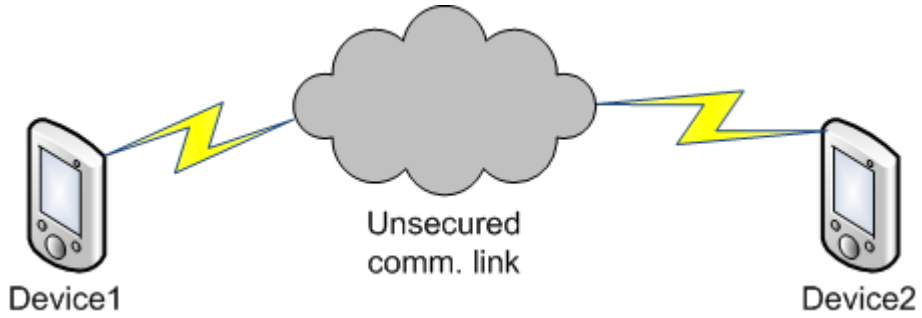
Advanced Embedded System Design

Secure Communication for Embedded System

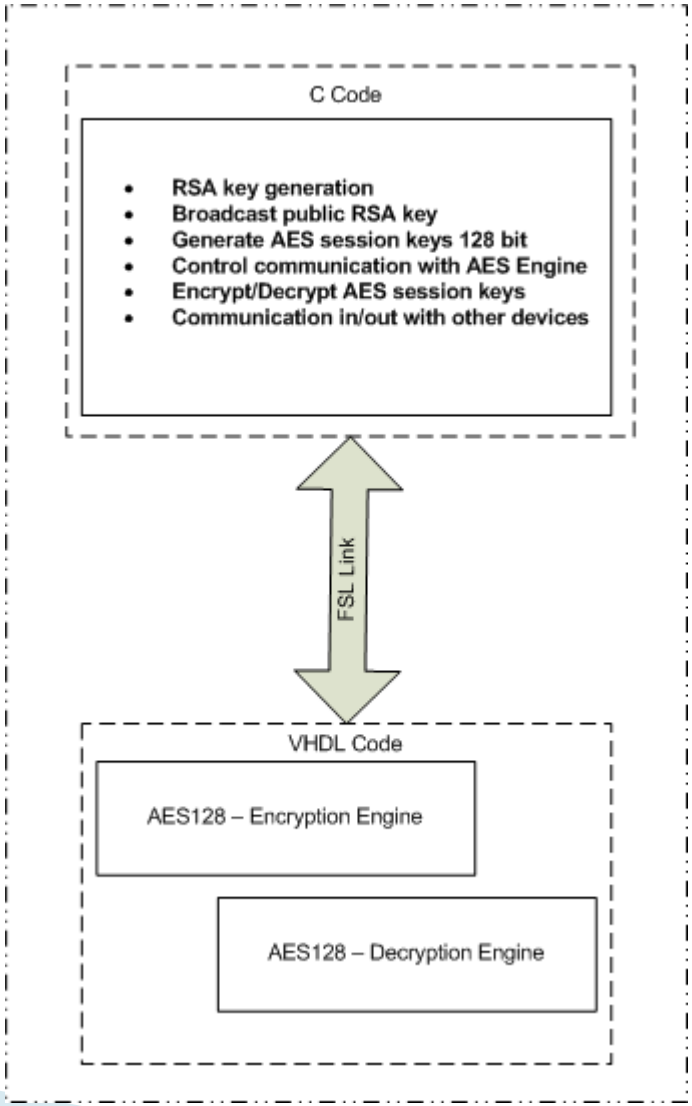
by
Ahmed, Mohammed & Orges

System overview



- Device1 communicates via unsecured link to Device2
- Data is exchanged using hybrid(asymmetric & symmetric) encryption
- AES128 bit is used for symmetric encryption of the message(s)
- RSA is used for asymmetric encryption of AES session key

Block diagram overview



Further development

- Usage of RS232 com link for initial development, but..
- Possible extension to
  - RF link
  - Ethernet link