سیستم رمزنگاری برای اپلیکشن‌های داده‌ای در حوزه IOT

حمید فرزین پور

علوم تحقیقات-دی ماه 99

فهرست

- اینترنت اشیا
- چالش امنیت در IOT
- مدل AES
- مدل ESB
- مدل CBC
- مدل CBC
- برد UDOO Neo
- سیستم احراز هویت

اینترنت اشیا

- کاربران شخصی
- حمل و نقل
- خانه هوشمند
- پزشکی
- صنعت
- آموزش
- و...

چالش امنیت در IOT

- افزایش کاربردها و خدمات مبتنی بر اینترنت اشیا در صنایع مختلف
- دسترسی راحت و گسترده به اینترنت معضلات امنیتی فضای سایبری
- افزایش انگیزه‌ها برای انجام فعالیت‌های مخرب امنیتی در حوزه اینترنت اشیا
- نقش کارکردی و انکارناپذیر آسیب‌پذیری‌های امنیتی در بروز و ظهور فعالیت‌های مخرب در حوزه اینترنت اشیا
- توسعه تکنیک‌ها و مفاهیم برای بهینه‌سازی امنیت و کاهش آسیب‌پذیری‌ها
- تعریف قوانین جدید در زمینه گسترش کاربری و توسعه کسب‌وکارها با ممانعت از ایجاد آسیب‌پذیری‌ها و حفظ حریم خصوصی

Advanced Encryption Standard(AES)

- موسسه ملی فناوری امریکا 2001
- الگوریتم کلید متقارن
- سایز بلاک ۱۲۸،۱۹۲،۲۵۶
- کلید Encryption
- کلید Dencryption

Electonic Code Book(ECB)

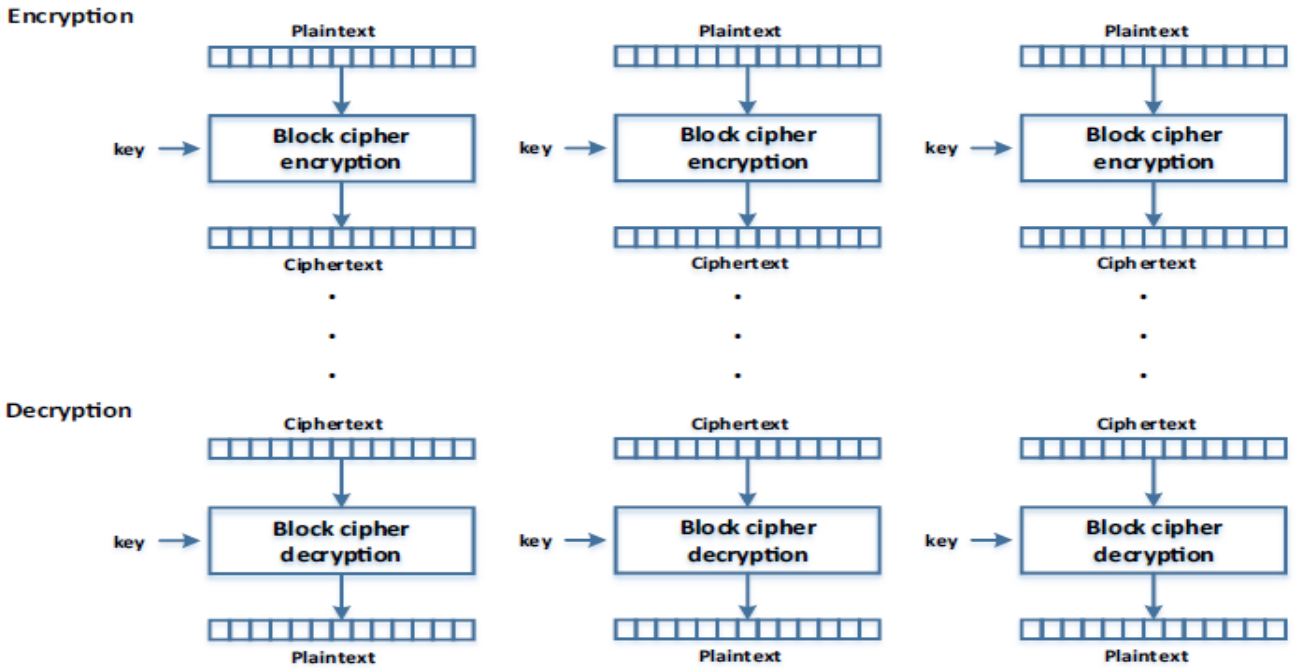


Fig. 1. Electronic code book (ECB) mode of AES.

Cipher Block Chaining (CBC)

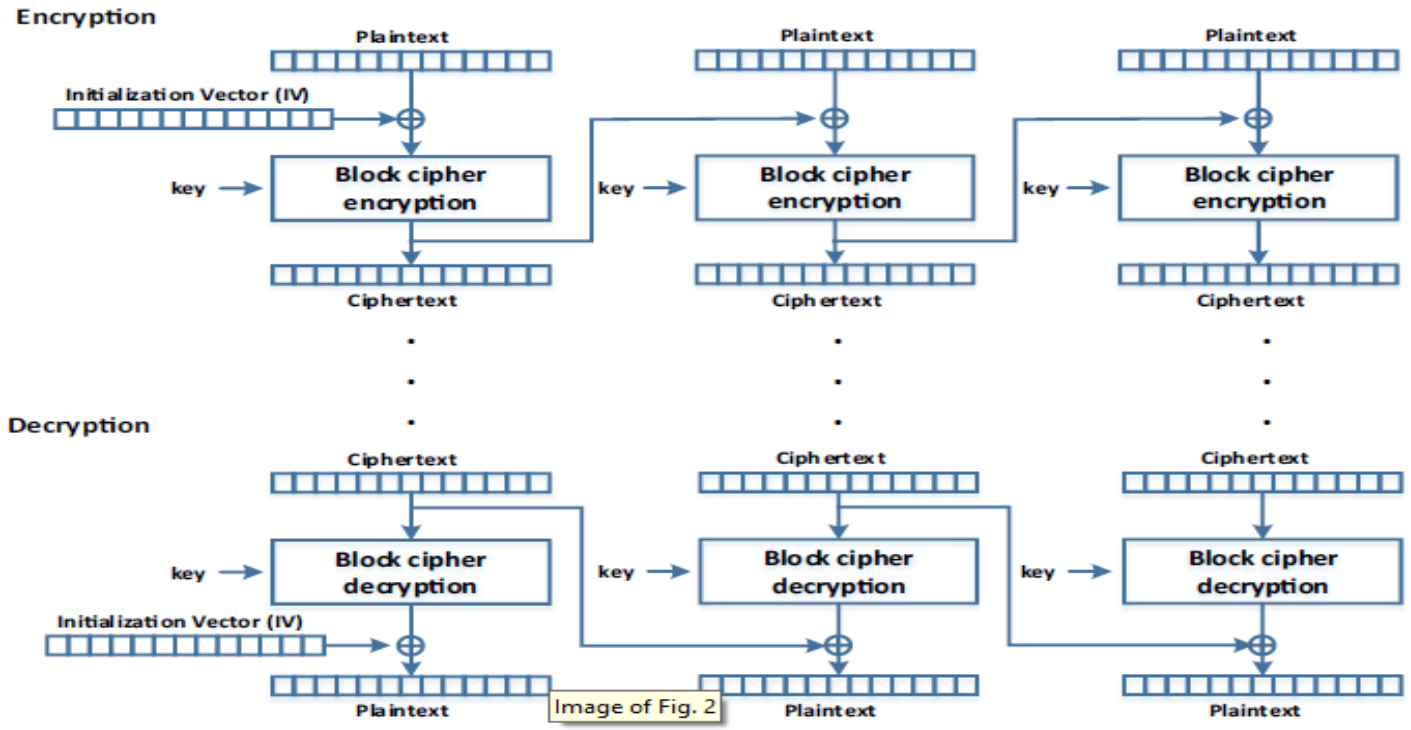
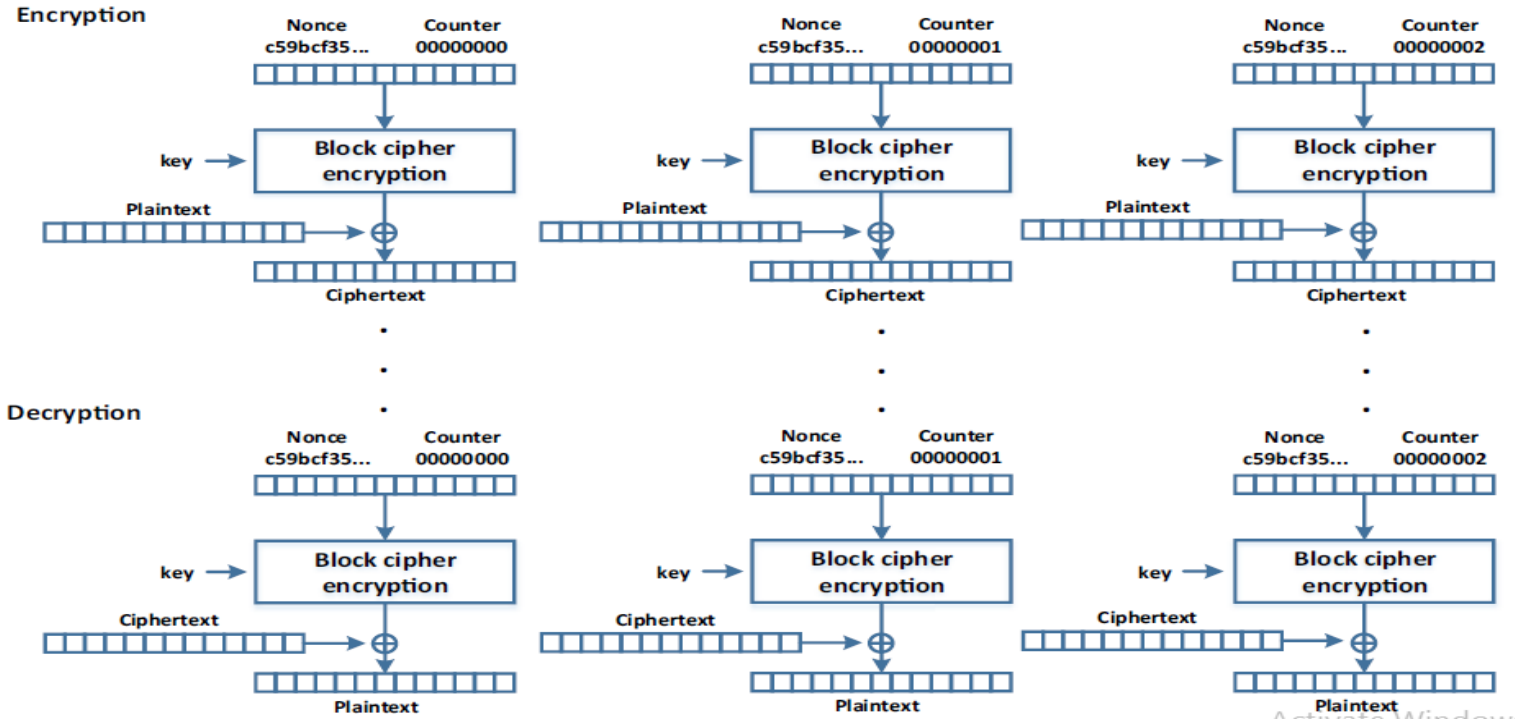


Fig. 2. Cipher block chaining (CBC) mode of AES.

Counter(CTR)


Encryption
Nonce
c59bcf35...
Counter
00000000
key
Block cipher encryption
Plaintext
Ciphertext
Nonce
c59bcf35...
Counter
00000001
key
Block cipher encryption
Plaintext
Ciphertext
Nonce
c59bcf35...
Counter
00000002
key
Block cipher encryption
Plaintext
Ciphertext
Decryption
Nonce
c59bcf35...
Counter
00000000
key
Block cipher encryption
Ciphertext
Plaintext
Nonce
c59bcf35...
Counter
00000001
key
Block cipher encryption
Ciphertext
Plaintext
Nonce
c59bcf35...
Counter
00000002
key
Block cipher encryption
Ciphertext
Plaintext

UDOO Neo Bord

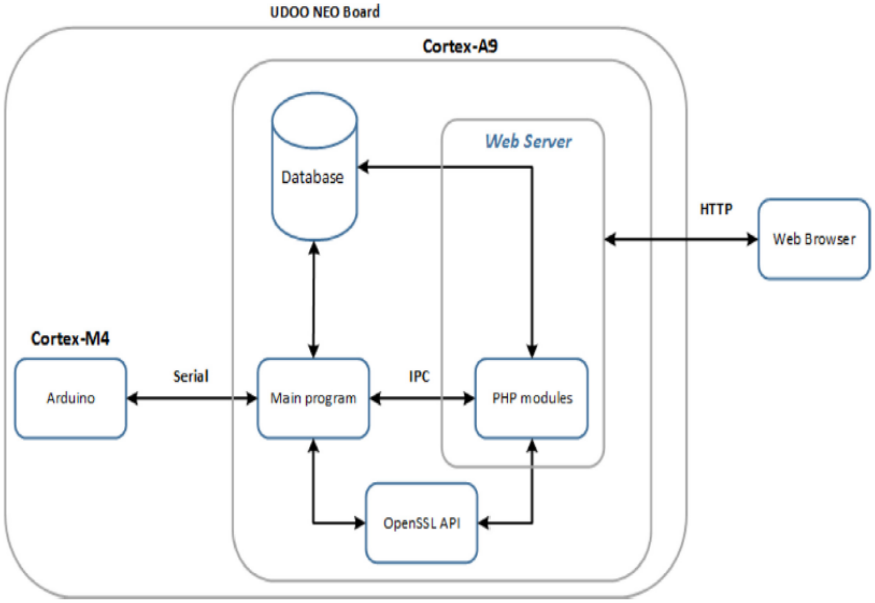


Fig. 4. Proposed system architecture.

- دو پردازنده ARM Cortex-A9 , ARM Cortex-M4به ترتیب 1 GHz و 200 MHz
- مشخصات Wi-Fi with IEEE 802.11 b/g/n
- سرویس دهی به 10 کاربر بصورت همزمان
- سیستم عامل UDOObuntu 2 بدون GUI
- هزینه کم
- بردهای سری
- عملکرد مناسب
- قابلیت ذخیره سازی کافی
- مصرف انرژی مناسب

سیستم احراز هویت

OPT

پایان
سپاس از توجه شما