ESCUELA SUPERIOR DE INGENIERÍA

Grado en Ingeniería Informática

Infraestructura de red de nodos cifradores/descifradores AES basada en ApSoC

Curso 2019-2020

Jesús Rodríguez Heras

Puerto Real, 28 de Noviembre de 2019

ESCUELA SUPERIOR DE INGENIERÍA

Grado en Ingeniería Informática

Infraestructura de red de nodos cifradores/descifradores AES basada en ApSoC

DEPARTAMENTO: Ingeniería Informática.
DIRECTORA DEL PROYECTO: María Ángeles Cifredo Chacón.
CODIRECTORA DEL PROYECTO: María Mercedes Rodríguez García.
AUTOR DEL PROYECTO: Jesús Rodríguez Heras.

Puerto Real, 28 de Noviembre de 2019

Fdo.: Jesús Rodríguez Heras

Declaración personal de auditoría

Jesús Rodríguez Heras con DNI 32088516C, estudiante del título de Grado de Ingeniería Informática en la Escuela Superior de Ingeniería de la Universidad de Cádiz, como autor de este documento académico titulado "Infraestructura de red de nodos cifradores/descifradores AES basada en ApSoC" y presentado como Trabajo Final de Grado

DECLARO QUE:

Es un trabajo original, que no copio ni utilizo parte de obra alguna sin mencionar de forma clara y precisa su origen tanto en el cuerpo del texto como en su bibliografía y que no empleo datos de terceros sin la debida autorización, de acuerdo con la legislación vigente. Asimismo, declaro que soy plenamente consciente de que no respetar esta obligación podrá implicar la aplicación de sanciones académicas, sin perjuicio de otras actuaciones que pudieran iniciarse.

En Puerto Real, a 28 de Noviembre de 2019.

Fdo.: Jesús Rodríguez Heras

Agradecimientos

Me gustaría mostrar mis agradecimientos a la gente.

Resumen

Infraestructura de red para conectar los nodos zybo.

Palabras clave

Red, Infraestructura, Zybo, Conexión.

Contenido

Lista de Figuras

Lista of Tablas

Parte I

Introducción

Capítulo 1

Objetivos

1.1 Objetivo principal

El objetivo del trabajo es diseñar una red de nodos basada en tecnología ApSoC, de modo que cada uno de los nodos/elementos de la red reciban un fichero de datos, lo descifre, inserte información adicional y lo vuelva a cifrar antes de enviarlo a otro elemento de la red. El monitor generará el primer conjunto de datos que enviará a uno de los nodos, y cuando haya pasado por todos, recibirá el conjunto final. La red será privada y contará con un monitor basado en un ordenador personal.

Capítulo 2

Descripción

Cada uno de los nodos de la red será una tarjeta basada en la tecnología Zynq de Xilinx. Esta tecnología incluye un procesador ARM dual-core que se encargará de gestionar las comunicaciones en la red mediante protocolo TCP/IP. El otro elemento constituyente de Zynq es lógica programable, en la que estará implementado el periféricos o IP, ya diseñado y verificado, para el cifrado/descifrado AES. Se evaluará la posibilidad de que cada tarjeta incluya solo lo necesario para contar con comunicación TCP/IP o bien un sistema operativo basado en Linux.

El diseño de la infraestructura de red implica la instalación de un arranque autónomo de cada tarjeta desde memoria SD. La interconexión física de las tarjetas y el monitor a través de un switch mediante topología Ethernet, siendo el número de nodos ampliable de forma dinámica y automática. La creación y ejecución de un conjunto de pruebas que permitan confirmar el correcto funcionamiento de la red, en primera instancia, y el correcto funcionamiento del sistema de envío/recepción de datos, en segunda.

Capítulo 3

Alcance

El trabajo incluirá:

- Instalación física del ordenador personal que actuará como monitor.
- Creación de una imagen de arranque en tarjeta SD para las placas que formarán parte de la red. El arranque incluirá el bitstream necesario para configurar la lógica programable de Zynq con el IP AES core, así como el resto de elementos. necesarios para completar la funcionalidad de cada placa.
- Instalación física de cada tarjeta en la red y configuración del switch.
- Creación de los scripts necesarios para que cada nodo/tarjeta sea capaz de:
  - Recibir datos.
  - Descifre datos.
  - Modifique datos.
  - Cifre datos.
  - Envíe datos a otro nodo.
- Creación y ejecución de los tests que permitan comprobar el correcto funcionamiento de la infraestructura.
- Preparación del fichero de datos inicial en el monitor.
- Creación y ejecución de los tests que permitan comprobar el correcto funcionamiento de la transferencia y modificación de datos.

Parte II

Metodología

Capítulo 4

Marco teórico

Introducir el marco teórico en el que nos encontramos

Capítulo 5

Tecnologías a utilizar

5.1 Diseño de la arquitectura

No se si debería poner los siguientes apartados

5.1.1 Arquitectura física

5.1.2 Arquitectura lógica

5.1.3 Arquitectura de diseño

5.2 Diseño de componentes

Capítulo 6

Análisis del sistema

Aparte de lo que hay debajo, añadir por ahí también que son capaces de descifrar y añadir información proporcionada por el usuario mediante un pendrive.

6.1 Hardware

Requisitos de la red en si, explicando lo que tendrá que haber y como deberá conectarse, sin decir todavía cómo.

6.2 Software

Hablará de los test que habrá que diseñar y luego de los scripts que deberán automatizar el funcionamiento del sistema.

Capítulo 7

Diseño y desarrollo

7.1 Hardware

Aquí explicamos lo citado en el apartado de análisis.

7.2 Software

Aquí explicamos lo citado en el apartado de análisis.

Capítulo 8

Pruebas del sistema

Aquí describimos los scripts para hacer pruebas e incluir las pruebas que hice para ver su funcionamiento.

8.1 Hardware

8.2 Software

No se si poner los siguientes puntos también (del 8.3 hasta el 8.6)

8.3 Pruebas unitarias

Cada script funciona de forma independiente(?)

8.4 Pruebas de integración

Todo funciona porque es en bash

8.5 Pruebas de sistema

Todo lo he probado yo personalmente

8.5.1 Pruebas funcionales

No se que prueba va aquí

8.5.2 Pruebas no funcionales

No se que prueba va aquí

8.6 Pruebas de aceptación

No se que prueba va aquí

Parte III

Conclusiones y trabajo futuro

Capítulo 9

Conclusiones

Capítulo 10

Trabajo futuro

Parte IV

Referencias/Bibliografía

Capítulo 11

Referencias bibliográficas

Parte V

Anexos técnicos

Apéndice A

Manual de usuario

Aquí puedo poner mis manuales.

Apéndice B

Datos técnicos

Aquí puedo poner algún dato técnico a tener en cuenta en el proyecto.

Apéndice C

Códigos

Aquí puedo incrustar tal cual los scripts del proyecto.