به نام خدا

سیستم رمزنگاری برای اپلیکشن‌های داده‌ای در حوزه IOT

****

نام استاد مربوطه:

خانم دکتر جاسبی

تهیه کننده:

حمید فــرزین پور

مقدمه

اینترنت اشیاء به عنوان چهارمین انقلاب صنعتی توانمندسازی اشیاء برای اتصال در هر زمان و در هر مکانی، با هر چیزی و هر شخصی است که از هر مسیر یا شبکه و خدمتی به صورت ایده آل استفاده می کند. این فناوری جدید به حضور نافذ محیطی توجه دارد و جهانی که به شکل واقعی، دیجیتال و مجازی است و به سمت شکل‌گیری محیط های هوشمند، همگرا می شوند. این فناوری در حوزه‌های مختلف نظیر انرژی، حمل و نقل و سلامت مورد بهره برداری قرار می گیرد.

این فناوری نوپا با توجه به گسترش کاربری آن، دارای آسیب‌پذیری‌ها و چالش‌هایی در ارتباط با امنیت است، به‌طوری‌که می‌توان از امنیت، تحت عنوان «پاشنه آشیل اینترنت اشیا» یاد کرد. این آسیب‌پذیری‌ها باعث ایجاد نگرانی‌های جدی از توسعه این فناوری شده است. نگرانی‌های مربوط به امنیت اینترنت اشیا و آسیب‌پذیری‌های آن شامل این موارد است:

-افزایش کاربردها و خدمات مبتنی بر اینترنت اشیا در صنایع مختلف.
-فراهم آوردن امنیت و حریم خصوصی، دسترسی راحت و گسترده به اینترنت معضلات امنیتی فضای سایبری را گریبانگیر این فناوری کرده است.
-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.
با توجه به موارد فوق و همچنین محدود بودن منابع مالی و انسانی، هزینه و زمانی که باید برای جبران خسارت ناشی از حفره‌های امنیتی موجود در فناوری اینترنت اشیا صرف کرد و حتی صدمات جانی‌ای که ممکن است عدم توجه و شناخت موضوعات امنیتی در این حوزه به بار آورد، ضرورت شناسایی و پرداختن به مسائل و چالش‌های امنیتی آن احساس می‌شود.
در حال حاضر ، توسعه اینترنت بیشتر با تبادل فوری داده ها شکل می گیرد. الگوی استفاده از دستگاه به روشی گسترده و طاقت فرسا ، توانایی برقراری ارتباط و به اشتراک گذاری اطلاعات به کاربران است. به همین دلیل ، نیاز به محافظت از دستگاه ها و انتشار اطلاعات در بین آنها اجباری تعیین می‌شود. اینترنت اشیا، می تواند به عنوان یک دامنه کاربردی توصیف شود که زمینه های مختلف فن آوری و اجتماعی را با هم ادغام می کند بعلاوه ، اینترنت اشیا می تواند مدلهای رمزنگاری و طرحهای امنیتی را برای اهداف پیاده سازی را به ارمغان بیاورد.
اهدف اصلی سیستم پیشنهادی تأثیرگذاری بر سیستم های حریم خصوصی است که هم برای دانشگاه ها و هم نیازهای صنعت مفید است، زیرا IoT طی سالهای اخیر بیشتر مورد توجه قرار گرفته است. سیستم رمزنگاری می تواند یک راه حل تعاملی و قابل اعتماد ، در راه انتخاب متون داده ، تصاویر و پرونده های الکترونیکی داده ها ، برای برنامه های حفظ حریم خصوصی ارائه دهد. می تواند به عنوان یک پیاده سازی در زمان واقعی استفاده شود و برای موفقیت در هر دو بخش صنعت و دانشگاه یا برای نیازهای افراد مورد استفاده قرار گیرد.
علاوه بر این ، این کار یک سیستم رمزنگاری کامل اینترنت اشیا را ارائه می دهد، که بر اساس برد UDOO NEO است ، به عنوان متمایز از کارهای دیگر که در پیشنهاد شده است ، و همچنین بر امنیت و کاربردهای رمزگذاری یک اینترنت اشیا تمرکز دارد. سیستم

پیاده سازی این سیستم اینترنت اشیا بر اساس استاندارد رمزگذاری پیشرفته (AES) در حالت های مختلف عملکرد ساخته شده است.

از نظر تحلیلی بیشتر از حالت های عملکرد Elecode Code Book (ECB)، Cipher Block Chaining (CBC) و Counter (CTR) پشتیبانی می کند. این عمل هم برای رمزگذاری و هم برای رمزگشایی کارآمد است. این با موفقیت برای کاربران جایگزین برنامه های پیام متنی ، پرونده های تصویری از انواع مختلف و برنامه های الکترونیکی داده ، از همه لحاظ ، عمل می کند. علاوه بر این، سعی شده است سازوکارهای امنیتی اضافی بیشتری پیشنهاد و اجرا شود. با تجزیه و تحلیل بیشتر، تازه‌های معرفی شده در این کار، که طراحی و پیاده سازی شده اند که عبارتند از:

1. پشتیبانی از جریان رمزگذاری داده، به اضافه‌ی رمزگذاری بلوک اصلی AES. این امر بدون هزینه اضافی، براساس روش عملکرد Counter (CTR) حاصل می شود. برای راه کار برای مواردی که برنامه‌های کاربردی که دارای داده سنگین نیستند یا نیازهای کاربر نیست، پیشنهاد می‌شود.

2. AES Galois / Counter Mode (GCM) و AES Galois کد احراز هویت پیام (GMAC). طبق تحقیقات ما ، GCM با استفاده از مکانیزم احراز هویت، مکانیسم احراز هویت را با هدف پشتیبانی از اصالت و محرمانه بودن، بدون هیچ گونه هزینه اضافی، در منابع سخت افزاری ادغام می کند. از طرف دیگر ، طرح پیشنهادی دیگر AES GMAC، می تواند به عنوان کد احراز هویت پیام، رویکرد قابل اعتماد استفاده شود. GCM و GMAC در رابطه با منابع موجود از نظر بهینه سازی پیشنهاد می شوند ، زیرا مولفه مهم سیستم پیشنهادی هسته AES است.

3. ثبت نام و اعتبارسنجی کاربر، از طریق سخت افزار. این امر می تواند از طریق دکمه های فشاری پنل موجود، بدون هیچ گونه هزینه اضافی و یا کاهش عملکرد، محقق شود. همچنین می توان از دکمه های فشار اختصاصی استفاده کرد.

4- احراز هویت دو عاملی کاربر، پس از ورود موفقیت آمیز ، فرآیند توصیف شده قبلی. این رمزهای عبور با یک بار ورود (OTP) که بصورت تصادفی تولید می شوند ، پیشنهاد و تلفیق می شوند.

فناوری اینترنت اشیا: به سمت دوره ای جدید

همانطور که قبلاً اشاره شد، اینترنت اشیا به شبکه دستگاههای فیزیکی (به عنوان مثال تلفن‌های هوشمند، لپ تاپ‌ها، ساعت‌های هوشمند و غیره اشاره دارد که به اینترنت متصل شده ، داده ها را جمع آوری و به اشتراک می گذارند. با نگاهی فراتر از تعداد زیادی از برنامه های مختلف، مانند خانه‌های هوشمند، شهرهای هوشمند، زیرساخت های بهداشتی هوشمند، می توان با استفاده از چنین فناوری هایی ، سطح دیجیتالی شدن را درک و درک کرد. سطح هوش دستگاه می تواند آنها را قادر به برقراری ارتباط بدون دخالت یک انسان ، ادغام دنیای دیجیتال و فیزیکی کند. بهبود سریع IoT می تواند به افراد کمک کند تا با غلبه بر مشکلات روزمره ، محیط خود را هوشمندانه و قابل اندازه گیری کنند.

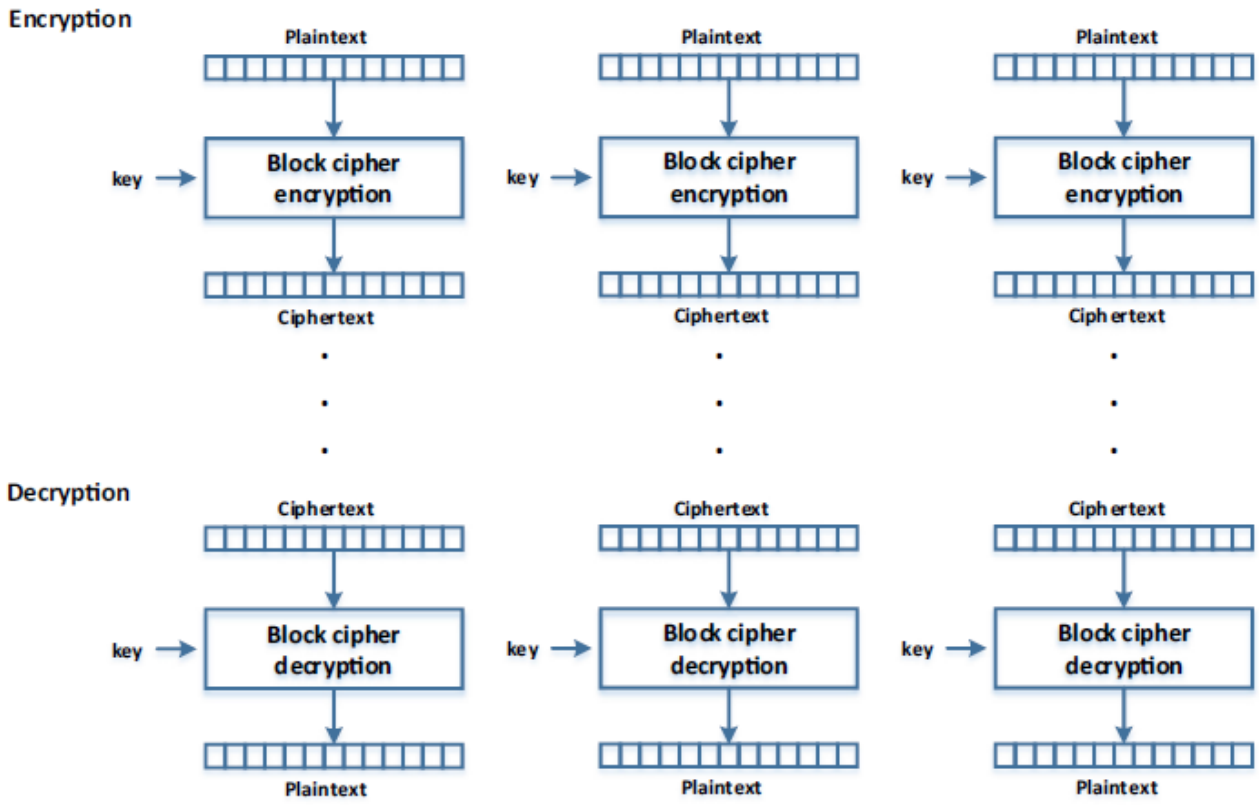

Fig. 1. Electronic code book (ECB) mode of AES.

از آنجایی که فناوری زندگی انسان را به طور مداوم تغییر می دهد، دستگاه های فیزیکی این مزیت را دارند که متصل شوند و به طور متناوب مورد استفاده قرار گیرند. به همین دلیل، هر دو صنعت و دانشگاه می توانند از روش ها برای کاهش هزینه های عملیاتی خود استفاده کنند. بعلاوه ، روش‌های استفاده یا حتی استفاده مجدد از دستگاههای قابل حمل کاملاً قابل قبول است. برای توسعه سیستم های خاص با هزینه کم و عملکرد بالا می توان دستگاه ها را به فناوری کنونی متصل کرد. این روش جدید این مزیت را به مردم می دهد که از سراسر جهان از طریق یک سیستم سخت افزاری متصل، سازگار ، پایدار و ایمن به یکدیگر متصل شوند. سیستم رمزنگاری پیشنهادی را می توان با موفقیت به عنوان یک بستر زمان واقعی برای استفاده روزمره به کار برد. بعلاوه می توان از آن برای اهداف تحقیقاتی، و روشهای آموزشی یا فعالیتهای آموزشی ، در بخشهای صنعت و دانشگاه استفاده کرد.

حریم خصوصی و رمزنگاری بدوی

در این بخش، ما اصول اولیه و تعاریف رمزنگاری و همچنین مکان یابهای بلوک کلید متقارن را برای فرآیندهای رمزگذاری و رمزگشایی ارائه می دهیم. رمزنگاری کلید متقارن Operation نامیده می شود، هنگامی که از همان کلید برای رمزگذاری و رمزگشایی استفاده می شود. با استفاده از این فرایند که فرستنده متن ساده را با استفاده از یک کلید و یک رمز بلوک انتخاب شده رمزگذاری می کند. به این ترتیب متن رمز تولید می شود. در طرف دیگر ، گیرنده متن رمز را با استفاده از همان کلید و رمز بلوک رمزگشایی می کند.

مبادله کلید به صورت ایمن انجام می شود ، زیرا قبل از تبادل اطلاعات در یک کانال امن منتقل می شود. در این مرحله ، یک فرد مخرب (دشمن) در حال تلاش برای نظارت بر ارتباطات و یا تغییر داده ها است، اما به دلیل روش های شناخته شده حمله غیرقابل اجرا است ، با این فرض که یک کلید بزرگ به طور گسترده استفاده می شود.

بلوک به بلوک ، روش کار توسط رمز بلوک متقارن به منظور پردازش داده ها استفاده می شود. اندازه هر بلوک به n بیت ثابت است، می تواند $n = 128$ بیتی باشد. اگر متن ساده حاوی بیش از یک بلاک n بیتی باشد، حالت های اصلی دیگری نیز وجود دارد که از عملکرد اصلی رمزگذاری بلوک پشتیبانی می کند. در زمینه این کار ، سه حالت عملکرد ارائه شده است. حالت کد بوک الکترونیکی (ECB) ، زنجیره رمزگذاری بلوک رمز (CBC) و شمارنده(CTR).

استاندارد رمزگذاری پیشرفته AES بلوک های داده $n = 128$ بیتی را تغییر می دهد و برای حالت رمزگذاری بلوک متقارن اجرا می شود. پرکاربردترین حالت ECB است (شکل 1) ، و متن ساده را به بلوک های i شکسته و هر بلوک را به طور جداگانه رمزگذاری می کند. هر بلاکی که به متن ساده اشاره دارد با استفاده از یک کلید رمزگذاری شده و یک بلوک متن رمز را به طور مستقل تولید می کند. از طرف دیگر ، در فرآیند رمزگشایی فرآیند رمزگذاری معکوس اتفاق می افتد. هر بلوک متن رمز شده با استفاده از یک کلید رمزگشایی شده و متن ساده را تولید می کند.

در حالت عملکرد CBC ، همانطور که در شکل 2 ارائه شده است ، از یک بردار اولیه در بلوک اول، از فرآیند رمزگذاری استفاده می شود. IV برای اینکه با اولین بلوک متن ساده XOR شود ، از یک تابع منطقی منحصر به فرد یا OR استفاده می کند. نتیجه رمزگذاری می شود و به این ترتیب اولین بلوک متن رمز تولید می شود. سپس ، هر بلوک متن ساده با خروجی متن رمز مرحله قبل XOR می شود. در فرایند مخالف ، برای رمزگشایی بلوک متن رمز ، بلوک متن رمز از عملکرد XOR با بلوک مرحله قبلی استفاده می کند و متن ساده تولید می شود. باید توجه داشته باشیم که در این حالت ، IV فقط یک بار در ابتدای فرآیند رمزگشایی با استفاده از عملیات XOR با اولین بلوک رمزگشایی تولید شده از بلوک متن رمز اول استفاده می شود ، زیرا مرحله قبلی وجود ندارد. به این ترتیب اولین بلوک متن ساده تولید می شود. در حالت عملکرد ECB و CBC ، اگر متن ساده تولید شده برابر با اولیه باشد ، برای هر بلوک ورودی ، هر دو فرآیند (رمزگذاری و رمزگشایی) با موفقیت انجام می شوند.

این فرض می‌شودکه برای هر دوی آنها از یک کلید استفاده شده است. با این حال ، همانطور که در حالت ECB نشان داده شده است ، رمزگذاری بلوک های متن ساده یکسان ، بلوک های متن رمز یکسان را تولید می کند و بالعکس. این جدی ترین نقطه ضعف این حالت است ، زیرا همه بلوک ها به طور مستقل رمزگذاری می شوند و تمام پیام های استفاده شده نباید بیشتر از یک بلوک باشند. در حالت CBC ، این نقطه ضعف ذکر شده وجود ندارد. این از مکانیزم رمزگذاری هر بلوک متن ساده با بلوک قبلی (مکانیزم زنجیره ای) استفاده می کند. یک مزیت حالت CBC این است که استفاده متفاوت از IV ها ، اما با همان کلید در مرحله اول رمزگذاری ، در نهایت به متن های مختلف رمزنگاری منجر می شود.

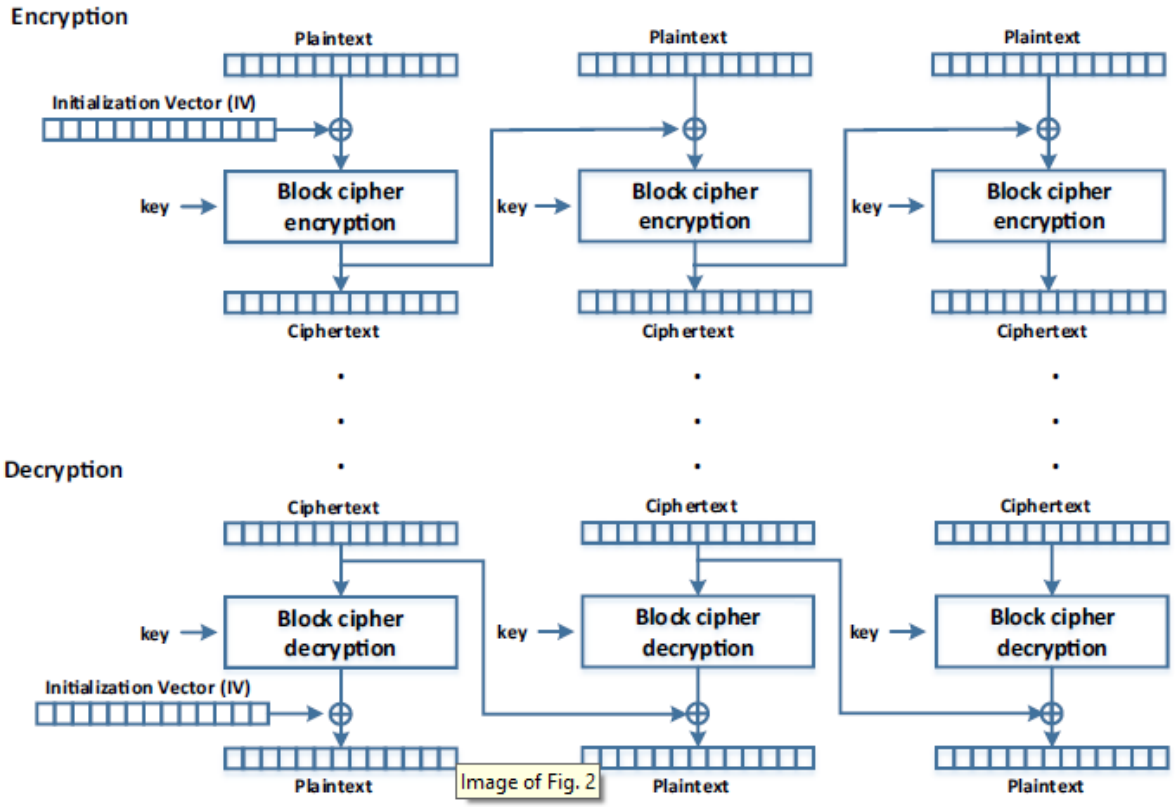

Fig. 2. Cipher block chaining (CBC) mode of AES.

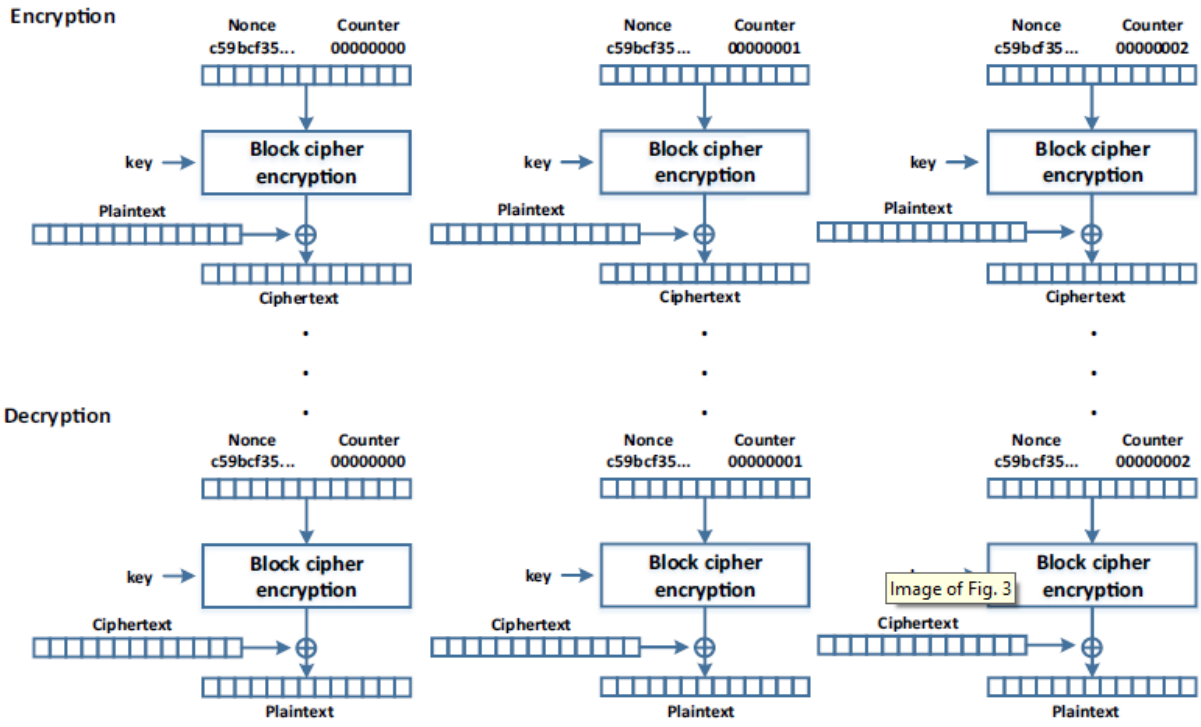

Fig. 3. Counter (CTR) mode of AES.

علاوه بر حالت های ECB و CBC ، با عملکرد CTR (شکل 3) ، یک رمز بلوک به عنوان رمزگذار جریان ، همزمان کار می کند ، بدون هیچ هزینه اضافی. با رمزگذاری مقادیر "COUNTER" قادر است بلوک جریان اصلی بعدی را ایجاد کند. COUNTER تابعی است که یک عدد توالی ارائه می کند، که برای مدت طولانی تکرار نمی شود. در حالت CTR مقدار nonce تصادفی است و همچنین مشابه بردار اولیه (IV) است. برای تولید یک بلوک شمارنده منحصر به فرد برای رمزگذاری، می توان آن را با COUNTER ترکیب کرد ، برای مثال از یک تابع XOR استفاده کرد. در صورت وجود nonce غیر تصادفی ، هر دو nonce و COUNTER باید به سادگی با افزودن یا XOR کردن آنها در یک مقدار واحد متصل شوند. هنگامی که یک مهاجم کنترل جفت COUNTER و نوشتن متن رمز شده با متن ساده شناخته شده را می دهد ، مقداری را بدست می آورد که وقتی XOR با متن رمز بلوک بعدی استفاده می شود ، بلوک رمزگشایی می شود.

برد IoT انتخاب شده

برد UDOO Neo به عنوان پایه ای برای پیاده سازی یک راه حل کامل اینترنت اشیا ، به منظور ترکیب ماژول های مختلف برای سیستم پیشنهادی، استفاده می شود. این برد کم هزینه ، بردهای سری، با عملکرد خوب ، قابلیت ذخیره سازی کافی، استقلال انعطاف پذیر و مصرف انرژی مناسب است. این ویژگی ها برای تحقیقات ما اثبات شده اند ، و همیشه تعادل خوبی بین آنها حفظ می کنند. این توازن ، معیار عمده انتخاب برد UDOO Neo است ، زیرا تحقیقات ما به هیچ یک از آنها نیازی ندارد یا اولویت خاصی ندارد. به این ترتیب می توان نتایج منصفانه و رضایت بخشی را در مقایسه با سایر کارها و رویکردهای قبلی که دارای معیارهای طراحی شده یا سایر اولویت ها و نیازهای اختصاصی هستند ، به دست آورد. نکته آخر اینکه ، طراحی و اجرای سیستم پیشنهادی به هیچ یک از ویژگیهای خاص برد انتخابی بستگی ندارد و با توجه به نیاز ، در دسترس بودن و تصمیم گیری کاربر ، هر بار با موفقیت مشابه قابل اجرا است. این به عنوان یکی دیگر از مزیت های اصلی سیستم رمزنگاری پیشنهادی اثبات شده است

با تجزیه و تحلیل بیشتر ، اخیراً یک رایانه تک بردی، مبتنی بر با Android یا Linux ، با حسگرها ، بلوتوث 4.0 و ماژول Wi-Fi تجهیز شده است در ابتدا ، از آن به عنوان سیستم تست کم هزینه آموزش استفاده شد ، جایی که چندین برنامه و سرویس جدید می تواند توسعه یابد. به طور تفصیلی ، مشخصات برد UDOO Neo به شرح زیر است:

پردازنده NXP / Freescale iMX 6SoloX ، دارای دو پردازنده ناهمگن روی تراشه یکسان ، یک پردازنده ARM Cortex-A9 و یک پردازنده ARM Cortex-M4 ، دارای ساعت به ترتیب در 1 گیگاهرتز و 200 مگاهرتز. این دو پردازنده از طریق یک رابط سریال مجازی ارتباط برقرار می کنند که از حافظه مشترک برای تبادل داده استفاده می کند. همچنین پردازنده ها از ویژگی های سخت افزار پیاده سازی شده ارائه شده توسط معماری استفاده می کنند. iMX 6SoloX به لوازم جانبی سنسورها ، بلوتوث 4.0 و ماژول Wi-Fi متصل است. تجهیزات جانبی از طریق یک گذرگاه پرسرعت AXI و با استفاده از رابط سخت افزاری مختلف (I2C، SPI، GPIO، UART و سایر موارد) به پردازنده ها متصل می شوند. با مخلوط کردن قابل ویرایش ، از طریق پد پردازنده می توان به تمام ویژگی های سخت افزاری برد UDOO Neo دسترسی پیدا کرد و آنها را متصل کرد. بنابراین ، توابع ثابت نیستند ، اما در پدهای مختلف می توان به آنها دسترسی داشت. بعضی از اینها به هر دو پردازنده به پایه های خارجی متصل می شوند و به کاربران امکان می دهند لوازم جانبی خود را به یکدیگر متصل کنند. پین های ورودی/خروجی هدف عمومی (GPIO) را می توان به صورت پویا و در زمان راه اندازی ، بین پردازنده های Cortex-A9 و Cortex-M4 به اشتراک گذاشت.

سیستم رمزنگاری پیشنهادی

یک سیستم رمزنگاری جدید ارائه شده است ، که برای فناوری اینترنت اشیا طراحی شده است و با جزئیات ارائه می شود. از برد UDOO Neo استفاده می کند. برد پیاده سازی بر اساس سیستم عاملهای متفاوتی نسبت به معمول تعریف شده به نام UDOObuntu 2 است که مبتنی بر Ubuntu 14.04 است ، بدون هیچ گونه رابط کاربری گرافیکی (GUI). معماری نرم افزار پیشنهادی در شکل 4 توضیح داده شده است. ماژول Wi-Fi براساس پروتکل IEEE 802.11 b/g/n به عنوان یک نقطه دسترسی عمل می کند. دستگاه با این حالت می تواند حداکثر 10 مشتری را اداره کند. برد UDOO Neo به عنوان یک برنامه وب از ماژول های Apache و PHP تشکیل شده است. همچنین می تواند درخواست های پروتکل انتقال متن (HTTP) از مرورگرهای وب را کنترل کند. این رابط با فن آوری های وب ، مانند Hyper-Text Markup Language (HTML)، Cascading Style Sheets (CSS) و زبان برنامه نویسی JavaScript توسعه یافته است. کاربر از طریق مرورگر وب به این فناوری ها دسترسی پیدا می کند ، همچنین از طریق پروتکل Wi-Fi ارتباط برقرار می کند.

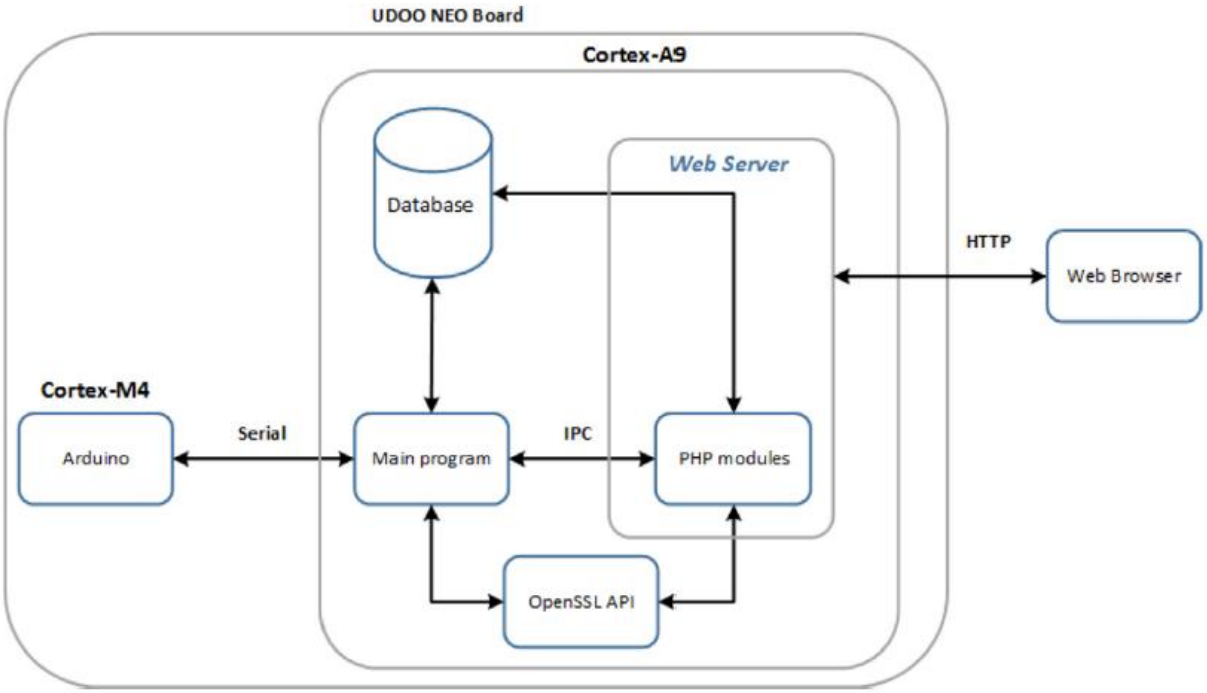

Fig. 4. Proposed system architecture.

شایان ذکر است که سیستم با استفاده از رابط برنامه نویسی برنامه OpenSSL (API) با زبان برنامه نویسی C / C ++ پیاده سازی شده است. API شامل اطلاعات مربوط به اینترفیس، رمزگذاری یا رمزگشایی مانند درخواست های HTTP است. فرآیند به شرح زیر است:

در ابتدا درخواستی (رمزگذاری یا رمزگشایی) به ماژول OpenSSL ارسال می شود ، سپس انتظار می رود نتایج رمزنگاری همزمان یا ناهمزمان بدست آید. Python برای تفسیر عملکرد ابزار استفاده می شود. همچنین دستورات دقیق را برای صرفه جویی در تاریخ و سایر عملیات انجام می دهد. برنامه پایتون از طریق رابط Cortex-M4 و ارتباط بین پردازش (IPC) با ماژول PHP ارتباط برقرار

می کند. استفاده از پایگاه داده برای ذخیره سازی داده ها کاملاً ضروری است. با رفتن به Cortex-M4 ، می توانیم نشان دهیم که یک کد مبتنی بر Arduino در حال اجرا است. این کد وظیفه کنترل تمام وسایل جانبی خارجی مانند دکمه ای را دارد که باید فشار داده شود تا وضعیت مناسب LED های RGB را نشان دهد ، در صورت گزارش داده های سنسور بر روی برد. همه تعاملات و گزارش ها، سپس از طریق ارتباط سریال دو طرفه ، به عملکرد اصلی ابزار منتقل می شوند.

در شکل 5 ، ما می توانیم با استفاده از برد UDOO Neo و وسایل جانبی، توسعه سیستم پیشنهادی را روشن کنیم. یکی از این لوازم جانبی نمایشگر رنگی TFT ILI9163 است که می تواند به صورت اختیاری و فقط در صورت اهداف نظارت مورد استفاده قرار گیرد.

از طریق یک درگاه Serial Peripheral Interface (SPI) و یک DHT11 سنسور رطوبت و دما متصل می شود ، و از طریق یک رابط سریالی و با استفاده از یک سیم، پروتکل دو طرفه ارتباط برقرار می شود. علاوه بر این ، یک RGB led با حالت Pulse Width Modulation (PWM) به پایه های خروجی متصل می شود. دو دکمه فشار به پین های ورودی متصل می شوند ، با مقاومت های کششی و با وقفه ها کار می کنند. یک شخص می تواند از طریق یک طرح امنیتی ثبت نام و اعتبار سنجی، براساس ماژول های سخت افزاری داخلی سیستم پیشنهادی، یک کاربر ثبت شده در سیستم پیشنهادی باشد (شکل 6).

تحلیلی بیشتر در این پیاده سازی، با دو دکمه فشار بر روی این برد اجرا می شود. از طریق فرآیند ثبت نام ، کاربر برای مدت زمان باقیمانده فرآیند (شکل 6 الف) ، نتیجه تأیید موفقیت آمیز (شکل 6 ب) ، وقفه های احتمالی عملیات انجام شده (شکل 6 ج) یا حتی تلاش ناموفق مطلع می شود (شکل 6 د) ، خصوصاً در صورت هک یا حمله احتمالی.

احراز هویت دو عاملی کاربر نیز به عنوان یک طرح احراز هویت اساسی پیاده سازی و پشتیبانی می شود. پس از ورود موفقیت آمیز، از فرآیند شرح داده شده در بالا دنبال می شود. تکنیک کاربردی که اتخاذ شده رمزهای یکبار مصرف (OTP) است. آخرین موارد به صورت تصادفی و با استفاده از دستگاه و بدون هیچ گونه هزینه اضافی تولید می شوند. در مورد ما از شتاب‌سنج به منظور بهینه سازی عملکرد یک بایت شبه تصادفی رایج، عملکردی که با روال نرم افزاری اجرا می شود، استفاده می شود. به این ترتیب، تعداد تصادفی بهتری تولید می شود، از لحاظ دامنه برداری ، احتمال حدس و غیره. ابتدا تعداد بایت مناسب و همچنین سطح نمونه گیری حسگر انتخاب می شود: شکاف های زمانی ، دامنه وکتور تولید شده و غیره سپس شتاب سنج توسط کاربر به صورت تصادفی جابجا می شود و از مقادیر "تصادفی" نمونه برداری می شود. در صورت عدم نتیجه مطلوب، این فرایند با قابلیت لغو پشتیبانی می شود. وقتی پیشرفت فرآیند به پایان رسید ، 100٪ ، بایت های دامنه‌ای به خروجی تولید می شوند (شکل 7).

پیشنهاد پیاده سازی سیستم IoT

در این بخش ، پیاده سازی سیستم اینترنت اشیا پیشنهاد شده ارائه شده است. مرحله اول شامل اتصال دستگاه کاربر به سیستم IoT پیشنهادی، از طریق نقطه دسترسی Wi-Fi است. در مرحله بعدی ، از مرورگر وب برای دسترسی به سرویسهای پشتیبانی شده استفاده می شود. سپس، کاربر یک حساب کاربری ایجاد می‌کند و با آدرس ایمیل و رمز عبور دلخواه خود در آن ثبت نام می کند. اعتبار سنجی حساب با استفاده از دو دکمه فشار دستگاه به روشی فیزیکی دنبال می شود. پس از این ، یک فرآیند اعتبارسنجی دیگر انجام می شود: احراز هویت دو عاملی. در این مرحله ، دستگاه اینترنت اشیا به طور تصادفی رمز عبور یک بار (OTP) را ایجاد می کند. این رمز عبور برابر با چهار کاراکتر است و میتواند بر روی صفحه نمایش داده شود. کاربر برای دسترسی به داده های

رمزگشایی سیستم، این OTP را وارد می کند. هنگامی که کاربر به رابط سیستم دسترسی پیدا کرد، می تواند رمزگذاری یا رمزگشایی را انجام دهد ، همانطور که قبلا گفته شده است، با استفاده از AES ، در سه نوع کاربرد مختلف:

1. متن داده: کاربر متن ورودی.
2. تصویر: فرمت های فایل شناخته شده تصویر (bmp، png، jpeg و غیره).
3. Electronic Files: سایر قالب های داده.

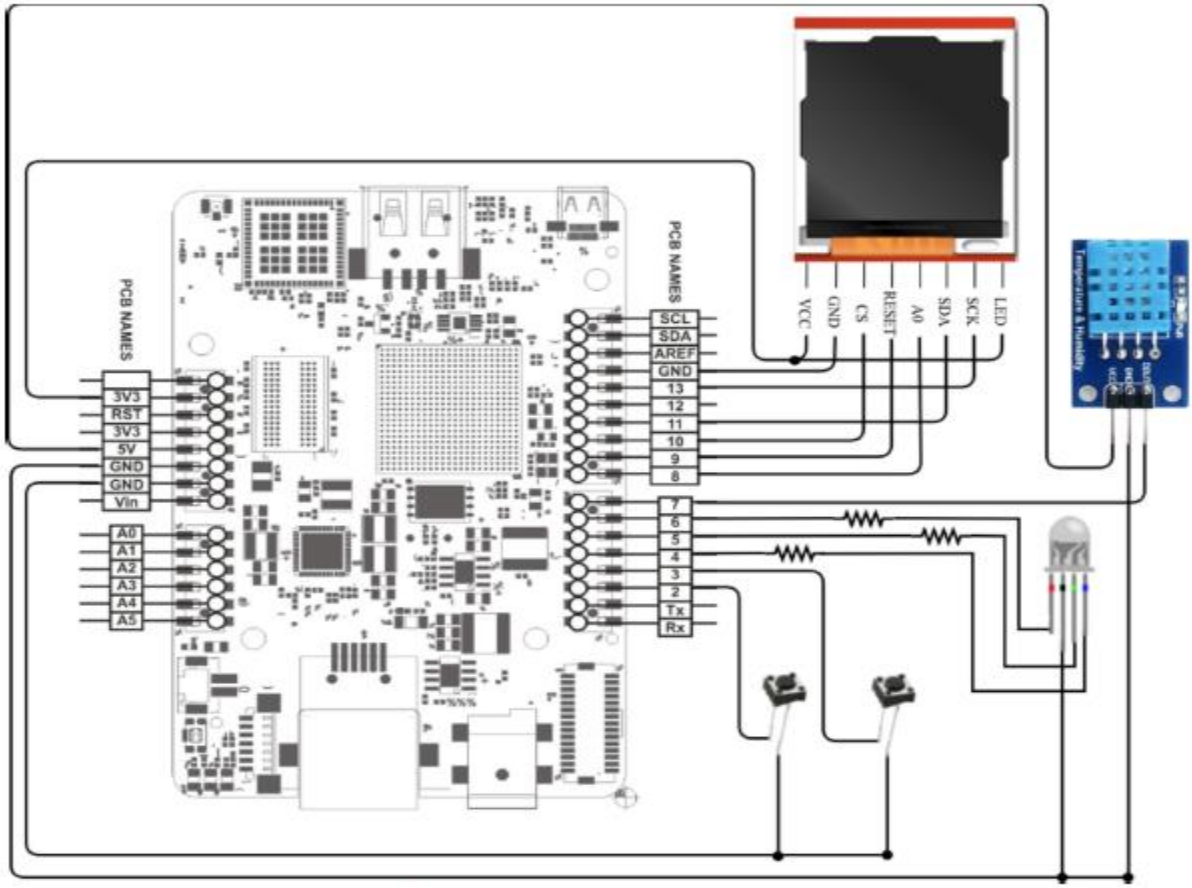

Fig. 5. Proposed system: implementation device and peripherals.

Fig. 6. User's validation module and two factors authentication scheme.

Fig. 7. Random numbers generation.

علاوه بر این ، کاربر می تواند انواع مختلفی از حریم خصوصی را برای انجام رمزگذاری و یا رمزگشایی انتخاب کند. طرح های حریم خصوصی پشتیبانی شده توسط سیستم پیشنهادی به شرح زیر است:

1. AES "اصلی"
2. AES Galois / حالت شمارنده (GCM)
3. کد احراز هویت پیام AES Galois (GMAC)
4. حالت های عملکرد (ECB، CBC، CTR)
5. طول کلید (128- ، 192- ، 256 بیتی)
6. padding (بدون بالشتک ، PKCS # 7 padding)
7. رمز عبور (کلید با استفاده از یک تابع Key مشتق –KDF تولید می شود)
8. کلید - استفاده از نماد هگزادسیمال. اندازه به طول کلید
9. IV (فقط در حالت CBC) - با استفاده از نماد هگزادسیمال بستگی دارد و برابر با اندازه بلوک (16 بایت) است.

همانطور که در بالا ذکر شد، سیستم پیشنهادی علاوه بر محرمانگی که در AES یکپارچه صلی الف) بدست می آورد، پیشنهاد و AES Galois / Counter Mode (GCM) ب و AES Galois Message Authentication Code (GMAC) ب را اجرا می کند، همانطور که در شکل 8 جزئیات نشان داده شده است.

طبق این تحقیق ، اجرای AES GCM به عنوان یک طرح امنیتی احراز هویت ادغام شده است که هدف آن ارائه اصالت و رازداری است ، بدون هیچ گونه هزینه اضافی ، از لحاظ سخت افزاری. از طرف دیگر، ادغام AES GMAC معرفی شده برای کد تأیید پیام ، به عنوان یک راه حل انعطاف پذیر و قابل اعتماد در عین حال، ارائه شده است. هر دو AES GCM و GMAC پیشنهاد می شوند ، به این دلیل که هزینه سخت افزار اضافی در مقایسه با ماژول اصلی AES یکپارچه حداقل است.

همانطور که قبلاً در این کار ذکر شد ، مثالی ذکر خواهد شد که معایب اساسی عملکرد ECB را نشان می دهد. این مثال بر اساس خدمات پشتیبانی شده سیستم ارائه شده است. این سناریو تصویری را که به فرمت فایل BMP تبدیل شده است ، اعمال می کند. هدر این رمزگذاری استخراج می شود. بدنه تصویر با استفاده از AES و طرح های حریم خصوصی کاربر رمزگذاری شده است. سپس، بدنه رمزگذاری شده به هدر متصل می شود. کل تصویر رمزگذاری شده در شکل 9 بعدی نشان داده شده است. یک کاربر می تواند تصویر نمونه را رمزگذاری کند. نمونه نمونه انتخاب شده آرم رسمی دانشگاه پاترا (دانشگاه ما) است. هدر ثابت تصویر تبدیل شده 138 بایت و بدنه آن 1،866،400 بایت است.

AES رمزگذاری 1،866،400 / 16 بایت (اندازه بلوک) = 1،166،500 بلوک را انجام می دهد و نیازی به پر کردن برای تصویر انتخاب شده نیست. پارامترهای مورد استفاده برای رمزگذاری تصویر عبارتند از: رمزگذاری AES ، حالت عملکرد ECB ، طول کلید 128 بیتی ، بدون نیاز به پر کردن و بردار مقداردهی اولیه برابر با "0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 BCD15075 0 ". تصویری که در زیر نشان داده شده است از همان الگوی داده استفاده می کند. این بدان معنی است که بلوک های داده‌ای که رمزگذاری شده اند، از همان الگو پیروی می کنند و از تصویر استخراج می‌شود. استفاده از کلید ، طول مشخص شده و عبارت رمز عبور متکی به یکدیگر نیستند و از تصویر به هر روشی بهره برداری می شود.

از تصویر اعمال شده نیز برای رمزگذاری استفاده می شود که پارامترهای مشابه را انتخاب می کند اما از حالت عملکرد CBC استفاده می کند. کلید استفاده شده مانند قبلی است و IV برابر با صفر انتخاب شده است.

همانطور که در شکل 10 d نشان داده شده است ، تصویر رمزگذاری شده با حالت CBC با حذف همه الگوهای قبلی ، تصویر را با موفقیت رمزگذاری می کند. در حالت عملکرد CBC ، مزیت این است که یک دشمن احتمالی نمی تواند تصویری که رمزگذاری شده را شناسایی کند. در حالی که از یک تصویر با کیفیت دیگر به عنوان نمونه رمزگذاری استفاده می شود ، بر اساس سیستم پیشنهادی ، تصور می شود که با همان کلید از AES در حالت ECB استفاده شده است. نتیجه تصویر رمزگذاری شده در قسمت سمت راست ، شکل 11 نشان داده شده است. مهمترین مسئله این است که تصویر رمزگذاری شده قابل شناسایی نیست. اگر می خواهیم دقیق تر باشیم و تصویر رمزگذاری شده را از نزدیک بررسی کنیم ، می توانیم الگوهای مشابهی را نیز در این مورد پیدا کنیم. اگر بتوانیم دقیق تر در تصویر رمزگذاری شده و بر بایت های آن تمرکز کنیم ، یک دشمن می تواند همان بلوک های متن رمز را تشخیص دهد که منجر به ایجاد بلوک های دندانی در تصویر اصلی می شود. در نتیجه ، می توان حالت رمزگذاری CBC را دقیق تر و انعطاف پذیرتر تعریف کرد ، تا به مسئله رمزگذاری ارائه شده قبلاً پاسخ دهد.

Fig. 9. (a) original image, (b) encrypted image using AES-ECB mode.

Fig. 10. (a) Linux "Tux" original image, (b) one encryption AES-ECB, (c) multiple encryptions, AES-ECB, (d) Er Image of Fig. 10 CBC.

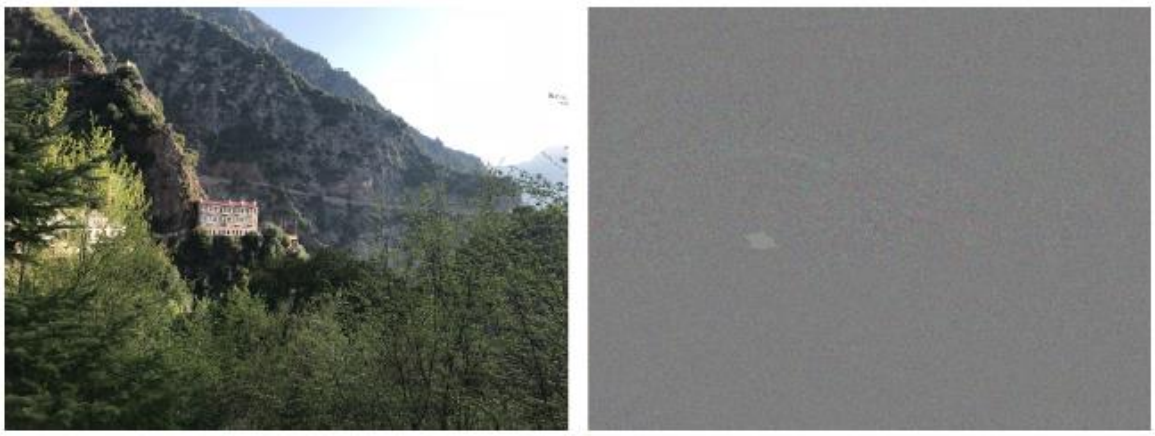

Fig. 11. (a) original high quality image, (b) encrypted image using AES-ECB mode.

رمزگذاری و رمزگشایی حالت ECB به راحتی با استفاده از چندین هسته AES قابل تقسیم است. از طرف دیگر ، رمزگذاری حالت CBC نمی تواند به طور موازی انجام شود ، زیرا رمزگذاری یک بلوک متن ساده ، به رمزگذاری بلوک های متن ساده قبلی بستگی دارد. این وابستگی زنجیره ای را نمی توان به طور موازی انجام داد ، بنابراین فقط رمز AES می تواند موازی شود. در مقابل ، فرآیند رمزگشایی حالت CBC به دلیل عدم وابستگی بلوک های رمزگشایی شده قبلی ، می تواند موازی شود. در شکل 12 ، تعداد سیکل های ساعت در هر بلوک را بین رمزگذاری غیر موازی با ECB و حالت عملکرد CBC که برد UDOO Neo نیاز دارد مقایسه می کنیم. در محور x ، تعداد بلوک هایی که رمزگذاری می شوند نشان داده می شود در حالی که در محور y چرخه های ساعت ارائه می شوند. همانطور که از نمودار نشان داده شده است ، حالت عملکرد ECB ، تعداد چرخه های ساعت کمتر از حالت CBC را صرف می کند. این به دلیل این واقعیت است که حالت CBC ، برای هر رمزگذاری از یک بلوک متن ساده ، عملکرد XOR را انجام می دهد.

اگر بخواهیم بین این دو حالت رمزگذاری موازی سازی کنیم ، نتایج متفاوت اثبات می شود. شکل 13 نشان می دهد که برای تعداد کمی از بلوک ها ، حالت ECB می تواند با موفقیت موازی شود و چرخه های ساعت لازم برای رمزگذاری این بلوک ها مداوم هستند. با این حال ، حالت CBC نمی تواند موازی باشد و چرخه های ساعت بیشتری را نسبت به قبل صرف کند.

نتایج و مقایسه ها

در این بخش ، ما نتایج استخراج شده از رمزهای مختلف را که قبلاً معرفی شده بود ، مقایسه می کنیم. ما می توانیم این کاربردها را در دو نوع تشخیص دهیم: از نظر رمزنگاری متقارن و نامتقارن. در مورد رمزنگاری متقارن می توان به موارد پیاده سازی شده در برد توسعه LPC1769 با 512 کیلوبایت حافظه فلش و 64 کیلوبایت حافظه داده که از طرح پیشنهادی ما استفاده می کند که از برد UDOO Neo استفاده می کند که الگوریتم AES را پیاده سازی می کند. با یک کلید 128 بیتی و حالت عملکرد ECB و CBC ، (شکل 14).

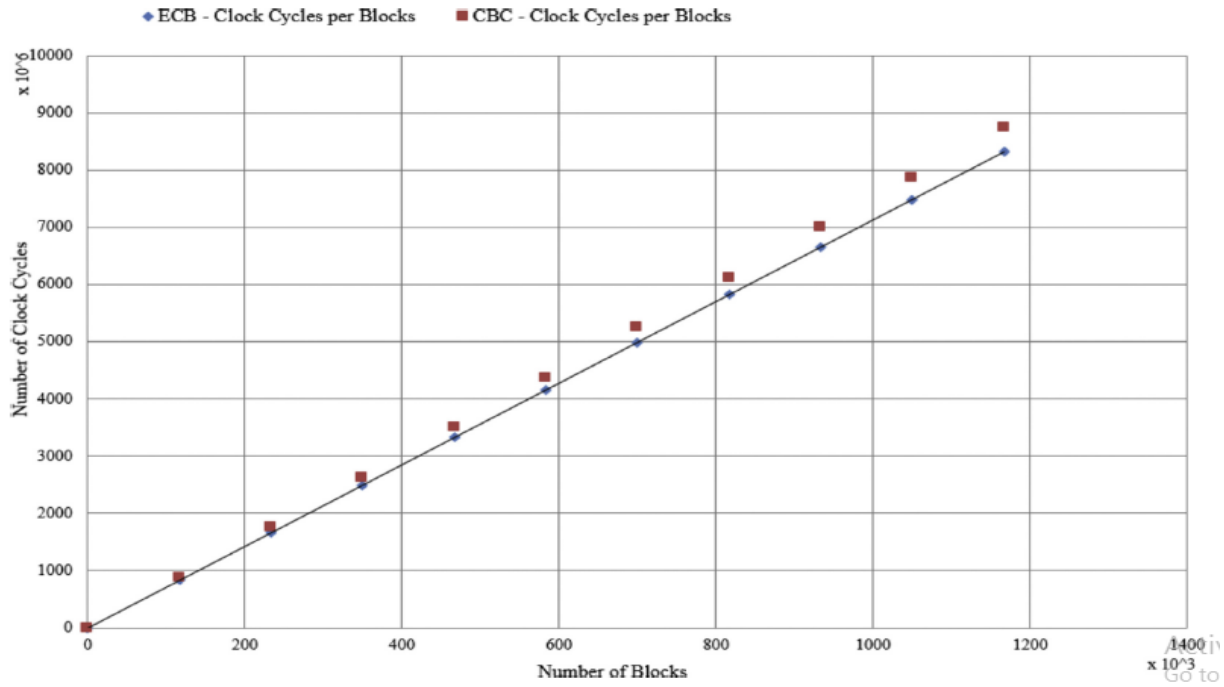

Fig. 12. AES performance: clock cycles/Blocks: Not parallel implementation.

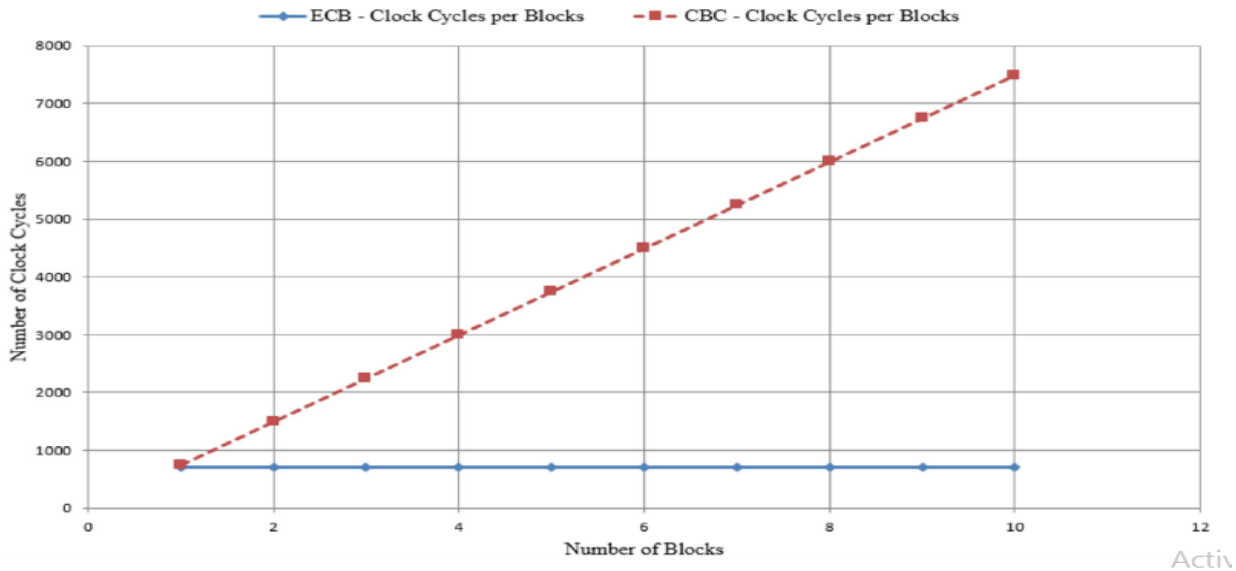

Fig. 13. AES performance: clock cycles/Blocks: Parallel implementation.

نتیجه گیری و چشم انداز

برای داشتن ارتباط انعطاف پذیر بین دنیای فیزیکی و مجازی ، نیاز به یک سیستم رمزنگاری قابل اعتماد ، که از فناوری IoT بهره برداری و پیاده سازی کند ، بیش از حد ضروری است. به همین دلایل ، یک سیستم رمزنگاری IoT جدید در این کار ارائه شده است، که تعداد زیادی از طرح های امنیتی را ارائه می دهد. روشی از سطوح مختلف امنیتی ، از نظر رمزگذاری / رمزگشایی و اجرای کارآمد آنها ، در دستگاه اینترنت اشیا ارائه می شود. بعلاوه، یک اشاره کوتاه به سطوح امنیتی در رابطه با ارتباط بین لایه های اینترنت اشیا معماری ، با جزئیات بررسی شده است.

برای داشتن ارتباط انعطاف پذیر بین دنیای فیزیکی و مجازی ، نیاز به یک سیستم رمزنگاری قابل اعتماد ، که از فناوری IoT بهره برداری و پیاده سازی کند ، بیش از حد ضروری است. به همین دلایل ، یک سیستم رمزنگاری IoT جدید در این کار ارائه شده است، که تعداد زیادی از طرح های امنیتی را ارائه می دهد. روشی از سطوح مختلف امنیتی ، از نظر رمزگذاری / رمزگشایی و اجرای کارآمد آنها ، در دستگاه اینترنت اشیا ارائه می شود. بعلاوه ، یک اشاره کوتاه به سطوح امنیتی در رابطه با ارتباط بین لایه های اینترنت اشیا معماری ، با جزئیات بررسی شده است. سیستم رمزنگاری پیشنهادی ، به عنوان یک کار دعوت شده گسترده از انتشار اولیه ما [3] ، می تواند به عنوان یک طراحی پیچیده تر و یک سیستم قدرتمند ، بیشتر گسترش یابد. هدف می تواند گسترش سیستم با اجرای سایر موارد اولیه رمزنگاری ، مانند رمزنگاری کلید عمومی ، هش کردن و امضای دیجیتالی باشد. رمزنگاری سبک وزن ، مانند رمزهای جریان ، نیز می تواند در نظر گرفته شود [19 ، 20] ، و همچنین سیستم های رمزنگاری و امنیتی ، برای منطقه حساس از برنامه های بهداشتی و پزشکی ، همچنین می تواند جهت گیری های مهم آینده باشد.علاوه بر این ، این سیستم باید به تبادل چند تایی با استفاده از همان فناوری بستر های نرم افزاری ، برای تبادل اطلاعات وصل شود و راه حل هایی برای مشکلات امنیتی مختلف پیشنهاد کند.