بهبود امنیت در شبکه‌های کامپیوتری با استفاده از خوشه‌بندی و تکنیک داده‌کاوی مبتنی بر الگوریتم‌های فرا ابتکاری

عباس حسینی*[1]

۱- دانشجوی کارشناسی ارشد مهندسی نرم افزار موسسه آموزش عالی ادیبان گرمسار abbas.hosseini.ir@gmail.com

خلاصه

در این مطالعه، مزایا و چالش‌های بهره‌برداری از اینترنت اشیا در صنایع مختلف و تأثیر آن بر شیوه زندگی و کار انسان‌ها بررسی‌شده است. امنیت و حفظ حریم خصوصی به‌عنوان چالش‌های اصلی در این حوزه موردتوجه قرارگرفته‌اند. مسائلی همچون احراز هویت، کنترل دسترسی، حفاظت از حریم خصوصی و اعتماد ازجمله موارد مهم در اینترنت اشیا به شمار می‌آیند. با در نظر گرفتن محدودیت‌های منابع و پیچیدگی شبکه‌ها، مشکلات امنیتی نظیر حفره‌های امنیتی و حملات مختلف ممکن است رخ دهد. لذا، اهمیت توجه به امنیت، شامل احراز هویت، کنترل دسترسی، حفاظت از حریم خصوصی و اعتماد، بسیار ضروری است. این پژوهش به ارائه راهکارهایی برای تأمین امنیت در اینترنت اشیا پرداخته و استفاده از رمزنگاری به‌عنوان یکی از این راهکارها معرفی‌شده است. به دلیل محدودیت منابع در اینترنت اشیا، الگوریتم‌های رمزنگاری سبک و امن مورداستفاده قرار می‌گیرند. در بخش ارزیابی، راهکار پیشنهادی با بهره‌گیری از الگوریتم‌های رمزنگاری بلوفیش و خم‌های بیضوی همراه با تکنیک ایجاد کد هش MD5 بررسی‌شده است. نتایج حاکی از آن است که راهکار پیشنهادی در مقایسه با الگوریتم‌های رمزنگاری AES، DES و RSA، ازنظر زمان اجرا، گذردهی و مصرف حافظه عملکرد بهتری دارد. به‌طورکلی، این تحقیق نشان می‌دهد که با بهره‌گیری از راهکارهای امنیتی مناسب، می‌توان امنیت اینترنت اشیا را بهبود بخشید و با استفاده از الگوریتم‌های رمزنگاری سبک و امن، کارایی و امنیت در انتقال داده‌ها افزایش می‌یابد. این پژوهش می‌تواند به توسعه و گسترش فناوری اینترنت اشیا کمک شایانی کند..

کلمات کلیدی: امنیت، شبکه‌های کامپیوتری، خوشه‌بندی، داده‌کاوی، فرا ابتکاری، اینترنت اشیاء

۱. مقدمه

با رشد روزافزون استفاده از شبکه‌های کامپیوتری به‌ویژه اینترنت و افزایش مهارت‌های کاربران و مهاجمان، ایمن‌سازی سیستم‌ها و شبکه‌ها نسبت به گذشته اهمیت بیشتری پیدا کرده است. هنگامی‌که یک سیستم کامپیوتری به یک شبکه متصل می‌شود، در معرض خطرات بالایی قرار می‌گیرد. تهدیداتی نظیر ویروس‌ها و نفوذها ازجمله این خطرات هستند. ویروس‌ها به‌طور گسترده با نصب نرم‌افزارهای آنتی‌ویروس و به‌روزرسانی منظم کنترل می‌شوند.هرگونه دسترسی غیرمجاز به منابع یک کامپیوتر، به‌عنوان نفوذ شناخته می‌شود. برای مقابله با این تهدیدها، تکنیک‌های امنیتی متعددی طی دهه‌های گذشته موردمطالعه قرارگرفته‌اند؛ ازجمله رمزنگاری، دیواره‌های آتش، تشخیص نفوذ و ناهنجاری. تشخیص نفوذ در شبکه به‌عنوان یکی از مؤثرترین روش‌ها برای دفاع در برابر رفتارهای دینامیکی و پیچیده تلقی می‌شود. یک سیستم تشخیص نفوذ، فعالیت‌های یک محیط داده‌شده را نظارت می‌کند. و تعیین می‌کند که آیا این فعالیت‌ها مخرب یا طبیعی هستند، بر اساس یکپارچگی، قابلیت اعتماد و دسترسی‌پذیری منابع اطلاعات.سیستم‌های تشخیص نفوذ، اطلاعات مربوط به سیستم مشاهده‌شده را گردآوری می‌کنند. این داده‌های جمع‌آوری‌شده توسط تشخیص‌دهنده پردازش می‌شوند. تشخیص‌دهنده اطلاعات غیرضروری را حذف کرده و سپس تصمیم می‌گیرد که آیا فعالیت مذکور به‌عنوان نشانه‌ای از نفوذ تلقی می‌شود یا خیر.

نفوذ: نفوذ شامل مجموعه‌ای از اقدامات غیرقانونی است که صحت، محرمانگی و یا دسترسی به یک منبع را به خطر می‌اندازد. نفوذها به دسته‌های زیر تقسیم می‌شوند:

ورودی غیرقانونی: هنگامی رخ می‌دهد که یک فرد خارجی به شناسه کاربر و کلمه رمز معتبر دسترسی پیدا کند.

حملات ایفای نقش: زمانی اتفاق می‌افتد که نفوذگر سیستم را متقاعد کند که یک کاربر مجاز با امتیازات بالا است.

زمینه مناسب کنترل امنیت: نفوذگر سعی می‌کند جنبه‌های امنیتی سیستم مانند کلمات رمز را اصلاح کند.

نشت اطلاعات: انتقال اطلاعات به خارج از سیستم.

جلوگیری از سرویس: منابع برای سایر کاربران غیرقابل دسترسی می‌شوند.

استفاده خرابکارانه: شامل حملات مختلفی از قبیل حذف فایل‌ها و سوءاستفاده از منابع.

۲. شبکه حسگر بی‌سیم

شبکه‌های حسگر بی‌سیم (Wireless Sensor Networks - WSNs) انقلابی درزمینه ی جمع‌آوری و پردازش داده‌ها ایجاد کرده‌اند. این شبکه‌ها از تعداد زیادی گره‌های حسگر کوچک و کم‌مصرف تشکیل‌شده‌اند که در یک محیط توزیع شده و به‌صورت بی‌سیم با یکدیگر ارتباط برقرار می‌کنند. هر گره حسگر مجهز به حسگرهایی برای اندازه‌گیری پارامترهای مختلف محیطی مانند دما، رطوبت، فشار، نور، صدا و ... است. داده‌های جمع‌آوری‌شده توسط گره‌ها به یک یا چند گره مرکزی (Sink Node) ارسال می‌شوند که وظیفه پردازش، تحلیل و ذخیره‌سازی داده‌ها را بر عهده‌دارند.

۳. کاربردهای شبکه‌های حسگر بی‌سیم

شبکه‌های حسگر بی‌سیم شامل تعداد و انواع مختلفی از حسگرها مانند لرزه‌نگاری، حرکت، حرارتی، گازی، تغییر شکل، نوری، مادون‌قرمز، فشار، صوتی و غیره می‌باشند که توانایی نظارت بر شرایط طبیعی گسترده رادارند. برخی از کاربردهای این حسگرها عبارت‌اند از:

رطوبت: اندازه‌گیری و نظارت بر میزان رطوبت در محیط‌های مختلف مانند مزارع کشاورزی.

تحرک وسایل نقلیه: ردیابی و نظارت بر حرکت وسایل نقلیه در جاده‌ها و مناطق شهری.

سطح نویز موجود در محیط: اندازه‌گیری سطح نویز برای بررسی آلودگی صوتی در محیط‌های شهری و صنعتی.

وجود یا عدم حضور شیء خاص در محیط: تشخیص حضور یا عدم حضور اشیاء در محیط‌های مختلف.

سطح فشار مکانیکی وارد بر یک شیء: اندازه‌گیری فشار مکانیکی وارد بر اشیاء مختلف.

گره‌های حسگر می‌توانند برای حس کردن پیوسته محیط، آشکارسازی رویداد، حس کردن محلی و کنترل محلی محرک‌ها مورداستفاده قرار گیرند.

۴. انواع شبکه‌های بی‌سیم

شبکه‌های بی‌سیم به دسته‌های مختلفی تقسیم می‌شوند. ارتباط بی‌سیم یا مخابرات بی‌سیم به انتقال اطلاعات بدون استفاده از سیم و به‌وسیله امواج الکترومغناطیسی گفته می‌شود. شبکه‌های بی‌سیم شامل موارد زیر هستند:

- شبکه‌های محلی بی‌سیم (WLAN): ارائه ارتباطات بی‌سیم در یک محدوده محدود مانند یک ساختمان یا سازمان.
- شبکه‌های شخصی بی‌سیم (WPAN): ارتباطات بی‌سیم در محدوده کوتاه مانند بلوتوث و مادون‌قرمز برای کاربردهای خانگی.
- شبکه‌های گسترده بی‌سیم (WWAN): شبکه‌هایی با پوشش بی‌سیم بالا مانند شبکه‌های سلولی مورداستفاده در تلفن‌های همراه.

مزایا و چالش‌های شبکه‌های حسگر بی‌سیم

شبکه‌های حسگر بی‌سیم دارای مزایا و چالش‌هایی هستند که در ادامه به آن‌ها می‌پردازیم:

مزایا:

قابلیت مانیتورینگ گسترده: امکان نظارت بر شرایط محیطی و جمع‌آوری داده‌های مختلف در محیط‌های گسترده.

انعطاف‌پذیری و مقیاس‌پذیری: قابلیت افزودن یا حذف حسگرها بدون نیاز به تغییرات عمده در ساختار شبکه.

کاهش هزینه‌ها: به دلیل استفاده از حسگرهای ارزان و بدون نیاز به سیم‌کشی گسترده.

چالش‌ها:

محدودیت منابع انرژی: نیاز به مدیریت کارآمد انرژی برای افزایش طول عمر حسگرها.

امکان تداخل: مشکلات تداخل امواج رادیویی در محیط‌های شلوغ.

امنیت: نیاز به تأمین امنیت برای جلوگیری از دسترسی غیرمجاز و حفظ حریم خصوصی داده‌ها.

پایداری و تحمل خطا: نیاز به طراحی سیستم‌هایی که بتوانند در برابر خرابی‌ها و اختلالات محیطی مقاومت کنند.

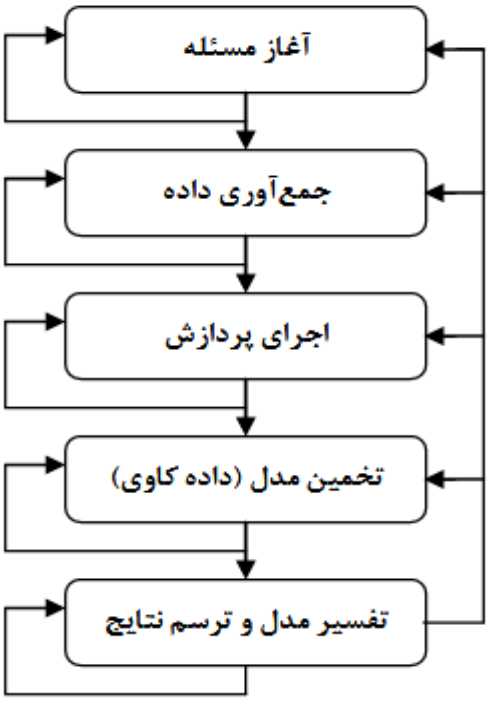
۵. تکنیک‌های داده‌کاوی

تکنیک‌های داده‌کاوی شامل روش‌ها و الگوریتم‌های متعددی هستند که هرکدام برای نوع خاصی از تحلیل داده‌ها استفاده می‌شوند. در ادامه به برخی از مهم‌ترین تکنیک‌های داده‌کاوی اشاره می‌شود:

1. دسته‌بندی (Classification): دسته‌بندی فرایند تخصیص داده‌ها به دسته‌ها یا کلاس‌های از پیش تعریف‌شده است. الگوریتم‌های دسته‌بندی شامل درخت تصمیم(Decision Tree) ، ماشین بردار پشتیبان(SVM) ، شبکه‌های عصبی (Neural Networks)و بیز ساده (Naive Bayes) هستند.
2. خوشه‌بندی (Clustering): خوشه‌بندی فرایند گروه‌بندی داده‌ها به خوشه‌های مشابه است که داده‌های داخل هر خوشه بیشترین شباهت را به هم دارند. الگوریتم‌های خوشه‌بندی شامل k-means ، خوشه‌بندی سلسله‌مراتبی (Hierarchical Clustering)و DBSCAN هستند.
3. کشف قوانین انجمنی (Association Rule Mining): این تکنیک برای کشف روابط و قوانین انجمنی بین اقلام در مجموعه داده‌ها استفاده می‌شود. الگوریتم‌های معروف در این زمینه شامل Apriori و FP-Growth هستند.
4. تحلیل رگرسیون (Regression Analysis): تحلیل رگرسیون برای مدل‌سازی و پیش‌بینی روابط بین متغیرها استفاده می‌شود. این تکنیک شامل رگرسیون خطی (Linear Regression) و رگرسیون لجستیک (Logistic Regression)است.
5. تحلیل توالی (Sequence Analysis): این تکنیک برای کشف الگوهای توالی در داده‌ها استفاده می‌شود و معمولاً در تحلیل رفتار مشتریان و تحلیل سری‌های زمانی کاربرد دارد.
۶. کشف ناهنجاری‌ها (Anomaly Detection): کشف ناهنجاری‌ها به شناسایی داده‌های غیرعادی و ناهنجار که با الگوهای معمول تفاوت دارند، می‌پردازد. این تکنیک در تشخیص تقلب و امنیت اطلاعات کاربرد دارد.

۶. فرآیند داده‌کاوی

در فرآیند داده‌کاوی پس از تعریف مسئله و مطلوبات موردنظر، نیازمند جمع‌آوری داده هستیم، سپس با در اختیار داشتن داده موردنیاز و تعریف الگوریتم مناسب سعی در تولید مدل داده‌کاوی منطبق بر مفاهیم ذکرشده در بالا خواهیم نمود.به‌طورکلی فرآیند داده‌کاوی را می‌توان مشابه شکل ۱ بیان نمود:



۷. خوشه‌بندی

خوشه‌بندی یکی از تکنیک‌های اصلی در داده‌کاوی و یادگیری ماشین است که به فرآیند گروه‌بندی مجموعه‌ای از اشیاء به خوشه‌های مختلف بر اساس شباهت‌های آن‌ها اشاره دارد. هدف اصلی خوشه‌بندی، سازمان‌دهی داده‌ها به‌صورت گروه‌های مشابه است به‌طوری‌که داده‌های داخل هر خوشه بیشترین شباهت را به هم داشته باشند و داده‌های بین خوشه‌ها کمترین شباهت را داشته باشند.

۸. انواع روش‌های خوشه‌بندی

روش‌های خوشه‌بندی به چندین دسته تقسیم می‌شوند که هرکدام رویکردهای متفاوتی برای گروه‌بندی داده‌ها دارند. در ادامه به معرفی برخی از متداول‌ترین روش‌های خوشه‌بندی پرداخته می‌شود:

خوشه‌بندی مبتنی بر پارتیشن(Partition-based Clustering)

این روش‌ها داده‌ها را به k خوشه تقسیم می‌کنند که در آن k تعداد خوشه‌های موردنظر است. هدف این روش‌ها بهینه‌سازی تابعی است که نشان‌دهنده فاصله بین نقاط داده و مراکز خوشه‌ها است.

- k-means: یکی از معروف‌ترین الگوریتم‌های خوشه‌بندی است که داده‌ها را به k خوشه تقسیم می‌کند و مراکز خوشه‌ها را به‌گونه‌ای تنظیم می‌کند که مجموع فاصله‌های اقلیدسی نقاط داده به مراکز خوشه‌ها کمینه شود.
- k-medoids (PAM): مشابه k-means است با این تفاوت که به جای استفاده از میانگین نقاط داده به‌عنوان مرکز خوشه، از نقاط واقعی داده به‌عنوان مرکز خوشه (medoid) استفاده می‌کند.

خوشه‌بندی سلسله‌مراتبی(Hierarchical Clustering)

این روش‌ها خوشه‌بندی داده‌ها را به‌صورت سلسله‌مراتبی انجام می‌دهند و یک درخت سلسله‌مراتبی (دندروگرام) ایجاد می‌کنند که نشان‌دهنده روابط بین خوشه‌ها است.

- خوشه‌بندی تجمیعی :(Agglomerative Clustering) این روش با هر داده به‌عنوان یک خوشه شروع می‌شود و به‌تدریج خوشه‌ها را با هم ترکیب می‌کند تا زمانی که همه داده‌ها در یک خوشه قرار بگیرند. روش‌های مختلفی برای ترکیب خوشه‌ها وجود دارد مانند روش تک‌پیوندی(Single Linkage) ، روش پیوند کامل (Complete Linkage) و روش پیوند میانگین.(Average Linkage)
- خوشه‌بندی تجزیه‌ای :(Divisive Clustering) این روش با تمام داده‌ها به‌عنوان یک خوشه شروع می‌شود و به‌تدریج خوشه‌ها را به خوشه‌های کوچکتر تقسیم می‌کند تا هر داده در یک خوشه جداگانه قرار بگیرد.

خوشه‌بندی مبتنی بر چگالی(Density-based Clustering)

این روش‌ها خوشه‌ها را بر اساس چگالی نقاط داده شناسایی می‌کنند. این روش‌ها معمولاً برای شناسایی خوشه‌های با شکل‌های نامنظم و ناهنجاری‌ها استفاده می‌شوند.

- DBSCAN (Density-Based Spatial Clustering of Applications with Noise):این الگوریتم نقاط داده را به خوشه‌هایی با چگالی بالا تقسیم می‌کند و نقاط داده با چگالی پایین را به‌عنوان ناهنجاری‌ها شناسایی می‌کند.
- OPTICS (Ordering Points To Identify the Clustering Structure):این الگوریتم مشابه DBSCANاست، اما می‌تواند خوشه‌های با چگالی‌های مختلف را شناسایی کند.
- خوشه‌بندی مبتنی بر مدل(Model-based Clustering)

این روش‌ها فرض می‌کنند که داده‌ها از یک مدل خاص پیروی می‌کنند و سعی می‌کنند پارامترهای آن مدل را تخمین بزنند.

- خوشه‌بندی مبتنی بر گوسی (Gaussian Mixture Models, GMM): این روش فرض می‌کند که داده‌ها از ترکیبی از توزیع‌های گوسی پیروی می‌کنند و پارامترهای این توزیع‌ها را تخمین می‌زند.

۹. ارزیابی خوشه‌بندی

ارزیابی کیفیت خوشه‌بندی یکی از مراحل مهم در فرآیند خوشه‌بندی است. معیارهای مختلفی برای ارزیابی خوشه‌بندی وجود دارد که در ادامه به برخی از مهم‌ترین آن‌ها اشاره می‌شود:

- شاخص داویس-بولدین :(Davies-Bouldin Index) این شاخص میانگین نسبت فاصله‌های درون خوشه‌ای به فاصله‌های بین خوشه‌ای را اندازه‌گیری می‌کند. مقدار کمتر این شاخص نشان‌دهنده کیفیت بهتر خوشه‌بندی است.
- شاخص سیلوئت :(Silhouette Index) این شاخص میانگین شباهت هر نقطه به خوشه خودش را در مقایسه با خوشه‌های دیگر اندازه‌گیری می‌کند. مقدار بیشتر این شاخص نشان‌دهنده کیفیت بهتر خوشه‌بندی است.
- شاخص دانی (Dunn Index): این شاخص نسبت کمترین فاصله بین خوشه‌ها به بیشترین قطر درون خوشه‌ای را اندازه‌گیری می‌کند. مقدار بیشتر این شاخص نشان‌دهنده کیفیت بهتر خوشه‌بندی است.

۱۲. الگوریتم کلونی زنبورعسل مصنوعی

الگوریتم کلونی زنبورعسل مصنوعی (Artificial Bee Colony Algorithm - ABC) یک الگوریتم بهینه‌سازی مبتنی بر هوش جمعی است که از رفتار جستجوی غذای زنبورهای عسل الهام گرفته‌شده است. این الگوریتم در سال ۲۰۰۵ توسط Dervis Karaboga معرفی شد و به دلیل سادگی، انعطاف‌پذیری و کارایی بالا در حل مسائل بهینه‌سازی پیچیده، توجه زیادی را به خود جلب کرده است.

۱۱. مفاهیم اصلی الگوریتم ABC:

الگوریتم ABC بر اساس سه نوع زنبورعسل عمل می‌کند:

زنبورهای کارگر (Employed Bees): هر زنبور کارگر با یک منبع غذایی (راه‌حل ممکن برای مسئله) مرتبط است و وظیفه آن بهبود کیفیت منبع غذایی خود است.

زنبورهای ناظر (Onlooker Bees): این زنبورها منتظر اطلاعاتی از زنبورهای کارگر هستند و بر اساس کیفیت منابع غذایی گزارش‌شده، یک منبع غذایی را برای بهره‌برداری انتخاب می‌کنند.

زنبورهای پیشاهنگ (Scout Bees): این زنبورها به‌صورت تصادفی در فضای جستجو به دنبال منابع غذایی جدید می‌گردند.

مراحل الگوریتم ABC:

مقداردهی اولیه: جمعیت اولیه‌ای از راه‌حل‌های ممکن (منابع غذایی) به‌صورت تصادفی ایجاد می‌شود.

فاز زنبورهای کارگر: هر زنبور کارگر یک راه‌حل جدید در همسایگی راه‌حل فعلی خود تولید می‌کند و اگر راه‌حل جدید بهتر باشد، آن را جایگزین راه‌حل فعلی می‌کند.

فاز زنبورهای ناظر: زنبورهای ناظر بر اساس کیفیت منابع غذایی گزارش‌شده توسط زنبورهای کارگر، یک منبع غذایی را برای بهره‌برداری انتخاب می‌کنند. احتمال انتخاب یک منبع غذایی باکیفیت بالاتر، بیشتر است.

فاز زنبورهای پیشاهنگ: اگر یک منبع غذایی برای مدت مشخصی بهبود نیابد، زنبور کارگر مرتبط با آن به یک زنبور پیشاهنگ تبدیل می‌شود و به‌صورت تصادفی به دنبال یک منبع غذایی جدید می‌گردد.

بررسی شرط خاتمه: الگوریتم تا زمانی که شرط خاتمه (مانند تعداد تکرارها یا رسیدن به یک مقدار بهینگی مشخص) برقرار شود، ادامه می‌یابد.

مزایای الگوریتم ABC:

سادگی: الگوریتم ABC دارای ساختار ساده و قابل‌فهم است.

انعطاف‌پذیری: این الگوریتم می‌تواند به‌راحتی برای حل انواع مسائل بهینه‌سازی پیوسته و گسسته تطبیق داده شود.

کارایی: الگوریتم ABC در مقایسه با بسیاری از الگوریتم‌های بهینه‌سازی دیگر، کارایی بالایی در یافتن راه‌حل‌های بهینه دارد.

قابلیت موازی‌سازی: این الگوریتم به‌راحتی قابل موازی‌سازی است و می‌تواند از مزایای پردازش موازی بهره‌مند شود.

کاربردهای الگوریتم ABC:

الگوریتم ABC در طیف وسیعی از مسائل بهینه‌سازی ازجمله موارد زیر استفاده‌شده است:

بهینه‌سازی توابع ریاضی: یافتن مقادیر کمینه یا بیشینه توابع ریاضی پیچیده.

مسائل زمان‌بندی: زمان‌بندی کارها در سیستم‌های تولیدی یا کامپیوتری.

مسائل مسیریابی: یافتن کوتاه‌ترین یا کم‌هزینه‌ترین مسیر در شبکه‌ها.

طراحی مهندسی: بهینه‌سازی طراحی سازه‌ها، سیستم‌های کنترل و ...

۱۲. گام‌های کلی راهکار

در ابتدا باید اشاره شود که گام‌های زیر بر اساس مدل ارائه‌شده در فصل قبل، جهت تأمین امنیت اطلاعات و همچنین ایجاد حداقل سربار انجام می‌گیرد:
قبل از عملیات رمزنگاری، با استفاده از تابع درهم‌ساز MD-5 کد هش مربوط به داده اصلی ایجاد می‌شود.
.2کد درهم‌ساز تولیدشده به همراه کلید رمزنگاری خصوصی جهت رمزنگاری و همچنین ایجاد امضای دیجیتال به کار می‌رود.
ایجاد امضای دیجیتال با استفاده از کلید عمومی خم‌های بیضوی انجام می‌شود.
سپس، قبل از ارسال داده، داده موردنظر با استفاده از الگوریتم رمزنگاری متقارن بلوفیش (Blowfish) رمزنگاری می‌شود تا متن رمزی تولید شود. در این مرحله، از کلید متقارن برای عملیات رمزنگاری و تولید رشته داده رمزنگاری شده از داده اصلی استفاده می‌شود. سپس داده رمزنگاری شده به همراه رشته الحاقی رمزنگاری شده در مرحله قبل ارسال می‌شود.
رمزنگاری امضای دیجیتال، تابع درهم‌ساز و کلید خصوصی با کمک خم‌های بیضوی انجام می‌شود.
در سمت گیرنده، فرآیند معکوس به کار گرفته می‌شود؛ اطلاعات دریافتی با استفاده از کلید خصوصی رمزگشایی می‌شود .داده اصلی نیز با استفاده از کلید الگوریتم متقارن بلوفیش (Blowfish) رمزگشایی می‌شود، سپس فرآیند بازبینی و اعتبارسنجی به کمک تابع درهم‌ساز (امضای دیجیتال) انجام می‌گیرد.

۱۳. محیط شبیه‌سازی

پیاده‌سازی راهکار پیشنهادی در محیط نرم‌افزار اکلیپس و با استفاده از کیت توسعه جاوا نسخه ۷ انجام‌شده است.در کیت توسعه جاوا، توابع رمزنگاری با کمک دو کتابخانه اصلی زیر امکان‌پذیر است:
کتابخانه معماری رمزنگاری جاوا(JCA)
کتابخانه افزودنی رمزنگاری جاوا(JCE)
همچنین سخت‌افزار مورداستفاده دارای پردازنده Intel Core2 Duo با فرکانس ۲.۵ گیگاهرتز می‌باشد. کلیه ارزیابی‌ها در محیط ویندوز ۷ اجرا شده است. در شکل ۴-۳، نمونه‌ای از اجرای راهکار در محیط کنسول اکلیپس نشان داده‌شده است.

۱۴. نحوه ارزیابی راهکار

برای ارزیابی راهکار پیشنهادی، این روش با الگوریتم‌های رمزنگاری زیر مقایسه و بررسی‌شده است:
الگوریتم استاندارد رمزنگاریAES
استاندارد رمزنگاری پیشرفته (AES) به هر دو صورت سخت‌افزاری و نرم‌افزاری سریع است و برخلاف DES از رمزنگاری فیستل استفاده نمی‌کند AES .دارای اندازه بلوک ثابت ۱۲۸ بیتی و اندازه کلید ۱۲۸، ۱۹۲ و ۲۵۶ بیتی است و روی ماتریسی ۴×۴ از بایت‌ها با ترتیب ستونی عمل می‌کند. تعداد چرخه‌های تکرار به‌صورت زیر است:
10چرخه تکرار برای کلیدهای ۱۲۸ بیتی
12چرخه تکرار برای کلیدهای ۱۹۲ بیتی

14چرخه تکرار برای کلیدهای ۲۵۶ بیتی

الگوریتم رمزنگاریDES

این الگوریتم در کلاس روش‌های رمزنگاری متقارن مبتنی بر بلوک است که بر اساس جعبه‌های جایگشت با تعداد بیت‌های ورودی کمتر از بیت‌های خروجی می‌باشد DES .دارای ساختار ۱۲ دوری فیستل، با اندازه بلوک ۶۴ بیتی و اندازه کلید بین ۴۰ تا ۱۲۸ بیتی (اما تنها با افزایش ۸ بیت) است. قطعات شامل جعبه بزرگ ۸×۳۲ جایگزینی، کلید وابسته به چرخش‌ها، جمع و تفریق مدوله شده و عمل XOR می‌باشد.

الگوریتم رمزنگاریRSA

الگوریتم RSA از دو کلید برای رمزنگاری استفاده می‌کند: کلید خصوصی و کلید عمومی. این کلیدها با استفاده از روش‌های ریاضی و ترکیب اعداد اول تولید می‌شوند. اصل اساسی که باید در رمزنگاری RSA رعایت شود آن است که کدهای Pi که به هر بلوک نسبت داده می‌شود باید در شرط $Pi < n \geq ۰$ صدق کند. بنابراین اگر بلوک‌ها به‌صورت رشته k بیتی مدل شوند، باید شرط $k < n^{۲}$ برقرار باشد.

۱۵. معیارهای ارزیابی

معیارهای مختلفی جهت ارزیابی راهکارهای تأمین امنیت وجود دارد که هر یک با توجه به شرایط مختلف ارزیابی و همچنین نحوه بررسی الگوریتم‌ها متفاوت هستند. با توجه به اینکه در این پژوهش قصد داریم راهکار پیشنهادی را برای محیط‌های مبتنی بر اینترنت اشیا بکار ببریم، درنتیجه با بررسی مقالات مختلف، معیارهای زیر جهت ارزیابی و بررسی راهکار با سایر روش‌ها در نظر گرفته‌شده است:

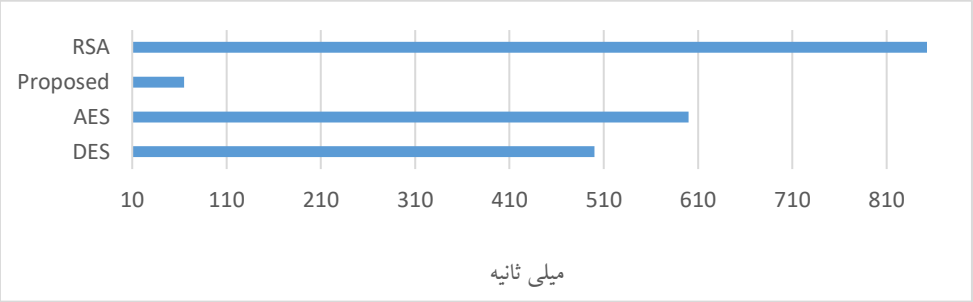
- **زمان اجرا** :برابر با مدت‌زمانی است که طول می‌کشد تا عملیات رمزنگاری انجام گیرد.
- **گذردهی** :به تعداد پردازش‌هایی که در واحد زمان تکمیل می‌شوند، اطلاق می‌گردد.
- **میزان حافظه مصرفی**

۱۶. نتایج ارزیابی

نتایج حاصل از این بررسی در شکل‌های ۴-۳ تا ۴-۱۰ نشان داده‌شده است. ابتدا راهکارها با سایز داده‌ای کم مورد ارزیابی قرارگرفته‌اند تا بتوان نحوه عملکرد آن‌ها را در حالت کوچک بودن سایز داده‌ها مشاهده و بررسی کرد. در ادامه به خوبی می‌توان افزایش سرعت و گذردهی عملیات رمزنگاری را بر پایه راهکار پیشنهادی مشاهده نمود که این امر به شکل قابل‌توجهی در افزایش کارایی و همچنین امنیت در اینترنت اشیا مؤثر خواهد بود.

مقایسه زمان اجرا در این الگوریتم‌ها به روشنی بهینگی اجرا و افزایش کارایی را در روش ارائه‌شده نشان می‌دهد. به‌طوری‌که در ارزیابی اول که بر پایه داده‌های با اندازه ۵۰ کیلوبایت انجام‌گرفته است، زمان اجرا نسبت به الگوریتم‌هایRSA ، AES و DES به ترتیب به میزان ۶۹۰، ۳۹۰ و ۲۹۰ میلی‌ثانیه کاهش‌یافته است، که نشان‌دهنده انجام عملیات رمزنگاری در زمان کمتری است. این کاهش در زمان اجرا از طریق بهبود و بکارگیری الگوریتم بلوفیش در هسته راهکار به‌دست‌آمده است، زیرا بلوفیش با توجه به اینکه جزء رمزهای قطعه‌ای است، یکی از سریع‌ترین روش‌های رمزنگاری می‌باشد. از طرفی دیگر بکارگیری

خم‌های بیضوی فقط در بخش رمزنگاری کلید و افزودن امضای دیجیتال صورت گرفته که درنتیجه زمان اجرای کمی نیاز دارد. ولی همان‌طور که در شکل ۴-۳ مشاهده می‌شود، بکارگیری الگوریتم‌های رمزنگاری جهت ایمن‌سازی داده اصلی می‌تواند زمان اجرا را به دلیل نامتقارن بودن آن به شدت بالا ببرد که در شکل ۴-۳ الگوریتم RSA این مورد را نشان می‌دهد.



شکل ۴- ۱ زمان اجرا – میلی‌ثانیه (اندازه داده: ۵۰ کیلوبایت)

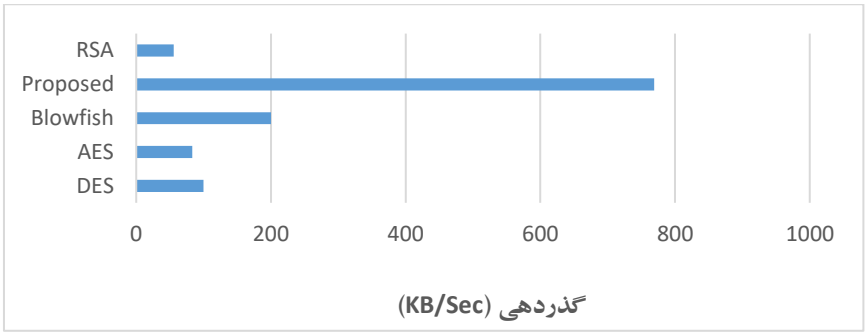
از طرف دیگر، گذردهی نیز نسبت به سایر راهکارها بهبودیافته است. به‌این‌ترتیب، در مقایسه با الگوریتم‌هایRSA ، AES و DES میزان بهینگی بسیار بالاتری دارد. البته با توجه به اینکه الگوریتم RSA جزء الگوریتم‌های نامتقارن است، زمان اجرای آن همواره نسبت به سایر راهکارها بالاتر خواهد بود. اما در راهکار پیشنهادی از الگوریتم نامتقارن خم‌های بیضوی تنها برای رمزنگاری کلید و خلاصه کد هش استفاده‌شده است که اندازه آن بسیار محدود است و درنتیجه تأثیر چندانی بر زمان اجرا نخواهد داشت. نتایج ارزیابی نیز این امر را تأیید می‌کند.

درواقع، با توجه به اینکه زمان اجرا رابطه مستقیمی با گذردهی دارد، نتیجه می‌شود که هرچه زمان اجرای یک الگوریتم رمزنگاری کمتر باشد، گذردهی آن نیز بالاتر خواهد رفت. به‌عبارتی‌دیگر، بهبود زمان اجرا به‌طور مستقیم منجر به افزایش گذردهی می‌شود.

نتایج ارزیابی نشان می‌دهند که در راهکار پیشنهادی، به دلیل استفاده از الگوریتم بلوفیش به‌عنوان الگوریتم اصلی رمزنگاری داده، زمان اجرا به‌طور قابل‌ملاحظه‌ای کاهش‌یافته است. بلوفیش با ساختار ساده و کارآمد خود یکی از سریع‌ترین الگوریتم‌های رمزنگاری محسوب می‌شود. استفاده از الگوریتم خم‌های بیضوی تنها در بخش‌های حساس مانند رمزنگاری کلید و امضای دیجیتال باعث شده تا سربار اضافی زیادی ایجاد نشود و زمان اجرا کاهش یابد.

نتایج نشان می‌دهد که راهکار پیشنهادی نه‌تنها درزمینه ی زمان اجرا بهینه است، بلکه گذردهی بسیار بالاتری نسبت به سایر الگوریتم‌های رمزنگاری مانندRSA ، AESو DES دارد. استفاده از الگوریتم‌های سبک‌وزن مانند بلوفیش در کنار الگوریتم نامتقارن خم‌های بیضوی، امنیت و کارایی را به‌طور همزمان تأمین می‌کند. این امر در محیط‌های با محدودیت منابع

مانند اینترنت اشیا بسیار حیاتی است و می‌تواند به بهبود امنیت و عملکرد سیستم‌های مبتنی بر این فناوری کمک شایانی نماید.



شکل ۴- ۲ میزان گذردهی – کیلوبایت بر ثانیه (اندازه داده: ۵۰ کیلوبایت)

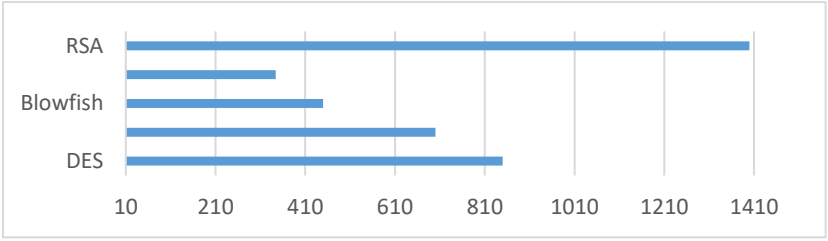
با توجه به اینکه اندازه داده‌های قابل رمزنگاری می‌تواند در زمان اجرای عملیات تأثیرگذار باشد، در آزمایش دوم، اندازه داده‌ها به ۱ مگابایت (۱۰۲۴ کیلوبایت) افزایش‌یافته تا کارایی الگوریتم‌ها در این حجم داده مقایسه شود. همان‌طور که در شکل ۴-۴ قابل‌مشاهده است، راهکار پیشنهادی نسبت به سایر راهکارها دوباره بسیار بهتر عمل کرده و علاوه برافزایش گذردهی، زمان اجرا نیز به شکل قابل‌توجهی کاهش‌یافته است. به‌طوری‌که زمان اجرا در مقایسه با الگوریتم‌های متقارن DES و AES به ترتیب به میزان ۳۵۶ و ۵۰۶ میلی‌ثانیه کاهش‌یافته که این خود بیانگر سریع‌تر عمل کردن راهکار پیشنهادی نسبت به دو راهکار قبلی می‌باشد. همچنین در مقایسه با الگوریتم RSA نیز بیش از ۱۰۰۰ میلی‌ثانیه کاهش زمان اجرا به وجود آمده است که این نشان‌دهنده سریع‌تر اجراشدن راهکار است.

نتایج آزمایش دوم نشان می‌دهند که راهکار پیشنهادی در مقایسه با سایر الگوریتم‌ها حتی با افزایش حجم داده‌ها نیز عملکرد بهتری دارد. کاهش زمان اجرا و افزایش گذردهی در حجم داده‌های ۱ مگابایتی بیانگر این است که استفاده از ترکیب الگوریتم بلوفیش و خم‌های بیضوی نه‌تنها امنیت لازم را فراهم می‌کند بلکه کارایی سیستم را نیز بهبود می‌بخشد.

این بهبود قابل‌توجه در زمان اجرا و گذردهی می‌تواند به‌طور مستقیم به کاهش مصرف انرژی و افزایش طول عمر دستگاه‌های اینترنت اشیا منجر شود. استفاده از الگوریتم‌های سبک‌وزن و بهینه‌سازی شده در محیط‌هایی با محدودیت منابع از اهمیت

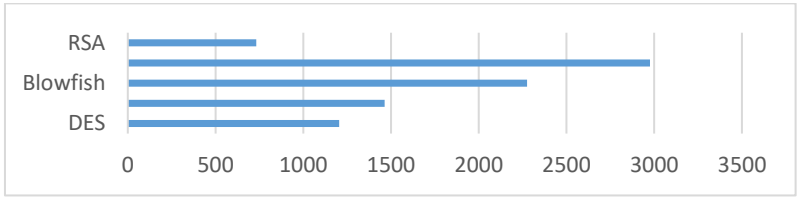
بالایی برخوردار است و نتایج این تحقیق نشان می‌دهد که راهکار پیشنهادی می‌تواند یک گزینه مناسب برای تأمین امنیت در این محیط‌ها باشد.

به‌طورکلی، نتایج این ارزیابی‌ها نشان می‌دهد که راهکار پیشنهادی درزمینه ی رمزنگاری داده‌ها برای اینترنت اشیا، علاوه بر تأمین امنیت بالا، ازنظر زمان اجرا و گذردهی نیز عملکرد بسیار بهینه‌تری نسبت به سایر الگوریتم‌های مورد بررسی دارد.



شکل ۴- ۳ زمان اجرا – میلی‌ثانیه (اندازه داده: ۱۰۲۴ کیلوبایت)

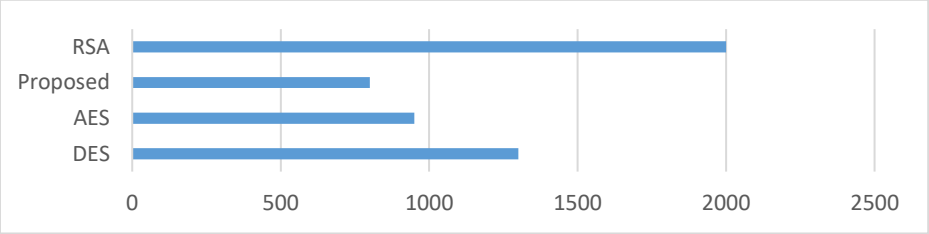
در ادامه و در شکل ۴-۵ نیز میزان گذردهی راهکارها نشان داده‌شده است که با توجه به کمتر بودن زمان اجرا، افزایش میزان گذردهی نیز قابل پیش‌بینی بود. همان‌طور که ملاحظه می‌شود در این آزمایش میزان گذردهی داده‌ها در راهکار پیشنهادی بسیار بالاتر می‌باشد. بطوریکه میزان گذردهی به نسبت AES و DES به‌طور میانگین بیش از ۴۰ درصد می‌باشد. درواقع با توجه به آن‌که در راهکار ارائه‌شده بیشترین زمان اجرا مربوط به رمزنگاری داده اصلی می‌باشد که توسط الگوریتم بلوفیش است، درنتیجه این بخش از راهکار توانسته کمک شایانی به کاهش زمان اجرا و درنتیجه افزایش گذردهی نماید. در مقایسه با الگوریتم نامتقارن RSA نیز این میزان بهینگی بسیار چشم‌گیرتر است.



شکل ۴- ۴ میزان گذردهی – کیلوبایت/ثانیه (اندازه داده: ۱۰۲۴ کیلوبایت)

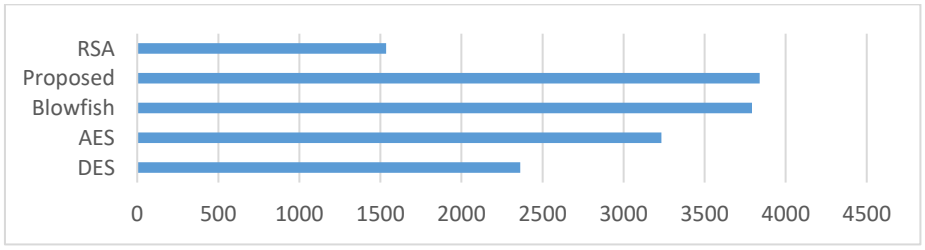
نهایتاً در آزمایش آخر الگوریتم‌های موردنظر با حجم داده ۳۰۷۲ کیلوبایت (۳ مگابایت) مورد ارزیابی قرارگرفته‌اند که نمودارهای ۴-۶ و ۴-۷ به روشنی بهینه‌تر بودن راهکار پیشنهادی را نشان می‌دهد. همان‌طور که قابل‌مشاهده است، هرچه حجم داده‌ها افزایش می‌یابد، میزان گذردهی نیز بیشتر می‌شود ولی مدت‌زمان رمزنگاری را تحت تأثیر قرار می‌دهد و باعث می‌شود زمان بیشتری موردنیاز باشد، هرچند که راهکار ارائه‌شده توانسته در زمان کمتری نسبت به سایر الگوریتم‌ها عملیات را به اتمام رساند. بر همین اساس زمان اجرای نسبت به دو الگوریتم‌های متقارن DES و AES به ترتیب بین ۵۰۰ و ۱۵۰

میلی‌ثانیه کاهش‌یافته و از طرف دیگر گذردهی نیز بسیار بهینه‌تر شده که در شکل ۴-۶ قابل‌مشاهده است. در مورد الگوریتم نامتقارن RSA نیز زمان اجرا بیش از ۱۲۰۰ میلی‌ثانیه کاهش‌یافته است.



شکل ۴- ۵ زمان اجرا – میلی‌ثانیه (اندازه داده: ۳۰۷۲ کیلوبایت)

همانطورکه در شکل ۴-۷ ملاحظه می‌شود با افزایش سایز داده‌ها میزان گذردهی راهکار نیز بالاتر رفته است درواقع خصوصیات قابل‌توجه این الگوریتم که طراحی آن شامل کلید- وابسته به s-box بسیار پیچیده است، علاوه بر اینکه باعث شده است، امنیت آن بالا باشد، قابلیت بکارگیری و اجرا در سیستم‌های با توان پردازشی محدود ازجمله دستگاه‌های شبکه‌های کامپیوتری را نیز میسر کرده است. بر همین اساس در نمودارهای ۴-۷ و ۴-۷ نیز ملاحظه می‌شود که زمان اجرا و گذردهی آن به نسبت سایر الگوریتم‌ها بسیار بالاتر است. در کنار آن با توجه به اینکه در روش پیشنهادی قسمت رمزنگاری داده از رمزنگاری کلیدها جدا شده است درنتیجه بکارگیری همزمان بلوفیش و الگوریتم خم‌های بیضوی تأثیر چندانی در افت کارایی و زمان اجرا نداشته است. زیرا در این حالت فقط کلید خصوصی و کد هش توسط خم‌های بیضوی رمزنگاری شده است و با توجه به حجم بسیار پایین آن‌ها، کمترین تأثیر را در زمان اجرا داشته است. از طرف دیگر داده اصلی که حجم آن به نسبت بالا می‌باشد، توسط الگوریتم بلوفیش، رمزنگاری شده است که با توجه به کارایی بالای آن، زمان اجرا و میزان گذردهی به نسبت سایر راهکارها بسیار بالاتر می‌باشد.

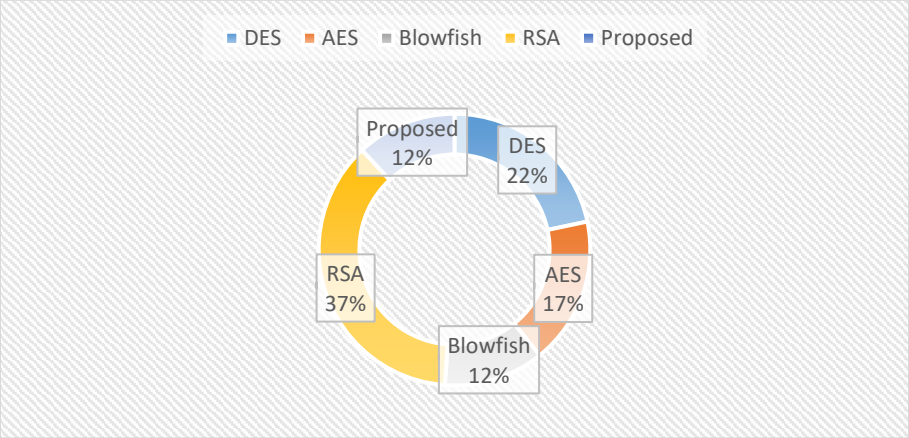


شکل ۴- ۶ میزان گذردهی – کیلوبایت بر ثانیه (اندازه داده: ۳۰۷۲ کیلوبایت)

۴-۷-۱ میزان حافظه مصرفی

با توجه به آنکه قصد داریم راهکار امنیتی پیشنهادی را در اینترنت اشیاء مورداستفاده قرار دهیم، درنتیجه میزان حافظه مصرفی نیز علاوه بر زمان اجرا و گذردهی، مهم است. بر همین اساس در این بخش میزان حافظه مصرفی روش پیشنهادی در مقایسه با سایر راهکارهای رمزنگاری متداول مورد ارزیابی و بررسی قرارگرفته است. بر همین اساس نتایج حاصل از ارزیابی

در شکل (۴-۸) نشان داده‌شده است. در این آزمایش سایز داده مورداستفاده جهت ارزیابی، برابر با ۵۰ کیلوبایت درنظر گرفته‌شده است.



شکل ۴- ۷ میزان حافظه مصرفی راهکارها

همانطورکه در شکل ۴-۸ ملاحظه می‌شود روش پیشنهادی دارای کمترین میزان حافظه مصرفی است. دلیل بالا بودن این میزان از کارایی در بهینگی هسته رمزنگاری است که بر اساس الگوریتم بلوفیش و خم‌های بیضوی می‌باشد و همین امر سبب افزایش گذردهی و کاهش میزان مصرف حافظه شده است زیرا در حالت عادی نیز الگوریتم بلوفیش جزء بهینه‌ترین الگوریتم‌ها درزمینه ی اشغال حافظه و زمان اجرا می‌باشد. زیرا بلوفیش تنها ۴ کیلوبایت از فضای حافظه دسترسی تصادفی (RAM) را به خود اختصاص می‌دهد. این محدودیت نه‌تنها مشکلی برای کامپیوترهای قدیمی و لپ‌تاپ‌ها به حساب نمی‌آید، بلکه آن را برای استفاده در کوچک‌ترین سیستم‌های تعبیه شده، مانند کارت‌های هوشمند و دستگاه‌های شبکه‌های کامپیوتری مناسب می‌کند. بر همین اساس در مقایسه با الگوریتم‌های DES،AES و RSA ملاحظه می‌شود، به‌طور میانگین بیش از ۳۰ درصد در مصرف حافظه صرفه‌جویی به عمل آمده است. درنتیجه این راهکار جهت بکارگیری در اینترنت اشیاء می‌تواند بسیار سودمند باشد و علاوه برافزایش امنیت، کمترین میزان استفاده از حافظه مصرفی را به همراه خواهد داشت.

۱۷. خلاصه و نتیجه‌گیری

اینترنت اشیا از پتانسیل کافی برای متحول کردن صنایع، شیوه زندگی و کار انسان‌ها برخوردار است، زیرا با استفاده از آن می‌توان داده‌ها را به‌طور مشترک و با همکاری دسته‌جمعی مورداستفاده قرارداد. اما با تمام این مزیت‌ها، مشکلاتی نیز بر سر راه استفاده از اینترنت اشیا وجود دارد که ازجمله آن می‌توان به امنیت و حریم خصوصی، چالش‌های همگرایی و ادغام داده‌ها، سیاست‌گذاری و استانداردها اشاره کرد. در این بین امنیت و حفظ حریم خصوصی از مهم‌ترین چالش‌ها است. از طرفی دیگر محدودیت منابع در اینترنت اشیا و همچنین پیچیدگی شبکه و ویژگی‌های ارتباطی همه‌پخشی در این شبکه‌ها باعث بوجود آمدن حفره‌های امنیتی جهت حمله می‌شود. همچنین در کنار آن به دلیل وجود بحث مالکیت اشیا و همینطور حفظ حریم خصوصی افراد، توجه به نکات امنیتی مرتبط با احراز هویت، کنترل دسترسی، حریم خصوصی و اعتماد نیز در اینترنت اشیا از اهمیت بیشتری برخوردار خواهد بود. یکی از راهکارهای تأمین امنیت در اینترنت اشیا بهره‌گیری از رمزنگاری می‌باشد از

طرفی با توجه به قدرت پردازشی کم، کمبود انرژی و محدودیت توان مصرفی گره‌های انتهایی اینترنت اشیاء و همچنین کمبود حافظه برای بار کردن نرم افزار، نیاز به الگوریتم‌های رمزنگاری سبک و امن است تا بتوان از طریق آن‌ها نیازمندی‌های امنیتی اینترنت اشیاء را تأمین کرد. رمزنگاری داده‌ها در هنگام انتقال بین دستگاه‌های اینترنت اشیا از الگوریتم‌های رمزنگاری استاندارد می‌تواند به جلوگیری از شنود داده‌ها توسط نفوذگرها کمک کند که در این زمینه مطالعات بسیار کمی صورت گرفته است. اشاره به‌تمامی این موارد ضرورت انجام تحقیق در مورداستفاده از رمزنگاری در امنیت اینترنت اشیا را دو چندان می‌کند.درواقع می‌توان گفت؛ امنیت داده* به محافظت از محرمانگی، جامعیت و دسترس پذیری اطلاعات، اشاره دارد. اطمینان از اینکه تنها کاربران مجاز (محرمانگی) به اطلاعات کامل و دقیق (جامعیت) در هنگام نیاز (دسترس‌پذیری) دسترسی دارند. هدف امنیت اطلاعات، محافظت اطلاعات و سامانه‌های اطلاعاتی از دسترسی و استفاده غیرمجاز، افشا، تغییر یا خرابی است. حال اگر بتوان سازوکاری ارائه نمود تا امنیت و سرعت در اینترنت اشیا افزایش یابد به گسترش و توسعه این فناوری کمک نموده‌ایم. به‌عبارت‌دیگر در این پژوهش هدف اصلی افزایش امنیت، کارایی و بهبود عملکرد انتقال ایمن داده‌ها در اینترنت اشیا است. از طرفی در بهره‌گیری از الگوریتم‌های رمزنگاری، همواره ایجاد یک نوع تعادل بهینه بین میزان امنیت و سرعت سرویس موردنظر یک چالش اساسی می‌باشد زیرا استفاده از روش‌های رمزنگاری پیچیده می‌تواند بر میزان کارایی سرویس‌های قابل ارائه به شدت تأثیرگذار باشد و با توجه به محدودیت منابع در اینترنت اشیا این چالش دوچندان می‌شود.

با توجه به به کارگیری این روش در اینترنت اشیا، در این پایان‌نامه تمرکز اصلی بر روی پایین بودن پیچیدگی و سادگی راهکار بوده است زیرا عملیات رمزنگاری هر چه پیچیده‌تر باشد نیاز به منابع پردازشی بالاتر و همچنین انرژی بیشتری خواهد بود که درواقع در اینترنت اشیا با محدودیت در این پارامترها روبرو هستیم. بر همین اساس در این پژوهش یک چهارچوب کلی جهت تأمین امنیت داده‌ها، در زمان ذخیره‌سازی و بازیابی آن‌ها در اینترنت اشیا ارائه گردید. راهکار پیشنهادی از دو الگوریتم رمزنگاری متقارن بلوفیش و نامتقارن خم‌های بیضوی به همراه تکنیک ایجاد کد هش MD5، به‌عنوان یک راهکار ترکیبی و بهینه جهت تأمین امنیت داده‌ها استفاده‌شده است.در ادامه پس از ارائه این الگوریتم ترکیبی، در بخش ارزیابی، نحوه عملکرد رمزنگاری نسبت به سایر الگوریتم‌های متداول رمزنگاری (AES،DES، و RSA) مورد بررسی قرار گرفت. زیرا هرچه سرعت و گذردهی در این بخش که همان هسته اصلی عملیات است، بیشتر باشد، سرعت و عملکرد کلی راهکار نیز بالاتر خواهد رفت. نهایتاً در محیط برنامه نویسی اکلیپس و به کمک زبان برنامه‌نویسی جاوا راهکار پیشنهادی پیاده‌سازی و در اندازه‌های مختلف داده مورد ارزیابی قرار گرفت و کلیه تست‌های انجام‌گرفته بر روی راهکار ارائه‌شده، بیانگر بهینه بودن آن نسبت به سایر روش‌ها بود. بطوریکه در آزمایش اول و با حجم داده ۵۰ کیلوبایت؛ زمان اجرا نسبت به الگوریتمAES ۵۰۶ میلی ثانیه کاهش‌یافته و به عبارتی در زمان بسیار کمتری عملیات رمزنگاری انجام‌گرفته است. نسبت به الگوریتم DES زمان اجرا بیش از ۳۵۶ میلی‌ثانیه کمتر بوده که بهینه‌تر بودن راهکار ترکیبی را نشان می‌دهد در مورد گذردهی نیز به همین صورت و راهکار ارائه‌شده از سایر روش‌ها بهینه‌تر می‌باشد. در آزمایش دوم که با حجم داده ۱۰۲۴ کیلوبایت انجام گرفت، این بار نیز راهکار پیشنهادی نسبت به سایر راهکارها بهتر عمل کرده است، بطوزیکه نسبت به الگوریتم DES زمان اجرا بیش از ۴۵۰ میلی‌ثانیه کاهش‌یافته است و در مقایسه با الگوریتم AES نیز علاوه برافزایش گذردهی، زمان اجرا نیز بیش از

* Data security

۳۰۰ میلی‌ثانیه کاهش‌یافته که این خود بیانگر سریعتر عمل کردن راهکار پیشنهادی نسبت به این دو الگوریتم، با افزایش سایز داده می‌باشد. نهایتاً در ارزیابی سوم و با حجم داده ۳۰۷۲ کیلوبایت، دوباره راهکار پیشنهادی نسبت به سایر الگوریتم‌ها بهتر عمل نموده، بر همین اساس زمان اجرای نسبت به دو الگوریتم متقارن DES و AES به ترتیب بین ۵۰۰ و ۱۵۰ میلی‌ثانیه کاهش‌یافته و از طرف دیگر گذردهی نیز بسیار بهینه‌تر شده است. در مورد الگوریتم نامتقارن RSA نیز زمان اجرا بیش از هزار میلی‌ثانیه کاهش‌یافته است.همچنین با توجه به آنکه قصد داریم راهکار امنیتی پیشنهادی را در اینترنت اشیاء مورداستفاده قرار دهیم، درنتیجه میزان حافظه مصرفی نیز علاوه بر زمان اجرا و گذردهی، مهم است. بر همین اساس در این بخش میزان حافظه مصرفی روش پیشنهادی در مقایسه با سایر راهکارهای رمزنگاری متداول مورد ارزیابی و بررسی قرارگرفته است. در این آزمایش نیز، روش پیشنهادی دارای کمترین میزان حافظه مصرفی است. دلیل بالا بودن این میزان از کارایی در بهینگی هسته رمزنگاری است که بر اساس الگوریتم بلوفیش و خم‌های بیضوی می‌باشد و همین امر سبب افزایش گذردهی و کاهش میزان مصرف حافظه شده است زیرا در حالت عادی نیز الگوریتم بلوفیش جزء بهینه‌ترین الگوریتم‌ها درزمینه ی اشغال حافظه و زمان اجرا می‌باشد. درواقع این الگوریتم تنها ۴ کیلوبایت از فضای حافظه دسترسی تصادفی (RAM) را به خود اختصاص می‌دهد. این محدودیت نه‌تنها مشکلی برای کامپیوترهای قدیمی و لپ‌تاپ‌ها به حساب نمی‌آید، بلکه آن را برای استفاده در کوچک‌ترین سیستم‌های تعبیه شده، مانند کارت‌های هوشمند و دستگاه‌های شبکه‌های کامپیوتری مناسب می‌کند.درواقع اساس بهینه‌تر بودن راهکار ترکیبی نسبت به دو راهکار دیگر، در هسته رمزنگاری داده آن می‌باشد که مبتنی بر الگوریتم بلوفیش است و این الگوریتم همواره دارای زمان اجرای کمتری نسبت به سایر الگوریتم‌های متداول می‌باشد بر همین اساس با بکارگیری آن در کنار الگوریتمی مانند خم‌های بیضوی و همچنین تکنیک MD5 و امضای دیجیتال مبتنی بر آن، می‌توان علاوه بر تضمین امنیت، کارائی را نیز در اینترنت اشیا تا سطح مطلوبی افزایش داد.

۱۸. کارهای آینده

در کارهای آتی می‌توان از تکنیک پردازش کارت‌گرافیکی و موازی‌سازی لوله‌ای استفاده نمود تا درنتیجه بتوان دستورالعمل‌هایی که قابل موازی‌سازی هستند را در زمان کمتری و به کمک کارت‌گرافیکی انجام داد و سایر بخش‌هایی که قابل موازی‌سازی نیستند را از طریق پردازنده اجرا نمود. برای این منظور می‌توان از تکنیک‌های نرم‌افزاری مبتنی بر کودا* استفاده نمود.

۱۹. مراجع

1. [1] Dang, Q. V. (2020, October). Active learning for intrusion detection systems. In 2020 RIVF International Conference on Computing and Communication Technologies (RIVF) (pp. 1-3). IEEE
2. [2] Singh, R., Kalra, M., & Solanki, S. (2020). A hybrid approach for intrusion detection based on machine learning. International Journal of Security and Networks, 15(4), 233-242

* CUDA

3. [3] Lee, J., Kim, J., Kim, I., & Han, K. (2019). Cyber threat detection based on artificial neural networks using event profiles. IEEE Access, 7, 165607-165626
4. [4] Abdulazeez, A., Salim, B., Zeebaree, D., & Doghramachi, D. (2020). Comparison of VPN Protocols at Network Layer Focusing on Wire Guard Protocol
5. [5] Ugochukwu, C. J., Bennett, E. O., & Harcourt, P. (2019). An intrusion etection system using machine learning algorithm. LAP LAMBERT Academic Publishing
6. [6] Salih, A. A., & Abdulrazaq, M. B. (2019, April). Combining best features selection using three classifiers in intrusion detection system. In 2019 International Conference on Advanced Science and Engineering (ICOASE)
7. (pp. 94-99). IEEE
8. [7] Ghanem, W. A. H., Jantan, A., Ghaleb, S. A. A., & Nasser, A. B. (2020). "An Efficient Intrusion Detection Model Based on Hybridization of Artificial Bee Colony and Dragonfly Algorithms for Training Multilayer Perceptrons". IEEE Access, 8, 130452-130475.
9. [8] Alamiedy, T. A., Anbar, M., Alqattan, Z. N., & Alzubi, Q. M. (2019). "Anomaly-based intrusion detection system using multi-objective grey wolf optimisation algorithm". Journal of Ambient Intelligence and Humanized Computing, 1-22.
10. [9] Bhumgara, A., & Pitale, A. (2019, July). Detection of Network Intrusions using Hybrid Intelligent Systems. In 2019 1st International Conference on dvances in Information Technology (ICAIT) (pp. 500-506). IEEE
11. [10] Rai, A. (2020, June). Optimizing a New Intrusion Detection System Using Ensemble Methods and Deep Neural Network. In 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184) (pp.
12. 527-532). IEEE
13. [11] Mirza, A. H. (2018, May). Computer network intrusion detection using various classifiers and ensemble learning. In 2018 26th Signal Processing and Communications Applications Conference (SIU) (pp. 1-4). IEEE
14. [12] Ahmad, S., Arif, F., Zabeehullah, Z., & Iltaf, N. (2020, June). Novel Approach Using Deep Learning for Intrusion Detection and Classification of the Network Traffic. In 2020 IEEE International Conference on Computational
15. Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA) (pp. 1-6). IEEE
16. [13] Hasan, D. A., & Abdulazeez, A. M. (2020). A Modified Convolutional Neural Networks Model for Medical Image Segmentation. learning, 20, 22
17. [14] Phadke, A., Kulkarni, M., Bhawalkar, P., & Bhattad, R. (2019, March). A Review of Machine Learning Methodologies for Network Intrusion etection. In 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC) (pp. 272-275). IEEE
18. [15] Golrang, A., Golrang, A. M., Yayilgan, S. Y., & Elezaj, O. (2020). A Novel Hybrid IDS Based on Modified NSGAII-ANN and Random Forest. Electronics, 9(4), 577
19. [16] Shashank, K., & Balachandra, M. (2018, August). Review on Network Intrusion Detection Techniques using Machine Learning. In 2018 IEEE Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER)
20. (pp. 104-109). IEEE

21.[17] Yihunie, F., Abdelfattah, E., & Regmi, A. (2019, May). Applying machine learning to anomaly-based intrusion detection systems. In 2019 IEEE Long Island Systems, Applications and Technology Conference (LISAT) (pp.5). IEEE

22.[18] Zeebaree, D. Q., Haron, H., Abdulazeez, A. M., & Zebari, D. A. (2019, April). Machine learning and region growing for breast cancer segmentation. In 2019 International Conference on Advanced Science and Engineering (ICOASE) (pp. 88-93). IEEE

23.[19] Talingdan, J. A. (2019, May). Performance comparison of different classification algorithms for household poverty classification. In 2019 4th International Conference on Information Systems Engineering (ICISE) (pp. 11-5). IEEE

24.[20] Jahwar, A. F., & Abdulazeez, A. M. (2020). Meta-Heuristic Algorithms For K-Means Clustering: A Review. PalArch's Journal of Archaeology of Egypt/Egyptology, 17(7), 12002-12020

25.[21] Ahmed, M. R. A. G., & Ali, F. M. A. (2019, September). Enhancing Hybrid Intrusion Detection and Prevention System for Flooding Attacks Using Decision Tree. In 2019 International Conference on Computer, Control,

26.Electrical, and Electronics Engineering (ICCCEEE) (pp. 1-4). IEEE

27.[22] Ahmad, U., Asim, H., Hassan, M. T., & Naseer, S. (2019, November). Analysis of Classification Techniques for Intrusion Detection. In 2019 International Conference on Innovative Computing (ICIC) (pp. 1-6). IEEE

28.[23] Zeebaree, D. Q., Haron, H., & Abdulazeez, A. M. (2018, October). Gene selection and classification of microarray data using convolutional neural network. In 2018 International Conference on Advanced Science and

29.Engineering (ICOASE) (pp. 145-150). IEEE

30.[24] Zebari, D. A., Zeebaree, D. Q., Abdulazeez, A. M., Haron, H., & Hamed, H. N. A. (2020). Improved Threshold Based and Trainable Fully Automated Segmentation for Breast Cancer Boundary and Pectoral Muscle in

31.Mammogram Images. IEEE Access, 8, 203097-203116

32.[25] Abdulqader, D. M., Abdulazeez, A. M., & Zeebaree, D. Q. (2020). Machine Learning Supervised Algorithms of Gene Selection: A Review. Machine Learning, 62(03)

33.[26] Abhale, A. B., & Manivannan, S. S. (2020). Supervised Machine Learning Classification Algorithmic Approach for Finding Anomaly Type of Intrusion Detection in Wireless Sensor Network. Optical Memory and Neural

34.Networks, 29(3), 244-256