فصلنامه سیستم‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند
Intelligent Multimedia Processing and Communication Systems (IMPCS)

Winter 2020, 1 (2), 51-59
DOR: 20.1001.1.27832570.1399.1.2.1.7

Received: 9 Nov. 2019
Accepted: 13 Jan. 2020

Improvement of IOT Security in ZigBee Network Using AES256 Algorithm

MohammadJavad Zand,[1], Mohammad Tahghighi Sharabyan*[2]

1. Roozbeh Institute of Higher Education of Zanjan, Zanjan, Iran. zandmj@gmail.com

2. Assistant Professor, Faculty of Electrical and Computer Engineering, Zanjan Branch, Islamic Azad University, Zanjan Iran.*(corresponding Author)* mntahghighi@gmail.com

Abstract

Introduction: The Internet of Things is a new paradigm in the information technology industry that provides a new future for the Internet by integrating users, computing systems, and almost all objects. ZigBee technology is one of the most popular wireless technologies used to connect Internet of Things devices. This technology creates a hierarchical network to enable a number of devices to communicate with each other. The development of services based on the Internet of Things requires improved levels of security and confidentiality. To ensure the confidentiality of information during data transmission, the most common method is data encryption. Lightweight cryptography has been proposed as a concept for managing security in resource-constrained devices, which are the major constituent of the Internet of Things. Lightweight cryptography is based on conventional cryptography principles but aims to design algorithms with little hardware and software footprint. The concept of style extends to methods of decoding and maintaining a balance between performance, security, and cost of algorithms. In this article, the AES algorithm is evaluated as a lightweight algorithm.

Method: In this article, an encryption method with a 256-bit symmetric key with AES standard is proposed, and the information packet that includes application data and authentication information is encrypted and then decrypted by the proposed algorithm Both AES128 (common) and AES256 (recommended) methods are implemented to improve information security, and the impact of the password size is also analyzed.

Results: The proposed method is compared against the legacy AED128 method. The simulation results substantiate that the proposed method reaches a higher level of security by increasing the data decryption time. Even though this improvement has incurred extra computation costs the results show this cost is acceptable.

Discussion: In the proposed method of research, compared to the previous methods, an upgraded method in terms of data security has been used to encrypt the input data in such a way that the data extraction cost is increased and an elevated level of the data security is reached, which This is very useful in improving the security of IoT systems.

Keywords: IoT, Security, Encryption, Confidentiality.

فصلنامه سیستم‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند
Intelligent Multimedia Processing and Communication Systems (IMPCS)
انجمن علمی تجارت الکترونیکی ایران
واحد زنجان

ارتقای امنیت اینترنت اشیا در شبکه زیگبی با استفاده از الگوریتم AES256

تاریخ دریافت: ۱۳۹۹/۰۸/۱۸ دورهٔ اول ، زمستان ۱۳۹۹
تاریخ پذیرش: ۱۳۹۹/۱۰/۲۳ شمارهٔ دوم ، صص: ۵۱ -۵۹

محمدجواد زند[۱]، محمد تحقیقی شربیان[۲*]

۱. کارشناسی ارشد، مؤسسه آموزش عالی روزبه زنجان، زنجان، ایران. zandmj@gmail.com
۲. استادیار، دانشکده مهندسی برق و کامپیوتر، واحد زنجان، دانشگاه آزاد اسلامی، زنجان، ایران. (نویسنده مسئول)
mntahghighi@gmail.com

چکیده: اینترنت اشیا مفهومی جدید در صنعت فناوری اطلاعات است که آینده‌ای جدید از اینترنت را با تلفیق نمودن کاربران، سیستم‌های محاسباتی و تمام اشیا روزمره فراهم‌می‌آورد. مسئله این است که توسعه واقعی این سرویس‌ها، به سطوح ارتقاءیافته امنیت و حفظ محرمانگی نیاز دارد. برای اطمینان از محرمانه‌بودن اطلاعات حین انتقال داده‌ها، عمومی‌ترین روش رمزنگاری داده‌ها است. در این مقاله ابتدا چالش‌های پیش روی در امنیت اینترنت اشیا، شامل حجم انبوه اطلاعات و ارتباطات میان سختافزار سیستم‌ها، بررسی‌شده و چالش امنیتی مورد هدف قرار گرفته‌است. سپس ضمن بررسی و تشریح روش رمزنگاری متداول AES128 که در پروتکل‌های اینترنت اشیا از آن استفاده‌می‌شود، فرایند ارتقای این روش به بالاترین سطح امنیتی این الگوریتم یعنی AES256 و پیاده‌سازی و شبیه‌سازی عملکرد آن بر روی بسته اطلاعاتی انجام‌شده و نتایج حاصل از این ارتقاء و خروجی‌های مورد نظر جهت تحلیل و مقایسه روش پیشنهادی نیز با استفاده از نرم‌افزار متلب تولید و بیان‌می‌گردد.

واژه‌های کلیدی: اینترنت اشیا، امنیت، رمزنگاری، محرمانگی.

۱. مقدمه

اینترنت اشیا (IoT) مفهومی جدید در دنیای فناوری و ارتباطات به شمار می‌آید اما عبارت اینترنت چیزها، برای نخستین بار در سال ۱۹۹۹ توسط کوین اشتون مورد استفاده قرارگرفت و جهانی را توصیف‌کرد که در آن هر چیزی، از جمله اشیای بی‌جان، برای خود هویت دیجیتال داشته‌باشند و به کامپیوترها اجازه‌دهند آن‌ها را سازماندهی و مدیریت‌کنند. اینترنت در حال حاضر همه مردم را به هم متصل‌می‌کند ولی با اینترنت چیزها تمام اشیا به هم متصل‌می‌شوند. البته پیش از آن کوین کلی در کتاب قوانین نوین اقتصادی در عصر شبکه‌ها (۱۹۹۸) موضوع نودهای کوچک هوشمند (مانند سنسور باز و بسته بودن درب) که به شبکه جهانی اینترنت وصل می‌باشند را مطرح نمود. امروزه کارهایی که ازطریق اینترنت صورت‌می‌گیرد مورد توجه اکثر مردم قرارگرفته و سیر تکاملی ارتباطات را دنبال‌می‌کند که ارتباط دستگاه‌های اتوماتیک را با یکدیگر ممکن‌می‌سازد [۵].

اینترنت اشیا آینده امیدوارکننده‌ای برای همه سهامداران در زمینه تکنولوژی از محققین گرفته تا مصرف‌کنندگان، ارائه‌می‌دهد. این موضوع شامل شبکه‌ای از نهادها از جمله اهداف روزمره می‌باشد که قابلیت سنجش، پردازش، ذخیره‌سازی داده‌ها و ارتباط با نهادهای دیگر را دارند. این نهادها یا اشیا می‌توانند به اینترنت متصل‌شده و از طریق یک سرویس روی ماژولی دیگر مانند یک دستگاه موبایل یا برنامه کامپیوتری، نظارت و کنترل گردند. این مدل محاسباتی رایج، چالش بزرگی در زمینه حفظ امنیت ارائه‌می‌دهد یعنی مسائلی چون محرمانه بودن، یکپارچگی، احراز هویت و عدم رد داده‌ها در قالب دستگاه‌های عملیاتی روی منابع محدود[۶].

توسعه اینترنت اشیا و عدم افزایش امنیت باعث بروز حملات بسیاری از سوی هکرها می‌شود. کاربردهای اینترنتی بسیاری امروز امکان پذیر است مانند سیستم حمل ونقل هوشمند- سلامت الکترونیک- کارت‌های هوشمند و غیره. برخی کاربردهای دیگر اینترنت درزمینه‌های تجاری است مانند سیستم بانکداری- بیمه- قراردادها و غیره. در این زمینه به امنیت همه‌جانبه و گسترده ای نیازمندیم. مخصوصاً در زمینه کاربردهای حساس، این امنیت بیشتر اهمیت دارد [۵].

تکنولوژی زیگبی (Zigbee) که به آن در عنوان تحقیق اشاره‌شده است یکی از محبوب‌ترین فناوری‌های بی‌سیم است که برای اتصال دستگاه‌های اینترنت اشیا استفاده‌می‌شود و بر اساس استاندارد IEEE 802.15.4 ساخته و توسعه‌یافته‌است و یک پروتکل مش است[۷]. این تکنولوژی یک شبکه را به صورت سلسله مراتبی ایجادمی‌کند تا تعدادی از دستگاه‌ها را برای برقراری ارتباط با یکدیگر و برخی ارتباطات و ویژگی‌هایی مانند احراز هویت و رمزگذاری فعال‌کند[۷].

اینترنت اشیا، شبکه‌ای از اشیا با قابلیت شناسایی واضح عناصر است که به کمک هوش نرم‌افزاری و حسگرها، امکان اتصال از هر مکان به اینترنت را داشته و با استفاده از زیرساخت‌های مخابراتی اینترنت، چیزها یا اشیا را برای تبادل اطلاعات با تولیدکننده، اپراتور و یا سایر دستگاه‌های متصل، توانمند می‌سازد. این فناوری به اشیا فیزیکی (برای ارائه اطلاعات خاص)، اجازه درک‌کردن و کنترل از راه دور از طریق اینترنت را می‌دهد و فرصت‌هایی برای یکپارچه‌سازی بیشتر بین دنیای فیزیکی و سیستم‌های کامپیوتری به وجود آورده که موجب بهبود کارایی، دقت و سود اقتصادی می‌شود. در اینترنت اشیا هر شی با استفاده از سیستم محاسباتی طراحی‌شده، به‌طور منحصربه‌فرد شناسایی‌می‌شود و می‌تواند با زیرساخت‌های موجود در اینترنت همکاری‌کند[۸].

۲. چالش‌های امنیتی در نگاه اول

اینترنت اشیا، یکی از مهم‌ترین و در عین حال، در هم‌گسیخته‌ترین فناوری‌های سده حاضر می‌باشد. اینترنت اشیا در واقع تکامل طبیعی اینترنت (کامپیوترها) برای سیستم‌های تعبیه‌شده و سایبرفیزیکی است. اشیائی که با وجود این که خودشان لزوماً کامپیوتر نیستند اما در خود، کامپیوتر جای‌داده‌اند که با شبکه ای ارزان و اشیای به هم متصل، جمع‌آوری اطلاعات درباره جهان و محیط ما را می‌توانند با طبقه‌بندی بسیار بیشتر به‌دست‌آورند. قطعاً چنین دانش دقیقی می‌تواند بازدهی‌ها را افزایش‌داده و خدمات پیشرفته را در بازه گسترده‌ای از دامنه‌های گسترده کاربردی همانند مراقبت از سلامت همگانی و خدمات شهرهای هوشمند ارائه‌کند. با این جمع‌آوری فراگیر، متراکم و بسیار غیرقابل‌رؤیت، پردازش و انتشار داده در میان زندگی افراد منجر به نگرانی‌های محرمانگی و امنیت جدی می‌شود. از طرفی این داده‌ها را می‌توان به منظور ارائه بازه‌ای از خدمات شخصی‌سازی شده و پیچیده در اختیار عموم قرارداد و از طرفی دیگر، در این داده‌ها اطلاعاتی تعبیه‌شده که می‌توان از آن استفاده‌نمود تا به صورت الگوریتمی، بیوگرافی مجازی از فعالیت‌های ما تشکیل‌داده که الگوهای سبک زندگی و رفتار خصوصی ما را به تصویر می‌کشد[۹].

ریسک محرمانگی اینترنت اشیا به دلیل عدم وجود محافظ‌های اساسی امنیت در بسیاری از محصولات نسل اول اینترنت اشیا در بازار تشدید می‌شود. نقاط ضعف امنیتی فراوانی در دستگاه‌های متصل شناسایی‌شده‌اند همانند قفل‌های هوشمند، وسایل نقلیه. چندین خصیصه درونی اینترنت اشیا، چالش‌های امنیتی و محرمانگی آن را تشدید می‌کند که این موارد، شامل عدم وجود کنترل مرکزی، ناهمگونی در منابع دستگاه، چندین سطح حمله، طبیعت موقعیتی، ماهیت وضعیتی، ماهیت آگاه از خطرات و مقیاس می‌شود[۹].

۳. امنیت و رمزنگاری در اینترنت اشیا

رمزنگاری سبک به عنوان یک مفهوم برای مدیریت امنیت در دستگاه‌های محدود منابع، ارائه‌شده‌است و اینترنت اشیا یک بخش اصلی در چنین دستگاه‌هایی است. رمزنگاری سبک بر اساس اصول مرسوم رمزنگاری است، اما هدف آن طراحی الگوریتم‌ها با جای‌گیری کم در سخت‌افزار و نرم‌افزار است. مفهوم سبک به روش‌های رمزگشایی و حفظ تعادل بین عملکرد، امنیت و هزینه الگوریتم‌ها گسترش‌می‌یابد[۶].

برای اینکه هر الگوریتم رمزنگاری به صورت کاملاً ایمن پذیرفته‌شود، باید چهار شرط را شامل‌شود :

- محرمانه‌بودن: داده‌ها تنها توسط فرستنده یا گیرنده قابل دسترسی باشد
- انسجام: داده‌ها توسط کاربر غیرمجاز تغییر نکند
- تأیید اعتبار: امکان تأیید داده‌ها و کاربر وجودداشته‌باشد
- عدم انصراف: کاربر نتواند ارتباط با داده‌های ارسال‌شده را رد کند.

تا سال ۲۰۲۰، پیش‌بینی‌هایی از منابع مختلف نظیر Gartner، Cisco و HP نشان‌می‌دهد که تعداد دستگاه‌های اینترنت اشیا به ۵۰ میلیارد افزایش‌یافته‌است که این رقم چشمگیر است، زیرا امنیت هنوز در مراحل اولیه تحقیق قراردارد[۶].

۴. بررسی پروتکل ارتباطی زیگبی

همگام‌سازی همه دستگاه‌های خانگی هوشمند آسان نیست ونیاز به یک زبان مشترک برای همکاری با فناوری‌های تولیدکنندگان مختلف دارد. زیگبی یا Zigbee یکی از پروتکل‌های پیشرو در بحث برقراری ارتباط تکنولوژی‌های مختلف با یکدیگر است. طی چند سال گذشته، ما از موقعیت سیستم‌های قطع‌شده به دنیایی با هاب‌های در حال ظهور منتقل‌شده‌ایم، با دستگاه‌های بزرگ مانند Amazon Echo و Google Home که به عنوان هاب‌ها عمل‌می‌کنند تا همه خدمات خود را از طریق سیستم عامل‌های جدیدی مانند اپل HomeKit و SmartThings سامسونگ به یکدیگر متصل‌کنند[۱].

زیگبی از استانداردهای شبکه محلی IEEE 802.15.4 برای ارتباط با دستگاه‌های دیگر زیگبی که در فواصل بین ۱۰-۲۰ متر می‌باشند، با توجه به چند عامل استفاده می‌کند و به همین دلیل این پروتکل بسیار مهم است. چراکه یک مش ایجادمی‌شود، جایی که هر یک از دستگاه‌های متصل در یک موقعیت پیش‌فرض، قادر به برقراری ارتباط با دستگاه بعدی می‌شوند. زیگبی باید از بسیاری از دستگاه‌های موجود در شبکه پشتیبانی‌کند و خوشبختانه، این مقدار در هر زمانی معادل ۶۵۰۰۰ برابر می‌شود. بدون نیاز به یک مرکز متمرکز، از لحاظ نظری، دستگاه‌ها می‌توانند در یک منطقه بزرگ کارکنند و اطلاعات را در اطراف مش قرار دهند. زیگبی ارائه دهنده شبکه کامل مش است که می‌تواند صدها دستگاه را در یک شبکه واحد پشتیبانی‌کند.Zigbee PRO 2017 اکنون با توجه به درس‌هایی که از پیاده‌سازی و توسعه Zigbee PRO بر روی ده‌ها دستگاه در سراسر جهان داشته حاصل شده که دارای به‌روزترین ویژگی‌هاست. زیگبی تنها راه‌حل کامل اینترنت اشیا است که، از شبکه مش به صورت زبانی جهانی استفاده‌می‌کند و اجازه‌می‌دهد که اجزای هوشمند باهم کارکنند[۱].

Zigbee 3.0 از رمزگذاری متقارن AES و کلید ۱۲۸ بیتی سودمی‌برد، بنابر این اطلاعاتی که در اطراف مش قراردادهمی‌شود بسیار امن است. ZigBee 3.0 انتخاب و انعطاف‌پذیری را برای کاربران و توسعه‌دهندگان افزایش‌می‌دهد و اطمینان حاصل‌می‌کند که محصولات و سرویس‌ها در همه لایه‌های پشته سازگاری‌دارند. راه‌حل ZigBee 3.0 شامل آزمودن، گواهینامه، نام تجاری و پشتیبانی بازاریابی است تا از طریق توسعه و فروش محصولات و راه‌حل‌های متقابل، ساده‌تر شود. بدین ترتیب فرصت‌های رشد را در حالی فراهم‌می‌کند که نوآوری را قادرمی‌سازد تا توانایی‌های جدید را در خانه، کار و جاده‌ها فعال‌کند. ZigBee 3.0 بر روی Zigbee PRO ساخته‌شده‌است که با استاندارد شبکه IEEE 802.15.4 با افزودن شبکه مش و لایه‌های امنیتی همراه با یک چارچوب کاربردی و تبدیل‌شدن به یک پشته کامل، قدرتمند و قابل اطمینان، راه‌حل متقابل زیگبی را بهبودمی‌بخشد.

۵. الگوریتم‌های رمزنگاری در اینترنت اشیا

رمزنگاری بهینه‌ترین روش برای حفظ امنیت شبکه‌ها می‌باشد. لغت رمزنگاری در انگلیسی Cryptography می‌باشد که ریشه این واژه Kruptos به معنای پنهان از زبان یونانی گرفته شده است. کلیدی که در رمزنگاری استفاده می شود طی یک فرآیند بسیار پیچیده اطلاعات را پنهان‌نموده که بدون کلید رمزگشا قابل کشف نیست. مشکل‌ترین بخش حفظ امنیت کلید است. در الگوریتم کلید نامتقارن، فرآیند رمزکردن یک پیغام و بازکردن رمز، توسط دو کلید متفاوت، یکی برای رمزکردن و دیگری برای رمزگشایی، صورت‌می‌پذیرد. در الگوریتم کلید متقارن، این فرآیند معمولاً توسط یک کلید انجام‌می‌شود[۲].

در این مقاله الگوریتم کلید متقارن و به‌خصوص الگوریتم AES مورد بحث می‌باشد. الگوریتم‌های رمزنگاری متعارف در سناریوی اینترنت اشیا به دلیل محدودیت‌های منابع و شرایط موجود مانند مصرف انرژی، محدودیت استفاده از باتری، و زمان واقعی اجرا مناسب نبوده، بنابراین از رمزنگاری سبک وزن به علت سازگاری بیشتر در محیط اینترنت اشیا استفاده‌می‌گردد. تعدادی از الگوریتم‌های رمزنگاری سبک وزن وجود دارد که در حال حاضر در دسته‌های تحقیقاتی الگوریتم‌های متقارن و نامتقارن تقسیم‌بندی می‌شوند. اما این الگوریتم‌های سبک وزن هنوز تضمین امنیت در زمان واقعی، زمان اجرا، مصرف انرژی و نیاز به حافظه را نمی‌دهد. الگوریتم‌های متقارن فاقد احراز هویت بوده در حالی که الگوریتم‌های نامتقارن دارای مسئله اندازه کلید بزرگتر و مصرف حافظه بیشتر می‌باشد. این امر بر روی جمع‌آوری و پردازش اطلاعات در زمان واقعی تأثیر گذاشته و باعث اتلاف منابع اینترنت اشیا می‌گردد. جدول۱ چند الگوریتم رمزنگاری سبک وزن متقارن و جدول ۲ چند الگوریتم رمزنگاری سبک وزن نامتقارن در حوزه اینترنت اشیا به همراه حملات احتمالی که از آن جلوگیری‌می‌شود را نشان‌می‌دهد[۱۰].

جدول ۱ : چند الگوریتم رمزنگاری سبک وزن متقارن[۱۰]

الگوریتم متقارن	طول کد	اندازه کلید	جلوگیری از حملات احتمالی
AES	2606	128	MITM
HIGHT	5672	128	Saturation Attack
TEA	1140	128	Related Key Attack

PRESENT	936	80	Differential Attack

جدول ۲ : چند الگوریتم رمزنگاری سبک وزن نامتقارن[۱۰]

الگوریتم نامتقارن	طول کد	اندازه کلید	جلوگیری از حملات احتمالی
RSA	900	1024	ModulesAttack
ECC	8838	160	Timing Attack

الگوریتم AES دارای سه نسخه ۱۲۸، ۱۹۲ و ۲۵۶ بیتی است. این الگوریتم در لایه برنامه کاربردی اینترنت اشیا وتحت پروتکل CoAP اجرا می‌گردد[۳]. کلید الگوریتم HIGHT در مرحله‌های رمزنگاری و رمزگشایی تولیدمی‌شود. لی و همکاران وی پیشنهاد یک اجرای موازی را که نیاز به انرژی کمتری دارد ارائه‌کردند[۱۱]. از الگوریتم TEA برای محیط‌های محدود مانند شبکه حسگر یا اشیای هوشمند استفاده می‌شود. کد این الگوریتم در چند خط نوشته‌شده‌است. نه از یک برنامه پیچیده بلکه از عملیات ساده XOR جهت اضافه‌کردن و تغییردادن استفاده‌می‌نماید.PRESENT به عنوان الگوریتم سبک وزن برای امنیت استفاده‌می‌شود[۳].

الگوریتم RSA به دلیل اندازه کلید بزرگ آن متعلق به سیستم رمزنگاری سبک وزن نیست. اما به دلیل استفاده از دو عدد اول بزرگ و اجرای عملیات ماجولار، دارای امنیت بیشتر بوده و باعث افزایش حریم خصوصی کاربران می‌شود. الگوریتم ECC نیاز به کلیدکوچکتر دارد به این ترتیب، سرعت پردازش آن سریعتر بوده و نیاز به حافظه کمتری دارد و مناسب پیاده سازی در سخت افزارهای اینترنت اشیا است[۱۲].

۶. اهمیت محرمانگی در دستگاه‌های اینترنت اشیا

دسترسی یا دستکاری غیرمجاز در سخت‌افزار و نرم‌افزار مربوط به دستگاه‌ها ممکن است باعث نشت اطلاعات حساس شود. به عنوان نمونه، یک فرد نفوذگر می‌تواند با برنامه‌ریزی مجدد دوربین مداربسته، کاری کند که علاوه بر ارسال داده‌ها به سرور مجاز، یک نسخه از داده‌ها نیز برای وی ارسال‌شود. بنابراین برای دستگاه‌هایی که اطلاعات حساس را جمع آوری‌می‌کنند، استحکام و نفوذ ناپذیری از ویژگی‌های مهم آنها به حساب می‌آید. برای اطمینان از امنیت اینترنت اشیا، استفاده از فناوری محاسبات قابل‌اعتماد، از جمله اعتبارسنجی صحت دستگاه، ماژول‌های مقاوم در برابر نفوذ و استفاده از فضاهای امن، می‌تواند مفید واقع‌شود. به منظور فراهم‌آوردن حریم خصوصی در دستگاه‌ها، با مشکلات زیادی مواجه‌هستیم که یکی از آن‌ها محرمانگی آدرس دستگاه، یعنی مخفی ماندن موقعیت دستگاه و مالک آن است، به عبارت دیگر به معنی حفاظت در مقابل شناسایی دقیق ماهیت دستگاه و حفاظت از اطلاعات شخصی دربرابر سرقت و یا مفقودشدن دستگاه و مقاومت دربرابر حملات کانال جانبی می‌باشد. محرمانگی موقعیت مکانی در شبکه‌های بی‌سیم با استفاده از الگوریتم چند مسیریابی تصادفی مابین حسگرهای بی‌سیم به‌وجودمی‌آید[۴].

۷. اهمیت محرمانگی در خلال ارتباطات

برای اطمینان از محرمانه بودن اطلاعات حین انتقال داده‌ها، عمومی ترین روش رمزگذاری است. در رمزگذاری، داده‌های خاصی به بسته‌های ارسالی افزوده‌می‌شوند که باعث‌می‌شود این بسته‌ها قابل ردیابی باشند مانند دنباله ای از اعداد، شاخص پارامتر امنیت و. ...، این اعداد برای تجزیه و تحلیل شبکه و ارتباط بسته‌ها با هم استفاده‌می‌شوند. استفاده از پروتکل ارتباط امن روش مناسبی برای ایجاد محرمانگی حین انتقال است. به منظور کاهش آسیب‌پذیری در طول انتقال داده‌ها، می‌توان از جایگزین کردن نام‌های مستعار در رمزگذاری استفاده‌کرد به صورتی که شناسایی دستگاه یا کاربری که اطلاعات را ارسال یا دریافت‌می‌کند امکان‌پذیر نباشد. یکی از مثال‌های نام آشنا، استفاده از هویت موقت است. همچنین برای از بین بردن احتمال افشای اطلاعات ناشی از انتقال داده‌ها، دستگاه‌ها فقط در صورت نیاز باید ارتباط برقرارکنند[۴].

۸. روش پیشنهادی

اینترنت اشیا با توجه به گسترش کاربری آن، دارای آسیب‌پذیری‌ها و چالش‌هایی در ارتباط با امنیت است، به طوری‌که می‌توان از امنیت، تحت عنوان «پاشنه آشیل اینترنت اشیا» یاد کرد. این آسیب‌پذیری‌ها باعث ایجاد نگرانی‌های جدی از توسعه این فناوری شده‌است. نگرانی‌های مربوط به امنیت اینترنت اشیا و آسیب‌پذیری‌های آن شامل افزایش روزافزون کاربردها و خدمات مبتنی بر اینترنت اشیا در صنایع مختلف ضرورت فراهم‌آوردن امنیت و حریم خصوصی، دسترسی راحت و گسترده به اینترنت، معضلات امنیتی فضای سایبری را گریبانگیر این فناوری کرده است. از طرف دیگر 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 را دو چندان نمایان‌می‌سازد. توسعه تکنیک‌ها و مفاهیم برای بهینه‌سازی امنیت و کاهش آسیب‌پذیری‌ها و تعریف قوانین جدید در زمینه گسترش کاربری و توسعه کسب‌وکارها با ممانعت از ایجاد آسیب‌پذیری‌ها و حفظ حریم خصوصی یک مهم است که باید به آن دست‌یافت.

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 صرف‌کرد و حتی صدمات جانی که ممکن است عدم‌توجه و شناخت موضوعات امنیتی در این حوزه به‌بارآورد، ضرورت شناسایی و پرداختن به مسائل و چالش‌های امنیتی آن احساس می‌شود.

از این روی با توجه به نقش اساسی رمزنگاری در اینترنت اشیا و اهمیت حفظ محرمانگی اطلاعات و همچنین احراز هویت امن، در این مقاله یک روش رمزنگاری با کلید متقارن ۲۵۶ بیتی با استاندارد AES پیشنهادمی‌گردد و بسته اطلاعاتی که شامل داده‌های کاربردی و اطلاعات احراز هویت است توسط الگوریتم پیشنهادی رمزنگاری شده و

سپس رمزگشایی می‌گردد. همانگونه که در قبل به آن اشاره‌شد با توجه به اینکه کلید رمز متداول در پروتکل‌های در حال استفاده در اینترنت اشیا ۱۲۸ بیتی و در استاندارد AES هستند. در این مقاله هر دو روش AES128(متداول) و AES256 (پیشنهادی) پیاده‌سازی و اجرا شده تا ضمن ارتقای امنیت اطلاعات، نتایج تغییر در اندازه کلید رمز نیز مورد بررسی و تحلیل و نتیجه‌گیری این پژوهش قرارگیرد.

مدل ارائه‌شده در این مقاله در قالب شکل ۱ نشان‌داده‌شده که در ادامه روش اجرای الگوریتم با ذکر جزئیات، شرح داده شده‌است.

شکل ۱ : مراحل اجرای الگوریتم‌ها برروی داده‌های ورودی

۹. ابزار پیاده‌سازی

در این مقاله برای شبیه‌سازی مدل پیشنهادی مبتنی بر رمزنگاری با روش‌هاAES12 و AES256، از زبان برنامه‌نویسی MATLAB (64-bit) R2020a استفاده‌شده‌است که بر روی یک سرور با مشخصات زیر اجرا می‌گردد. Xeon E5-2690 2.9 GHz 12Core 8GB Ram

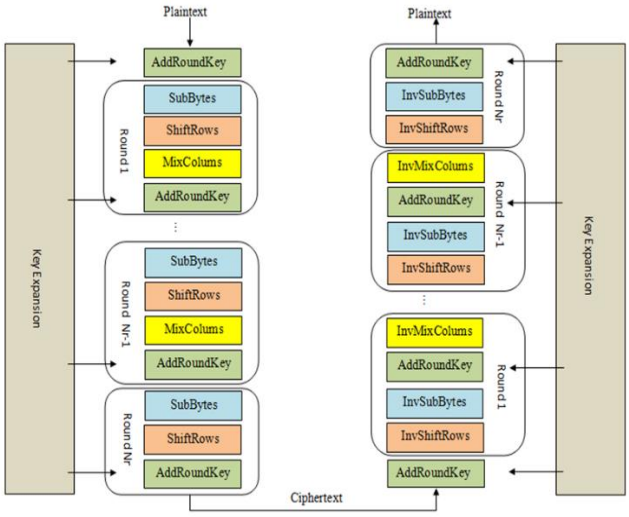
۱۰. الگوریتم رمزنگاری AES

رمزنگاری AES شامل سه بلاک رمز است که عبارتند از AES128، AES192 و AES256 هر ک از این سه روش، داده‌ها را به صورت بلاک‌های ۱۲۸ بیتی و به ترتیب با استفاده از کلیدهای رمزنگاری ۱۲۸، ۱۹۲ و ۲۵۶ بیتی رمزنگاری و رمزگشایی می‌کنند. رمزهای متقارن یا کلید مخفی از یک کلید یکسان هم برای رمزنگاری و هم برای رمزگشایی استفاده‌می‌کنند، بنابراین هم فرستنده و هم گیرنده باید از کلید مخفی یکسان اطلاع‌داشته و از آن استفاده‌کنند. هر سه طول کلید برای حفاظت از اطلاعات کافی می‌باشند ولی برای محافظت از اطلاعاتی که در سطح "مخفی" و "بسیار مخفی" طبقه‌بندی‌می‌شوند، کلیدهای ۱۹۲ یا ۲۵۶ بیتی موردنیاز هستند. سیستم‌های رمزنگاری کلید متقارن از یک کلید یکسان برای رمزنگاری متن آشکار و رمزگشایی متن رمزی استفاده‌می‌کنند. سیستم‌های کلید متقارن از مزیت ساده و سریع بودن برخوردار هستند. با این حال، عامل مهمی که باید در نظر گرفته‌شود، این است که طرفین انتقال باید کلید را به صورت امنی مبادله‌نمایند. AES مبتنی بر یک اصل طراحی است که با نام شبکه جایگزینی- جایگشت شناخته‌می‌شود و ترکیبی از جایگزینی و جایگشت می‌باشد، و از نظر نرم‌افزاری و سخت‌افزاری سریع است. AES بر روی یک ماتریس ۴ × ۴ بر حسب بایت عمل‌می‌کند که ماتریس حالت نامیده‌شده و به صورت ستونی در نظر گرفته‌می‌شود. اکثر محاسبات AES در یک میدان محدود مخصوصی($GF(2^8)$) انجام‌می‌شوند[۱۳].

اندازه کلید استفاده‌شده در رمزنگاری AES، تعداد تکرارهای چرخه‌های تبدیل (transformation) را تعیین‌می‌کند که ورودی، با نام متن عادی (plaintext) را به خروجی نهایی با نام متن رمزشده (ciphertext) تبدیل می‌نماید. تعداد چرخه‌های تکرار به صورت زیر است:

- ۱۰ چرخه تکرار برای کلیدهای ۱۲۸ بیتی
- ۱۲ چرخه تکرار برای کلیدهای ۱۹۲ بیتی
- ۱۴ چرخه تکرار برای کلیدهای ۲۵۶ بیتی

طبق شکل ۲ هر تکرار شامل چندین مرحله پردازشی است، که یک مرحله بستگی به کلید رمزنگاری دارد. مجموعه‌ای از چرخه‌های معکوس برای تبدیل متن رمزشده به متن اصلی با استفاده از همان کلید رمزنگاری به‌کار گرفته می‌شود.



شکل ۲ : توابع اجرا شونده در هر دور رمزنگاری

۱۱. ورودی‌های الگوریتم

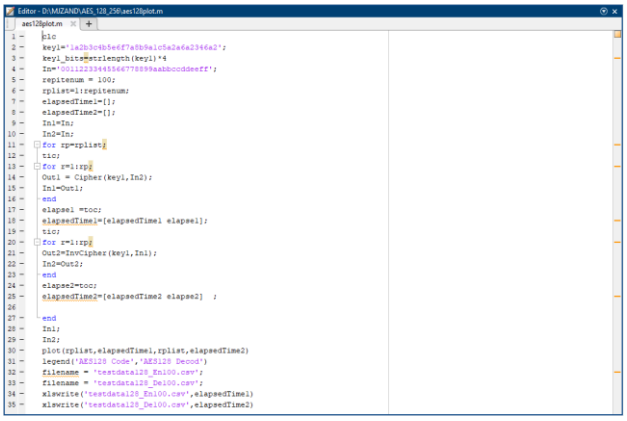
ورودی‌های الگوریتم‌های رمزنگاری یک آرایه ۱۲۸ بیتی است که بسته به شرایط می‌تواند برای انتقال داده‌های اساسی بین یک گره با یک کنترل‌کننده و یا یک گره با گره دیگر در محیط اینترنت اشیا استفاده-شود. البته ضروری است برای انتقال داده امن، حتماً بخشی از پیام مبادله شده جهت تشکیل نشست فعال، شناسایی و احراز هویت بین دو دستگاه استفاده‌گردد که با توجه به طول آرایه که ۱۲۸ بیت است در این پژوهش فرض بر آن است که ۶۴ بیت از ظرفیت برای مبادله دیتا و ۶۴ بیت باقیمانده برای مبادله اطلاعات هویتی و تشکیل نشست‌ها بین کنترل-کننده و گره و یا بین دو گره در نظرگرفته‌شده‌است. برای اجرای الگوریتم و فراخوانی توابع مربوط به چرخه‌های رمزنگاری در متلب [۱۴] طبق شکل ۳ و ۴ یک آرایه ۱۲۸ بیتی به نام In با مقادیری که دارای یک الگوی خاص قابل‌تشخیص است در نظر گرفته‌شده‌است تا پس از رمزگشایی متن رمزشده، صحت عملکرد الگوریتم به‌وضوح نمایان‌گردد.

In='00112233445566778899aabbccddeeff';

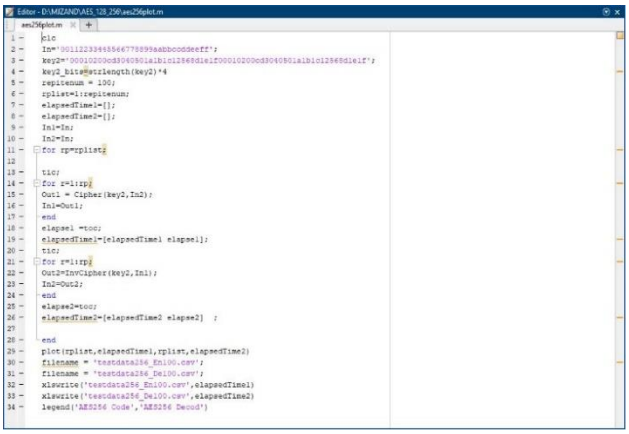
در رشته ورودی In هر دو کاراکتر نمایانگر یک بایت اطلاعات در مبنای ۱۶ است که معادل عددی آن بین ۰ تا ۲۵۵ خواهدبود. برای تعیین کلید رمزنگاری از متغیر استفاده‌شده که برای کلید ۱۲۸ بیتی از متغیر key1 و برای کلید ۲۵۶ بیتی از متغیر key2 استفاده‌می‌شود. مقادیر تصادفی تعیین‌شده برای هر کلید به شرح زیر است :

key1='1a2b3c4b5e6f7a8b9a1c5a2a6a2346a2';
key2='00010200cd3040501a1b1c12568d1e1f00010200cd3040501a1b1c12568d1e1f';

در رشته‌های ورودی فوق نیز هر دو کاراکتر نمایانگر یک بایت اطلاعات بر مبنای ۱۶ است که معادل عددی آن بین ۰ تا ۲۵۵ خواهد بود.



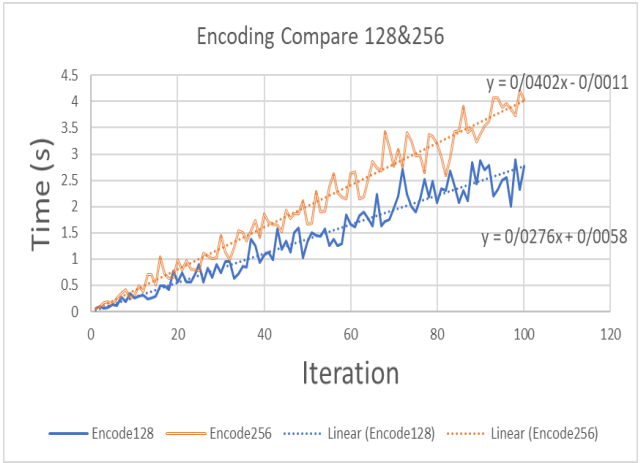
شکل ۳ : کد اجرایی فراخوانی توابع رمزنگاری AES128



شکل ۴ : کد اجرایی فراخوانی توابع رمزنگاری AES256

۱۲. خروجی الگوریتم

با توجه به توضیحاتی که در خصوص الگوریتم رمزنگاری AES به صورت مفصل بیان‌گردید خروجی‌های الگوریتم‌ها در روش پیشنهادی همان داده‌های ورودی رمزنگاری‌شده با دو روش به طول کلید ۱۲۸ بیتی(متداول) و ۲۵۶ بیتی (پیشنهادی در این پژوهش) خواهندبود که عمل رمزگشایی بر روی آن‌ها با دو روش مذکور با موفقیت انجام‌شده است. جهت حصول نتایج قابل‌مقایسه و تعیین مسیر رشد نتایج، دو الگوریتم بصورت دنباله عددی(۱تا۱۰۰) به دفعات مشخص بر روی ورودی‌های یکسان اجراشده و نتایج زمانی اجراها جهت رسم نمودارهای زمانی همانند شکل۵ و ۶ و مسیر رشد نتایج آن‌ها استفاده‌می‌گردد. در ادامه برای مقایسه و تحلیل روش پیشنهادی با محاسبه زمان تقریبی مورد نیاز برای اجرا در تکرار مرتبه ۱۰۰، درصد افزایش زمان اجرا با ارتقای روش رمزنگاری به‌صورت جداگانه برای دو فرایند رمزنگاری و رمزگشایی محاسبه‌شده‌است.



شکل ۵ : مقایسه زمانی رمزنگاری‌ها (۱۲۸و۲۵۶ بیتی)

رمزنگاری AES256 :

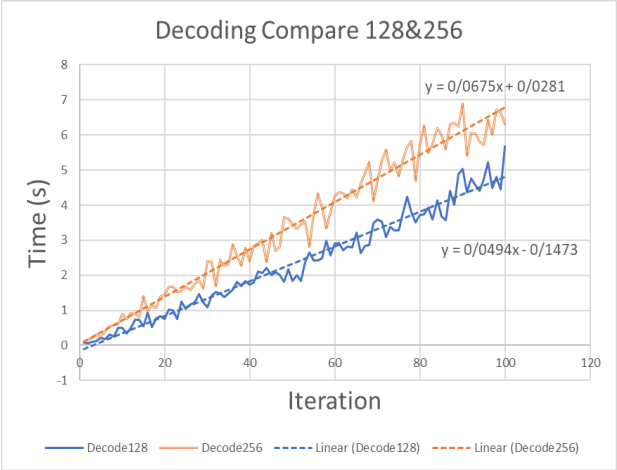
$$\left\{ \begin{matrix} if\ x=100 \\ y=0.0402x-0.0011 \end{matrix} \right\} \rightarrow y = 4.0189$$

رمزنگاری AES128 :

$$\left\{ \begin{matrix} if\ x=100 \\ y=0.0276x+0.0058 \end{matrix} \right\} \rightarrow y = 2.7658$$

مقدار درصد افزایش زمان رمزنگاری :

$$\frac{4.0189-2.7658}{2.7658}\times 100 = 45.3069$$



شکل ۶ : مقایسه زمانی رمزگشایی‌ها (۱۲۸و۲۵۶ بیتی)

رمزگشایی AES256 :

$$\left\{\begin{matrix} if\ x=100 \\ y=0.0675x-0.0281 \end{matrix}\right\} \rightarrow y = 6.7781$$

رمزگشایی AES128 :

$$\left\{\begin{matrix} if\ x=100 \\ y=0.0494x+0.1473 \end{matrix}\right\} \rightarrow y = 4.7927$$

مقدار درصد افزایش زمان رمزگشایی :

$$\frac{6.7781-4.7927}{4.7927}\times 100 = 41.4255$$

۱۳. نتایج و یافته‌ها

در این مقاله تأثیر افزایش طول کلید در افزایش هزینه ارتقای امنیت رمزنگاری در اینترنت اشیا با استفاده از الگوریتم رمزنگاری AES256 بررسی‌شده‌است. اینترنت اشیا نشان دهنده تکامل اینترنت در آینده می باشد. به کمک این فناوری می‌توان داده‌های خام را به اطلاعات و سپس اطلاعات را به دانش و در نهایت دانش را به خبرگی تبدیل‌نمود. مسئله حریم خصوصی در بین ابعاد امنیتی اینترنت اشیا دارای اهمیت فراوانی است، چرا که عدم‌حفظ حریم خصوصی موجب عدم‌پذیرش سیستم و سرویس‌های اینترنت اشیا توسط مردم و سازمان‌های مختلف می‌شود که در نتیجه هدف نهایی از میان می‌رود. مقوله حریم خصوصی در اینترنت اشیا بسیار حیاتی است. نگرانی‌های مربوط به امنیت اینترنت اشیا و آسیب‌پذیری‌های آن شامل افزایش روزافزون کاربردها و خدمات مبتنی بر اینترنت اشیا در صنایع مختلف ضرورت فراهم‌آوردن امنیت و حریم خصوصی، دسترسی راحت و گسترده به اینترنت و معضلات امنیتی فضای سایبری را گریبانگیر این فناوری کرده‌است. از طرف دیگر 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 را دو چندان نمایان‌می‌سازد. توسعه تکنیک‌ها و مفاهیم برای بهینه‌سازی امنیت و کاهش آسیب‌پذیری‌ها و تعریف قوانین جدید در زمینه گسترش کاربری و توسعه کسب وکارها با ممانعت از ایجاد آسیب‌پذیری‌ها و حفظ حریم خصوصی یک مهم است که باید به آن دست یافت. برخلاف اینترنت معمولی، حجم اطلاعات اندازه‌گیری شده در اینترنت اشیا (از افراد یا توسط افراد) بسیار بیشتر است و بنابراین خطر افشای اطلاعات شخصی افراد به مراتب بیشتر خواهد بود. با توجه به مطالب مطرح شده، در این پژوهش سعی برآن شد تا با استفاده از الگوریتم رمزنگاری AES256 ارتقای امنیت اینترنت اشیا در شبکه زیگبی که از رمزنگاری به روش AES128 استفاده می‌کند حاصل گردد.

در روش پیشنهادی در این پژوهش در مقایسه با روش‌های پیشین از یک روش ارتقاء یافته از لحاظ امنیت داده‌ها برای رمزنگاری داده‌های ورودی استفاده شده است و نتیجه آن استخراج درصد افزایش هزینه ارتقاء با رسیدن به سطح بسیار مخفی در امنیت داده‌ها است، که این در بهبود امنیت سیستم‌های اینترنت اشیا بسیار مفید است. با توجه به نوین بودن موضوع اینترنت اشیا، محققان پیشین اغلب به مسئله امنیت پرداخته اند، اما به لحاظ ذات طراحی این تکنولوژی که کاهش هزینه‌ها امری مهم در آن است و روش ارتقای امنیت پیشنهادی اگر چه یک روش رمزنگاری سبک وزن محسوب می‌شود ولی به لحاظ طول کلید و تعداد چرخه، مقداری هزینه در برخواهد داشت که باعث شده محققان کمتری در این حیطه به پژوهش بپردازند. از این روی روش پیشنهادی در این پژوهش روشی نوین می‌باشد.

مراجع

[۱] ف. عابدینی, "آشنایی و بررسی پروتکل ارتباطی زیگبی," مجله میم تک, vol. 21, 1397, [Online]. Available: http://mimtech.ir/mag/zigbee/.

[۲] ح. کریمانپور and س. پویان, "افزایش امنیت در ارتباطات مراکز دیسپاچینگ نیرو از طریق بکارگیری الگوریتمهای پیشرفته رمزنگاری اطلاعات AES با مطالعه موردی الگوریتم," vol. 30, 1394, [Online]. Available: http://psc-ir.com/cd/2015/include/paper.html?1135.

[۳] ب. پهلوانزاده and س. کلینی, "بررسی معماری امنیتی اینترنت اشیاء : چالش‌ها و راهکارها," ۱۳۹۷, [Online]. Available: csj.isi.org.ir/uploadfiles/068729352%20(2).pdf.

[۴] ف. پدیداران مقدم and ا. معنوی, "چالش‌های امنیتی، اهمیت محرمانگی و فرهنگ پدیداران مقدم شکاف اطلاعاتی و ارتباطی در اینترنت اشیاء," نخستین کنفرانس سراسری مهندسی برق، کامپیوتر و فناوری اطلاعات،شیراز, ۱۳۹۵, [Online]. Available: https://civilica.com/doc/585440/.

[5] D. Minoli and B. Occhiogrosso, "Blockchain mechanisms for IoT security," Internet of Things, vol. 1–2, pp. 1–13, Sep. 2018, doi: 10.1016/j.iot.2018.05.002.

[6] W. Julian Okello, Q. Liu, F. Ali Siddiqui, and C. Zhang, "A survey of the current state of lightweight cryptography for the Internet of things," in 2017 International Conference on Computer, Information and Telecommunication Systems (CITS), Dalian, China, Jul. 2017, pp. 292–296, doi: 10.1109/CITS.2017.8035317.

[7] M. Alshahrani, I. Traore, and I. Woungang, “Anonymous mutual IoT interdevice authentication and key agreement scheme based on the ZigBee technique,” Internet of Things, vol. 7, p. 100061, Sep. 2019, doi: 10.1016/j.iot.2019.100061.
[8] V. L. Shivraj, M. A. Rajan, M. Singh, and P. Balamuralidhar, “One time password authentication scheme based on elliptic curves for Internet of Things (IoT),” in 2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW), Riyadh, Saudi Arabia, Feb. 2015, pp. 1–6, doi: 10.1109/NSITNSW.2015.7176384.
[9] A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in internet of things: Challenges and Solutions,” arXiv:1608.05187 [cs], Aug. 2016, Accessed: Nov. 27, 2020. [Online]. Available: http://arxiv.org/abs/1608.05187.
[10] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, “Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions,” J Ambient Intell Human Comput, May 2017, doi: 10.1007/s12652-017-0494-4.
[11] Q. Chai and G. Gong, “A Cryptanalysis of HummingBird-2: The DifferentialSequence Analysis,” p. IACR Cryptology ePrint Archive 2012, 233, 2012.
[12] D. Lee, D.-C. Kim, D. Kwon, and H. Kim, “Efficient Hardware Implementation of the Lightweight Block Encryption Algorithm LEA,” Sensors, vol. 14, no. 1, pp. 975–994, Jan. 2014, doi: 10.3390/s140100975.
[13] S. Rawal, “Advanced Encryption Standard (AES) and It’s Working,” vol. 03, no. 08, Aug. 2016, [Online]. Available: https://www.irjet.net.
[14] D. Hill, “Advanced Encryption Standard (AES)-128,192, 256,” MATLAB Central File Exchange, Feb. 02, 2021. https://www.mathworks.com/matlabcentral/fileexchange/73412.