. *Usecase diagram*

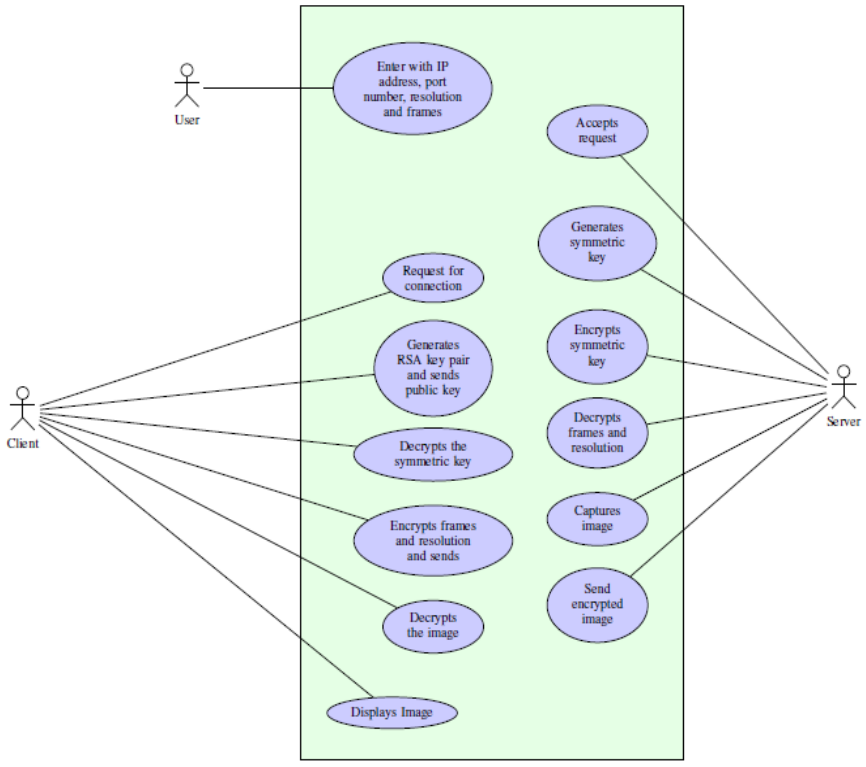


Fig. 1: Use Case Diagram

*B. Sequence diagram*


Fig. 2: Sequence Diagram

## IV. Cryptographic Approach

### *A. **Client-Server Implementation:***

For implementation of security we used asymmetric RSA and symmetric XOR algorithms. RSA key pair was generated in the Client side and Server side. We haven't used the server RSA key. The symmetric key was generated in the Server side. The Client share's the public key to the Server. The Server is encrypting the symmetric key with Client's RSA public key. The Encrypted key is sent to the Client and client decrypts it with its own private key. The Client encrypts the frequency and resolution using symmetric key and XOR cipher and sends to the server. The Server decrypts the frequency and resoultion. Server captures the image and then encrypts the image and sends to the Client. The Client decrypts the image using the symmetric key and XOR cipher and dispalys the image.

### *B. **Mechanisms (other than cryptography) you think are relevant to implement in your system in order to improve its security properties***

To make the system more secure, the images needs to be secured while the data is on-transit and at-rest.The images can be saved in the client machines after decrypting the image data and at that time it is visible to all or authenticated users of

the client machines. In order to limit this vulnerability, in our system, the images are continuously streamed to the GUI rather than save and display it. To protect the images captured by cameras, identity and access management (IAM) system can be implemented in the console application. It enables only the right individuals to access right resources. The ”on-transit” data can be secured by using password-protected zipped images along the encryption. This may impact the performance of data transfer due to compression logic, but it gives additional layer of protection to the data. Another option is to transfer images after implementing stegano-graphic images in order to hide the actual images those are captured by each Cameras.

## V. Interesting and Challenging

Receiving the public key in the server side, Decrypting the images in client side is an intersting and tedious task to achieve. Implementation of RSA is very challenging because of extremely intricate structure of the algorithm. Camera network was not stable and there is delay in the image capturing. Debugging the Cyptography algorithms is more time consuming approach. The RSA and XOR encryption and decryption call between server and client machines can be implemented in different sequences. It was an opportunity for the team to sequence out the data transfer along the encryption logic differently and to discuss the pros-and-cons of each implementations. OpenSSL and was initially tried out in server and client modules for encryption, but later we understood that OpenSSL may not support in server side. So, the RSA encryption was implemented from base logic.

## References

[1] https://en.wikipedia.org/wiki/Cryptography
[2] http://mathworld.wolfram.com/RSAEncryption.html