ITRC ICT Research Institute (Iran Telecommunication Research Center)

Journal of Information and Communication Technology

Iranian Society of Information and Communication Technology

Volume 16, Issue 61-62, Autumn and Winter 2024, pp. 282-294

Providing A Lightweight Encryption Solution to Secure Data in Internet Of Things

Wahab Aminiazar[1*], Rasoul Farahi[2] and Fatemeh Dashti[3]

[1] Department of Computer Engineering and Information Technology, Faculty of Electrical and Computer Engineering, Islamic Azad University, Mahabad Branch, Mahabad, Iran

[2] Department of Computer Engineering and Information Technology, Faculty of Electrical and Computer Engineering, Islamic Azad University, Mahabad Branch, Mahabad, Iran

[3] PhD Student in Computer Science, Tabriz Electricity Distribution Company, Tabriz, Iran

Received: 04 May 2024, Revised: 16 August 2024, Accepted: 31 August 2024

Paper type: Research

Abstract

In order to use the Internet of Things as a secure infrastructure, there are various challenges and problems, of which security is one of the most important. Establishing security in such networks has many complications due to the limitation of various resources, including processing resources and low energy, and there is a need to establish a kind of compromise between security and available resources. These conditions have caused security to become an important challenge in these networks, and various methods have been presented to improve and optimize this challenge. Accordingly, in this article, a lightweight encryption solution based on symmetric and asymmetric encryption is presented to ensure data security on the Internet of Things. In the proposed method, first, the main data is encrypted by the symmetric Bluefish algorithm, and then its key is secured with the help of the elliptic curve encryption algorithm, so that as a result, data security can be ensured in a short time and with high security in infrastructures based on the Internet of Things provided. In the end, the proposed solution has been evaluated through the Eclipse simulator and by testing on the data volume of 20 to 1000 kilobytes. The simulation results show that the proposed method performs more optimally compared to other encryption algorithms in terms of evaluation criteria such as execution time and encryption and decryption throughput. These results indicate that the proposed solution, while establishing security, has had the least negative impact on the processing resources of IoT nodes.

Keywords: Internet of things, security, Lightweight Encryption Algorithms, Elliptic Curve Encryption Algorithms.

[*] Corresponding Author's email: Aminiazar@iau-mahabad.ac.ir

دوفصلنامه
فناوری اطلاعات و ارتباطات ایران

سال شانزدهم، شماره‌های ۶۱ و ۶۲، پاییز و زمستان ۱۴۰۳، صفحه ۲۸۲ الی ۲۹۴

ارائه یک راهکار رمزنگاری سبک وزن به منظور امنیت داده در اینترنت اشیا

وهاب امینی‌آذر[۱*]، رسول فرحی[۲]، فاطمه دشتی[۳]
[۱] دانشکده مهندسی برق و کامپیوتر، دانشگاه آزاد اسلامی واحد مهاباد، مهاباد، ایران
[۲] دانشکده مهندسی برق و کامپیوتر، دانشگاه آزاد اسلامی واحد مهاباد، مهاباد، ایران
[۳] دانشجوی دکترای کامپیوتر، شرکت توزیع نیروی برق تبریز، تبریز، ایران

تاریخ دریافت: ۱۴۰۳/۰۲/۱۵ تاریخ بازبینی: ۱۴۰۳/۰۵/۲۶ تاریخ پذیرش: ۱۴۰۳/۰۶/۱۰
نوع مقاله: پژوهشی

چکیده

جهت بکارگیری اینترنت اشیا به عنوان یک زیرساخت مطمئن، چالش‌های و مشکلات مختلفی وجود دارد که امنیت یکی از مهم‌ترین آنها می‌باشد. برقراری امنیت در چنین شبکه‌هایی با توجه به محدودیت منابع مختلف از جمله منابع پردازشی و انرژی پایین، دارای پیچیدگی‌های زیادی است و نیاز به برقراری یک نوع مصالحه بین امنیت و منابع در دسترس است. این شرایط موجب شده است تا امنیت به یک چالش مهم در این شبکه‌ها تبدیل شود و روش‌های مختلفی نیز برای بهبود و بهینگی این چالش ارائه شده است. بر همین اساس در این مقاله یک راهکار رمزنگاری سبک‌وزن مبتنی بر رمزنگاری متقارن و نامتقارن جهت تأمین امنیت داده در اینترنت اشیا ارائه شده است. در روش پیشنهادی در ابتدا داده اصلی توسط الگوریتم متقارن بلوفیش رمزنگاری می‌شود و سپس کلید آن به کمک الگوریتم رمزنگاری خم‌های بیضوی ایمن‌سازی می‌شود تا در نتیجه بتوان در زمان کم و با امنیت بالا امنیت داده را در زیرساخت‌های مبتنی بر اینترنت اشیا تأمین کرد. در انتها راهکار پیشنهادی، از طریق شبیه‌ساز Eclipse و با آزمایش بر روی حجم داده ۲۰ تا ۱۰۰۰ کیلوبایت مورد ارزیابی قرار داده شده است. نتایج حاصل از شبیه‌سازی نشان می‌دهد که روش پیشنهادی در مقایسه با سایر الگوریتم‌های رمزنگاری از نظر معیارهای ارزیابی هم چون زمان اجرا و توان عملیاتی رمزنگاری و رمزگشایی بهینه‌تر عمل می‌نماید. این نتایج؛ بیانگر آن است که راهکار پیشنهادی ضمن برقراری امنیت، کمترین تأثیر منفی را بر روی منابع پردازشی گره‌های IoT داشته است.

کلیدواژگان: اینترنت اشیا، امنیت، الگوریتم‌های رمزنگاری سبک وزن، الگوریتم‌های رمزنگاری خم بیضوی.

* رایانامهٔ نویسنده مسؤول: Aminiazar@iau-mahabad.ac.ir

۱- مقدمه

اینترنت اشیا یک ادغام از حسگرها و اشیاء مختلف است که بدون دخالت انسان می‌توانند مستقیماً با یکدیگر ارتباط برقرار کنند. «اشیا» در «اینترنت اشیا» شامل دستگاه‌های فیزیکی مانند حسگرها هستند که انواع داده‌ها را درباره ماشین‌ها و زندگی انسان‌ها جمع‌آوری و نظارت می‌کنند [۱]. ظهور اینترنت اشیا منجر به اتصال همیشگی و جهانی افراد، اشیا، حسگرها و خدمات شده است. هدف اصلی اینترنت اشیا ارائه زیرساخت شبکه‌ای با پروتکل‌ها و نرم‌افزارهای ارتباطی قابل تعامل برای اتصال و یکپارچه‌سازی حسگرهای فیزیکی/مجازی، رایانه‌های شخصی، دستگاه‌های هوشمند، خودروها و اشیاء مانند یخچال، ماشین ظرفشویی، فر و غذا و دارو را در هر زمان و هر شبکه امکان‌پذیر کند [۱] و[۲]. توسعه فناوری تلفن همراه اجازه می‌دهد تا اشیاء بی‌شماری از طریق حسگرهای مختلف تلفن همراه به بخشی از اینترنت اشیا تبدیل شوند. بااین‌حال، نیازهای موردنیاز برای استقرار گسترده اینترنت اشیا به‌سرعت در حال افزایش است که منجر به نگرانی جدی امنیتی می‌شود. مسائل امنیتی مانند حریم خصوصی، اعتبارسنجی، تأیید هویت، کنترل دسترسی، پیکربندی سیستم، ذخیره و مدیریت اطلاعات، چالش‌های اصلی در محیط اینترنت اشیا هستند [۲]. به‌عنوان‌مثال، برنامه‌های اینترنت اشیا مانند تلفن همراه و دستگاه‌های جاسازی‌شده، به فراهم کردن یک محیط دیجیتال برای اتصال جهانی که با حساسیت، سازگاری و واکنش‌گری نسبت به نیازهای انسانی عمل می‌کند، کمک می‌کنند. بااین‌حال، امنیت تضمین نمی‌شود و حریم خصوصی کاربران ممکن است به خطر بیافتد و اطلاعات آنها هنگامی‌که ارتباط کاربر متوقف یا دچار اختلال شود، قابل‌نفوذ گردد. برای بهره‌گیری حداکثری از اینترنت اشیا، این مسئله باید موردتوجه قرار گیرد تا اعتماد کاربران در امر حریم خصوصی و کنترل اطلاعات شخصی فراهم شود [۳]. در واقع توسعه اینترنت اشیا به‌طور قابل توجهی به حل مسائل امنیتی وابسته است. در سال‌های اخیر، بسیاری از تحقیقات به منظور مقابله با چالش‌های امنیتی مرتبط با اینترنت اشیا، مانند مسائل مدیریت کلید [۴]، حریم خصوصی، صحت داده، حفظ محرمانگی و امنیت صورت گرفته است. اکثر پژوهش‌های پیشین تلاش کرده‌اند تا راهکارهای امنیتی ارائه شده برای شبکه‌های بی‌سیم حسگری و اینترنت را در زمینه اینترنت اشیا انطباق دهند. با این حال، باید به این نکته اشاره کرد که چالش‌های اینترنت اشیا ابعاد جدیدی دارند و با استفاده از راهکارهای سنتی به سادگی قابل پیش‌بینی و حل نیستند. علاوه بر این، باید تأکید شود که بیشتر رویکردهای امنیتی بر پایه معماری‌های متمرکز تکیه می‌کنند، که در اینترنت اشیا به دلیل تعداد زیاد اشیا، استفاده از آنها به طرز چشمگیری پیچیده‌تر می‌شود [۵]. بر همین اساس در این مقاله به عنوان نوآوری یک راهکار رمزنگاری ترکیبی و سبک‌وزن، مبتنی بر الگوریتم بلوفیش و خم‌های بیضوی ارائه می‌شود بطوریکه از طریق آن علاوه بر بهبود امنیت در اینترنت اشیا بتوان زمان اجرا و توان عملیاتی را نیز بهینه نمود. بر همین اساس در راهکار پیشنهادی ابتدا داده اصلی توسط الگوریتم رمزنگاری متقارن بلوفیش که زمان اجرای پایینی دارد رمزنگاری می‌شود، سپس به منظور ایمن‌سازی کلید آن در فرایند ارسال و دریافت، از الگوریتم رمزنگاری خم‌های بیضوی استفاده می‌شود. از این طریق می‌توان یک مصالحه بین امنیت و کاهش مصرف منابع در فرایند رمزنگاری بوجود آورد.

این مقاله از پنج بخش تشکیل شده است. در بخش بعدی، خلاصه‌ای از روش‌های قبلی رمزنگاری به منظور تأمین امنیت داده در اینترنت اشیا بررسی می‌شود. بخش سوم، جزئیات الگوریتم پیشنهادی را ارائه می‌کند. نتایج شبیه‌سازی و ارزیابی روش پیشنهادی در بخش چهارم شرح داده می‌شود و در نهایت بخش پنجم به نتیجه‌گیری و کارهای آتی می‌پردازد.

۲- کارهای مرتبط

فراگا و همکاران [۶] یک چارچوب رمزنگاری با در نظر گرفتن پیچیدگی عملیات XOR و چکیده‌ساز برای حفاظت از داده‌ها در فناوری اینترنت اشیا در رایانش مه ارائه داده‌اند. در این پروتکل پیشنهادی، از رمزنگاری‌های پیچیده استفاده نشده است و از فرایند رمزنگاری فقط برای انتقال داده‌های محرمانه یا به منظور اهداف تأیید کاربر و داده‌ها استفاده می‌شود. برای اطمینان از اینکه پروتکل پیشنهادی امن است، توابع چکیده‌ساز استفاده می‌شوند. در نهایت، پس از اعمال معروف‌ترین حملاتی مانند BFU[1] بر روی الگوریتم پیشنهادی، نتایج نشان دادند که عملکرد و امنیت آن بالا است.

موسوی و همکاران [۷] یک رویکرد ترکیبی رمزنگاری مبتنی بر رمزنگاری منحنی بیضوی (ECC) برای سیستم‌های آبیاری هوشمند مبتنی بر اینترنت اشیا را ارائه داده‌اند. نتایج ارزیابی نشان می‌دهد که این رویکرد ترکیبی در مقابل حملات MiM[2] ایمن بوده و عملکرد بهتری نسبت به سایر الگوریتم‌های رمزنگاری دارد.

[1] Brute Force Attack
[2] Man-in-the-Middle Attack

دوی پریا و همکاران [۸] یک طرح احراز هویت چندعاملی مبتنی بر زنجیره هش را برای اینترنت اشیا ارائه کرده‌اند، آنها ثابت کرده‌اند که پروتکل احراز هویت آنها در مقابل حملات مختلف از امنیت کافی برخوردار است، ولی باید به این نکته توجه کرد که طرح آنها به‌تازگی گواهینامه‌ها بستگی دارد و مشکلاتی که طرح‌های مبتنی بر گواهینامه‌ها دارند را طرح آنها نیز داراست.

چن و همکارانش [۹] یک طرح احراز هویت دوعاملی سبک را ارائه کرده‌اند. اما این رویکرد پیشنهادی در برابر حدس زدن رمز عبور آفلاین آسیب پذیر است.

ژیا و همکاران [۱۰] پروتکل احرازهویت گروهی چآین [۹] را مورد بررسی قرار دادند و نشان دادند که مهاجم می‌تواند در یک مدل ارتباطی ناهمزمان، بدون شناسایی شدن، به عنوان یک گره مشروع خود را جا بزند.

معتمد و همکاران [۱۱] یک پروتکل احرازهویت گروهی مقیاس‌پذیر بر مبنای طرح‌های ترکیباتی با قابلیت تحمل‌پذیری خطا برای شبکه‌های IoT ارائه دادند. نظریه طراحی بیضوی، تحمل خطا بر مبنای تعداد اعضای گروه یک آستانه را مشخص می‌کند.

یائو و همکاران [۱۲] یک رویکرد احرازهویت و ایجاد کلید نشست سبک به نام LBAKA برای شبکه‌های UND کاربرمحور ارائه دادند که رویکرد احرازهویت دسته‌ای سبک وزن و توافق کلید یک به یک را با یکدیگر مطابقت می‌دهد. ارتباطات D2D به‌عنوان تکنولوژی ارتباط مستقیم کاربردهای گستردهای دارد و نقش مهمی را در 5G بازی می‌کند.

سان و همکاران [۱۳] یک مکانیزم کشف دستگاه نزدیک با قابلیت گمنامی و مکانیزم احرازهویت دستی برای D2Dهای ناهمگن بر مبنای یک امضای دسته‌ای بدون گواهینامه بی‌نیاز از جفت شدن و کارا ارائه دادند که احرازهویت متقابل و تائید دسته‌ای را بدون نیاز به گواهینامه فراهم می‌آورد.

پارک و همکاران [۱۴] یک پروتکل طرح احراز هویت مبتنی بر زنجیره هش را برای شناسایی حملات در برابر گره‌ها حسگر ارائه نمودند. در این پروتکل پیشنهادی یک نفوذگر ممکن است یک گره حسگر مورد تعرض قرار دهد و به محتویات درون آن دسترسی پیدا نماید. یکی ضعف‌های این پروتکل پیشنهادی در دستیابی به محرمانه بودن مقادیر داخل حسگرها می‌باشد به این دلیل که کلیدهای جلسه Ks را به عنوان یک مقدار هش محاسبه می‌کند و اگر کلید سرور kser شناخته شده باشد، می‌توان همه ورودی‌های تابع هش را به راحتی محاسبه کرد.

زو و همکاران [۱۵] پروتکل احراز هویت سه عاملی سبک و ناشناس مورد بررسی قرار دادند. نتایج آزمایشات نشان‌دهنده این می‌باشد که رویکرد پیشنهادی دارای محرمانگی است اما می‌تواند در برابر حملات آفلاین حدس زدن رمز عبور و همگام سازی آسیب‌پذیر باشد. یک پروتکل ساده احراز هویت متقابل و توافق کلید توسط سونی و سینگ در [۱۶] ارائه شده است. که این پروتکل بین بیماران و سرورهای مراکز درمانی اجرا می‌شود تا داده‌های بیمار به طور امن روی سرور ذخیره نماید. این پروتکل از تابع زنجیره‌ای هش و XOR استفاده می‌کند، اما در برابر حملات آفلاین حدس زدن رمز عبور آسیب‌پذیر است و به احراز هویت پزشکان به سرورها یا نحوه اجرای سیاست‌های کنترل دسترسی اشاره ای نمی‌کند.

اثر شریا و همکاران [۱۷] یک پروتکل احراز هویت متقابل و توافق کلید بین کاربر (پزشک)، سرور ابری پزشکی و دروازه اینترنت اشیا را ارائه می‌دهد. این دروازه داده‌ها را از حسگرهای پزشکی جمع آوری می‌کند تا توسط کادر درمان مورد پردازش قرار گیرد.. این پروتکل از رمزگذاری/رمزگشایی متقارن، هش و عملیات XOR استفاده می‌کند. اما این رویکرد پیشنهادی در برابر حدس زدن رمز عبور آفلاین آسیب پذیر است.

پاتل و همکاران [۱۸] یک رویکرد ترکیبی رمزنگاری مبتنی بر رمزنگاری منحنی بیضوی را به منظور افزایش امنیت داده‌های کاربران در فضای ابری موبایل ارائه کردند. روش پیشنهادی از یک فرایند تصادفی‌سازی برای رمزگذاری و رمزگشایی داده‌ها استفاده می‌کند که این عمل منجر به تولید کلید بهینه می‌شود، در نتیجه با اعمال این فرایند مهاجم قادر نخواهد بود داده‌ها را با موفقیت رمزگشایی کند حتی اگر کلید رمزگذاری را در اختیار داشته باشد. نتایج شبیه‌سازی نشان می‌دهد که روش پیشنهادی زمان فرایندهای رمزنگاری و رمزگشایی را در مقایسه با الگوریتم اصلی بلوفیش کاهش می‌دهد.

گانگیردی و همکاران [۱۹] یک رویکرد جدید را برای افزایش امنیت سایبری در فضای ابری مبتنی بر الگوریتم بلوفیش بهبود یافته به منظور انتخاب کلید بهینه معرفی کرده‌اند. در این رویکرد اطلاعات محرمانه با استفاده از الگوریتم خوشه‌بندی k-medoid خوشه‌بندی می‌شود و سپس داده‌ها با استفاده از رمزگذاری بلوفیش در فضای ابری رمزگذاری و ذخیره می‌شوند. نتایج شبیه‌سازی نشان می‌دهد که روش پیشنهادی دقت امنیت سایبری را برای تمام اطلاعات مخفی بهبود می‌بخشد و در مقایسه با الگوریتم‌های استانداردی هم چون بلوفیش، RSA و AES، زمان اجرای کمتری را در هنگام فرایندهای رمزگذاری و رمزگشایی به دست می‌آورد.

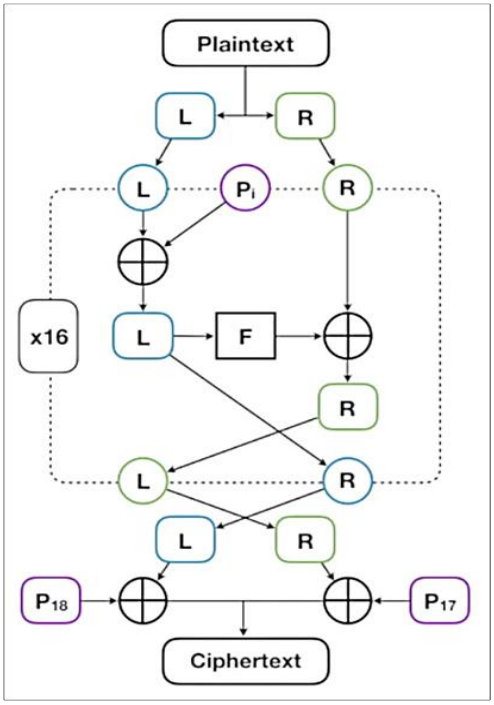
۳- روش پیشنهادی

رشد پیوسته اینترنت اشیا و استفاده گسترده آن در هر مکان، باعث می‌شود که امنیت به یکی از مسائل اساسی در این زیرساخت تبدیل شود. از سوی دیگر، منابع محدود گره‌های اینترنت اشیا باعث می‌شود که استفاده از رمزنگاری‌های مختلف در این بستر به چالشی تبدیل شود. به همین دلیل، تمرکز اصلی بر استفاده از روش‌های رمزنگاری سبک‌وزن به‌منظور ارائه امنیت با حداقل مصرف منابع است. در این پژوهش، قصد داریم از یک راهکار ترکیبی برای تضمین امنیت در اینترنت اشیا استفاده کنیم. در این روش، داده اصلی با استفاده از الگوریتم متقارن بهبودیافته بلوفیش رمزنگاری می‌شود و سپس کلید رمزگذاری با استفاده از خم‌های بیضوی ایمن‌سازی می‌شود. به این ترتیب، با کمترین زمان و با سطح بالای امنیت، فرایند تبادل داده در زیرساخت‌های مبتنی بر اینترنت اشیا انجام می‌شود. این بهبود در رمزنگاری می‌تواند مزایای زیادی در محیط اینترنت اشیا داشته باشد. در ادامه این بخش، الگوریتم بلوفیش موردبررسی قرار می‌گیرد و سپس نحوه استفاده از راهکار ترکیبی شرح داده می‌شود.

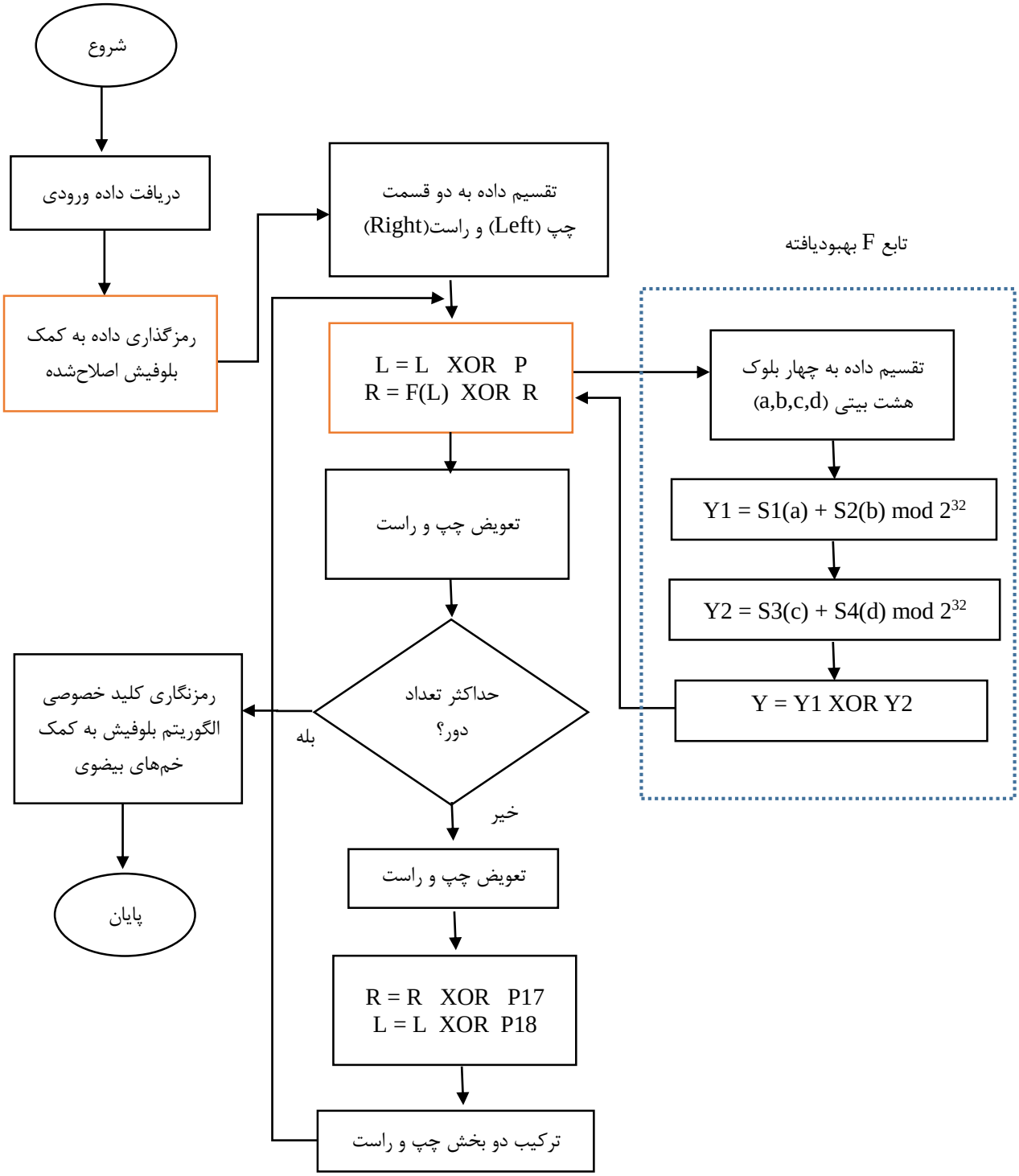
۳-۱- الگوریتم بلوفیش

الگوریتم بلوفیش یک راهکار رمزنگاری متقارن است که از یک کلید برای عملیات رمزنگاری و رمزگشایی داده‌ها بهره می‌برد. این الگوریتم یک رمزگذار بلوکی است که پیام را در طول فرآیند رمزنگاری و رمزگشایی به بلوک‌هایی با طول ثابت تقسیم می‌کند. طول بلوک در بلوفیش ۶۴ بیت است و برای پیام‌هایی که طول‌شان مضربی از هشت بایت نیست، باید با فاصله‌گذاری تصحیح شوند. این الگوریتم شامل عملیات جمع، جستجوی جدول و XOR است. همچنین دارای یک جدول شامل چهار S-box و یک آرایه است. مهم‌ترین نکته این است که بلوفیش یک روش رمزنگاری مبتنی بر فایستل است و از تابع F برای ساده‌سازی اصول استفاده‌شده در DES استفاده می‌کند تا با سرعت و کارایی بالاتری امنیت را فراهم آورد. این الگوریتم بسیار سریع است و می‌تواند با حافظه کمتر از ۵ کیلوبایت اجرا شود. بلوفیش دارای دو بخش است: بسط کلید و رمزنگاری داده‌ها. در مرحله بسط، کلید مربوطه به چندین آرایه از کلید و یک مجموعه ۴۱۶۸ بایتی تبدیل می‌شود. همچنین آرایه P وجود دارد که شامل هجده P-box ۳۲ بیتی است و همچنین چهار آرایه S-box ۳۲ بیتی با ۲۵۶ درایه وجود دارد [۲۰]. در مرحله مقداردهی، ۳۲ بیت اول کلید با استفاده از P1 (اولین بسته ۳۲ بیتی در آرایه p) XOR می‌شوند. سپس ۳۲ بیت دوم کلید با استفاده از P2 دوباره XOR می‌شود و این فرآیند تا زمانی که تمام ۴۴۸ بیت کلید XOR شوند، ادامه می‌یابد. این چرخه روی بیت‌های کلید از طریق بازگشت به ابتدای کلید تکرار می‌شود تا درنتیجه کل آرایه Pبا کلید XOR شود. سپس تمام رشته‌ها با استفاده از الگوریتم و تابع F رمزنگاری می‌شوند تا به یک بلوک ۶۴ بیتی برسیم. سپس P1 با ۳۲ بیت اول خروجی و P2 با ۳۲ بیت دوم خروجی (از بلوک ۶۴ بیتی) جایگزین می‌شوند. خروجی ۶۴ بیتی به‌عنوان ورودی برای بلوفیش استفاده می‌شود تا یک بلوک ۶۴ بیتی جدید تولید شود. این فرآیند برای تمامی مقادیر در آرایه P و تمامیS-box ها تکرار می‌شود. در شکل ۱ نمای کلی رمزنگاری مبتنی بر الگوریتم بلوفیش نشان داده شده است.

با توجه به آنکه تابع فایستل F یکی از عوامل اساسی برای پیچیدگی زمانی الگوریتم است، در این مقاله، هدف اصلی اصلاح تابع F است تا زمان اجرا را کاهش داده و کارایی الگوریتم را افزایش دهیم. سپس با استفاده از الگوریتم بلوفیش، داده اصلی بهینه‌شده و در نهایت با استفاده از الگوریتم خم‌های بیضوی، کلید رمزنگاری می‌شود بر این اساس، در ادامهٔ این بخش، ابتدا نحوه اصلاح تابع F به منظور بهبود کارایی الگوریتم بررسی شده و سپس در قدم بعدی نحوه ایمن‌سازی کلید آن با استفاده از رمزنگاری نامتقارن تشریح می‌شود. در شکل ۲ فلوچارت و راهکار پیشنهادی براساس الگوریتم بلوفیش بهبود یافته پیشنهادی نشان داده شده است.



شکل ۱. فرایند رمزنگاری مبتنی بر الگوریتم بلوفیش [۱۷].



شکل ۲. فلوچارت الگوریتم پیشنهادی

۳-۱-۱- تابع F بهبوده داده شده در روش پیشنهادی

تابع F در الگوریتم رمزنگاری بلوفیش نقش مهمی ایفا می‌کند و بر روی زمان اجرا تأثیر قابل توجهی دارد. در این مقاله، تصمیم به اصلاح این تابع به منظور کاهش زمان اجرا گرفته شده است. در حالت کلی، تابع F به شکلی که در شکل ۳ نمایش داده شده است عمل می‌کند.

$$F\ (DL) = \big((\mathrm{S1, a}\ +\ \mathrm{S2, b}\bmod 232)\mathrm{XOR}\ \mathrm{S3, c}\big) + \mathrm{S4, d}\bmod 232 \quad (۱)$$

براساس این تغییرات، می‌توان تابع F را به منظور موازی‌سازی و اجرای سریع‌تر الگوریتم به شکل رابطه (۲) تغییر داد. تابع F بهبود داده شده به شکلی که در شکل ۴ نمایش داده شده است تغییر پیدا می‌کند.

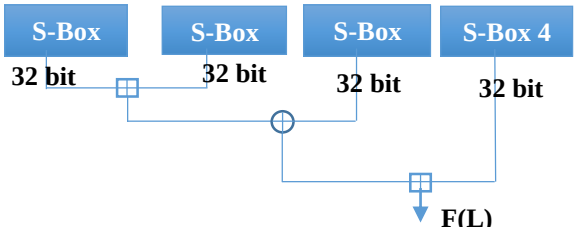
$$F'\ (XL) = (\mathrm{S1, a}\ +\ \mathrm{S2, b}\bmod 2^{32})(\mathrm{S3, c} + \mathrm{S4, d}\bmod 2^{32} \quad (۲)$$

تغییرات اعمال شده در تابع F منجر به اجرای همزمان دو عملیات XOR می‌شود. در تابع F اصلی، این عملیات به صورت سریالی اجرا می‌شود و نیازمند ۳۲ عمل جمع و ۱۶ عمل XOR بود. اما با تغییرات اعمال شده در تابع F اصلاح‌شده، نیاز به انجام ۴۸ عمل منطقی (۳۲ عمل XOR و ۱۶ عمل جمع) است. با این حال، زمان صرف شده برای اجرای این ۴۸ عمل به دلیل مکانیزم چندنخی کاهش می‌یابد. در ادامه شبه کد تابع F بهبوده داده شده روش پیشنهادی در شکل ۵ نشان داده شده است.

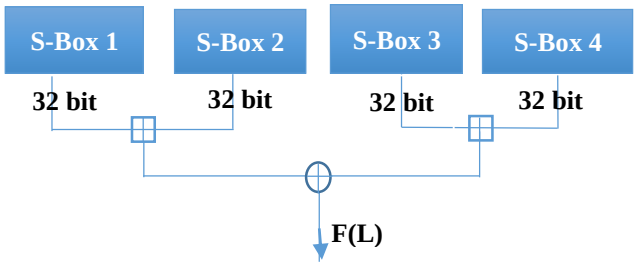
به منظور حل مشکلات مربوط به انتقال کلید خصوصی در الگوریتم بلوفیش، در این تحقیق از رمزنگاری نامتقارن مبتنی بر خم‌های بیضوی (EC) استفاده می‌شود. رمزنگاری خم‌های بیضوی یک روش برای رمزنگاری مبتنی بر کلید عمومی است که بر اساس منحنی‌های بیضوی در میدان‌های متناهی عمل می‌کند [۲۱]. این الگوریتم قابلیت ارائه امنیت با استفاده از کلید ۱۶۴ بیتی را دارا بوده و به دلیل مصرف انرژی کمتر، عملکرد بهتری نسبت به روش‌های قبلی ارائه می‌دهد. در واقع، نسبت به سایر روش‌های رمزنگاری نامتقارن، این روش دارای بالاترین سطح محرمانگی، مصرف کمتر انرژی و نیاز کمتر به حافظه در سیستم است [۲۲]. یکی از ویژگی‌های مهم این رمزنگاری، انجام عملیات بر روی میدان‌های متناهی است. رمزنگاری مبتنی بر خم‌های بیضوی بر اساس مسئله لگاریتم منحنی گسسته بیضوی تعریف می‌شود که یک مسئله NP-Hard است. یک منحنی بیضوی توسط رابطه (۳) تعریف می‌شود:

$$y^2\ +\ xy\ =\ x^3 + ax\ +\ b \quad (۳)$$

یکی از ویژگی‌های اساسی در منحنی بیضوی این است که برای یافتن نقطه سوم روی منحنی، می‌توان یک قانون جهت اضافه کردن دو نقطه به منظور به دست آوردن آن نقطه سومی روی منحنی، مشخص کرد. این نقاط و قانون اضافه کردن، یک دسته آبلی متناهی را شکل می‌دهد. برای تعریف مناسب عمل اضافه کردن دو نقطه، لازم است یک نقطه صفر اضافی را مشخص کنیم که معادلات منحنی بیضوی را برآورده نمی‌کند. این نقطه صفر به عنوان نقطه همانند در منحنی در نظر گرفته می‌شود. ترتیب منحنی برابر با تعداد نقاط مشخص در منحنی است و شامل نقطه صفر نیز می‌شود [۲۱].



شکل ۳. نحوه عملکرد تابع F



شکل ۴. نحوه عملکرد تابع F بهبود یافته

Algorithm 1: The Bluefish algorithm has been improved along with the F function

```
Input: data d
Output: encrypted d
Split d into two 32-bit: dLeft, dRight
For j = 1 to 16:
        dL = dL XOR Pj
        dR = F(xL) XOR dR
        Swap dL & dR
Next j
Swap dL & dR
dR = dR XOR P17
dL = dL XOR P18
Merge xL & xR
Func F
Split dL in four 8-bit: a, b, c, d
F(dL) = (S1,a + S2,b mod 2^32) XOR (S3,c +
S4,d mod 2^32)
```

شکل ۵. شبه کد تابع F بهبوده داده شده روش پیشنهادی

۳-۱-۲- انتخاب منحنی ثابت

برای انتخاب منحنی ثابت، فرض می‌گردد عدد p یک عدد اول بزرگ است و میدان متناهی GF(p) شامل مجموعه‌ای از اعداد کمتر از p می‌باشند. در نتیجه، از طریق حذف عبارت xy از رابطه (۳) و با توجه به رابطهٔ $4a^3 + 27b^2 \neq 0$ می‌توان خم بیضوی را به صورت رابطه (۴) تعریف کرد:

$$y_2 = x_3 + ax^2 + b \qquad (۴)$$

برای رمزنگاری مبتنی بر الگوریتم EC، ابتدا یک عدد تصادفی k از مجموعه محدود [۱, n-1] که در میدان قرار دارد، انتخاب می‌شود.

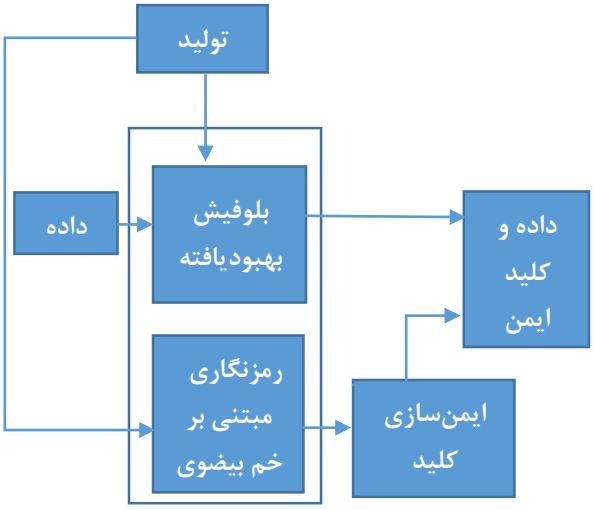
این عدد تصادفی در واقع به عنوان کلید خصوصی در نظر گرفته می‌شود. سپس کلید عمومی R با استفاده از رابطه R = Fk محاسبه می‌شود، که در آن F یک نقطه بر روی خم‌بیضوی می‌باشد. در این صورت، محاسبه k با استفاده از نقاط Q و F دارای پیچیدگی زمانی نمایی است. برای افزایش امنیت، نقطه‌ی ثابت و منحنی به گونه‌ای انتخاب می‌شوند که مرتبه نقطه‌ی F یک عدد اول بسیار بزرگ باشند. مرتبه منحنی به‌وسیله‌ی الگوریتم اسچوف مشخص می‌گردد. اگر مرتبه نقطه‌ی ثابت F یک عدد اول n-بیتی باشد، محاسبه‌ی k با استفاده از kF و F به‌طور تقریبی به $2^{\frac{n}{2}}$ عملیات نیاز دارد. این امر نشان می‌دهد که استفاده از منحنی‌های بیضوی توجیه‌پذیر است، به این معنی که کلیدهای عمومی نسبت به الگوریتم نامتقارن از جمله RSA بسیار کوچکتر خواهد بود، در حالی که همچنان امنیت لازم را فراهم می‌کنند.

۳-۱-۳- نحوه رمزنگاری EC

با توجه به فرضیات مطرح شده، در این سناریو باب، آلیس، دیوید و کتی بر روی یک منحنی بیضوی غیرمحرمانه و یک نقطه منحنی ثابت غیرمحرمانه f توافق کرده‌اند. آلیس عدد صحیح محرمانه مانند Key_kرا تعیین می‌کند که به عنوان کلید رمز او عمل می‌کند و نقطه منحنی $Key_p = Key_{kF}$ را به عنوان کلید عمومی خود منتشر می‌کند. باب، کتی و دیوید همچنین همین عمل را انجام می‌دهند. حال آلیس می‌خواهد پیغامی را به باب ارسال کند. برای این منظور، آلیس ابتدا key_kBp را محاسبه می‌کند و از حاصل آن به عنوان کلید برای رمزنگاری بهره می‌برد. همچنین، باب هم می‌تواند این عدد را از طریق محاسبه $BkKey_p$ تعیین کند. زیرا داریم:

$$B_kA_p = B_k.(A_kF) = A_k.(B_kF) = A_kB_{kp} \qquad (۵)$$

امنیت راهکار ترکیبی برای ایمن‌سازی داده و کلید در شکل ۶ معمولاً بر اساس رمزنگاری مبتنی بر خم‌های بیضوی استوار است.



شکل ۶. روش ترکیبی پیشنهادی بمنظور ایمن‌سازی داده در کنار کلید خصوصی

این روش امنیتی بر پایه محاسبات ریاضی بر روی خم‌های بیضوی در میدان متناهی عمل می‌کند. در این راهکار، ابتدا یک منحنی بیضوی غیرمحرمانه و یک نقطه ثابت نیز غیرمحرمانه تعیین می‌شوند. سپس کاربران (مانند آلیس، باب، کتی و دیوید) اعداد صحیح محرمانه خود را بر روی منحنی بیضوی انتخاب می‌کنند و از نقطه‌ای برروی منحنی به عنوان کلید عمومی خود استفاده می‌کنند. برای ایمن‌سازی داده، کاربران با استفاده از کلیدهای عمومی یکدیگر، ابتدا نقاطی را روی منحنی بیضوی محاسبه می‌کنند و سپس از این نقاط برای رمزنگاری و امضای داده‌ها استفاده می‌کنند. برای محاسبه این نقاط، اعمالی مشخص روی منحنی بیضوی (مانند جمع نقاط) انجام می‌شود.امنیت این روش بر پایه پیچیدگی محاسباتی محاسبه کلیدها و عملیات روی خم‌های بیضوی استوار است. با توجه به خواص ریاضی خم‌های بیضوی، محاسبه کلیدها و عملیات روی آنها با توان مصرفی کمتر و در زمان کمتری نسبت به روش‌های دیگر صورت می‌گیرد. این باعث می‌شود که کلیدهای عمومی و امضاهای مبتنی بر ECC به نسبت الگوریتم‌های نامتقارن دیگر کوچکتر و موثرتر باشند، در حالی که همان سطح امنیت را فراهم می‌کنند. به این ترتیب، راهکار ترکیبی مبتنی بر ECC امنیت بالا و کارایی برتر را با هم ترکیب می‌کند، که آن را به یک گزینه محبوب برای رمزنگاری و امضای داده‌ها در سیستم‌های امنیتی مختلف می‌کند.

۴- شبیه‌سازی روش پیشنهادی

راهکار پیشنهادی و روش‌های مورد مقایسه با استفاده از محیط Eclipse و با استفاده از JDK نسخه ۷ کدنویسی شده‌اند و در سیستم عامل ویندوز ۶۴ بیتی و با حافظه 16G اجرا گردیده است.

در JDK، توابع رمزنگاری با استفاده از دو کتابخانه اصلی JCA و JCE قابل استفاده هستند. کتابخانه JCA به طور کامل با هسته APIهای جاوا ترکیب شده است و قادر است بیشتر قابلیت‌های پایه‌ای رمزنگاری را فراهم کند و همچنین، برای عملیات‌های پیشرفته رمزنگاری از کتابخانه JCE استفاده شده است.

۴-۱- ارزیابی روش پیشنهادی

برای ارزیابی راهکار ارائه شده، از معیارهای مختلفی مانند زمان اجرا، توان عملیاتی و میانگین میزان محرمانگی استفاده شده است. به دلیل تأثیر حجم داده‌ها بر زمان اجرا و توان عملیاتی الگوریتم‌های رمزنگاری، در ادامه ارزیابی‌ها با استفاده از حجم داده‌ها متنی (۲۰ تا ۱۰۰۰ کیلوبایت) اجرا و کارایی آنها بررسی شده است. بر همین اساس در ابتدا، ارزیابی‌ها با حجم کوچک داده‌ها متنی انجام می‌شوند و سپس به حجم داده‌های متنی افزوده می‌شود تا بتوان به میزان کارآیی راهکارها درهر دو حالت پرداخت. در این حالت، تأثیر افزایش حجم داده‌ها بر عملکرد راهکارها سنجیده می‌شود زیرا فرایند رمزنگاری تا حد زیادی تحت تأثیر اندازه داده‌ها قرار می‌گیرد و الگوریتمی که در زمان کمتری عملیات رمزنگاری را انجام دهد، مناسب‌تر است.

۴-۲- معیارهای ارزیابی

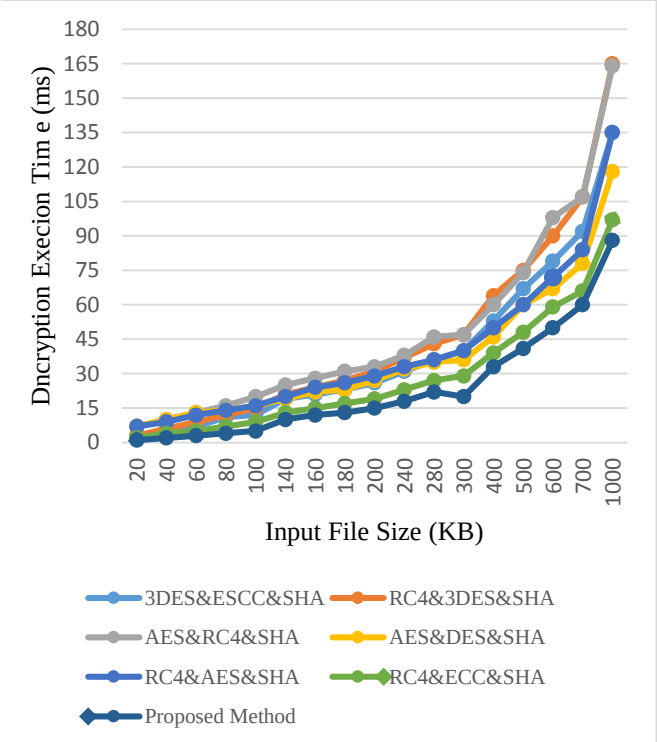
همانطور که گفته شد معیارها و پارامترهای ارزیابی که در روش پیشنهادی در نظر گرفته شده است زمان اجرا، توان عملیاتی و میانگین میزان محرمانگی می‌باشند. کارهایی که جهت مقایسه با روش پیشنهادی در نظر گرفته شده است الگوریتم‌های رمزنگاری در مقاله [۷] می‌باشند. علت انتخاب این روش‌ها سازگاری بیشتر روش‌های مورد مقایسه با محیط شبیه‌سازی و استفاده از الگوریتم‌های رمزنگاری متقارن و غیر متقارن می‌باشد. ایده روش پیشنهاد شده در این مقاله، ارائه یک راهکار رمزنگاری ترکیبی و سبک‌وزن، مبتنی بر الگوریتم بلوفیش و خم‌های بیضوی برای حل مساله بهبود امنیت در اینترنت اشیا می‌باشد که در رویکرد ارائه شده سعی می‌شود براساس راهکار رمزنگاری ترکیبی و سبک‌وزن بتوان در بهینه نمودن زمان اجرا، توان عملیاتی و میانگین میزان محرمانگی تاثیرگذار باشیم، برای بررسی روش پیشنهادی و روش‌های مورد مقایسه از شبیه‌ساز Eclipse استفاده شده است. در ادامه نمودارهای حاصل از شبیه‌سازی بر روی حجم داده‌ها (۲۰ تا ۱۰۰۰ کیلوبایت) در شکل‌های ۷ تا ۱۳ برای معیارهای رویکرد پیشنهادی مورد نظر آورده شده است.

۴-۲-۱- بررسی زمان اجرا

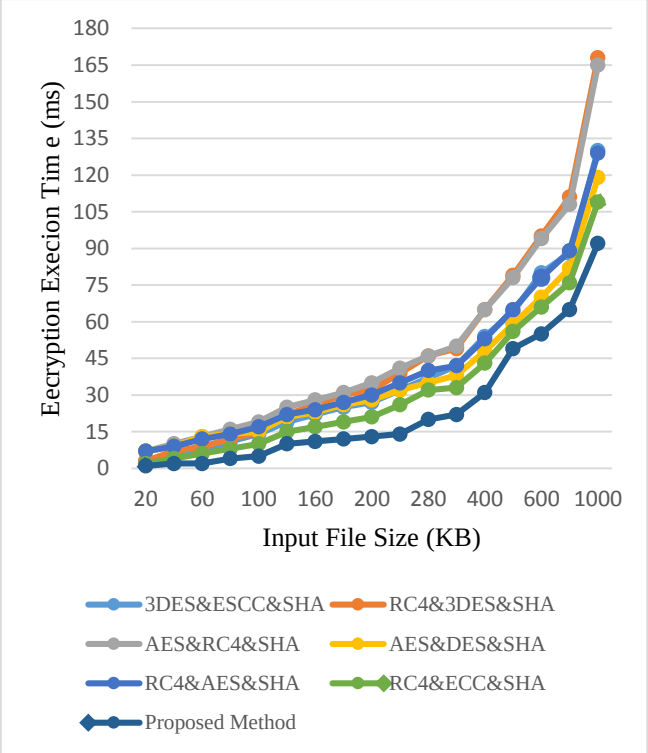
این معیار میزان زمان مورد نیاز برای انجام عملیات رمزنگاری و رمزگشایی را نشان می‌دهد. کاهش زمان اجرا نشانگر کارایی بالاتر راهکار است. زمان اجرا از طریق رابطهٔ (۶) محاسبه می‌شود:

$$\text{Execution Time(ms)} = \text{EncryotStartTime} - \text{End Time} \quad (۶)$$

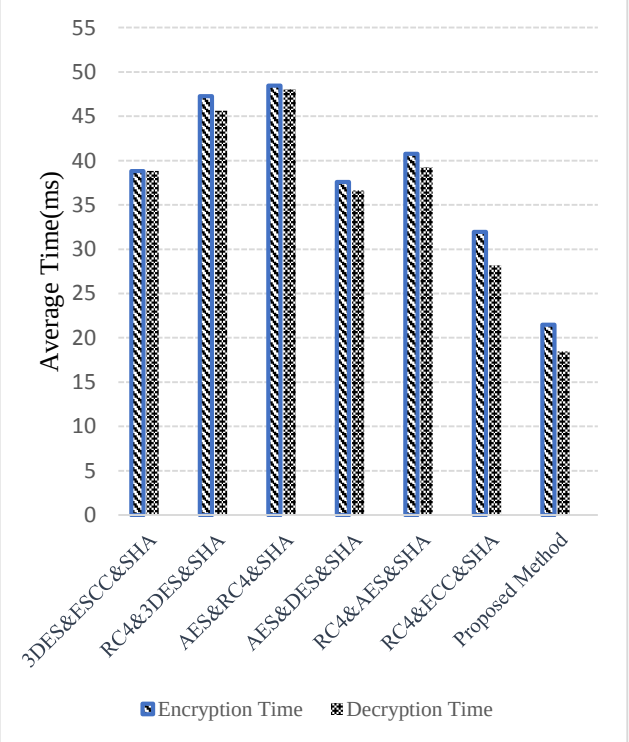
در ادامه این بخش و به ترتیب در شکل‌های ۷ و ۸ مقایسه زمان اجرای علملیات رمزنگاری و رمزگشایی روش پیشنهادی با سایر روش‌های موجود در [۷] آمده است. همان‌طور که در شکل ۹ مشاهده می‌شود، میانگین زمان اجرای رمزنگاری و رمزگشایی روش پیشنهادی به طرز چشمگیری کمتر از سایر روش‌های مورد ارزیابی است. در روش پیشنهادی، به ترتیب زمان اجرای رمزنگاری ۱۸,۴۷میلی‌ثانیه و زمان اجرای رمزگشایی برابر با ۲۱,۴۵ میلی‌ثانیه می‌باشد. دلیل این کارایی بالا روش پیشنهادی در مقایسه با الگوریتم‌های مورد ارزیابی استفاده از رویکرد رمزنگاری پیشنهادی است که در رویکرد پیشنهادی عملیات رمزنگاری داده‌ها با استفاده از الگوریتم متقارن بلوفیش صورت می‌گیرد و همچنین با استفاده از روش رمزنگاری نامتقارن مبتنی بر خم‌های بیضوی ایمن‌سازی کلید انجام می‌شود، بر همین اساس این موضوع باعث کمترین تأثیر روی زمان اجرا می‌شود.



شکل ۷. مقایسه زمان اجرای رمزنگاری روش پیشنهادی با سایر روش‌های پیشین



شکل ۸. مقایسه زمان اجرای رمزگشایی روش پیشنهادی با سایر روش‌های پیشین



شکل ۹. مقایسه میانگین زمان اجرای رمزنگاری و رمزگشایی روش پیشنهادی با سایر روش‌های پیشین

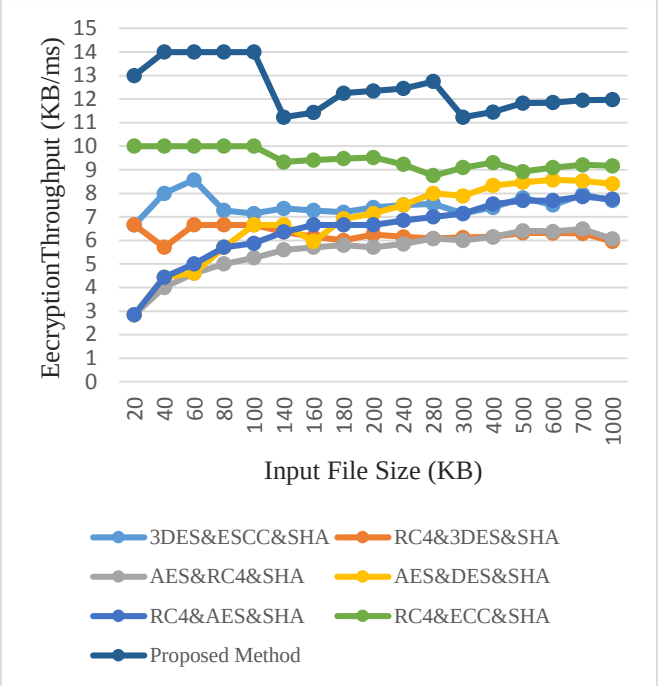
۴-۲-۲- بررسی توان عملیاتی

این معیار میزان تعداد عملیات رمزنگاری و رمزگشایی انجام شده در واحد زمان را نشان می‌دهد. برای ارزیابی کارایی راهکار، باید تعداد عملیات موفقیت‌آمیز واحد زمان محاسبه شود. همچنین به کمک رابطه (۷) زیر می‌توان به ترتیب میزان توان عملیاتی عملیات رمزنگاری و رمزگشایی در طی فرایند ارزیابی را بدست آورد:

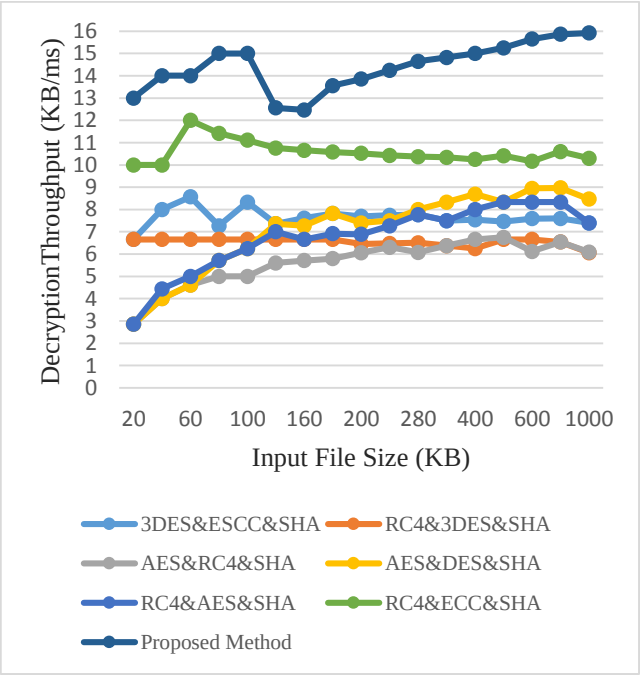
$$\text{Throughput}\left(\frac{\text{KB}}{\text{ms}}\right) = \frac{\text{Data Size}}{\text{Excution Time}} \quad (۷)$$

در رابطه (۷)، توان عملیاتی به وسیله تقسیم سایز داده‌هایی که در ارزیابی استفاده می‌شوند بر زمان اجرای مورد نیاز محاسبه می‌شود. به عبارتی می‌توان گفت که مقدار توان عملیاتی با تقسیم سایز داده‌های مورد ارزیابی بر زمان اجرای لازم به دست می‌آید. در شکل‌های ۱۰ و ۱۱ مقایسه توان عملیاتی علملیات رمزنگاری و رمزگشایی روش پیشنهادی با سایر روش‌های موجود در مقاله [۷] آمده است.

همانطور که در شکل ۱۲ ملاحظه می‌شود، توان عملیاتی راهکار پیشنهادی در حالت رمزنگاری برابر ۱۲,۴۵ کیلوبایت/ ثانیه و در حالت رمزگشایی برابر با ۱۴,۴۰ کیلوبایت/ ثانیه می‌باشد که بر همین اساس توان عملیاتی روش پیشنهادی در مقایسه با سایر راهکارهای مورد ارزیابی بالاتر است. به عبارت دیگر، در راهکار پیشنهادی، با زمان کمتری، حجم بیشتری از داده‌ها رمزنگاری می‌شود که نشان از بهبود عملکرد و کارایی راهکار می‌دهد. این افزایش کارایی به دلیل استفاده از راهکار رمزنگاری ترکیبی و اصلاح هسته رمزنگاری الگوریتم بلوفیش است. در این حالت، تابع F که عامل اصلی پیچیدگی الگوریتم است، تغییر داده شده است و این تغییر باعث اجرای همزمان دو عملیات XOR در فرایند رمزنگاری می‌شود. این موضوع سبب کاهش پیچیدگی و افزایش زمان اجرا و توان عملیاتی الگوریتم می‌شود. در واقع، در این حالت تغییراتی که در تابع F اعمال شده، باعث گردیده که پیچیدگی الگوریتم کاهش پیدا کرده و در نتیجه زمان اجرا و توان عملیاتی بهبود یابد. در کل، راهکار پیشنهادی با ترکیب این دو رویکرد موفق به ارائه راهکاری با کارایی بالا در زمینه رمزنگاری شده است.



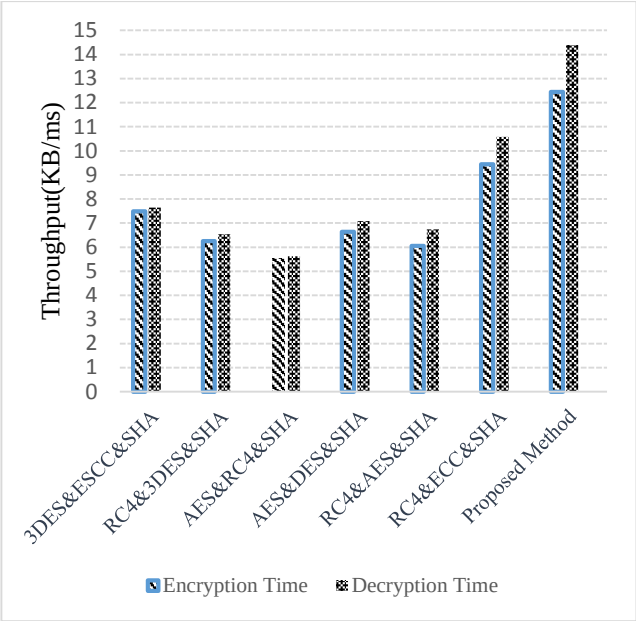
شکل ۱۰. مقایسه توان عملیاتی رمزنگاری روش پیشنهادی با سایر روش‌های پیشین



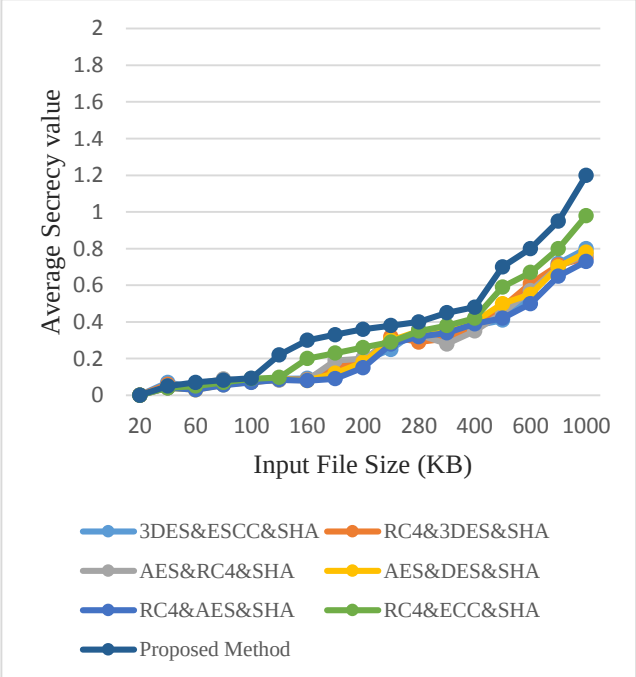
شکل ۱۱. مقایسه توان عملیاتی رمزگشایی روش پیشنهادی با سایر روش‌های پیشین

۴-۲-۳- بررسی میزان محرمانگی

در این بخش به مقایسه تحلیل امنیتی مدل پیشنهادی با سایر مدل‌های مقاله [۷] پرداخته شده است. بر همین اساس اصل حریم خصوصی با استفاده از قانون شانون [۲۳] محاسبه می‌شود که هدف از این معیار بررسی محرمانه بودن داده‌ها است.



شکل ۱۲. مقایسه میانگین توان عملیاتی رمزنگاری و رمزگشایی روش پیشنهادی با سایر روش‌های پیشین



شکل ۱۳. مقایسه میانگین میزان محرمانگی روش پیشنهادی با سایر روش‌های پیشین

در شکل ۱۳ میانگین میزان محرمانگی بدست آمده توسط مدل پیشنهادی، DES&ECC&SHA، RC4&3DES&SHA، ECS&RC4&SHA، AES&DES&SHA، RC4&AES&SHA، DES&ECC&SHA به ترتیب ۱,۳۸۳۰، ۰,۹۸۲۸، ۰,۸۴۴۳، ۱,۰۹۷، ۰,۹۹۸۸، ۰,۸۴۵۵، ۱,۷۱۵ با آزمایش بر روی حجم داده

۲۰ تا ۱۰۰۰ کیلوبایت نشان داده شده است. همانطور که در شکل ۱۳ ملاحظه می‌شود، روش پیشنهادی از نظر میانگین میزان محرمانگی مزایای آشکاری نسبت به سایر الگوریتم‌های مذکور را دارا می‌باشد.

۴-۲-۴- بررسی ویژگی‌های امنیتی

در این بخش، تجزیه و تحلیل امنیتی براساس ۱۰ پارامتر به منظور مقایسه روش پیشنهادی با سایر الگوریتم‌های رمزنگاری مقاله [۷] انجام شده است. بر همین اساس جدول ۱ تجزیه و تحلیل امنیتی مدل پیشنهادی را با مدل‌های دیگر بر اساس چندین ویژگی امنیتی مانند احراز هویت، محرمانگی، یکپارچگی و مقاوم بودن در برابر حملات مختلف نشان می‌دهد [۲۴]. همانطور از مقایسه‌هایی که در جدول ۱ انجام گرفته است، واضح است که مدل پیشنهادی با تمام الزامات امنیتی موافق است و احراز هویتی را ارائه می‌کند که تاکنون اکثر مدل‌ها نتوانستند این الزامات امنیتی را کامل کنند. همچنین، به دلیل اینکه مدل پیشنهادی مبتنی بر ECC است، یکپارچگی و محرمانه بودن اصلی را فراهم می‌کند.

جدول ۱. مقایسه مدل پیشنهادی براساس ویژگی‌های امنیتی با سایر روش‌هاس پیشین

Model	3DES& ECC& SHA	RC4&3DE S&SHA	AES&RC4 &SHA	AES&3DE S&SHA	RC4&AES &SHA	3DES&EC C&SHA	Proposed Method
Authentication key	✓	×	×	×	×	×	✓
Key agreement	✓	×	×	×	×	×	✓
Integrity	✓	✓	✓	✓	×	✓	✓
Confidentiality	✓	×	×	×	×	×	✓
Secrecy	×	×	×	×	×	×	✓
Resistant to man-in-the-middle attack	✓	×	×	×	×	✓	✓
Resistant to malicious user attack	×	×	×	×	×	×	✓
Resistant to insider attack	×	×	×	×	×	✓	✓
Resistant to brute Force	×	×	×	×	×	×	✓
Attack Key exchange	✓	×	×	×	×	✓	✓

۵- نتیجه‌گیری

حفظ امنیت در همه مراحل اینترنت اشیا از اهمیت بالایی برخوردار است و نیازمند رویکردهای جامع و سیستماتیک برای حفاظت از داده‌ها و سیستم‌ها در این زمینه می‌باشد. تلاش‌ها در جهت بهبود استانداردها و فناوری‌های امنیتی در حال ادامه است تا راهکارهایی مؤثر و کارآمد در این زمینه ارائه شوند. راهکار رمزنگاری ترکیبی مبتنی بر الگوریتم بلوفیش و خم‌های بیضوی که در این پژوهش ارائه شده است، بهبودهایی را در کارایی و امنیت فراهم می‌کند. از آنجا که الگوریتم بلوفیش در این روش استفاده می‌شود، تغییراتی در الگوریتم اعمال شده است تا پیچیدگی کلی رمزنگاری کاهش یابد و بلوفیش تغییریافته، تابع F که به طور عادی به صورت سریالی اجرا می‌شود، به صورت همزمان اجرا می‌شود و نیازمند ۴۸ عمل منطقی است که شامل ۳۲ عمل XOR و ۱۶ عمل جمع است. با این وجود، زمان اجرای این ۴۸ عمل به دلیل مکانیزم چندنخی کاهش می‌یابد. بعد از انجام رمزنگاری با الگوریتم بلوفیش تغییریافته، کلید خصوصی ایمن‌سازی می‌شود. این عملیات ایمن‌سازی از طریق رمزنگاری نامتقارن خم‌های بیضوی انجام می‌شود. رمزنگاری خم‌های بیضوی یک روش رمزنگاری مبتنی بر کلید عمومی است که بر پایه منحنی‌های بیضوی در میدان‌های متناهی عمل می‌کند. این الگوریتم از کلید ۱۶۴ بیتی استفاده می‌کند و در مقایسه با روش‌های قبلی، به دلیل مصرف انرژی کمتر، دارای کارایی بالاتری است. همچنین، این روش نیاز به حافظه کمتری دارد و از نظر محرمانگی و امنیت، محدودیت‌های کمتری نسبت به روش‌های دیگر دارد. به طور کلی، استفاده از رمزنگاری ترکیبی مبتنی بر الگوریتم بلوفیش و خم‌های بیضوی می‌تواند امنیت بالا، کارایی مناسب و مصرف انرژی کمتری را در فرایند رمزنگاری و رمزگشایی داده‌ها فراهم کند. در پایان، پیاده‌سازی راهکار پیشنهادی با استفاده از زبان برنامه‌نویسی جاوا و کیت توسعه جاوا ۷ در محیط Eclipse IDE انجام شده است. این راهکار با استفاده از الگوریتم‌های رمزنگاری مجود در مقاله [۷] برای حجم مختلف داده‌ها مقایسه شده است. نتایج ارزیابی نشان می‌دهد که این راهکار، با توجه به معیارهای زمان اجرا و توان عملیاتی بهینه‌تر عمل کرده است. در مقایسه با سایر الگوریتم‌ها، راهکار پیشنهادی در تمامی ارزیابی‌های انجام شده، کمترین زمان اجرا و بیشترین توان عملیاتی را داشته است. این نتایج نشان می‌دهد که عملکرد این راهکار بهبود یافته است و در مقایسه

با روش‌های دیگر، کارایی بالاتری دارد. برای کارهای آتی استفاده از رویکرد پیشنهادی در رایانش لبه می‌تواند به دلیل مصرف پایین حافظه، منجر به بهبود عملکرد و کارایی سامانه‌های موجود در لبه شبکه شود. به عبارتی، با کاهش مصرف حافظه، منابع محدود رایانش لبه بیشتر مورد بهره‌برداری قرار خواهند گرفت و تعداد بیشتری از وظایف رمزنگاری و رمزگشایی قابل انجام خواهند بود. همچنین، با مصرف کمتر حافظه و کاهش زمان اجرا، امکان اجرای همزمان بیشتری از وظایف رمزنگاری و رمزگشایی در دستگاه‌های رایانش لبه وجود دارد که بهبود قابل توجهی در پاسخگویی سیستم به دست می‌اید. بنابراین، از این راهکار پیشنهادی در رایانش لبه می‌توان بهره‌برداری کرده و با بهینه‌سازی مصرف حافظه و افزایش توان عملیاتی، کارایی و کاربردی‌تر شدن سامانه‌های رایانش لبه را تسهیل کرد.

مراجع

[1] Hassija V, Chamola V, Saxena V, Jain D, Goyal P, Sikdar B. A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access. 2019 Jun 20;7:82721-43.

[2] Ammar M, Russello G, Crispo B. Internet of Things: A survey on the security of IoT frameworks. Journal of Information Security and Applications. 2018 Feb 1;38:8-27.

[3] Mrabet H, Belguith S, Alhomoud A, Jemai A. A survey of IoT security based on a layered architecture of sensing and data analysis. Sensors. 2020 Jun 28;20(13):3625.

[4] HaddadPajouh H, Dehghantanha A, Parizi RM, Aledhari M, Karimipour H. A survey on internet of things security: Requirements, challenges, and solutions. Internet of Things. 2021 Jun 1;14:100129.

[5] Mousavi SK, Ghaffari A, Besharat S, Afshari H. Security of internet of things based on cryptographic algorithms: a survey. Wireless Networks. 2021 Feb;27(2):1515-55.

[6] Fraga-Lamas P, Fernández-Caramés TM, Suárez-Albela M, Castedo L, González-López M. A review on internet of things for defense and public safety. Sensors. 2016 Oct 5;16(10):1644.

[7] Mousavi SK, Ghaffari A, Besharat S, Afshari H. Improving the security of internet of things using cryptographic algorithms: a case of smart irrigation systems. Journal of Ambient Intelligence and Humanized Computing. 2021 Feb;12(2):2033-51.

[8] D. Wang, W. Li, and P. Wang, "Measuring TwoFactor Authentication Schemes for Real-Time Data Access in Industrial Wireless Sensor Networks," IEEE Trans. Ind. Informatics, vol. 14, no. 9, pp. 4081–4092, 2018.

[9] C. M. Chen, S. Liu, X. Li, S. Kumari, and L. Li, "Design and Analysis of a Provable Secure TwoFactor Authentication Protocol for Internet of Things," Secur. Commun. Networks, vol. 2022.

[10] Xia Z, Liu Y, Hsu CF, Chang CC. Cryptanalysis and improvement of a group authentication scheme with multiple trials and multiple authentications. Security and Communication Networks. 2020 Jul 13;2020:1-8.

[11] El Mouaatamid O, Lahmer M, Belkasmi M. A scalable group authentication scheme based on combinatorial designs with fault tolerance for the Internet of things. SN Computer Science. 2020 Jul;1:1-3.

[12] Yao Y, Chang X, Mišić J, Mišić VB. Lightweight batch AKA scheme for user-centric ultra-dense networks. IEEE Transactions on Cognitive Communications and Networking. 2020 Mar 20;6(2):597-606.

[13] Sun Y, Cao J, Ma M, Zhang Y, Li H, Niu B. EAP-DDBA: efficient anonymity proximity device discovery and batch authentication mechanism for massive D2D communication devices in 3GPP 5G HetNet. IEEE transactions on dependable and secure computing. 2020 Apr 23;19(1):370-87.

[14] Park K, Noh S, Lee H, Das AK, Kim M, Park Y, Wazid M. LAKS-NVT: Provably secure and lightweight authentication and key agreement scheme without verification table in medical internet of things. IEEE Access. 2020 Jun 29;8:119387-404.

[15] Zhu L, Xiang H, Zhang K. A Light and Anonymous Three-Factor Authentication Protocol for Wireless Sensor Networks. Symmetry 2022, 14, 46. Optimization and Applications of Modern Wireless Networks and Symmetry. 2021:3.

[16] Wu F, Li X, Sangaiah AK, Xu L, Kumari S, Wu L, Shen J. A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks. Future Generation Computer Systems. 2018 May 1;82:727-37.

[17] Shreya S, Chatterjee K, Singh A. A smart secure healthcare monitoring system with Internet of Medical Things. Computers and Electrical Engineering. 2022 Jul 1;101:107969.

[18] Patel P, Patel R, Patel N. Integrated ECC and Blowfish for smartphone security. Procedia Computer Science. 2016 Jan 1;78:210-6.

[19] Gangireddy VK, Kannan S, Subburathinam K. RETRACTED ARTICLE: Implementation of enhanced blowfish algorithm in cloud environment. Journal of Ambient Intelligence and Humanized Computing. 2021 Mar;12(3):3999-4005.

[20] Adhikary T, Jana AD, Chakrabarty A, Jana SK. The internet of things (iot) augmentation in healthcare: An application analytics. ICICCT 2019–System Reliability, Quality Control, Safety, Maintenance and Management: Applications to Electrical, Electronics and Computer Science and Engineering. 2020:576-83.

[21] Dhillon PK, Kalra S. Elliptic curve cryptography for real time embedded systems in IoT networks. In2016 5th international conference on wireless networks and embedded systems (WECON) 2016 Oct 14 (pp. 1-6). IEEE.

[22] Durairaj M, Muthuramalingam K. A new authentication scheme with elliptical curve cryptography for internet of things (IoT) environments. Int. J. Eng. Technol. 2018;7(2.26):119-24.

[23] Weerasinghe TD. An effective RC4 stream cipher. In2013 IEEE 8th international conference on industrial and information systems 2013 Dec 17 (pp. 69-74). IEEE.

[24] Lohachab A, Karambir B. Critical analysis of DDoS—An emerging security threat over IoT networks. Journal of Communications and Information Networks. 2018 Sep;3:57-78.