ED-Crypt

Ethernet Dongle for Encryption Decryption

8/15/2010

Anshul Jain (2008cs10160)
Akash Singh (2008cs10154)
Aseem Garg (2008cs10165)
Ujjaval Kumar Singh (2008cs10196)

INDEX

Encrypting network data smartly

1. Project Specification

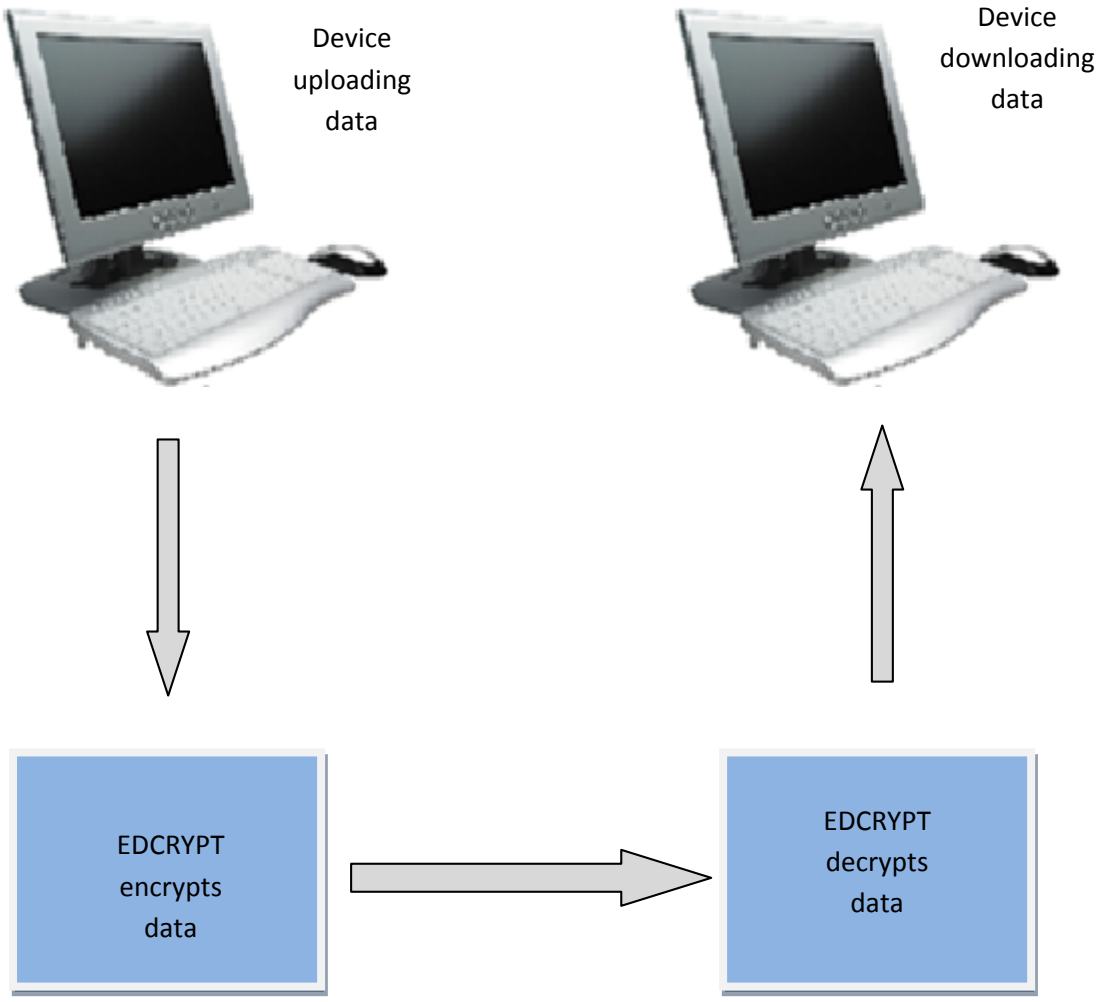
This project aims to build a network dongle that can be used to implement encryption for data being transmitted or being received over the internet. The device will have an FPGA chip for implementing the encryption algorithms in hardware to achieve high speeds. The TCP/IP would be implemented in software on a microprocessor (that can be soft core also) which would act as the main processor to the FPGA co-processor.
The project finally aims to build the dongle that can be attached in the network permanently and can relay data without encryption/decryption also. Only the data being transmitted over a special protocol (in the application layer) would be encrypted and decrypted at the other end. This can be viewed as if the device implements a new layer below the application layer in the network protocol that would encrypt the data being transmitted over special protocols. Such a device would provide following advantages:

1. Encryption in real time. Encryption in software usually takes a long time due to the high computational work involved. Implementation of such algorithms in hardware would give the speeds required to encrypt/decrypt data on the fly.
2. Even the most well written encryption programs are susceptible to attack from various kinds of viruses and trojans that forcibly insert a backdoor in the program running or manage to extract the key during the encryption process. Implementing such algorithms outside of main operating system makes the communication lot more secure.
3. Such a device due to use of both FPGA and microprocessor, gives extreme flexibility in terms of reconfiguration of the both hardware and software to cope with the newest advances in the field of cryptography.

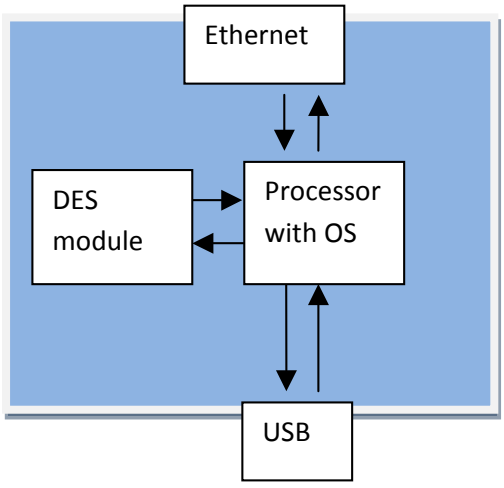
2. CSP315 Deliverable

In CSP315 we would try to implement a very simplified version of EDCrypt. We would try to implement any simple encryption like DES that can be downloaded from the internet. At this stage the device would not cater to data that is not encrypted. However we will try to achieve very high speeds of communication – at least 10 Mb/s. The project would be implemented on a development board available off the shelf. We would try to get an operating system running on the processor to implement TCP/IP. Depending on the kind of board we use the device would talk to the end system through Ethernet or USB. Also we would be implementing only Ethernet based dongle at this stage.

3. Method and Block diagram



ED-Crypt Module:



4. Hardware

We are undecided over the kit that we would be using at this time. We are presently looking into the following kits available:

- **TS-7300**
  https://www.embeddedARM.com/products/board-detail.php?tab=options&product=TS-7300#

- **TS-7800**
  http://www.embeddedarm.com/products/board-detail.php?product=ts-7800#

We are also trying to implement a softcore processor running on a Digilent kit available in the lab and get an OS running on it. If we can do that easily we would order a FPGA kit that that has USB capabilities.

5. Scheduled time span

August:

Week 3 and 4: identifying and procuring the board, running EDK, implementing processor and installing the OS.

September:

Week 1 and 2: Studying TCP/IP APIs for the OS and successfully using the Ethernet port to relay the data to a PC on the other end.

Week 3 and 4: Studying USB protocols for the OS and successfully using the USB port to relay the data to a PC on the other end.

October:

Week 1: Implementing the DES encryption algorithm on the FPGA and running it successfully.

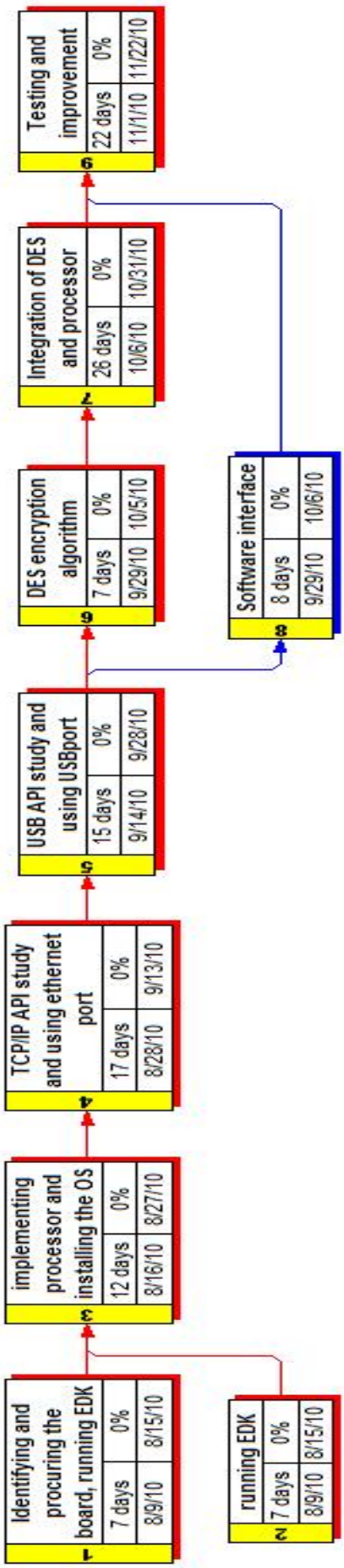
Week 2,3,4: Integrating the above mentioned DES module with the processor on the board.

November:

Week 1: Implementing the software part of the USB interface with the PC.

Week 2,3,4: Running tests on the device developed, optimization and fine tuning of all the modules.

PERT
CHART


Identifying and procuring the board, running EDK
1
7 days
0%
8/9/10
8/15/10
running EDK
2
7 days
0%
8/9/10
8/15/10
implementing processor and installing the OS
3
12 days
0%
8/16/10
8/27/10
TCP/IP API study and using ethernet port
4
17 days
0%
8/28/10
9/13/10
USB API study and using USBport
5
15 days
0%
9/14/10
9/28/10
DES encryption algorithm
6
7 days
0%
9/29/10
10/5/10
Software interface
8
8 days
0%
9/29/10
10/6/10
Integration of DES and processor
7
26 days
0%
10/6/10
10/31/10
Testing and improvement
8
22 days
0%
11/1/10
11/22/10

6. Visit the project's webpage

https://sites.google.com/site/edcrypt2010/