Abstract

In early days, the data transfer was done by wired media like co-axial cable(s), fiber optic cable(s) etc. The era has gone. Nowadays wired media is replaced by wireless means, for which Wi-Fi, ZigBee, Bluetooth and Dash7 (Wireless Sensor Networks) are used. Out of these techniques, Bluetooth is mostly used nowadays. This study emphasizes that wireless communication system for secured data transfer can be done by Bluetooth connectivity. Bluetooth devices are short range and meant for low power utilization, allowing communication between various devices. Various algorithms have been developed for the purpose of providing security to the data to be transferred. Main techniques are DES (Data Encryption Standards), AES (Advanced Encryption Standards), and EES (Escrowed Encryption Standards). Out of them, the Advanced Encryption Standards is the most widely used. This study analyzes the development of fully secured wireless connection terminals on a FPGA where connection is established using Bluetooth technology and advanced encryption standards (AES) are used to initialize the secured algorithm for data exchange. RC-10 Prototyping board with Xilinx Spartan-III XC3S1500L-4-FG320 FPGA device is used for hardware evaluation of system design.
References

- Anurag Gupta, Afandi Ahmadd, Mhd Saeed Sharif And Abbes Amira, "Rapid Prototyping of AES Encryption For Wireless Communication System On FPGA".
- [online ] available on : http://www. mentor. com/

**Index Terms**

Computer Science

Wireless

**Keywords**

Advanced Encryption Standard (AES)  Field Programmable Gate Array (FPGA)