Ethernet Dongle for Encryption/ Decryption

ED-Crypt

By-
Akash Singh (2008cs10154) Anshul Jain (2008cs10160)
Aseem Garg (2008cs10165) Ujjaval Kumar Singh(2008cs10195)

Introduction

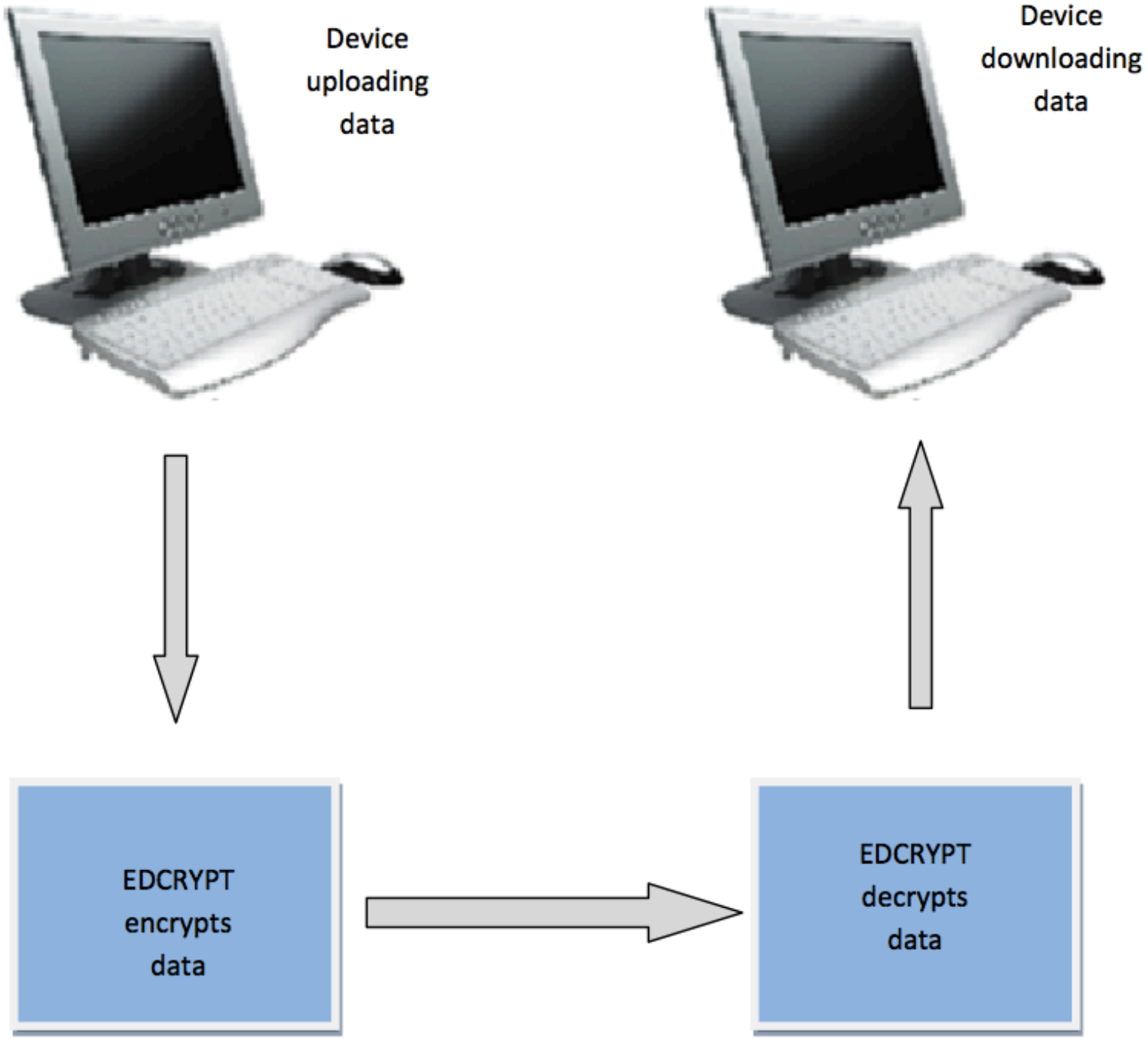
- This project seeks to build a device that can encrypt and decrypt data being transmitted or received over the internet.

- The device will be in the form of a **dongle** (a small device that processes transient data) connected between the PC and the internet.

Introduction (Cont.)

- Support for normal (unencrypted) data transfer

- Run time functionality : Data encryption on the fly.


Device uploading data
Device downloading data
EDCRYPT encrypts data
EDCRYPT decrypts data

ADVANTAGES OF ED-Crypt

- **Encryption in real time:** Encryption in software usually takes a long time due to the high computational work involved. Hardware would give the speeds required to encrypt/decrypt data on the fly.

- **Extra Safety:** Encryption programs are susceptible to attack from various kinds of viruses and trojans. Implementation outside of main operating system makes the communication lot more secure. Also, hardware is difficult to replicate.

- ***Reconfigurable Computing:***

  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.

CSP Deliverable

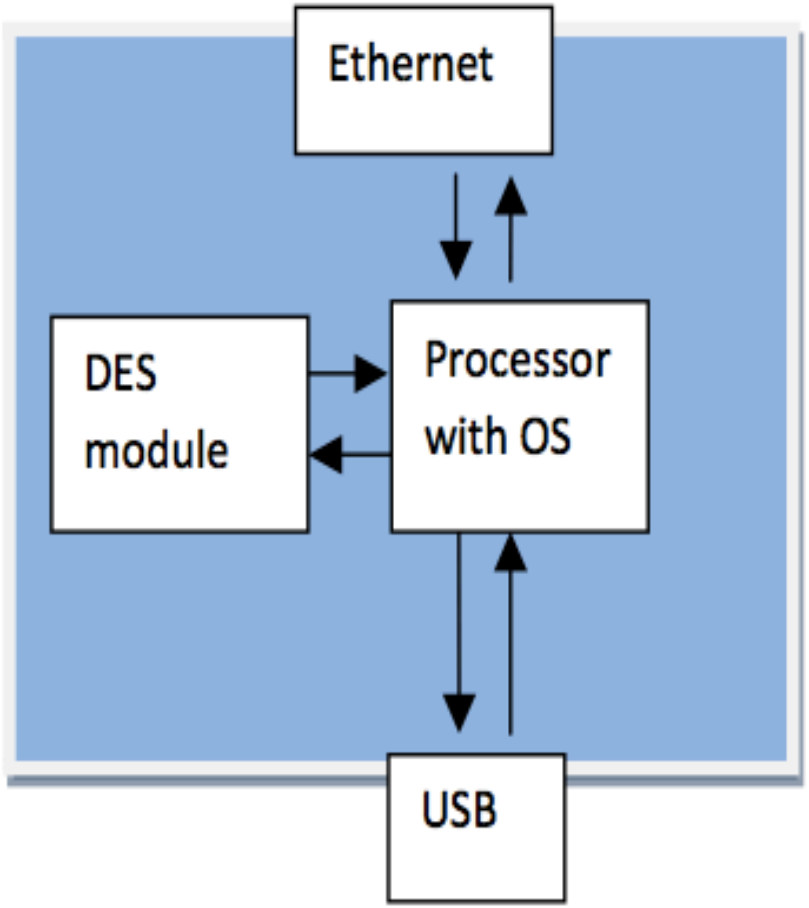
- The project currently aims to develop a device for encryption / decryption for all data passing through it, and transfer it to another PC/ device connected directly to the first device via USB/ethernet cable respectively.

IMPLEMENTATION

- 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.

ED-Crypt Module:



PLAN

- At this stage the device will encrypt everything, and try to achieve high speeds of communication – at least 10 Mbps.

- We would try to get an operating system running on the processor to implement TCP/IP. The device would talk to the end system through Ethernet or USB.

- We would be implementing only Ethernet based dongle at this stage.

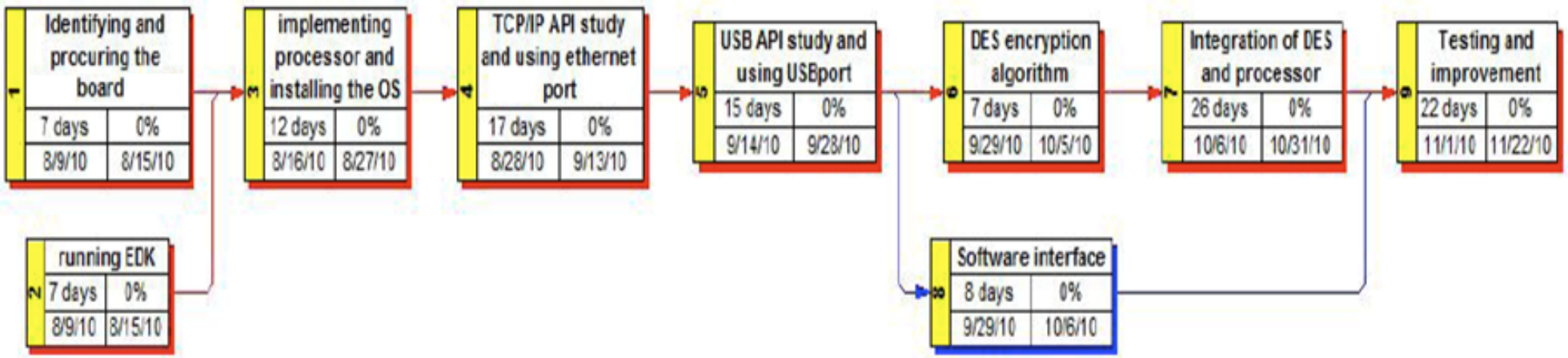
Hardware

- We are intend to work on Xilinx ML310 platform.

- Features:
  - Virtex 2V Pro FPGA
  - 2 USB ports
  - Ethernet port
  - Power PC processor inbuilt on the FPGA chip
  - MMU (Memory Management Unit)
  - SD Card and 512 MB Flash memory.

- We will burn the Linux OS on the processor to implement the USB and Ethernet operations. For this we will use Xilinx EDK.

TIME LINE


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

Possible Extensions

- Selective encryption of data.
- Multiple options for algorithms for encryption / decryption.
- Support for Wireless and Bluetooth.

Thank You