ارایه روش ترکیبی پرتکلهای امنیتی و بلاکچین به منظور بالا بردن امنیت داده های اینترنت اشیا در خانه های هوشمند

سید محمد رضا پورهاشمی

دانشجوی دانشکده برق و کامپیوتر، واحد شیراز، دانشگاه آزاد اسلامی

سید ابراهیم دشتی

عضو هیئت علمی دانشکده برق و کامپیوتر، واحد جهرم، دانشگاه آزاد اسلامی

چکیده:

استفاده از دستگاه های اینترنت اشیا در سال های اخیر بشدت در حال گسترش است و توجه بسیاری را به خود جلب نموده است، بدلیل ضعیف بودن و گستردگی این دستگاهها حملات مختلفی مثل DOS های توزیع شده از طریق آنها گسترش یافته است(Rudrakar and Rughani,2023)، یکی از نقاط ضعف این دستگاهها استخراج کلید SSL از طریق تجزیه و تحلیل لایه نرم افزاری firmware این دستگاهها می باشد. در نتیجه می توانند مورد نفوذ هکر ها در حملات مرد میانی قرار گیرد و داده های حساس این دستگاهها برداشته شود. (Bhardwaj et al ,2023) در این مقاله روش ترکیبی استفاده از پرتکل امنیتی و بلاک چین در اینترنت اشیا پیشنهاد شده است. در زمان ارتباط میان دستگاه های اینترنت اشیا با استفاده از پرتکل coap یک پرتکل oscore قرار داده شده است تا این ارتباط را امن سازی نماید. این مورد می تواند از حملات مرد میانی جلوگیری نماید اما در صورتی که رمز مشترک و یا رمز ssl برای ارتباطات بیرونی دستگاه های در فضای اینترنت برای برقراری ارتباط به اشتراک گذاشته شود، می تواند با تجزیه و تحلیل توسط هکرها کشف شود و عملا وجود این پرتکل ها نمیتواند از نشت اطلاعات جلوگیری نماید که برای حل این مشکل نیز پیشنهاد شده است از بلاکچین استفاده شود، با وجود بلاکچین و ایجاد یک سرور مشترک میان دستگاه های iot میتوان کلید ها را به صورت دوره ای میان دستگاه های iot (بلاک ها) به اشتراک گذاشت لذا از آن جا که این کلید به صورت دوره ای تغییر میکند هر کدام از این کلید ها که به هر روش مورد نفوذ قرار گرفته باشند به دلیل تغییر دوره ای از دسترسی هکرها و حملاتی مثل DOS جلوگیری می شود.

کلمات کلیدی: اینترنت اشیا، firmware، oscore، بلاکچین،DOS.

مقدمه:

در سال های اخیر به دلیل سهولت و کارایی، استفاده از دستگاه های اینترنت اشیا بسیار رشد داشته است به گونه ای که گفته شده است تا سال ۲۰۳۰ تعداد ۱۲۵ میلیارد دستگاه در جهان به یکدیگر متصل خواهند شد. پیش بینی های نشان میدهد که در آینده ای نزدیک داد های جهانی جمع آوری شده توسط دستگاه های اینترنت اشیا به یک میلیون ترابایت میرسد. (Zakariyya et al,2023)

با این حال با وجود رشد چشم گیر این دستگاه ها و همچنین جمع آوری داده ها توسط این موارد، مهاجمان سایبری با استفاده از روشهای ضد امنیتی از اطلاعات آن ها سوء استفاده می کنند این موارد شامل استفاده از بانت نت ها همچون mirai(از جمله بات نت های معروف در اینترنت اشیا)، حملات DDOS، استفاده از ویروس ها و ... می باشد.(Zakariyya et al,2023)

از جمله موارد با اهمیت در امنیت اینترنت اشیا استفاده از پرتکل ssl می باشد این پرتکل دیتای رد و بدل بین این دستگاه ها و سرور و یا کلاینت های کنترلی دیگر را رمزنگاری می کند. همچنین استفاده از پرتکل oscore موجب امنیت اطلاعات رد و بدل شده بین دستگاه های مختلف موجود در یک شبکه لوکال می شود بهره گیری از هر کدام از این پرتکل ها از حملاتی همچون حمله مرد میانی و از sniff شبکه جلوگیری می نماید. برخی هکر ها با استفاده از تجزیه و تحلیل firmware های این دستگاه ها کلید مربوط به هر کدام از این پرتکل ها را برداشته و این مهم موجب رمزگشایی اطلاعات ودیتاهای موجود در شبکه شامل دستگاه های iot شده و این دیتاها نشت می یابند. (Bhardwaj et al ,2023)

مطالعات پیشین:

سون و همکاران (۲۰۱۹) یک معماری جدید مدیریت سیستم عامل را بر اساس بلاک چین و سیستم فایل بین سیاره ای پیشنهاد کردند. اگرچه، از آنجایی که نمی توان از کنترل نسخه دستگاه اینترنت اشیا و صحت URLاطمینان حاصل کرد، دستگاه های اینترنت اشیاء اکنون می توانند به روز رسانی سیستم عامل را از طریق شبکه های بلاک چین دریافت کنند. رویکرد پیشنهادی امکان انتقال و به روز رسانی های سیستم عامل ایمن را فراهم می کند و پیش بینی می شود که سطح امنیتی دستگاه های اینترنت اشیا بهتر گردد.

ارتقاء و به روزرسانی سیستم عامل(firmware) از راه دور در دستگاه های IoT منجربه خرابی دوره ای دستگاه وبدتر شدن عملکرد می شود. برای آپلود کد به روز شده با به روز رسانی یا اصلاحات و نصب مجدد ابزار در زمینه، نیاز به دسترسی فیزیکی به کامپیوتر دارد. به روزرسانی های میان افزاری، روشی منحصربه فرد برای به روز رسانی دستگاه های مرتبط بدون تداخل با آن ها، از راه دور و پیوسته ارائه می دهد.

برای بررسی موضوع شباهت کد و تحلیل همسانی، ژو و همکاران.(۲۰۲۰) برطبقه بندی کد و ویژگی کیفی جنبه های کد متمرکز شدند. شناسایی کد های مضر در میان افزار، استخراج حساسیت، یافتن در پشتی و حفاظت از حق کپی رایت، همگی میتوانند از تجزیه و تحلیل های مشابه و همسانی کد های میان افزار درپایانه های اینترنت اشیا بهره ببرند. آنان یک رویکرد تجزیه و تحلیل پویا منحصربه فرد رابرای شناسایی مشکلات خرابی حافظه دربسته های میان افزار دستگاه اینترنت اشیا معرفی کردند. هدف اصلی این بود که کدبرنامه باینری را در حین اجرای پویا با استفاده از اجرای نمادین، فازی کنند. نویسندگان یک نمونه اولیه ایجاد کردند و یافته ها نشان داد که فریمورک پیشنهادی می تواند تست Fuzzingرابه طور متوسط در ۴۰ ثانیه انجام دهد. در مجموع، این فریم ورک سیستم عامل IoT را در ۲۱۰ثانیه بارگیری و ارزیابی کرد، از جمله ۱۷۰ثانیه برای

تجزیه و تحلیل استاتیک. سودمندی آن زمانی نشان داده شد که بر روی ۱۱۵ ایمیج میان افزار از ۱۷شرکت اعمال شد و مشخص شد که ۳۵مورد از آنها نقص های روز صفربودند.

احمد و همکاران (۲۰۲۰) در مقاله ای تحقیقاتی یک رویکرد مقیاس پذیربرای تأیید امنیتی سیستم عامل اینترنت اشیا دربرابر تهدید Mirai ارائه کردند، نویسندگان روش پیشنهادی را با تجزیه و تحلیل استاتیکی بیش از ۱۲۰۰ ایمج سخت افزار فعلی مورد آزمایش قرار دادند تا ببینند چقدر دربرابر بات نت Mirai مقاوم هستند. بر اساس یافته ها، ویروس Mirai در بیش از ۱۹۳ ایمیج از ۱۲۰۰ فریمورک وجود داشته است.

ژنگ و همکاران (۲۰۲۳) یک طرح احراز هویت انگیزشی برای تجزیه و تحلیل در IoV پیشنهاد کردند. هدف افزایش امنیت و حریم خصوصی اینترنت اشیا و در عین حال اطمینان از راحتی و تبادل داده در میان وسایل نقلیه هوشمندبوده است. این مقاله بر روی یک معماری سه لایه شامل یک لایه ابر، لایه مه، و لایه کاربر با استفاده از رمزگذاری بدون گواهی توسعه داده شده است.

سانتوشیرودراکار و همکاران (۲۰۲۳) اهمیت بالای امنیت در دستگاه های اینترنت اشیا در حوزه کشاورزی را بیان نموده و آسیب پذیری های موجود در دستگاه های اینترنت اشیا کشاورزی (Ag-iot) را بیان میدارند در این مقاله انواع آسیب پذیری ها، چالش های اینترنت اشیا در کشاورزی و ... بیان میشوند.

جدول۱:بررسی مقالات حوزه امنیت اینترنت اشیا در سال ۲۰۲۳ مرتبط با مقاله ارائه شده

موضوع	نوآوری	پارامتر ها	مزیت ها	معایب	مجموعه داده	ابزار شبیه سازی	هدف	سال انتشار	نام انتشارات
تجزیه و تحلیل قانونی و ارزیابی امنیتی سیستم عامل دوربین-های IoT در خانه‌های هوشمند	یک فرآیند دوازده مرحله‌ای منحصربه فرد برای انجام تجزیه و تحلیل سخت افزار و ارزیابی امنیتی	نوع firmware های استفاده شده در دستگاه های مختلف iot، میزان آنتروپی داده های انتقالی	شناسایی نقص امنیتی موجود در firmware دستگاه iot و بهره برداری از آسیب پذیری موجود در دوربین های اینترنت اشیا،	عدم شناسایی همه آسیب پذیری های موجود در دوربین های اینترنت اشیا	داده های واقعی دریافتی به صورت آنلاین از دوربین های موجود در خانه‌های هوشمند	استفاده از لینوکس توزیع کالی در مجازی ساز vmvare	اثبات وجود آسیب پذیری و نقص های امنیتی در برخی firmwareد وربین های مبتنی بر اینترنت اشیا و لزوم ایجاد قابلیت به روز رسانی در آنان	۲۰۲۳	Elsevier

	دوربین هوشمند مبتنی بر اینترنت اشیا								
Lightweight certificate revocation for low-power IoT with end-to-end security	طراحی لی ستهای ابطال گواهی فشرده (CCRL)با استفاده از فیلترهای Bloom همراه با TinyOCSP	مقایسه میزان تراکنشهای پروتکل های Online) Certificate Status ocsp(Protocol و tinyocsp	TinyOCSP می‌تواند حداقل هشت گواهی را به طور همزمان با بافر پیام کمتر از ۲۵۶ بایت تأیید کند، معرفی این پروتکل جدید، میتواند امکان پیاده سازی مدیریت کامل PKIcredential در اینترنت اشیا را تاییدنماید		این مقاله با استفاده از داده های واقعی صورت گرفته است.	ابزار شبیه سازی ندارد.	استفاده و معرفی پروتکل tinyocsp به جای پرتکل ocsp به دلیل مصرف انرژی کمتر در ارتباطات رادیویی اینترنت اشیا	۲۰۲۳	Elsevier

Innovative security and compression for constrained IoT networks	ترکیب دو مکانیزم کلیدی اینترنت اشیا دو پرتوکل schcو oscore		افزایش چشم گیر امنیت اینترنت اشیا با استفاه از روش ترکیبی گفته شده	**	در این مقاله دیتاستی استفاه نشده است	این مقاله با استفاده از یک محیط آزمایشی واقعی که مبتنی بر آردوئینو بوده است پیاده سازی شده است.	افزایش امنیت دستگاه های iot با استفاده از OSCOREو SCHCدر شبکه‌های LPWAN	۲۰۲۳	Elsevier
IoT based Agriculture (Ag-IoT): A detailed study on Architecture , Security and Forensics	بررسی ۱۳۲ مقاله درخصوص iot , ag-iotجهت بررسی امنیت، مسائل فارنزیکی و ارائه یک معماری در این مورد	این مقاله موارد افزایش امنیت، کارایی، انواع بد حملات سایبری و میزان مقاوت دستگاهای اینترنت اشیا را بررسی می کند	استفاده از اینترنت در Ag-IoT عملکرد بلادرنگ در یک سیستم کشاورزی را تسهیل می‌کند، می‌تواند خطر نقض امنیتی و حملات سایبری را افزایش دهد که باعث اختلال در عملکرد سیستم Ag-IoTمی‌شود و می‌تواند بر بهره‌وری آن تأثیر بگذارد	در این مقاله بیشتر به چالش های موجود پرداخته شده است و به موارد پاسخ آن کمتر پرداخته شده است.	دیتاستی در این مقاله نبوده و براساس داده های واقتی بوده است	Bevywise، IoTIFY، CupCarbon U Simple ،One IoT ،Simulator Mimic IoT ،Simulator Cooja.	اثبات مشکلات امنیتی در دستگاه های هوشمند کشاورزی مبتنی بر اینترنت اشیا	۲۰۲۳	Elsevier

Towards a robust, effective and resource efficient machine learning technique for IoT security monitoring	بهینه سازی ، افزایش کارایی و استحکام نظارت بر امنیت اینترنت اشیا مبتنی بر DNN	الگوریتم شناسایی میزان REDNN، پارامتر های مدل	REDNNدر برابر حملات استحکام نشان می‌دهد، حملات سایبری به شبکه‌های اینترنت اشیا را به دقت شناسایی می‌کند و منابع را به میزان قابل توجهی حفظ می کند.	نیاز به یادگیری موارد مختلف حوزه هک و امنیت داشته و این امر می تواند در قبال حملات زیرودی امن نباشد.	دیتاست های MNIST و CIFAR10 برای iot		معرفی یک روش بهینه در جهت ترکیب منظم سازی و شبیه سازی برای نظارت بر حملات اینترنت اشیا با استفاده از یادگیری عمیق	۲۰۲۳	Elsevier

روش تحقیق:

دستگاه های iot به دلیل لزوم ارتباط با بیرون از شبکه محلی می بایست با استفاده از پرتکل هایی همچون ssl و oscore امنیت دیتاهای رد و بدل شده را برقرار کند. اما گاها برخی از این دستگاه های از firmware هایی استفاده می کنند که در تجزیه و تحلیل آن ها، اطلاعات کلید ssl و پرتکل های امنیتی منتشر میشود این امر موجب نشت اطلاعات خواهد شد.

لو رفتن کلید ssl با استفاده از تجزیه و تحلیل firmware های موجود در iot با استفاده از ابزار فارنزیکی و کلیدی موجود در توزیع کالی لینوکس یا عنوان binwalk با فلگ های مختلف استخراج می گردد. . (Bhardwaj et al ,2023)

با توجه به مشکل موجود در این خصوص، راه حل پیشنهادی استفاده از کلید های داینامیک در ssl برای ارتباط با خارج از شبکه محلی و استفاه از کلید داینامیک در oscore به عنوان ارتباط امن داخل شبکه iot می باشد. (Höglund et al, 2023) همچنین دیتای موجود ما بین شبکه داخلی دستگاه های iot به صورت بلاک بلاک قرار می گیرند (بلاک چین) در یکی از این بلاک ها کلید ها به صورت رندم تولید شده و در اختیار دیگر بلاک ها قرار می گیرد.

الگوریتم روش پیشنهادی به صورت الگوریتم یک می باشد:

الگوریتم ۱:

Start

Get ssl from valid sites

Time=0 //the start of time (day)

For(i=0, i<30:i++){

Time++

If(time ==30)

use ssl for out of network //use ssl for every mounth

}

TimeOscore=0 //the start of time (day)

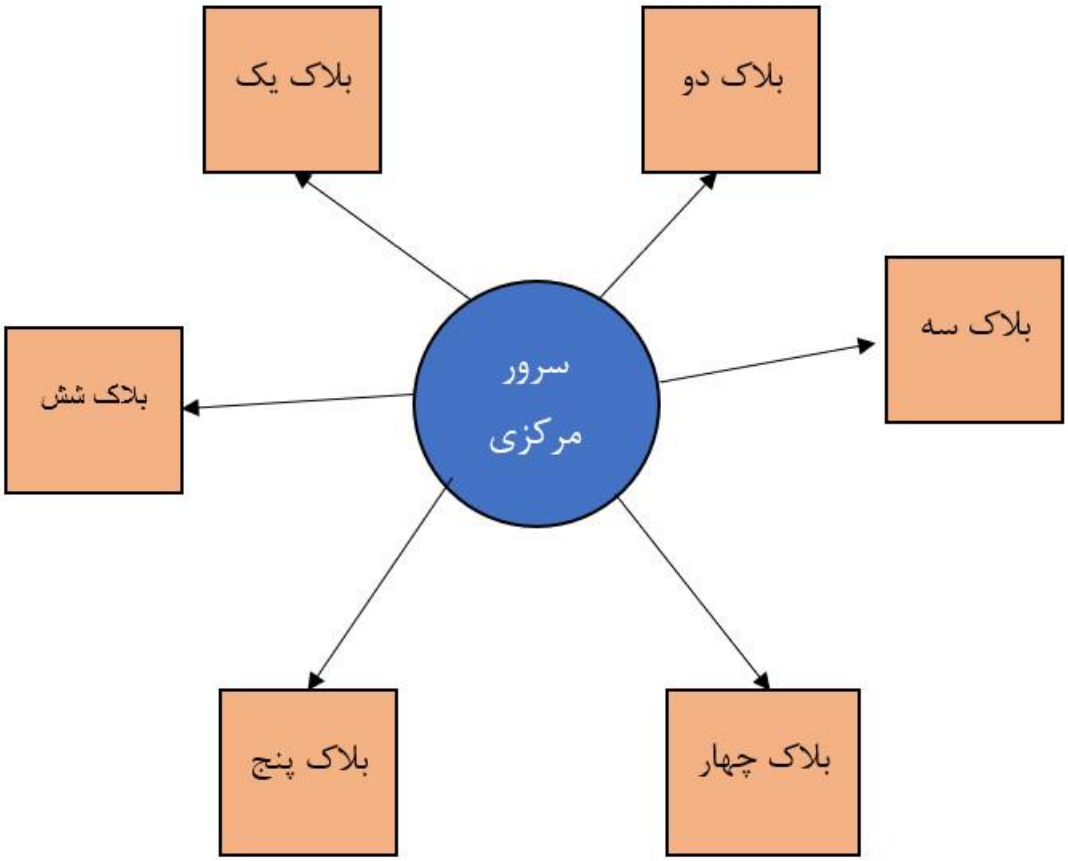
For(i=0, i<=2:i++){

TimeOscore++

If(TimeOscore ==2)

use oscore key for local network //use ssl for every mounth

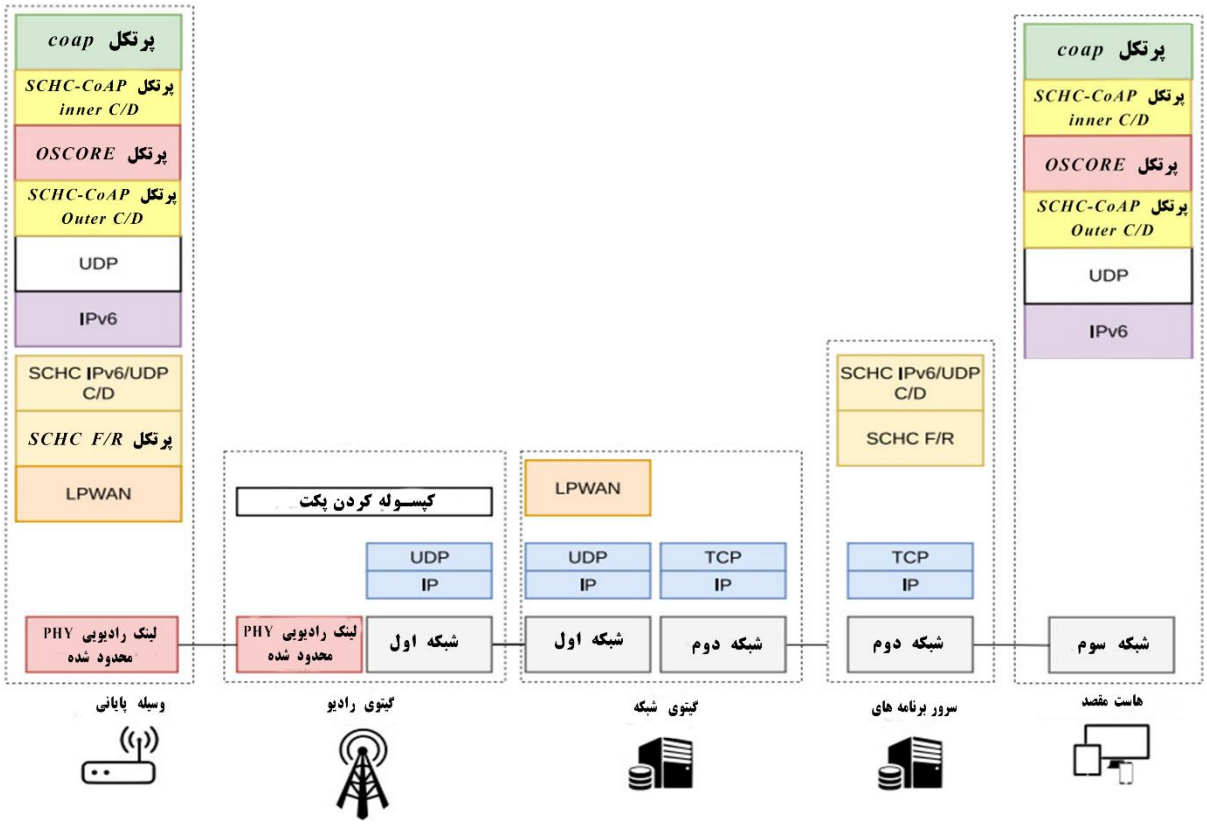
- }



شکل ۱: استفاده از بلاک چین در روش پیشنهادی(هر نود یک بلاک می باشد)

با توجه به شکل ۱ سرور مرکزی در میان بلاک ها کلید oscore را به اشتراک می گذارد و با استفاده از این کلید ارتباطات به صورت رمز شده در شبکه لوکال صورت می گیرد.

ارتباطات در شبکه لوکال با استفاده از پرتکل های oscore و coap به صورت دیاگرام ۲ می باشد:



شکل ۲: معماری oscore و coap

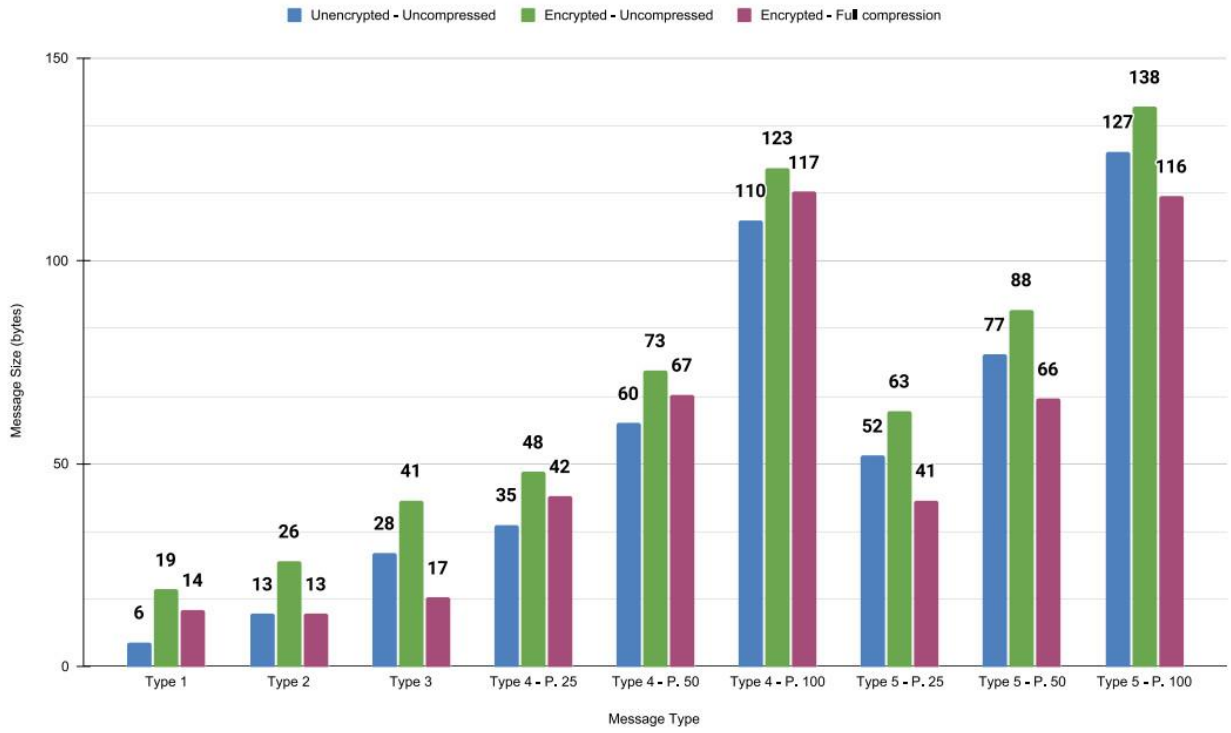
این معماری دستورالعمل‌های گروه کاری LPWAN IETF را دنبال می‌کند و بر پشته پروتکلی استوار است که از LoRaWAN، SCHC، IPv6، OSCORE، CoAP_SCHC و پروتکل‌های CoAP استفاده می‌کند. همانطور که در شکل ۲ نشان داده شده است، این معماری یک ادغام ساده از پروتکل امنیتی OSCORE برای CoAP روی پشته پروتکلی LPWAN IPv6-adapted را فراهم می‌کند.

(Höglund et al, 2023)

یافته ها:

با توجه به استفاده از روش داینامیک تغییر کلید های ssl و oscore در شبکه ارتباطی بین دستگاه های iot در شبکه داخلی و خارجی، احتمال حملات مرد میانی بسیار کاهش می یابد، همچنین در صورت لو رفتن کلید های ssl و oscore به دلیل داینامیک بودن ان ها این موارد به صورت دوره ای تغییر می کنند.

در نمودار یک بررسی میزان طول پیام های ارسالی در پروتکل های رمزگذاری مختلف در iot بررسی شده است:



نمودار ۱: بررسی میزان طول پیام های ارسالی در پرتکل های رمزگذاری شده.

با اعمال بلاک چین در این پرتکل می توان میزان دقت در خصوص نفوذ ها و تخریب های مختلف دیتا در هر گونه هک را گرفت با اعمال بلاکچین در این خصوص جلوگیری از این امر به میزان ۶ درصد افزایش خواهد داشت علاوه بر اینکه طول پیام هم تغییر چندانی نخواهد داشت و در نتیجه امنیت بیشتر شبکه iot موثر خواهد بود.

مراجع:

Bhardwaj, A., Kaushik, K., Bharany, S., & Kim, S. (2023). Forensic analysis and security assessment of IoT camera firmware for smart homes. *Egyptian Informatics Journal*, *24*(4), 100409.

Feijoo-Añazco, A., Garcia-Carrillo, D., Sanchez-Gomez, J., & Marin-Perez, R. (2023). Innovative security and compression for constrained IoT networks. *Internet of Things*, *24*, 100899.

Zakariyya, I., Kalutarage, H., & Al-Kadri, M. O. (2023). Towards a robust, effective and resource efficient machine learning technique for IoT security monitoring. *Computers & Security*, *133*, 103388.

Höglund, J., Furuhed, M., & Raza, S. (2023). Lightweight certificate revocation for low-power IoT with end-to-end security. *Journal of Information Security and Applications*, *73*, 103424.

Rudrakar, S., & Rughani, P. (2023). IoT based agriculture (Ag-IoT): A detailed study on architecture, security and forensics. *Information Processing in Agriculture*.