# معماری امنیتی برای اینترنت اشیا: تحلیل و بهبود مدل سه‌لایهٔ ابر اینترنت اشیا

**محمد شیردل**

*دانشجوی دکتری، گروه مدیریت فناوری اطلاعات، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران*

**مقصود امیری***[1]

*استاد، گروه مدیریت صنعتی، دانشکدهٔ مدیریت و حسابداری، دانشگاه علامه طباطبائی، تهران، ایران*

**محمدعلی افشار کاظمی**

*دانشیار، گروه مدیریت صنعتی، دانشکدهٔ مدیریت، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران*

**محمدرضا معتدل**

*استادیار، گروه مدیریت صنعتی، دانشکدهٔ مدیریت، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران*

**مدیریت اطلاعات**

**دوره ۱۰، شماره ۱**

**بهار و تابستان ۱۴۰۳**

**چکیده:** با گسترش تعداد دستگاه‌های هوشمند و برنامه‌های مرتبط، حجم چشمگیری داده تولید می‌شود که در خودکارسازی فعالیت‌های روزمره نقش مهمی ایفا می‌کند. این کلان‌داده‌ها به پردازش سریع، ذخیره‌سازی ایمن و انتقال مطمئن از طریق کانال های امن نیاز دارند تا از تهدیدها و حمله‌های مخرب محافظت شوند. حفاظت از حریم خصوصی، همواره یکی از چالش های اصلی فضای مجازی بوده و با ظهور اینترنت اشیا (IoT) این چالش ابعاد گسترده‌تری یافته است. در این مقاله، یک مدل ارزیابی مبتنی بر معماری سه‌لایهٔ اینترنت اشیا، شامل لایه‌های ادراک، انتقال و کاربرد ارائه شده است. برای هر لایه، شاخص‌های عملکردی خاصی تعریف و به‌کار گرفته شده است. به‌منظور ارزیابی عملکرد سیستم، نظرهای خبرگان جمع‌آوری شد و با استفاده از روش تصمیم‌گیری تاپسیس فازی، اولویت‌بندی شاخص‌ها صورت گرفت. همچنین، مدل‌های امنیتی نظیر رمزنگاری سبک‌وزن سایمون و احراز هویت متقابل، به‌صورت جداگانه به هر لایه افزوده و تأثیر هر یک بر عملکرد کلی سیستم تحلیل شد. برای پیاده‌سازی این الگوریتم‌ها، از میکروکنترلر STM32F4 با پردازندهٔ ARM Cortex-M4 که توانایی پردازشی مناسب و قابلیت اندازه‌گیری دقیق شاخص‌های امنیتی و عملکردی را فراهم می‌سازد، استفاده شد. نتایج نهایی نشان می‌دهد که مدل پیشنهادی به بهبود سطح امنیت و کاهش آسیب‌پذیری در برابر حمله‌های سایبری منجر می‌شود.

**کلیدواژه‌ها:** معماری امنیتی، اینترنت اشیا، مدل سه لایه ابر اینترنت اشیا.

---

۱. نویسنده مسئول: amir@atu.ir

## مقدمه

اینترنت اشیا (IoT) به‌عنوان یک فناوری نوظهور شناخته می‌شود که با اتصال تعداد زیادی از دستگاه‌ها به اینترنت، زمینه را برای بروز تهدیدها سایبری فراهم می‌آورد. این وضعیت به ظهور مسائل جدید امنیتی مرتبط با اینترنت اشیا منجر شده است. تهدیدهایی که دستگاه‌های اینترنت اشیا را هدف قرار می‌دهند، شامل حمله‌های شبکه‌ای، فیزیکی، محیطی، تحلیل رمزنگاری و نرم‌افزاری هستند (دیجنا، هارو و سیدونی[1]، ۲۰۲۱). حمله‌های شبکه‌ای مانند حمله‌های مردمیانی (MITM)[2]، بازپخش، تغییر ظاهر و حمله‌های انکار سرویس توزیع‌شده (DDoS)[3] از جمله این تهدیدها به شمار می‌روند (یانگ، وو، یین، لی و ژائو[4]، ۲۰۱۷).

برای مقابله با این خطرها در سیستم‌های اینترنت اشیا، ضروری است که پروتکل‌های ارتباطی از امنیت زیادی برخوردار باشند. به‌طور مثال، استفاده از الگوریتم‌های رمزگذاری سبک و تکنیک‌های پیشرفته، برای فیلتر کردن و پیش‌بینی تهدیدهای امنیتی، می‌تواند مؤثر باشد. امنیت در اینترنت اشیا بسیار مهم است؛ زیرا هر حملهٔ موفق، می‌تواند کل بخش‌های تولید، حمل‌ونقل، سیستم سلامت و سایر حوزه‌ها را مختل کند.

اینترنت اشیا ترکیبی از دستگاه‌ها، پروتکل‌های شبکه و فناوری‌هایی است که هر یک دارای آسیب‌پذیری‌های خاص خود هستند و این موضوع سطح حمله را در کل شبکه اینترنت اشیا افزایش می‌دهد. شبکه‌های اینترنت اشیا با فعال‌سازی سیستم‌های هوشمند و خودکار، جنبه‌های مختلف زندگی ما را متحول ساخته‌اند. با این حال، گسترش دستگاه‌های IoT چالش‌های امنیتی چشمگیری، به‌ویژه در زمینهٔ حریم خصوصی و امنیت اطلاعات، ایجاد می‌کند.

احراز هویت به‌عنوان یک سازوکار امنیتی اساسی، برای حفاظت از دستگاه‌های IoT و داده‌های حساسی که بین آن‌ها تبادل می‌شود، بسیار حیاتی است. چارچوب اینترنت اشیا در پی اتصال هر فرد، به هر چیزی، در هر مکان است. این فناوری معمولاً از معماری سه‌لایهٔ ادراک، شبکه و کاربرد تشکیل می‌شود. برای تحقق یک اینترنت اشیای امن، باید اصول امنیتی متعددی در هر لایه پیاده‌سازی شود. آینده چارچوب اینترنت اشیا، فقط در صورتی تضمین می‌شود که به‌طور جدی به مسائل امنیتی مرتبط با آن، توجه شود. بسیاری از محققان تلاش کرده‌اند تا با اجرای تدابیر مناسب، نگرانی‌های امنیتی خاص هر لایه و دستگاه‌های اینترنت اشیا را برطرف کنند. این مقاله به بررسی اصول امنیتی، چالش‌های تکنولوژیکی و امنیتی، اقدامات متقابل پیشنهادی و مسیرهای آینده برای ایمن‌سازی اینترنت اشیا می‌پردازد.

## مبانی نظری

اینترنت اشیا (IoT) یک فناوری شناخته شده است که بر بسیاری از زمینه‌ها، از جمله ارتباطات، کار، مراقبت‌های بهداشتی و اقتصاد تأثیر درخور توجهی دارد. اینترنت اشیا پتانسیل بهبود زندگی در زمینه‌های

1. Djenna, Harous & Saidouni
2. Man-in-the-Middle
3. distributed denial-of-service
4. Yang, Wu, Yin, Li & Zhao

مختلف، از شهرهای هوشمند گرفته تا کلاس‌های درس، با خودکارسازی وظایف، افزایش خروجی و کاهش اضطراب را دارد. از سوی دیگر حمله‌ها و تهدیدهای سایبری، بر برنامه‌های هوشمند اینترنت اشیا بسیار تأثیرگذارند. بسیاری از تکنیک‌های سنتی برای محافظت از اینترنت اشیا، به‌دلیل خطرها و آسیب‌پذیری‌های جدید، اکنون بی‌اثرند. سیستم‌های اینترنت اشیا، برای حفظ رویه‌های امنیتی خود در آینده، به یادگیری ماشینی کارآمد با هوش مصنوعی و یادگیری عمیق نیاز دارند. در صورتی نسل بعدی سیستم اینترنت اشیا، یک سیستم امنیتی دائم در حال تغییر و به‌روز خواهد بود که از قابلیت‌های هوش مصنوعی، به‌ویژه راه‌حل‌های یادگیری ماشینی و عمیق استفاده شود (مظهر و همکاران[1]، ۲۰۲۳). اطلاعات امنیتی IoT در این مقاله، از هر زاویه‌ای که در دسترس است بررسی شده است.

## حریم خصوصی

مسائل مربوط به حریم خصوصی، در برخی مکان‌ها بیشتر مطرح هستند. ممکن است مدیریت هویت در IoT فرصت‌های جدیدی را با ترکیب روش‌های مختلف تأیید هویت، برای افزایش امنیت انسان‌ها و ماشین‌ها ارائه دهد. برای مثال، شناسایی زیستی در ترکیب با یک شیء در شبکهٔ شخصی، می‌تواند برای باز کردن درب استفاده شود. باید تأکید کرد که حفظ حریم خصوصی و پیروی از آن، تحت نظارت قوانین کشوری قرار دارند. درک فضای اینترنت اشیا، نیازمند تعریف لایه‌ها و عناصر اینترنت اشیا، برای توصیف معماری‌های احتمالی اینترنت اشیا، بر اساس خدمات و زمینه‌های مورد نیاز است. معماری‌های مختلفی برای محیط‌های اینترنت اشیا ارائه شده است. به‌طورکلی معماری مورداستفاده در این مقاله، معماری سه لایه است. این کلاس متداول‌ترین نوع در بین بیشتر نشریه‌ها و محققان همکار است (ری[2]، ۲۰۱۸). این لایه، از طریق لایه‌های رویکرد از بالا به پایین ساختار یافته است که عبارت‌اند از:

الف) لایهٔ کاربردی که توابع برنامه و سرویس در آنجا کار می‌کنند؛

ب) لایهٔ شبکه / انتقال؛

ج) لایهٔ ادراک / لبه که مربوط به اشیا یا دستگاه‌های نقطهٔ پایان معماری است.

در ادامه تعریف هر یک از لایه‌ها ارائه‌شده است.

## معماری اینترنت اشیا

در مورد IoT توافق جهانی وجود دارد؛ اما در خصوص معماری آن اتفاق‌نظر واحدی وجود ندارد. محققان مختلف معماری‌های مختلفی را ارائه داده‌اند. ابتدایی‌ترین معماری، یک معماری سه لایه است (ماشال و همکاران[3]، ۲۰۱۵؛ سید و مسعود[4]، ۲۰۱۳؛ وو، لو، لینگ، سان و دو[5]، ۲۰۱۰). همان‌طور که در شکل ۱ نشان

1. Mazhar et al.
2. Ray
3. Mashal et al
4. Said and M.Masud
5. Wu, Lu, Ling, Sun & Du

داده شده است، تصویر در مراحل اولیه تحقیق در این زمینه، در سه لایه، یعنی لایه‌های ادراک، شبکه و کاربرد معرفی شد.


**شکل ۱.** معماری اینترنت اشیای ۳ لایه
منبع: (سطحی و سارنگی[1]، ۲۰۱۷)

۱. لایهٔ ادراک لایهٔ فیزیکی است که دارای حسگرهایی برای سنجش و جمع‌آوری اطلاعات در مورد محیط است. برخی پارامترهای فیزیکی را حس می‌کند یا سایر اشیا هوشمند موجود در محیط را شناسایی می‌کند.
۲. لایهٔ شبکه مسئول اتصال به سایر موارد هوشمند، دستگاه‌های شبکه و سرورهاست. از ویژگی‌های آن برای انتقال و پردازش داده‌های حسگر نیز استفاده می‌شود.
۳. لایهٔ کاربرد وظیفه ارائه خدمات خاص برنامه به کاربر را دارد. این برنامه‌های مختلفی را تعریف می‌کند که در آن می‌توان اینترنت اشیا را به‌کار برد، برای مثال، خانه‌های هوشمند، شهرهای هوشمند و سلامت هوشمند. معماری سه لایه، ایده اصلی را تعریف می‌کند.

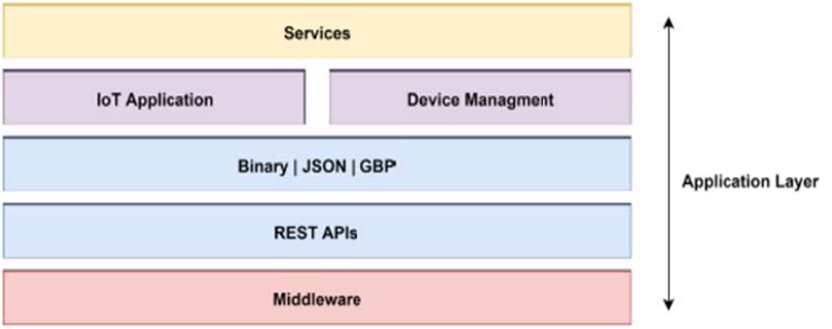
### نگرانی‌های امنیتی مربوط به لایه‌های مختلف

- لایهٔ کاربرد

استاندارد جامعی برای لایهٔ کاربرد IoT ارائه نشده است؛ اما این لایه می‌تواند طیف وسیعی از خدمات را در برنامه‌های مختلف ارائه دهد. به‌طور مثال، استفاده از اینترنت اشیا در شهرهای هوشمند و خانه‌ها (بینتی هاروم، زکریا، عمران، آیوپ و انوار[2]، ۲۰۱۹) ، شبکه‌های هوشمند (سخینی، کریمی‌پور، دهقان تنها، پریزی و سریواستاوا[3]، ۲۰۱۹؛ بحرا و همکاران[4]، ۲۰۱۹)، مراقبت‌های بهداشتی (سریواستاوا، پریزی، دهقان تنها و چو[5]، ۲۰۱۹)، وسایل نقلیه خودمختار (پارانجوتی، تانیک، وانگ و خان[6]، ۲۰۱۹؛ نگو، گوتیرز، متسیس، نپال و شنگ[7]، ۲۰۱۶). لایهٔ کاربرد همچنین می‌تواند به‌عنوان میان‌افزار، یک پروتکل ارتباطی و رایانش ابری برای

1. Sethi and Sarangi
2. N. Binti
3. Sakhnini, Karimipour, Dehghantanha, Parizi & Srivastava
4. Binti Harum, Zakaria, Emran, Ayop & Anawar
5. Srivastava, Parizi, Dehghantanha & Choo
6. Paranjothi, Tanik, Wang & Khan
7. Ngu, Gutierrez, Metsis, Nepal & Sheng

پشتیبانی سرویس عمل کند. بنابراین، نگرانی امنیتی بر اساس محیط و صنعت برنامه متفاوت خواهد بود. همان‌طور که در شکل ۲ در ساختار لایهٔ کاربرد دیده می‌شود، اجزای مختلفی تعریف شده است و هر یک از اجزای سازنده، به کاربرد محیط بستگی دارد. به‌طور مثال، در مراقبت‌های بهداشتی برای بازیابی سوابق پزشکی، نیاز به رابط برنامه‌نویسی برنامه‌های ویژه (API) یا برنامه‌های ویژه به‌عنوان باینری در سمت سرویس‌گیرنده و سرور در آنجا وجود دارد. بیشتر معماری‌های امنیتی برنامه‌ها بر ایمن‌سازی پروتکل CoAP با استفاده از DTLS متمرکزند. درحالی‌که سایر معماری‌های امنیتی کاربردی مدل خود را بر اساس رمزگذاری بارهای HTTP پیشنهاد کرده‌اند (چوی و همکاران[1]، ۲۰۱۸؛ آروبند و نارایان[2]، ۲۰۱۹). مؤلفه‌های شاخص لایه‌های کاربرد بر اساس مطالعات لی، شی، چنگ، چن و کودو[3] (۲۰۲۴) و لیو، یانگ و لیو[4] (۲۰۱۷) عبارت‌اند از: عملکرد ایمنی اطلاعات، سرعت پردازش تجارت، دقت پردازش تجارت و تحمل خطا و سازگاری.



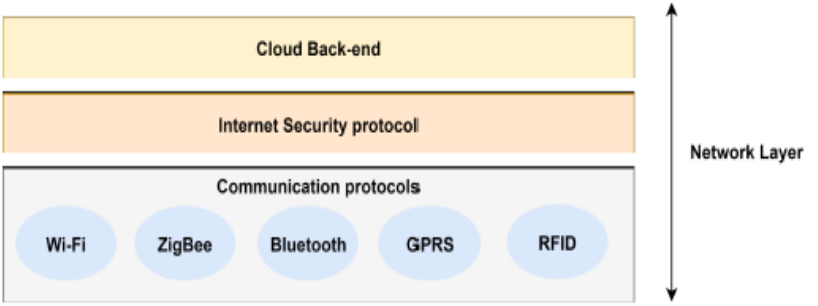

شکل ۲. مؤلفه‌های لایهٔ کاربرد در معماری IoT

- لایهٔ انتقال

در لایه شبکه انتقال داده در بین لایه‌های دیگر مدیریت می‌شود. این لایه همچنین از طریق استانداردها و پروتکل‌های مختلف مانند IEEE 802.x، سیستم موقعیت‌یابی جهانی (GPS) و ارتباطات میدان نزدیک (NFC) به لایهٔ ادراک دسترسی می‌دهد. همان‌طور که در شکل ۳ نشان داده شده است، این لایه همچنین توسط یک زیرساخت back-end cloud، دستگاه‌های تلفن همراه و پروتکل اینترنت پشتیبانی می‌شود (سانتوس و همکاران[5]، ۲۰۱۸). علاوه‌براین، لایه شبکه را می‌توان با جنبه‌های مختلف بر اساس محیط اعمال‌شده درمان کرد. بااین‌حال، رایج‌ترین سازوکار امنیت در لایه شبکه معماری اینترنت اشیا، شامل

1. Choi et al.
2. Arvind & Narayanan
3. Li, Shi, Cheng, Chen & Quevedo
4. Liu, Yang & Liu
5. Santos et al.

فناوری بلاکچین، سیستم‌های کشف هوشمند و مدیریت کلیدی و سیستم رمزگذاری است (علی و آواد[1]، ۲۰۱۸؛ صالح و خان[2]، ۲۰۱۸؛ بورک[3]، ۲۰۱۸؛ چن، تواتی و ژو[4]، ۲۰۱۹؛ زارکا و همکاران[5]، ۲۰۱۸).




شکل ۳. مؤلفه‌های لایه شبکه در معماری IoT

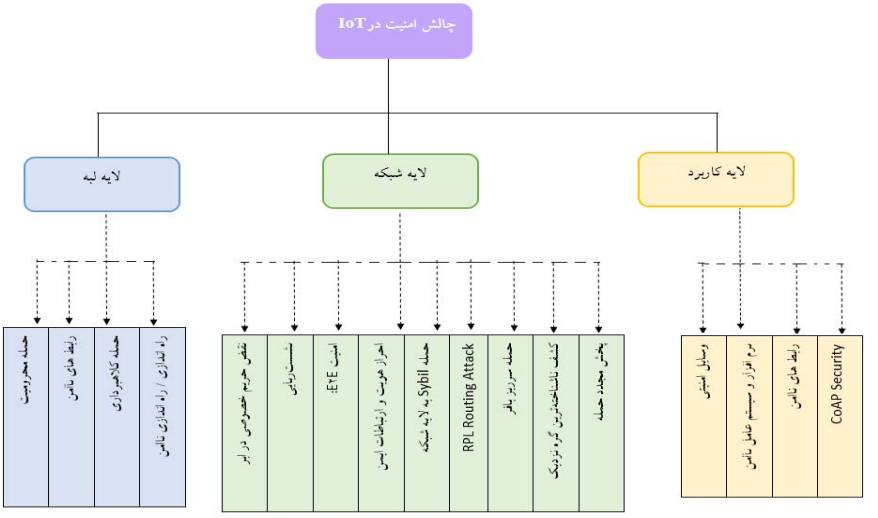
در این پژوهش شاخص‌های لایهٔ انتقال عبارت‌اند از: قابلیت اطمینان تجهیزات، دقت ادراک‌شده، دامنهٔ ادراکی و سرعت درک شده.

- لایهٔ لبه (ادراک)

در این لایه، کاربران نهایی لبه ابر[6] دستگاه‌های اینترنت اشیا، می‌توانند با مشتری یا قلمروهای کاری آن‌ها مانند سنسورها، کنتورهای هوشمند یا سرورهای لایهٔ لبه اینترنت اشیای یک درگاه که دارای نقش هماهنگ‌کننده در حوزهٔ کاری است، تعامل داشته باشند. به‌دلیل قرار گرفتن در معرض فیزیکی لایهٔ لبه در معماری اینترنت اشیا، این لایه با حمله‌های زیادی روبه‌رو می‌شود. رایج‌ترین مؤلفه‌های امنیتی که در این لایه اعمال می‌شود، شامل سازوکار احراز هویت چندعاملی، محلول ضد بدافزار نقطه پایان، کانال امن و راه‌حل‌های مبتنی بر یادگیری ماشین برای تشخیص ناهنجاری در دستگاه‌های لبه ابر است (پوتال، نپال، رانجان و چن[7]، ۲۰۱۶؛ کاندو و اسکلوم[8]، ۲۰۱۶؛ دووم و همکاران[9]، ۲۰۱۹؛ گرسی، گارسیا و فنتون[10]، ۲۰۱۷؛ رن، گو، خو و ژنگ[11]، ۲۰۱۷). در این پژوهش شاخص‌های لایهٔ ادراک، بر اساس مطالعات وانگ، وانگ و

1. Ali and Awad
2. Khan and Salah
3. Burke
4. Chen, Touati & Zhu
5. Zarca et al.
6. Cloud-edge
7. Puthal, Nepal, Ranjan & Chen
8. Canedo and Skjellum
9. Dovom et al.
10. Grassi, Garcia & Fenton
11. Ren, Guo, Xu & Zhang

جین[1] (۲۰۲۱) عبارت‌اند از: قابلیت اطمینان تجهیزات، دقت ادراک‌شده، دامنهٔ ادراکی و سرعت درک شده. در شکل ۴ چالش‌های امنیت در IoT در هر سه لایه نشان داده شده است.




شکل ۴. طبقه‌بندی چالش امنیتی اینترنت اشیا مبتنی بر معماری لایه‌ای

## پیشینهٔ تجربی پژوهش

شاهزاده فاضلی، قوه ندوشن، زارع‌پور و احمدآبادی (۱۴۰۳) مقاله‌ای با عنوان «بهبود سرعت سیستم تشخیص نفوذ از طریق کاهش حجم داده‌ها با استفاده از DBSCAN مبتنی بر هسته» انجام دادند. مقاله روی بهبود سرعت سیستم تشخیص نفوذ، به‌عنوان یک راه‌حل حیاتی برای امنیت اینترنت اشیا تمرکز دارد. در سیستم های تشخیص نفوذ، وجود حجم زیاد داده، موجب کاهش سرعت یادگیری می‌شود. در مقاله الگوریتم خوشه بندی DBSCAN با افزودن پارامتر حداقل همسایگی، جهت کاهش هدفمند نمونه ها اصلاح شده است که سعی در افزایش سرعت سیستم تشخیص نفوذ و کاهش زمان و هزینه یادگیری دارد. تنظیم پارامترهای DBSCAN اصلاح‌شده با الگوریتم ژنتیک انجام می‌شود. نتایج آزمایش‌ها روی مجموعه داده Kaggle و DDK_NSL نشان می‌دهد که مدل پیشنهادی، قادر است با کاهش حجم داده‌ها تا ۸۰درصد، دقت طبقه‌بندی را برای مجموعه داده Kaggle بالای ۹۶درصد و برای مجموعه داده KDD_NSL بالای ۹۲/۵۱درصد حفظ کند. همچنین، زمان محاسبات برای مجموعه دادهٔ Kaggle از ۴۵۸/۰۹ms به ۴۷/۲۱ms و برای مجموعه داده KDD_NSL از ۹۹۵/۲ms به ۲۲۳/۶۰ms، کاهش یافته است. به این ترتیب، با وجود بهبود در سرعت و کاهش زمان و هزینه، عملکرد مطلوب مدل حفظ شده است.

1. Wang, Wang & Jin

احمدوند و جهانشاهی (۱۴۰۲)، الگوی مطلوب قانون‌گذاری حفاظت از دادهٔ شخصی در بستر اینترنت اشیا، در پرتو مطالعات تطبیقی را ارائه کردند. اینترنت اشیا، به‌عنوان نسل جدید اتصال و ارتباط اشیای هوشمند از طریق اینترنت، مفهومی است که به‌تازگی وارد ادبیات حکمرانی کشور شده است. با توجّه به امکان شناسایی هویت و دسترسی به اطلاعات شخصی از طریق تحلیل و ترکیب داده‌های جمع‌آوری‌شده، حفاظت مؤثر از داده‌های شخصی به‌عنوان یک امر بایسته در بستر این فناوری مطرح‌شده است. نظام حقوقی ایران، به علت نوپا بودن کشور در این حوزه، قانونی ندارد که به حفاظت از داده‌های شخصی شهروندان در این مقوله اختصاص داشته باشد و صرفاً در مصوبه شورای عالی فضای مجازی به الزامات حاکم بر اینترنت اشیا در شبکه ملّی اطلاعات پرداخته شده است. پژوهش بر اساس روش تحلیلی ـ توصیفی با بررسی مجموع قوانین و مقررات نظام‌های حقوقی اتحادیه اروپایی، ایالات‌متحده آمریکا و جمهوری خلق چین، الگوهای قانون‌گذاری در حوزه موردبحث را استخراج کرده و به این پرسش پاسخ داده است که کدام نوع الگوی قانون‌گذاری، برای نظام حقوقی کشور مطلوب است. به نظر می‌رسد از میان رویکردهای مطرح‌شده، ترکیبی از الگوهای موجود، می‌تواند گزینهٔ مناسبی برای تدوین قانون در کشور باشد.

امیرحسین رنجبر (۱۴۰۱)، پژوهشی با عنوان «مروری بر ضرورت اینترنت اشیا در پروژه‌های شهر هوشمند؛ رویکرد نوین در توسعهٔ پایدار شهری» انجام داد. مفهوم شهر هوشمند بر ساختار، سامانه و هویت آبادی‌هایی دلالت دارد که فناوری ارتباطات از دور به آن‌ها حیات می‌بخشد. بر اساس بررسی ادبیات گسترده، مقاله ابتدا مفهوم شهر هوشمند را ارائه می‌کند که بر معماری شهر هوشمند و نقش داده‌ها در راه‌حل‌های شهر هوشمند تأکید می‌کند. در بخش دوم، اینترنت اشیا را با تمرکز بر فناوری اینترنت اشیا، استفاده از اینترنت اشیا در برنامه‌های کاربردی شهر هوشمند و امنیت ارائه می‌کند. مقالات بر اساس معیارهای ورود و خروج به مطالعه ارزیابی شدند. این پژوهش از نظر عمق مطالعه، کاربردی ـ توسعه‌ای است و از نظر هدف پژوهش، توصیفی است، به این دلیل که باهدف تبیین جنبه‌های مختلف شهرهای هوشمند، هوشمند سازی شهری و توسعه پایدار شهری انجام شده است. انتخاب مقالات بدین صورت بود که در ابتدا، فهرستی از عناوین و چکیدهٔ تمام مقالات موجود در پایگاه‌های اطلاعاتی توسط پژوهشگر تهیه و به‌منظور تعیین و انتخاب عناوین مرتبط بررسی شدند؛ سپس مقالات مرتبط به‌طور مستقل از همه موارد وارد فرایند پژوهش شدند. در انتهای جست‌وجو، تعداد ۸۴ مقاله به‌دست آمد و در نهایت ۱۴ مقاله که از کیفیت خوبی برخوردار بودند، وارد مطالعه مرور سیستماتیک شدند.

مظهر و همکاران (۲۰۲۳)، پژوهشی با عنوان «تجزیه‌وتحلیل چالش‌های امنیتی اینترنت اشیا و راه‌حل‌های آن با استفاده از هوش مصنوعی» انجام دادند. آن‌ها یک روش نوآورانه برای محافظت از دستگاه‌های اینترنت اشیا، در برابر انواع حمله‌های سایبری با استفاده از یادگیری ماشینی و یادگیری عمیق، برای به‌دست‌آوردن اطلاعات از داده‌های خام ارائه کردند. مقاله بررسی می‌کند که چگونه می‌توان از یادگیری ماشین و یادگیری عمیق، برای شناسایی الگوهای حمله در داده‌های بدون ساختار و محافظت از دستگاه‌های IoT استفاده کرد. با توجه به این یافته‌ها، چالش‌هایی که محققان با آن روبه‌رو هستند و همچنین جهت‌گیری‌های بالقوهٔ آینده برای این حوزه تحقیقاتی را موردبحث قرار می‌دهند.

طاهردوست[1] (۲۰۲۳) در پژوهشی با عنوان «امنیت و اینترنت اشیا: مزایا، چالش‌ها و چشم‌اندازهای آینده» انجام داد. با توجه به استفادهٔ گسترده از اینترنت اشیا (IoT)، سازمان‌ها باید تلاش خود را بر امنیت سیستم متمرکز کنند. هر آسیب‌پذیری می‌تواند به خرابی سیستم یا حملهٔ سایبری منجر شود که تأثیری در مقیاس بزرگ خواهد داشت. امنیت اینترنت اشیا یک استراتژی حفاظتی و سازوکار دفاعی است که در برابر احتمال حمله‌های سایبری که به‌طور خاص دستگاه‌های متصل به اینترنت اشیا را هدف قرار می‌دهند، محافظت می‌کند. تیم‌های امنیتی اینترنت اشیا در حال حاضر با مشکلات فزاینده‌ای مانند موجودی‌ها، عملیات، تنوع، مالکیت، حجم داده‌ها، تهدیدها و غیره دست‌وپنجه نرم می‌کنند. همچنین پتانسیل آیندهٔ امنیت شبکهٔ اینترنت اشیا در سال‌های اخیر، توجه بیشتری را از سوی محققان بین‌رشته‌ای و پراکنده جغرافیایی به خود جلب کرده است. یکپارچگی داده‌ها، محرمانه بودن، احراز هویت و مجوز باید به‌دلیل حجم زیاد داده‌ای که در دستگاه‌های شبکه جریان دارد تضمین شود. با این‌حال، حوزه امنیت اینترنت اشیا هنوز جای زیادی برای رشد دارد.

خان و همکاران[2] (۲۰۲۳)، پژوهشی با عنوان «تهدیدهای معماری برای امنیت و حریم خصوصی: چالشی برای برنامه‌های کاربردی اینترنت اشیا)» انجام دادند. امنیت برای محافظت از منابع فناوری در برابر دسترسی غیرمجاز یا هرگونه وقفه برای ایجاد اختلال در اتصال بی‌وقفه و همه‌جای اینترنت اشیا از لایهٔ ادراک به رایانه‌های ابری بسیار مهم در نظر گرفته می‌شود. با انگیزهٔ این موضوع، در خصوص فناوری و معماری لایه‌ای IoT به همراه برنامه‌های کاربردی حیاتی با تمرکز ویژه بر ویژگی‌های کلیدی خانه‌های هوشمند، کشاورزی هوشمند، حمل‌ونقل هوشمند و مراقبت‌های بهداشتی هوشمند مرور کلی انجام شده است. در مرحله بعد، تهدیدهای امنیتی و آسیب‌پذیری‌های موجود در حمله‌ها به هر لایهٔ اینترنت اشیا به‌صراحت توضیح داده شده است. طبقه‌بندی چالش‌های امنیتی مانند محرمانگی، یکپارچگی، حریم خصوصی، در دسترس بودن، احراز هویت، عدم انکار و مدیریت کلید، به‌طور کامل بررسی و درنهایت، جهت‌های تحقیقاتی آینده برای نگرانی‌های امنیتی شناسایی و ارائه شده است.

بالوق، گالو، پلوسزک، اسپیسک و زاجاک[3] (۲۰۲۱) پژوهشی با عنوان «چالش‌های امنیتی اینترنت اشیا: ابر و بلاکچین، رمزنگاری پسکوانتومی و تکنیک‌های تکاملی» انجام دادند. اینترنت اشیا دنیای فیزیکی و سایبرنتیک را به هم متصل می‌کند. به این‌ترتیب، مسائل امنیتی دستگاه‌های اینترنت اشیا، به‌ویژه هرچه آنچه آسیب‌زاست، باید موردتوجه قرار گیرند. در این مقاله نویسندگان به بررسی اجمالی مسائل امنیتی فعلی اینترنت اشیا با چشم‌انداز تهدیدهای آینده می‌پردازند. نویسندگان سه روند اصلی را شناسایی می‌کنند که باید به‌طور خاص موردتوجه قرار گیرند: مسائل امنیتی ادغام اینترنت اشیا با ابر و بلاکچین، تغییرات سریع در رمزنگاری به‌دلیل محاسبات کوانتومی و درنهایت ظهور روش‌های هوش مصنوعی و تکامل در حوزه امنیت اینترنت اشیا. آن‌ها یک نمای کلی از تهدیدها شناسایی‌شده ارائه دادند و راه‌حل‌هایی برای ایمن‌سازی اینترنت اشیا در آینده پیشنهاد کردند.

1. Taherdoost
2. Khan et al.
3. Balogh, Gallo, Ploszek, Spacek & Zajac

پژوهش‌های پیشین در حوزهٔ امنیت اینترنت اشیا (IoT) به‌طور قابل‌توجهی بر جنبه‌های مختلفی مانند کاهش حجم داده‌ها، استفاده از زیرساخت‌های شبکه‌های اجتماعی، تحلیل تعاملات امنیتی با نظریه بازی‌ها و بهره‌گیری از هوش مصنوعی متمرکز شده‌اند. با وجود دستاوردهای ارزشمند این تحقیقات، چندین شکاف پژوهشی کلیدی شناسایی شده است که به توجه فوری نیاز دارد: بیشتر پژوهش‌ها بر بهبود یک‌لایه خاص مانند لایه ابر تمرکز کرده‌اند؛ اما تعامل امن بین لایه‌های مختلف معماری سه‌لایه IoT (ادراک، انتقال و کاربرد) به‌صورت یکپارچه تحلیل نشده است. برای مثال، کاهش حجم داده تنها بر لایه ابر تأثیر می‌گذارد، در حالی‌که تأثیر آن بر امنیت end-to-end در لایه‌های دیگر نادیده گرفته شده است. این عدم یکپارچه‌سازی ممکن است به نقاط آسیب‌پذیر در ارتباط بین لایه‌ها منجر شود.

۱. رویکردهای مبتنی بر نظریه بازی‌ها یا یادگیری ماشین، عمدتاً در محیط‌های کنترل شده با داده‌های ایستا آزمایش شده‌اند؛ اما در سناریوهای واقعی IoT با دستگاه‌های ناهمگون و پویا، کارایی این روش‌ها کاهش می‌یابد. همچنین، روش‌هایی که از زیرساخت‌های موجود (مانند شبکه‌های اجتماعی) استفاده می‌کنند، ممکن است در مقیاس کلان با چالش‌های تأخیر و امنیت داده مواجه شوند.

۲. پژوهش‌هایی به بررسی تهدیدهای امنیتی پرداخته‌اند، اما راه‌کارهای ارائه شده، عمدتاً واکنشی و مبتنی بر شناسایی الگوهای شناخته شده هستند. در مقابل، حمله‌های نوظهور (مانند حمله‌های سایبر فیزیکی یا حمله‌های مبتنی بر هوش مصنوعی)، به‌ویژه در معماری‌های چندلایه IoT، نیازمند راه‌کارهای پیشگیرانه و تطبیقی هستند که در تحقیقات موجود کمتر دیده می‌شود.

معماری پیشنهادی این مقاله با پر کردن شکاف‌های موجود در پژوهش‌های پیشین، نه‌تنها امنیت end-to-end را در محیط‌های ناهمگن IoT تضمین می‌کند، بلکه سازگاری با الزامات کارایی و مقیاس‌پذیری را نیز بهبود می‌بخشد. این رویکرد با ترکیب نوآوری‌های چندوجهی (فنی، معماری، و الگوریتمی)، جایگاه تحقیق حاضر را به‌عنوان گامی پیشرو در حوزه امنیت IoT تثبیت می‌کند.

## روش‌شناسی پژوهش

در این پژوهش برای مرور ادبیات از به‌روزترین مقالات استفاده شده است. از پرسش‌نامهٔ مقایسه زوجی برای جمع‌آوری نظر خبرگان در مورد افزودن لایه‌های امنیتی به هر یک از لایه‌های مدل پژوهش استفاده شده است. روش کار به این صورت است که یک معماری جدید ارائه می‌شود که شامل افزودن لایه‌های امنیتی به سه‌لایه مدل ابر چینی (وانگ، مینگ، چن، ژنگ و ونگ[1]، ۲۰۱۸) است. این امر درنهایت به مدلی منجر می‌شود که کمتر دچار حمله سایبری می‌شود. با استفاده از نظرات خبرگان و تحلیل تاپسیس فازی برای اولویت‌بندی مؤلفه‌های هر شاخص و درنهایت با افزودن دو مدل امنیتی رمزنگاری سبک‌وزن و احراز هویت متقابل دوطرفه با استفاده از شبیه‌سازی به هر یک از لایه‌ها، میزان تغییرات عملکرد محاسبه شده است.

1. Wang, Ming, Chen, Zhang & Wang

برای پیاده‌سازی و ارزیابی مدل‌های امنیتی شامل الگوریتم رمزنگاری سبک‌وزن(Simon ) و احراز هویت متقابل در معماری سه‌لایه IoT، از میکروکنترلر STM32F4 با پردازندهٔ ARM Cortex-M4 استفاده شده است. این میکروکنترلر به‌دلیل توان پردازشی مناسب، مصرف انرژی قابل‌کنترل و ابزارهای اندازه‌گیری دقیق زمان اجرا و توان مصرفی، انتخاب شده است. بنابراین این مقاله سه فرضیه را بررسی می‌کند:

۱. افزودن مدل‌های امنیتی، بر عملکرد لایه سنجش سیستم اینترنت اشیا تحت سیستم ابر تأثیر مستقیم دارد.
۲. افزودن مدل‌های امنیتی، بر عملکرد لایهٔ انتقال سیستم اینترنت اشیا تحت سیستم ابر تأثیر مستقیم دارد.
۳. افزودن مدل‌های امنیتی، بر عملکرد لایهٔ کاربرد سیستم اینترنت اشیا تحت سیستم ابر تأثیر مستقیم دارد.

## تاپسیس فازی

تاپسیس یکی از روش‌های تصمیم‌گیری چند شاخصه است که معیار، رتبه‌بندی می‌کند. مبنای این روش، انتخاب گزینه‌ای است که کمترین فاصله را از جواب ایدئال مطلوب و بیشترین فاصله را از جواب ایدئال نامطلوب دارد. از طرفی دیگر، از آنجا که داده‌های یک فرایند تولید و یا یک مکانیزه خدمت‌رسانی، معمولاً پیچیده بوده و جمع‌آوری داده‌های صحیح از آن‌ها مشکل است، به نظر می‌رسد که برای کار با داده‌های غیرقطعی یا بازه‌ای از داده‌ها، باید روش‌های ویژه‌ای مورداستفاده قرار گیرد. ازاین‌رو، می‌توان از منطق فازی در تکنیک‌های تصمیم‌گیری مختلف استفاده کرد و از مزایای آن بهره‌مند شد. یکی از این روش‌ها، فن تاپسیس است که با کاربرد منطق فازی در آن، به فن تاپسیس فازی تبدیل می‌شود که روشی متفاوت از روش تاپسیس دارد. مبرهن است که منطق اصلی استفاده از تکنیک‌های تصمیم‌گیری به‌صورت فازی، تأثیرگذاری عدم قطعیت توأم با تفکرات آدمی، در تصمیم‌گیری‌ها هست.

هدف روش تاپسیس فازی در این مطالعه، رتبه‌بندی گزینه‌های موجود با توجه به معیارهای موردنظر در محیطی فازی و نادقیق است. در این پژوهش، متغیرهای گفتاری برای اهمیت وزن‌های فاکتورها به‌صورت خیلی زیاد (VH)، زیاد (H)، تا حد زیاد (MH)، بی‌تفاوت (M)، تا حدی کم (ML) ،کم (L) و خیلی کم (VL) است. همچنین متغیرهای گفتاری برای میزان معیارهای هر گزینه به‌صورت خیلی خوب (VG)، خوب (G)، تا حدی خوب (MG)، بی‌تفاوت (F)، تا حدی ضعیف (MP)، ضعیف (P) و خیلی ضعیف (VP) است. در میان انواع گوناگون اعداد فازی، اعداد فازی ذوزنقه‌ای، کاربرد بیشتری دارند. بدین منظور داده‌های موردنیاز روش پیشنهادی را به‌صورت ذوزنقه‌ای فرض کرده‌ایم.

## احراز هویت متقابل

در طرح پیشنهادی ما، یک سازوکار احراز هویت متقابل بین مشترک، کارگزار و ناشر پیاده‌سازی شده است که از مقادیر تصادفی استفاده می‌کند. روند به شرح زیر است.

در این طرح، هنگامی‌که پیام M1 از مشترک دریافت می‌شود، کارگزار شناسه‌های R1 = C10 را محاسبه می‌کند، $R1 = C10 \oplus IDs, C1\acute{1} = h[(S_s) \parallel R1]C1\acute{1} = [h(IDs)[r_s + s] \parallel R1]$ اگر $C11 = C1\acute{1}$ باشد، کارگزار مشترک را احراز هویت می‌کند. علاوه‌براین، پس از دریافت پیام M3، از ناشر، کارگزار $R3 = C140 \oplus IDp, \acute{X} = [S_p(GR2 + Gr_P \parallel R3 \parallel T3]$ را محاسبه می‌کند که در آن GR2 گواهی عمومی کارگزار و $Gr_P$ گواهی عمومی ناشر است.

اگر X = X0 باشد، کارگزار ناشر را احراز هویت می‌کند. پس از اینکه ناشر پیام M4 را از کارگزار دریافت کرد، ناشر $R2 = W \oplus C8, \acute{B} = GR3(s + r_P), \acute{B} = R3G_s + R3G_P$ را محاسبه می‌کند که در آن R3 برای ناشر شناخته شده است، Gs گواهی عمومی کارگزار و Grp گواهی عمومی ناشر است. ناشر بررسی می‌کند که آیا $B = \acute{B}$ است یا خیر. در این صورت، ناشر کارگزار را احراز هویت می‌کند. پس از دریافت پیام M5 از کارگزار، مشترک $R3 = C15 \oplus r_s, R2 = C16 \oplus C4$ و $\acute{Y} = [GR1\ r_s \parallel R2]$ که در آن Gr s گواهی عمومی S است و R1 برای مشترک شناخته شده است. اگر $Y = \acute{Y}$ باشد، مشترک کارگزار را احراز هویت می‌کند.

### رمزنگاری سبک‌وزن مدل سایمون

در این مقاله از مدل امنیتی سایمون خانواده‌ای از رمزهای بلوکی سبک‌وزن که توسط آژانس امنیت ملی (NSA) در ژوئن ۲۰۱۳ به‌طور عمومی منتشر شد، استفاده شده است. سایمون با ده رمز بلوکی مجزا با اندازه‌های بلوک و کلید متفاوت ارائه می‌شود. اکثر رمزهای بلوکی موجود برای عملکرد خوب در یک پلتفرم واحد طراحی شده‌اند و قرار نیست عملکرد بالایی را در طیف وسیعی از دستگاه‌ها ارائه دهند. هدف سایمون، رفع نیاز به رمزهای بلوکی سبک‌وزن، انعطاف‌پذیر و قابل‌تحلیل بود. هرکدام عملکرد عالی در پلتفرم‌های سخت‌افزاری و نرم‌افزاری ارائه می‌دهند، به اندازه کافی انعطاف‌پذیرند که انواع پیاده‌سازی‌ها را در یک پلتفرم خاص بپذیرند و با استفاده از تکنیک‌های موجود قابل تجزیه‌وتحلیل هستند. هر دو در طیف کاملی از برنامه‌های سبک‌وزن عملکرد بسیار خوبی دارند، سایمون برای عملکرد در پیاده‌سازی‌های سخت‌افزاری بهینه شده است، دلیل اینکه این الگوریتم‌ها در هر پلتفرم به خوبی کار می‌کنند این است که ساختار بسیار ساده‌ای دارد. بنابراین یافتن پیاده‌سازی‌های کارآمد بسیار آسان است. برای الگوریتم‌هایی مانند AES، یافتن پیاده‌سازی‌های تقریباً بهینه به زمان تحقیق طولانی‌تری نیاز داشت. رمزگذاری بلوکی سایمون با یک کلمه n بیتی (و بنابراین یک بلوک n۲ بیتی) با n2Simon نشان داده می‌شود که در آن n باید ۱۶، ۲۴، ۳۲، ۴۸ یا ۶۴ باشد. n2Simon با کلید word-m (bit-mn) به‌صورت mn/n2simon نامیده می‌شود. برای مثال، ۱۲۸/۶۴Simon به نسخه‌ای از Simon اشاره دارد که روی بلوک‌های متن ساده ۶۴ بیتی عمل می‌کند و از یک کلید ۱۲۸ بیتی استفاده می‌کند (اپل و همکاران[1]، ۲۰۱۶).

1. Appel et al.

$$..١١١١١٠١٠٠٠١٠٠١٠١٠١١٠٠٠٠١١١٠٠١١٠ = ...{}_{٢}u_{١}u.u = u,$$
$$..١٠٠٠١١١٠١١١١١٠٠١٠٠١١٠٠٠٠١٠١١٠١٠ = ...{}_{٢}v_{١}v.v = v,$$
$$....١٠٠٠٠١٠٠١٠١١٠٠١١١١١٠٠٠١١٠١١١٠١٠ = ...{}_{٢}w_{١}w.w = w$$

## یافته‌های پژوهش

### تحلیل تاپسیس فازی

فرضیه: افزودن مدل‌های امنیتی بر عملکرد لایه سنجش سیستم اینترنت اشیا تحت سیستم ابر تأثیر مستقیم دارد.

در جدول ۱ شاخص‌های این لایه همراه با توصیف آن‌ها ارائه شده است.

جدول ۱. شاخص‌های لایهٔ ادراک در مدل ابر

| هدف | شاخص | توصیف | عامل اصلی تأثیر |
|---|---|---|---|
| قابلیت اطمینان آگاه | قابلیت اطمینان تجهیزات (۱a) | احتمال کار بدون مشکل تجهیزات | محیط کار سطح فرایند |
| | این شاخص به احتمال اینکه تجهیزات بدون مشکل و با کارایی بالا عمل کنند، اشاره دارد. عوامل محیطی و سطح فرایند می‌توانند بر این قابلیت اطمینان تأثیر بگذارند. | | |
| | دقت ادراک‌شده (۲a) | درصد اطلاعات صحیح نسبت به کل اطلاعات | محیط کار عملکرد تجهیزات سازوکار و توافق |
| | این پارامتر نشان‌دهنده نسبت اطلاعات صحیح به کل اطلاعات دریافتی است. دقت بالا به‌معنای توانایی سیستم در ارائه اطلاعات دقیق و قابل اعتماد است که تحت تأثیر محیط کار، عملکرد تجهیزات و توافقات موجود قرار دارد. | | |
| | دامنهٔ ادراکی(۳a) | میزان پوشش‌دهی مؤثر تجهیزات | عملکرد تجهیزات محیط کار |
| | این شاخص به میزان پوشش‌دهی مؤثر تجهیزاتی که در سیستم استفاده می‌شوند، اشاره دارد. عملکرد تجهیزات و شرایط محیط کار می‌توانند بر این دامنه تأثیر بگذارند. | | |
| | سرعت درک شده (۴a) | توانایی درک سریع و دقیق اطلاعات | عملکرد تجهیزات محیط کار |
| | این پارامتر به توانایی سیستم در ارائه و پردازش سریع اطلاعات اشاره دارد. سرعت بالای درک اطلاعات می‌تواند به بهبود عملکرد کلی سیستم کمک کند و تحت تأثیر عملکرد تجهیزات و محیط کار قرار دارد. | | |

منبع: سطحی، آرکو و کرنانن[1] (۲۰۱۶)؛ الدولایمی و همکاران[2]، ۲۰۲۴

1. Sethi, Arkko & Keränen
2. Al-Dulaimy et al.

**شاخص‌ها**

- قابلیت اطمینان تجهیزات
- دقت ادراک‌شده
- دامنهٔ ادراکی
- سرعت درک شده

به‌طور خلاصه الگوریتم تاپسیس فازی به‌صورت زیر بیان می‌شود:

**گام۱:** تشکیل یک تیم تصمیم‌گیری و سپس تعیین گزینه‌ها و معیارهای ارزیابی آن‌ها.

**گام۲:** تعیین اهمیت معیارها توسط هر تصمیم‌گیرنده با استفاده از متغیرهای گفتاری از پیش تعیین‌شده. گام‌های ۱ و۲ با تشکیل پرسش‌نامه و جمع‌آوری اطلاعات انجام شد.

**گام۳:** تعیین نرخ‌های گزینه‌ها با توجه به هر معیار با استفاده از متغیرهای گفتاری از پیش تعیین‌شده.

**گام۴:** تشکیل ماتریس تصمیم‌گیری فازی.

محاسبه وزن در AHP در دو قسمت جداگانه موردبحث قرار می‌گیرد: وزن نسبی و وزن مطلق (نهایی). وزن نسبی از ماتریس مقایسهٔ زوجی به‌دست می‌آید، درحالی‌که وزن مطلق، رتبه نهایی هر گزینه است که از تلفیق وزن‌های نسبی محاسبه می‌شود. یکی از راه‌های محاسبه وزن نسبی در ماتریس‌های ناسازگار، استفاده از روش‌های تقریبی است. از جمله این روش‌ها می‌توان به روش میانگین هندسی اشاره کرد. هدف این بخش، بسط و توسعه این روش برای محاسبه وزن نسبی عناصر فازی ماتریس‌های مقایسات زوجی است. مراحل به‌کارگیری این روش برای استفاده از اعداد فازی مثلثی یا ذوزنقه‌ای به‌صورت زیر است:

- داده‌های ماتریس مقایسهٔ زوجی را به‌صورت اعداد فازی مثلثی (یا ذوزنقه‌ای) به‌دست می‌آید؛
- داده‌های فازی هر ستون به‌صورت نرمال درمی‌آید؛
- میانگین هندسی داده‌های نرمال شده محاسبه می‌شود تا وزن نسبی عناصر به‌صورت فازی به‌دست آید.

حال ارزیابی‌های به‌دست‌آمده در گام‌های دوم و سوم را به اعداد فازی ذوزنقه‌ای متناسب با آن تبدیل نموده تا ماتریس تصمیم‌گیری فازی و اعداد فازی وزن‌های گزینه‌ها به‌دست آید که نتایج در جدول ۲ نشان داده شده است:

جدول ۲. محاسبه میانگین هندسی و اوزان فازی نظرات خبرگان در لایهٔ ادراک IoT

| گزینه‌ها | میانگین هندسی فازی سطرها | | | وزن فازی معیارها | | |
|---|---|---|---|---|---|---|
| | r | | | w | | |
| قابلیت اطمینان آگاه از اطلاعات | ۳/۷۴۲۷ | ۴/۴۰۳ | ۵/۰۰۰ | ۰/۳۸۹ | ۰/۵۲۹ | ۰/۷۰۵ |
| قابلیت اطمینان تجهیزات | ۱/۶۰۵۴ | ۱/۸۸۴۲ | ۲/۱۴۸ | ۰/۱۶۷ | ۰/۲۲۶ | ۰/۳۰۳ |
| دقت ادراک‌شده | ۱/۲۰۱۳ | ۱/۴۲۵۲ | ۱/۷۶۷ | ۰/۱۲۵ | ۰/۱۷۱ | ۰/۲۴۹ |
| دامنهٔ ادراکی | ۰/۳۴۸۱ | ۰/۳۹۲۹ | ۰/۴۴۳۴ | ۰/۰۳۶ | ۰/۰۴۷ | ۰/۰۶۲ |
| سرعت درک شده | ۰/۱۹۲۳ | ۰/۲۱۵۱ | ۰/۲۴۵۷ | ۰/۰۲۰ | ۰/۰۲۵ | ۰/۰۳۴ |

**گام ۵:** محاسبهٔ وزن قطعی عناصر

جدول ۳. محاسبه اوزان قطعی نظرات خبرگان در لایهٔ ادراک IoT

| گزینه‌ها | وزن فازی معیارها | | | وزن قطعی معیارها |
|---|---|---|---|---|
| | w | | | BNP |
| قابلیت اطمینان آگاه از اطلاعات | ۰/۳۸۹۶۵۲ | ۰/۵۲۹۱۹۴ | ۰/۷۰۵۲۷ | ۰/۵۴۱۳۷۱۹۶۶ |
| قابلیت اطمینان تجهیزات | ۰/۱۶۷۱۳۷ | ۰/۲۲۶۴۴۳ | ۰/۳۰۳۰۸۳ | ۰/۲۳۲۲۲۱۰۳۵ |
| دقت ادراک‌شده | ۰/۱۲۵۰۶۷ | ۰/۱۷۱۲۸۱ | ۰/۲۴۹۲۳۲ | ۰/۱۸۱۸۵۹۸۳۴ |
| دامنهٔ ادراکی | ۰/۰۳۶۲۴۹ | ۰/۰۴۷۲۲۱ | ۰/۰۶۲۵۳۸ | ۰/۰۴۸۶۶۹۴۳۷ |
| سرعت درک شده | ۰/۰۲۰۰۲۲ | ۰/۰۲۵۸۶۲ | ۰/۰۳۴۶۵۶ | ۰/۰۲۶۸۴۶۷ |

**گام۶:** تشکیل ماتریس تصمیم‌گیری فازی نرمال شده.

جدول ۴. ماتریس نرمال شده در لایهٔ ادراک IoT

| | A | B | C | D | E |
|---|---|---|---|---|---|
| A | ۰/۵۸۲۵۷ | ۰/۸۳۴۹۸۹ | ۰/۴۱۴۱۵ | ۰/۳۲۶۲۵۸ | ۰/۲۷۹۶۶۲ |
| B | ۰/۰۷۲۵۹۲ | ۰/۱۰۳۲۳۷ | ۰/۴۱۶۲۷۹ | ۰/۳۱۳۱۹۹ | ۰/۲۷۲۱۱۵ |
| C | ۰/۲۰۰۲۵۱ | ۰/۰۳۵۲۴۸ | ۰/۱۳۳۷۷ | ۰/۳۱۱۷۲۸ | ۰/۲۵۲۶۰۱ |
| D | ۰/۰۷۱۹۹۵ | ۰/۰۱۳۲۹۹ | ۰/۰۱۷۳۱۵ | ۰/۰۴۰۰۱۱ | ۰/۱۶۱۰۴۵ |
| E | ۰/۰۷۲۵۹۲ | ۰/۰۱۳۲۲۷ | ۰/۰۱۸۴۸۶ | ۰/۰۰۸۸۰۴ | ۰/۰۳۴۵۷۷ |

**گام۷:** تشکیل ماتریس تصمیم‌گیری فازی نرمال وزین شده.

جدول ۵. مشخص ساختن وزن ماتریس نرمال شده در لایهٔ ادراک IoT

| | A | B | C | D | E | MEAN | |
|---|---|---|---|---|---|---|---|
| A | ۰/۵۸۲۵۷ | ۰/۸۳۴۹۸۹ | ۰/۴۱۴۱۵ | ۰/۳۲۶۲۵۸ | ۰/۲۷۹۶۶۲ | ۰/۴۸۷۵۲۶ | |
| B | ۰/۰۷۲۵۹۲ | ۰/۱۰۳۲۳۷ | ۰/۴۱۶۲۷۹ | ۰/۳۱۳۱۹۹ | ۰/۲۷۲۱۱۵ | ۰/۲۳۵۴۸۴ | |
| C | ۰/۲۰۰۲۵۱ | ۰/۰۳۵۲۴۸ | ۰/۱۳۳۷۷ | ۰/۳۱۱۷۲۸ | ۰/۲۵۲۶۰۱ | ۰/۱۸۶۷۱۹ | وزن معیارها |
| D | ۰/۰۷۱۹۹۵ | ۰/۰۱۳۲۹۹ | ۰/۰۱۷۳۱۵ | ۰/۰۴۰۰۱۱ | ۰/۱۶۱۰۴۵ | ۰/۰۶۰۷۳۳ | |
| E | ۰/۰۷۲۵۹۲ | ۰/۰۱۳۲۲۷ | ۰/۰۱۸۴۸۶ | ۰/۰۰۸۸۰۴ | ۰/۰۳۴۵۷۷ | ۰/۰۲۹۵۳۷ | |

**گام۸:** تشکیل ماتریس غیر فازی شده

جدول ۶. ماتریس غیرفازی شده در لایهٔ ادراک IoT

| | A | B | C | D | E |
|---|---|---|---|---|---|
| A | ۱ | ۸/۰۸۸۱۰۲ | ۳/۰۹۵۹۹۳ | ۸/۱۵۴۲۸۱ | ۸/۰۸۸۱۰۲ |
| B | ۰/۱۲۴۶۰۶ | ۱ | ۳/۱۱۱۹۱۵ | ۷/۸۲۷۹۰۶ | ۷/۸۶۹۸۴۵ |
| C | ۰/۳۴۳۷۳۷ | ۰/۳۴۱۴۲۷ | ۱ | ۷/۷۹۱۱۳۷ | ۷/۳۰۵۴۶۴ |
| D | ۰/۱۲۳۵۸۲ | ۰/۱۲۸۸۲۲ | ۰/۱۲۹۴۴ | ۱ | ۴/۶۵۷۵۹۷ |
| E | ۰/۱۲۴۶۰۶ | ۰/۱۲۸۱۲۴ | ۰/۱۳۸۱۹۶ | ۰/۲۲۰۰۴ | ۱ |
| | ۱/۷۱۶۵۳۲ | ۹/۶۸۶۴۷۵ | ۷/۴۷۵۵۴۴ | ۲۴/۹۹۳۳۶ | ۲۸/۹۲۱۰۱ |

**گام۹:** محاسبه ضریب سازگاری.

نسبت سازگاری ۰/۱ یا کمتر سازگاری در مقایسات را بیان می‌کند که بنا به مقدار به‌دست آمده (۰/۰۰۲<۰/۱) سازگاری در مقایسات تأیید می‌شود.

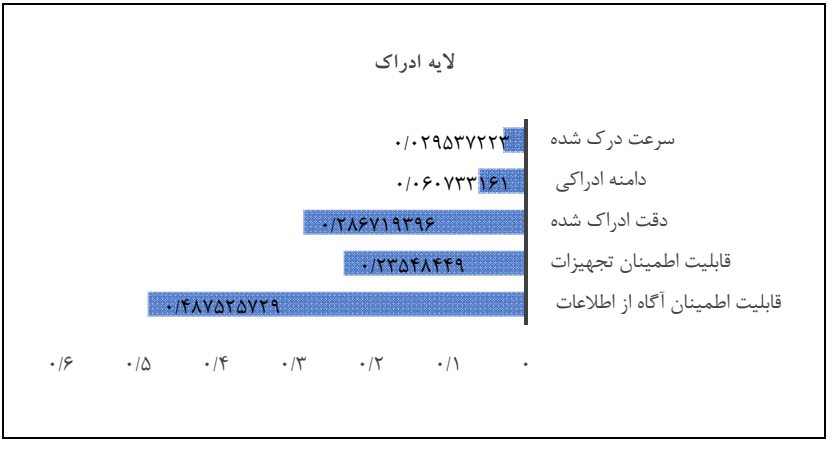
λ >>>>> ۶/۱۸۱۳۱

CI >>>>> ۰/۲۹۵۳۲۷

CR >>>> ۰/۰۲۴۶۱

n = ۵, RI = ۱/۱۲

**گام۱۰:** رتبه‌بندی گزینه‌ها




شکل ۵. اولویت مربوط به عملکرد لایهٔ ادراک

و به این ترتیب اولویت‌ها به شرح زیر مشخص می‌شود.

۱. قابلیت اطمینان آگاه از اطلاعات
۲. دقت ادراک‌شده
۳. قابلیت اطمینان تجهیزات
۴. دامنهٔ ادراکی
۵. سرعت درک شده

در این لایه از دو مدل امنیتی استفاده شده است:

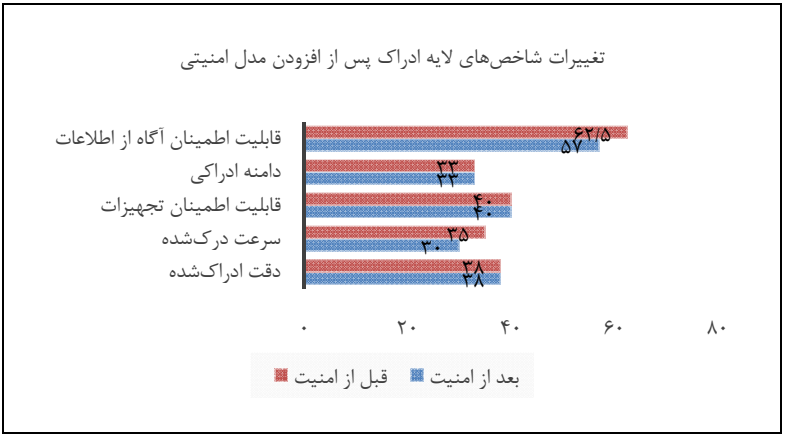
- رمزنگاری سبک‌وزن[1] سایمون
- احراز هویت متقابل[2]

تغییرات عملکرد لایهٔ ادارک قبل و بعد از افزودن این مدل‌های در جدول ۷ ارائه شده است.

جدول ۷. نتایج آزمایش شبیه‌سازی افزودن مدل‌های امنیتی در لایهٔ ادراک

| شاخص | قبل از امنیت | بعد از امنیت | تغییر (%) |
|---|---|---|---|
| دقت ادراک‌شده | ۳۸/۰ | ۳۸/۰ | ۰ |
| سرعت درک‌شده | ۳۵/۰ | ۳۰/۰ | ۵- ↓ |
| قابلیت اطمینان تجهیزات | ۴۰/۰ | ۴۰/۰ | ۰ |
| دامنهٔ ادراکی | ۳۳/۰ | ۳۳/۰ | ۰ |
| قابلیت اطمینان آگاه از اطلاعات | ۶۲/۵ | ۵۷/۰ | ۵/۵- ↓ |

تغییرات مربوط به پارامترهای شاخص لایهٔ ادراک نیز در شکل ۶ نشان داده شده است.




شکل ۶. افزودن مدل‌های امنیتی به لایهٔ ادراک

1. Lightweight Encryption
2. Mutual Authentication

افزودن هم‌زمان دو مدل امنیتی شامل رمزنگاری سبک‌وزن سایمون و احراز هویت متقابل، عملکرد لایهٔ ادراک از نظر امنیتی بهبود یافته است. شاخص‌هایی مانند سرعت درک‌شده و قابلیت اطمینان آگاه از اطلاعات کاهش جزئی داشته‌اند؛ اما این افت عملکرد در برابر کاهش نرخ موفقیت حمله‌ها و افزایش امنیت کلی سیستم، قابل قبول و توجیه‌پذیر است.

**فرضیه:** افزودن مدل‌های امنیتی بر عملکرد لایهٔ انتقال سیستم اینترنت اشیا تحت سیستم ابر تأثیر مستقیم دارد.

جدول ۸. شاخص‌های لایهٔ انتقال در مدل ابر

| هدف | شاخص | توصیف | عامل اصلی تأثیر |
|---|---|---|---|
| قابلیت اطمینان انتقال اطلاعات | ارتباط شبکه (t1) | احتمال اتصال همه گره‌ها | عملکرد ترمینال توپولوژی شبکه |
| | این شاخص به احتمال برقراری ارتباط بین تمامی گره‌های موجود در شبکه اشاره دارد. هرچه تعداد گره‌ها بیشتر باشد و ارتباط بین آن‌ها پایدارتر باشد، قابلیت اطمینان بیشتر خواهد بود. | | |
| | تأخیر پایان به پایان انتقال داده (t2) | تأخیر در انتقال داده‌ها | توپولوژی شبکه، محیط کار |
| | این شاخص نشان‌دهنده زمان لازم برای انتقال داده از منبع به مقصد است. تأخیر کمتر به‌معنای عملکرد بهتر شبکه است. | | |
| | ظرفیت شبکه (t3) | حداکثر ظرفیت انتقال داده‌های شبکه | محیط کار<br>تغییر توپولوژیک |
| | این پارامتر بیانگر حداکثر میزان داده‌ای است که شبکه قادر به انتقال در واحد زمان است. ظرفیت بالاتر به‌معنای توانایی بیشتر در مدیریت ترافیک داده‌ها است. | | |
| | نرخ خطا (t4) | احتمال خطای انتقال داده‌ها | محیط کار |
| | این شاخص به احتمال وقوع خطا در انتقال داده‌ها اشاره دارد. نرخ خطای پایین به‌معنای عملکرد بهتر و قابل اعتمادتر شبکه است. | | |
| | قابلیت اطمینان پایان(t5) | احتمال کار عادی پایان به پایان | توپولوژی شبکه محیط کار عملکرد تجهیزات |
| | این پارامتر نشان‌دهنده احتمال اینکه سیستم به‌طور عادی و بدون مشکل عمل کند، می‌باشد. عواملی مانند توپولوژی شبکه، محیط کار و عملکرد تجهیزات بر این شاخص تأثیر می‌گذارند. | | |

منبع: (مین و همکاران، ۲۰۲۴؛ الدولایمی و همکاران، ۲۰۲۴)

جدول ۹. محاسبه میانگین هندسی و وزن‌های فازی و وزن‌های قطعی نظرهای خبرگان در لایهٔ انتقالIoT

| وزن قطعی معیارها | وزن فازی معیارها | | | میانگین هندسی فازی سطرها | | |
|---|---|---|---|---|---|---|
| BNP | w | | | r | | |
| ۰/۴۰۷۲۲۶۴۱۹ | ۰/۶۶۵۱۵۱ | ۰/۳۷۰۸۸۸ | ۰/۱۸۵۶۴ | ۲/۸۷۱۷۵۹ | ۲/۲۰۶۷۸۸ | ۱/۴۵۳۹۲۵ |
| ۰/۳۰۸۹۲۵۲۰۷ | ۰/۴۸۹۰۶۸ | ۰/۲۷۹۳۳۵ | ۰/۱۵۸۳۷۲ | ۲/۱۱۱۵۳ | ۱/۶۶۲۰۴۷ | ۱/۲۴۰۳۶۴ |
| ۰/۱۴۶۱۳۷۱۰۵ | ۰/۲۳۴۷۲۷ | ۰/۱۳۰۱۴۸ | ۰/۰۷۳۵۳۶ | ۱/۰۱۳۴۲۳ | ۰/۷۷۴۳۸۲ | ۰/۵۷۵۹۳۳ |
| ۰/۱۸۴۵۲۵۰۶۱ | ۰/۳۰۳۳۹ | ۰/۱۵۵۷۹۶ | ۰/۰۹۴۳۸۹ | ۱/۳۰۹۸۷۴ | ۰/۹۲۶۹۸۵ | ۰/۷۳۹۲۵۲ |
| ۰/۰۷۴۹۴۶۶۰۴ | ۰/۱۲۱۶۸۲ | ۰/۰۶۳۸۳۴ | ۰/۰۳۹۳۲۴ | ۰/۵۲۵۳۵۸ | ۰/۳۷۹۸۱۱ | ۰/۳۰۷۹۸۱ |

تشکیل ماتریس تصمیم‌گیری فازی نرمال شده.

جدول ۱۰. ماتریس نرمال شده در لایهٔ انتقالIoT

| | A | B | C | D | E |
|---|---|---|---|---|---|
| A | ۰/۳۷۶۵۶۴ | ۰/۵۷۶۲۲۱ | ۰/۲۰۱۳۰۹ | ۰/۲۹۵۰۷۶ | ۰/۱۹۱۰۷۱ |
| B | ۰/۱۳۸۷۸۱ | ۰/۱۹۸۲۹۳ | ۰/۶۳۲۹۷۶ | ۰/۲۳۹۹۹ | ۰/۱۵۳۳۹۱ |
| C | ۰/۱۷۴۹۷۳ | ۰/۰۲۶۴۶۶ | ۰/۰۸۳۷۳ | ۰/۳۲۲۴۴۴ | ۰/۱۱۸۷۳۱ |
| D | ۰/۱۸۰۶۳۷ | ۰/۱۱۲۸۵۲ | ۰/۰۳۶۱۷ | ۰/۱۲۶۳۲ | ۰/۴۷۶۳۳۳ |
| E | ۰/۱۲۹۰۴۴ | ۰/۰۸۶۱۶۹ | ۰/۰۴۵۸۱۵ | ۰/۰۱۶۱۷ | ۰/۰۶۰۴۷۴ |

تشکیل ماتریس تصمیم‌گیری فازی نرمال وزین شده.

جدول ۱۱. مشخص ساختن وزن ماتریس نرمال شده در لایهٔ انتقالIoT

| | A | B | C | D | E | MEAN | |
|---|---|---|---|---|---|---|---|
| A | ۰/۳۷۶۵۶۴ | ۰/۵۷۶۲۲۱ | ۰/۲۰۱۳۰۹ | ۰/۲۹۵۰۷۶ | ۰/۱۹۱۰۷۱ | ۰/۳۲۸۰۴۸ | وزن معیارها |
| B | ۰/۱۳۸۷۸۱ | ۰/۱۹۸۲۹۳ | ۰/۶۳۲۹۷۶ | ۰/۲۳۹۹۹ | ۰/۱۵۳۳۹۱ | ۰/۲۷۲۶۸۶ | |
| C | ۰/۱۷۴۹۷۳ | ۰/۰۲۶۴۶۶ | ۰/۰۸۳۷۳ | ۰/۳۲۲۴۴۴ | ۰/۱۱۸۷۳۱ | ۰/۱۴۵۲۶۹ | |
| D | ۰/۱۸۰۶۳۷ | ۰/۱۱۲۸۵۲ | ۰/۰۳۶۱۷ | ۰/۱۲۶۳۲ | ۰/۴۷۶۳۳۳ | ۰/۱۸۶۴۶۲ | |
| E | ۰/۱۲۹۰۴۴ | ۰/۰۸۶۱۶۹ | ۰/۰۴۵۸۱۵ | ۰/۰۱۶۱۷ | ۰/۰۶۰۴۷۴ | ۰/۰۶۷۵۳۴ | |

تشکیل ماتریس غیر فازی شده

جدول ۱۲. ماتریس غیرفازی شده در لایهٔ انتقالIoT

| | A | B | C | D | E |
|---|---|---|---|---|---|
| A | ۱ | ۲/۹۰۵۹۱۲ | ۲/۴۰۴۲۶۸ | ۲/۳۳۵۹۵۱ | ۳/۱۵۹۵۶۸ |
| B | ۰/۳۶۸۵۴۶ | ۱ | ۷/۵۵۹۷۴۱ | ۱/۸۹۹۸۶۵ | ۲/۵۳۶۴۹ |
| C | ۰/۴۶۴۶۵۷ | ۰/۱۳۳۴۷ | ۱ | ۲/۵۵۲۶۰۱ | ۱/۹۶۳۳۵۳ |
| D | ۰/۴۷۹۶۹۹ | ۰/۵۶۹۱۱۷ | ۰/۴۳۱۹۹ | ۱ | ۷/۸۷۶۶۸۱ |
| E | ۰/۳۴۲۶۸۸ | ۰/۴۳۴۵۵۳ | ۰/۵۴۷۱۷۸ | ۰/۱۲۸۰۱ | ۱ |
| | ۲/۶۵۵۵۹ | ۵/۰۴۳۰۵۳ | ۱۱/۹۴۳۱۸ | ۷/۹۱۶۴۲۷ | ۱۶/۵۳۶۰۹ |

محاسبهٔ ضریب سازگاری.

λ >>>>>۶/۴۳۲۱۳۹

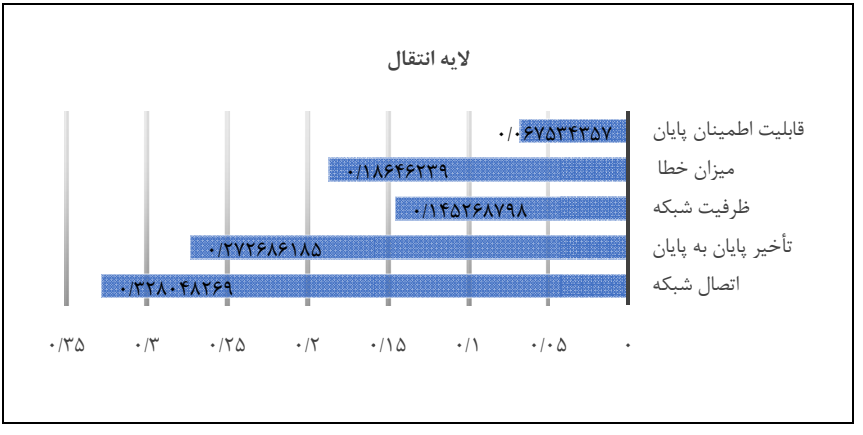
CI >>>>> ۰/۳۵۸۰۳۵

CR >>>> ۰/۰۰۹۶۷

n = ۵, RI = ۱/۱۲

که بنا به مقدار به‌دست آمده (۰/۱>۰/۰۰۹) سازگاری در مقایسات تأیید می‌شود.

در نهایت نیز رتبه‌بندی گزینه‌ها در نمودار ۶ ارائه‌شده است:




شکل ۷. اولویت مربوط به عملکرد لایهٔ انتقال

۱. اتصال شبکه
۲. تأخیر پایان به پایان
۳. میزان خطا

۴. ظرفیت شبکه

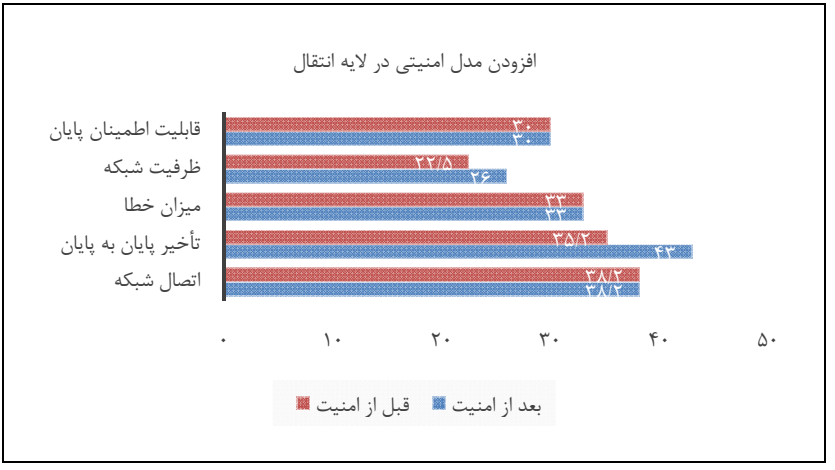
۵. قابلیت اطمینان پایان

در جدول ۱۳ تغییرات مربوط به عملکرد لایهٔ انتقال پس از افزودن دو مدل امنیتی نشان داده شده است.

جدول ۱۳. نتایج آزمایش شبیه‌سازی افزودن مدل‌های امنیتی در لایهٔ انتقال

| شاخص | قبل از امنیت | بعد از امنیت | تغییر (%) |
|---|---|---|---|
| اتصال شبکه | ۳۸/۲ | ۳۸/۲ | ۰ |
| تأخیر پایان به پایان | ۳۵/۲ | ۴۳/۰ | ۷/۸ ↑ |
| میزان خطا | ۳۳/۰ | ۳۳/۰ | ۰ |
| ظرفیت شبکه | ۲۶/۰ | ۲۲/۵ | -۴/۵ ↓ |
| قابلیت اطمینان پایان | ۳۰/۰ | ۳۰/۰ | ۰ |

تغییرات مربوط به پارامترهای شاخص لایهٔ انتقال نیز در شکل ۸ نشان داده شده است.




شکل ۸. افزودن مدل‌های امنیتی به لایهٔ انتقال

نتایج شبیه‌سازی نشان می‌دهد که اگرچه تأخیر پایان به پایان به میزان ۷/۸درصد افزایش یافته و ظرفیت شبکه با کاهش ۵/۴درصد مواجه شده است، سایر شاخص‌ها از جمله اتصال شبکه، میزان خطا و قابلیت اطمینان پایان ثابت باقی مانده‌اند. این تغییرات نشان می‌دهد که افزودن سازوکارهای امنیتی، بر پایداری و قابلیت اطمینان تأثیر چشمگیری ندارد و افزایش تأخیر نیز در محدوده‌ای قابل قبول و در ازای افزایش امنیت توجیه‌پذیر است.

**فرضیه:** افزودن مدل‌های امنیتی بر عملکرد لایهٔ کاربرد سیستم اینترنت اشیا تحت سیستم ابر تأثیر مستقیم دارد.

جدول ۱۴. شاخص‌های لایهٔ کاربرد

| هدف | شاخص | توصیف | عامل اصلی تأثیر |
|---|---|---|---|
| قابلیت اطمینان پردازش اطلاعات | عملکرد ایمنی اطلاعات (P۱) | امنیت سیستم | سازوکار و پردازش قابلیت اطمینان سطح توافق‌نامه، محیط کار |
| | این شاخص به امنیت سیستم و حفاظت از داده‌ها اشاره دارد. در یک سیستم اطلاعاتی، اطمینان از اینکه داده‌ها به درستی محافظت می‌شوند، بسیار مهم است. این قابلیت تحت تأثیر سازوکارها و فرایندهای امنیتی، سطح توافق‌نامه‌های امنیتی و شرایط محیط کار قرار دارد. | | |
| | سرعت پردازش (P۲) | زمان پردازش رویداد (مدت زمان لازم برای پردازش اطلاعات و رویدادها) | عملکرد تجهیزات |
| | این پارامتر مدت زمانی را که سیستم برای پردازش اطلاعات و رویدادها نیاز دارد، اندازه‌گیری می‌کند. سرعت بالای پردازش می‌تواند به افزایش کارایی سیستم کمک کند و معمولاً تحت تأثیر عملکرد تجهیزات قرار دارد | | |
| | دقت پردازش (p۳) | احتمال عدم خطا (احتمال بروز خطا در پردازش اطلاعات ) | عملکرد تجهیزات |
| | این شاخص نشان‌دهنده احتمال بروز خطا در حین پردازش اطلاعات است. دقت بالا به‌معنای توانایی سیستم در ارائه نتایج صحیح و قابل اعتماد است و معمولاً به عملکرد تجهیزات بستگی دارد. | | |
| | تحمل خطا و سازگاری (P۴) | توانایی مدیریت وضعیت غیرعادی (قابلیت سیستم در مواجهه با وضعیت‌های غیرعادی و حفظ عملکرد) | عملکرد تجهیزات عملکرد محیط کار |
| | این پارامتر به قابلیت سیستم در مواجهه با وضعیت‌های غیرعادی اشاره دارد. یک سیستم با تحمل خطای بالا می‌تواند در شرایط بحرانی یا غیرمنتظره به کار خود ادامه دهد و عملکرد خود را حفظ کند. این عامل تحت تأثیر عملکرد تجهیزات و شرایط محیط کار قرار دارد. | | |

منبع: (کرکاس، وینتر و رایشرت[1]، ۲۰۲۴؛ لی و همکاران، ۲۰۲۴)

1. Kirikkayis, Winter & Reichert

جدول ۱۵. محاسبه میانگین هندسی و وزن‌های فازی و وزن‌های قطعی نظرهای خبرگان در لایهٔ کاربرد IoT

| وزن قطعی معیارها | وزن فازی معیارها | | | میانگین هندسی فازی سطرها | | |
|---|---|---|---|---|---|---|
| BNP | w | | | r | | |
| ۰/۶۷۵۲۹ | ۰/۸۶۰ | ۰/۶۶۰ | ۰/۵۰۴ | ۴/۴۸۳۲ | ۴/۰۱۹۷ | ۳/۵۱۹۳ |
| ۰/۱۶۱۷۷ | ۰/۲۲۰ | ۰/۱۵۷ | ۰/۱۰۶ | ۱/۱۵۰۶ | ۰/۹۵۸ | ۰/۷۴۵ |
| ۰/۱۳۲۴۱ | ۰/۱۷۸ | ۰/۱۲۵ | ۰/۰۹۳۰ | ۰/۹۳۰۷ | ۰/۷۶۳۳ | ۰/۶۴۹۳ |
| ۰/۰۵۹۲۵ | ۰/۰۷۹ | ۰/۰۵۵ | ۰/۰۴۲۲ | ۰/۴۱۴۸ | ۰/۳۴۰۰ | ۰/۲۹۴۶ |

تشکیل ماتریس تصمیم‌گیری فازی نرمال شده.

جدول ۱۶. ماتریس نرمال شده در لایهٔ کاربرد IoT

| | A | B | C | D |
|---|---|---|---|---|
| A | ۰/۶۷۷۲۳۱ | ۰/۷۶۶۶۶۷ | ۰/۶۴۶۰۱۱ | ۰/۴۵۵۵۴۴ |
| B | ۰/۱۰۸۵۳۲ | ۰/۱۲۰۹۴۶ | ۰/۲۲۵۲۰۷ | ۰/۱۶۷۴۲۴ |
| C | ۰/۱۱۱۸۰۲ | ۰/۰۵۹۹۳۵ | ۰/۱۰۵۰۶۱ | ۰/۳۰۸۷۴۸ |
| D | ۰/۱۰۲۴۳۵ | ۰/۰۵۲۴۵۲ | ۰/۰۲۳۷۲۲ | ۰/۰۶۸۲۸۴ |

تشکیل ماتریس تصمیم‌گیری فازی نرمال وزین شده.

جدول ۱۷. مشخص ساختن وزن ماتریس نرمال شده در لایهٔ کاربرد IoT

| | A | B | C | D | MEAN | |
|---|---|---|---|---|---|---|
| A | ۰/۶۷۷۲۳۱ | ۰/۷۶۶۶۶۷ | ۰/۶۴۶۰۱۱ | ۰/۴۵۵۵۴۴ | ۰/۶۳۶۳۶۳ | وزن معیارها |
| B | ۰/۱۰۸۵۳۲ | ۰/۱۲۰۹۴۶ | ۰/۲۲۵۲۰۷ | ۰/۱۶۷۴۲۴ | ۰/۱۵۵۵۲۷ | |
| C | ۰/۱۱۱۸۰۲ | ۰/۰۵۹۹۳۵ | ۰/۱۰۵۰۶۱ | ۰/۳۰۸۷۴۸ | ۰/۱۴۶۳۸۶ | |
| D | ۰/۱۰۲۴۳۵ | ۰/۰۵۲۴۵۲ | ۰/۰۲۳۷۲۲ | ۰/۰۶۸۲۸۴ | ۰/۰۶۱۷۲۳ | |

تشکیل ماتریس غیر فازی شده

جدول ۱۸. ماتریس غیرفازی شده در لایهٔ کاربرد IoT

| | **A** | **B** | **C** | **D** |
|---|---|---|---|---|
| A | ۱ | ۶/۳۳۸۹۴۲ | ۶/۱۴۸۹۳۲ | ۶/۶۷۱۳۲۳ |
| B | ۰/۱۶۰۲۵۹ | ۱ | ۲/۱۴۳۵۸۸ | ۲/۴۵۱۸۸۲ |
| C | ۰/۱۶۵۰۸۷ | ۰/۴۹۵۵۵۷ | ۱ | ۴/۵۲۱۵۲۴ |
| D | ۰/۱۵۱۲۵۶ | ۰/۴۳۳۶۸۱ | ۰/۲۲۵۷۸۹ | ۱ |
| | ۱/۴۷۶۶۰۲ | ۸/۲۶۸۱۷۹ | ۹/۵۱۸۳۰۸ | ۱۴/۶۴۴۷۳ |

محاسبهٔ ضریب سازگاری.

λ >>>>> ۴/۳۹۸۸۸

CI >>>>>۰/۱۳۲۹۶

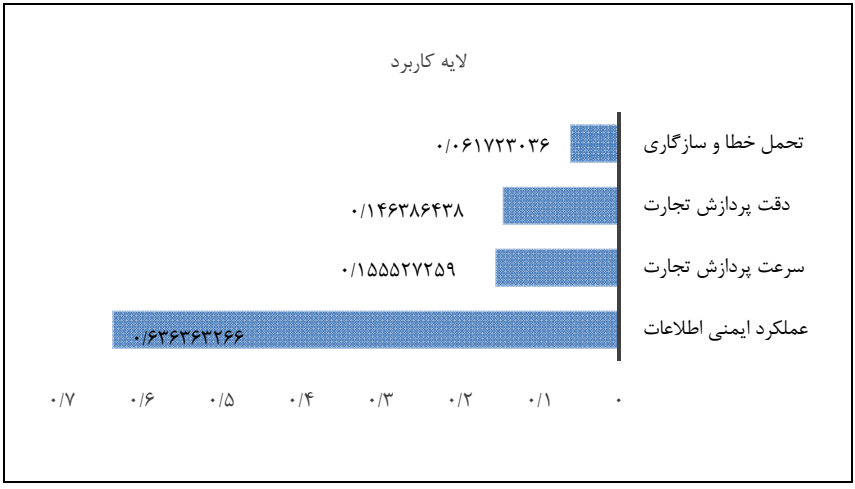
CR >>>>> ۰/۰۴۷۷۳

n =۴, RI =۰/۹

که بنا به مقدار به‌دست آمده (۰/۱> ۰/۰۴) سازگاری در مقایسات تأیید می‌شود.

در نهایت نیز رتبه‌بندی گزینه‌ها در شکل ۹ ارائه شده است:

- عملکرد ایمنی اطلاعات
- سرعت پردازش تجارت
- دقت پردازش تجارت
- تحمل خطا و سازگاری



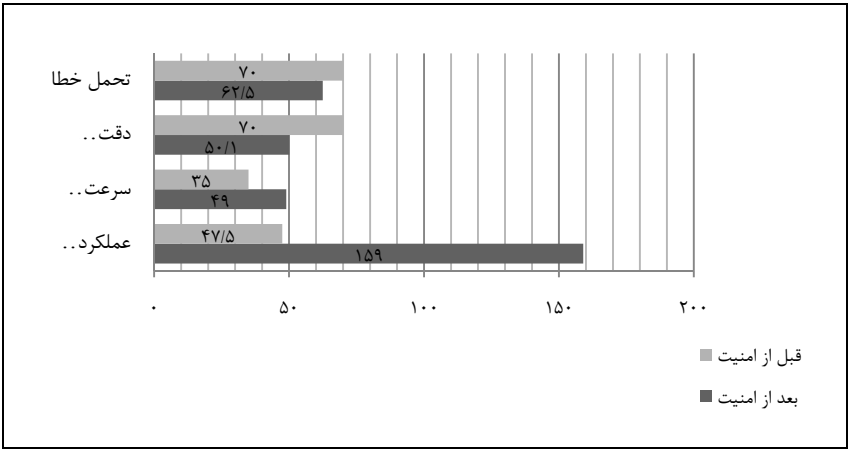

شکل ۹. اولویت مربوط به عملکرد لایهٔ کاربرد

نتایج شبیه‌سازی پس از افزودن دو مدل امنیتی در جدول ۱۹ ارائه شده است:

جدول ۱۹. نتایج آزمایش شبیه‌سازی افزودن مدل‌های امنیتی در لایهٔ کاربرد

| شاخص | قبل از امنیت | بعد از امنیت | تغییر (%) |
|---|---|---|---|
| عملکرد ایمنی اطلاعات | ۴۷/۵ | ۱۵۹/۰ | +۱۱/۵ ↑ |
| سرعت پردازش تجارت | ۴۹/۰ | ۳۵/۰ | -۱۴ ↓ |
| دقت پردازش تجارت | ۵۰/۱ | ۷۰/۰ | +۱۹/۹ ↑ |
| تحمل خطا | ۶۲/۵ | ۷۰/۰ | +۷/۵ ↑ |

تغییرات مربوط به پارامترهای شاخص لایهٔ انتقال نیز در شکل ۱۰ نشان داده شده است.




شکل ۱۰. افزودن مدل‌های امنیتی به لایهٔ کاربرد

عملکرد ایمنی اطلاعات با افزایش شایان توجه ۱۱/۵درصدی همراه بوده که نشان‌دهنده بهبود چشمگیر در محافظت از داده‌های کاربردی است. همچنین دقت پردازش تجارت و تحمل خطا به ترتیب ۱۹/۹درصد و ۷/۵درصد افزایش یافته‌اند که بیانگر ارتقای قابلیت اعتماد و استحکام عملکرد لایهٔ کاربرد در برابر اختلالات احتمالی است. اگرچه سرعت پردازش تجارت با کاهش ۱۴درصد مواجه شده است، اما این کاهش در برابر دستاوردهای امنیتی و دقت پردازش، توجیه‌پذیر و قابل قبول ارزیابی می‌شود.

## نتیجه‌گیری

تجزیه‌وتحلیل امنیتی حفظ حریم خصوصی برای سیستم‌های توصیه‌کننده خدمات اینترنت اشیا، مانند سیستم‌های توصیه‌کننده تشخیصی مبتنی بر اینترنت اشیا که در آن‌ها، باید اطلاعات حساس مربوط به کاربر حفظ شود، بسیار مهم است که با نتایج (ژانگ و همکاران[1]، ۲۰۱۸)، هم‌خوانی دارد. نتایج آزمون فرضیه‌های این پژوهش نشان داد که عملکرد سیستم لایهٔ ادراک اینترنت اشیا به‌دست‌آمده از طریق آزمایش‌های شبیه‌سازی عملکرد این لایه را در سطح ضعیف نمایش می‌دهد و افزودن مدل امنیتی در این لایه مفید نیست؛ زیرا با افزودن مدل‌های امنیتی بیشتر ابرها به پایین سقوط می‌کنند. یافته‌های این فرضیه نشان می‌دهد که افزودن مدل‌های امنیتی سنگین به لایهٔ ادراک باعث افت عملکرد می‌شود. این نتیجه با پژوهش (چی، کیارو و پیکالی[2]، ۲۰۲۵) هم‌سوست که از الگوریتم‌های رمزنگاری سبک‌وزن (مانند Cryptography Lightweight) در لایهٔ ادراک IoT استفاده کردند تا بدون کاهش قابلیت اطمینان، سرعت

1. Zhang et al
2. Qi, Chiaro & Piccialli

پردازش را حفظ کنند. عملکرد سیستم در لایهٔ انتقال اینترنت اشیا (IoT) از طریق آزمایش‌های شبیه‌سازی بهبود یافته است. بنابراین، برای اینکه اطلاعات به لایهٔ کاربرد منتقل شوند و شاهد کاهش بهره‌وری در عملکرد سیستم IoT نباشیم، نیاز به یک مدل امنیتی قوی در این لایه داریم. با افزودن مدل‌های امنیتی بیشتر، می‌توانیم اطمینان حاصل کنیم که عملکرد ابرها در نواحی بالا و متوسط بهینه باقی بماند. بهبود عملکرد لایهٔ انتقال پس از افزودن مدل‌های امنیتی، با نتایج پژوهش (کریشنامورتی، جوتی و کاروپیا[1]، ۲۰۲۳) هم‌خوانی دارد که از پروتکل‌های ترکیبی (ECC-AES Hybrid) برای توازن بین امنیت و تأخیر پایین استفاده کردند. عملکرد سیستم در لایهٔ کاربرد اینترنت اشیا نیز از طریق آزمایش‌های شبیه‌سازی به حد متوسطی رسیده است. بنابراین، بخشی از مدل‌های امنیتی باید در این لایه نیز پیاده‌سازی شود و می‌توان با استفاده از رمزنگاری، مدل امنیتی این لایه را تقویت کرد. استفاده از رمزنگاری تطبیقی[2] در این لایه می‌تواند به افزایش تحمل خطا کمک کند، همان طور که در (هالگاموژ و نیاتو[3]، ۲۰۲۵) نیز اشاره شده است. بنا به یافته‌های پژوهش پیشنهاد می‌شود به جای مدل‌های سنتی، از معماری‌های امنیتی مبتنی بر Based-Edge Learning Machine استفاده شود تا بار پردازشی به لایه ابر منتقل نشود. پیشنهاد می‌شود از چارچوب‌های Security Aware-QoS بهره گرفته شود که شاخص‌هایی مانند ظرفیت شبکه و تأخیر را به‌صورت پویا مدیریت می‌کنند. همچنین، ادغام فناوری Computing Edge برای پردازش محلی داده‌های حساس پیشنهاد می‌شود. برای ارزیابی دقیقتر تأثیر مدل‌های امنیتی، پیشنهاد می‌شود از چارچوب‌های Learning Federated جهت حفظ حریم خصوصی داده‌ها در لایهٔ ادراک استفاده شود. این رویکرد با پژوهش (الآمر[4]، ۲۰۲۴) هم‌سوست که از یادگیری فدرال برای آموزش مدل‌های امنیتی بدون اشتراک‌گذاری داده‌های خام استفاده کردند. برای جلوگیری از تضاد بین امنیت و عملکرد، پیشنهاد می‌شود یک چارچوب یکپارچه (مانند Architecture Design-by-Secure) طراحی شود که تعامل بین لایه‌ها را در نظر بگیرد. این ایده با پژوهش (اسماعیل، نومن، داوود و رضا[5]، ۲۰۲۴) مطابقت دارد که از معماری‌های مبتنی بر بلاکچین برای هماهنگی امنیتی بین لایهٔ انتقال و کاربرد بهره بردند.

با توجه به یافته‌های این پژوهش و مقایسه با مطالعات نوین، ضروری است مدل‌های امنیتی IoT به‌صورت لایه‌بندی شده و هوشمند طراحی شوند تا هم‌زمان با حفظ حریم خصوصی، عملکرد سیستم در سطح بهینه باقی بماند. ترکیب رویکردهای سبک‌وزن در لایهٔ ادراک، پروتکل‌های ترکیبی در لایهٔ انتقال، و رمزنگاری تطبیقی در لایهٔ کاربرد، می‌تواند گامی مؤثر به‌سوی سیستم‌های امن و کارآمد IoT باشد. با افزایش استفاده از دستگاه‌های اینترنت اشیا در بیشتر حوزه‌های تجاری وزندگی شخصی، نگرانی‌های امنیتی بیشتر می‌شود. با توجه به محدودیت منابع و تنوع اجزا در محیط‌های مختلف اینترنت اشیا، طیف وسیعی از آسیب‌پذیری‌ها پدید آمده است. بسیاری از این آسیب‌پذیری‌ها می‌توانند به شکست سیستم در محیط کاری

1. Krishnamurthy, Jothi & Karuppiah
2. Adaptive cryptography
3. Halgamuge & Niyato
4. Alamer
5. Ismail, Nouman, Dawoud & Reza

اینترنت اشیا منجر شوند. ازآنجایی‌که هیچ استاندارد از پیش تعریف شده‌ای برای محیط اینترنت اشیا وجود ندارد، اکثر تحقیقات انجام‌شده تا به امروز چالش‌ها و راه‌حل‌های امنیتی اینترنت اشیا را بدون ساختار خاصی ارائه کرده‌اند. در این مقاله، ما یک بررسی جامع در مورد الزامات، چالش‌ها و راه‌حل‌های امنیت اینترنت اشیا بر اساس ویژگی‌های امنیتی محیط مشترک اینترنت اشیا در یک ساختار معماری سه لایه انجام دادیم. ما همچنین یک طبقه‌بندی برای الزامات و چالش‌های امنیتی IoT موجود در لایه‌های کاربرد، اداره و انتقال ارائه کردیم و راه‌حل‌های مربوطه را برای آن چالش‌ها ارائه کردیم. ما امنیت اینترنت اشیا را به‌عنوان حوزه‌ای برای تکامل سایبرنتیک در نظر می‌گیریم: مهاجمان تکنیک‌های جدیدی را توسعه می‌دهند که سپس با سازوکارهای دفاعی جدید کاهش می‌یابند. تکنیک‌های تکاملی و یادگیری ماشین کاربردهای امنیتی زیادی دارند، به‌ویژه در پردازش تعداد زیادی از ترافیک شبکه و گزارش‌های تولید شده توسط دستگاه‌های IoT. این یک سؤال جالب است که آیا این نوع از تکامل سایبرنتیک که شبیه رابطه طبیعی طعمه و شکارچی است، می‌تواند به ظهور تکنیک‌های هوش مصنوعی جدید منجر شود؟ همچنین در مورد جهت‌گیری‌ها و رویکردهای بالقوه برای تحقیقات آینده، فضایی برای تحقیقات جدید در این زمینه وجود دارد و اینجاست که فرصتی برای توسعه استراتژی‌های مؤثر برای بهبود مستمر امنیت اینترنت اشیا ارائه می‌شود. ما معتقدیم که تحقیقات ما در مورد راه‌حل‌های امنیتی مبتنی بر محاسبات ابری گامی در مسیر درست است و به دیگر دانشگاهیان و متخصصان کمک می‌کند تا راه‌حل‌های امنیتی اینترنت اشیا را در آینده پیدا و پیاده‌سازی کنند. گزینه‌های امنیتی زیادی وجود دارد که می‌توانیم در روندهای آینده امنیت اینترنت اشیا در نظر بگیریم. چالش‌های مهمی به تعامل بین دستگاه‌های IoT و ابر متصل می‌شوند، با یک‌لایه اضافی که با ادغام در حال ظهور با فناوری‌های بلاکچین اضافه می‌شود. طراحی و توجه دقیق باید به ویژگی‌های امنیتی اساسی مانند محرمانه بودن، یکپارچگی و در دسترس بودن داده شود.

## فهرست منابع


احمدوند، بهناز و جهانشاهی، آرتین (۱۴۰۲). بررسی الگوی مطلوب قانون‌گذاری حفاظت از داده شخصی در بستر اینترنت اشیا در پرتو مطالعات تطبیقی، *سیاست‌گذاری عمومی*، ۹(۱)، ۴۷- ۶۳. https://doi.org/10.22059/jppolicy.2023.92988

رنجبر، امیرحسین (۱۴۰۱). مروری بر ضرورت اینترنت اشیا در پروژه‌های شهر هوشمند رویکرد نوین در توسعهٔ پایدار شهری. *پژوهش‌های کاربردی در مدیریت و علوم انسانی*، ۳(۷)، ۳۵-۴۶. https://civilica.com/doc/1700535

شاهزاده فاضلی، سیدابوالفضل؛ قوه ندوشن، اعظم و زارع‌پور احمدآبادی، جمال (۱۴۰۳). بهبود سرعت سیستم تشخیص نفوذ از طریق کاهش حجم داده ها با استفاده از DBSCAN مبتنی بر هسته. *پدافند الکترونیکی و سایبری*، ۱۲(۴)، ۸۹-۱۰۲.

Alamer, A. (2024). A privacy-preserving federated learning with a secure collaborative for malware detection models using Internet of Things resources. *Internet of Things*, 25(5), 1-25. https://doi.org/10.1016/j.IoT.2023.101015

Al-Dulaimy, A., Jansen, M., Johansson, B., Trivedi, A., Iosup, A., Ashjaei, M., ... & Papadopoulos, A. V. (2024). The computing continuum: From IoT to the cloud. *Internet of Things*, *27*, 101272.

Ali, B. & Awad, A. (2018). Cyber and physical security vulnerability assessment for IoT-based smart homes. *Journal Sensors,* 18(3), 1-17. http://dx.doi.org/10.3390/s18030817

Appel, M., Bossert, A., Cooper, S., Kußmaul, T., Löffler, J., Pauer, C. & Wiesmaier, A. (2016). Block ciphers for the iot–simon, speck, katan, led, tea, present, and sea compared.s*Proc. Appel Block CF*, 1-37. https://tubiblio.ulb.tu-darmstadt.de/id/eprint/104856

Arvind, S. & Narayanan, V. A. (2019). An Overview of Security in CoAP: Attack and Analysis. *International Conference on Advanced Computing & Communication Systems (ICACCS),* pp. 655–660, https://doi.org/10.1109/ICACCS.2019.8728533

Balogh, S., Gallo, O., Ploszek, R., Spacek, P. & Zajac, P. (2021). IoT Security Challenges: Cloud and Blockchain, Postquantum Cryptography, and Evolutionary Techniques. *Electronics,* 10(21), 2647. https://doi.org/10.3390/electronics10212647

Behera, M., Mohapatra, S. K., Samal, U. C., Khan, M. S., Daneshmand, M. & Gandomi, A. H. (2019). Residual energy-based cluster-head selection in wsns for IoT application. *IEEE Internet of Things Journal,* 6, 5132–5139. http://dx.doi.org/10.1109/JIOT. 2019.2897119

Binti Harum, N., Zakaria, N. A., Emran, N. A., Ayop, Z., & Anawar, S. (2019). Smart book reader for visual impairment person using IoT device. *International Journal of Advanced Computer Science and Applications, 10*(2), 251-255.

Burke, D. (2018). *Preventing DDOS Attacks against IoT Devices*. PhD Thesis, Utica College.

Canedo, J. & Skjellum, A. (2016). *Using machine learning to secure IoT systems. Annual Conference on Privacy, Security and Trust* (PST), pp. 219–222, IEEE. https://doi.org/10.1109/PST.2016.7906930

Chen, J., Touati, C. & Zhu, Q. (2019). Optimal secure two-layer IoT network design. *IEEE Transactions on Control of Network Systems.* https://doi.org/10.1109/TCNS.2019.2906893

Choi, J., In, Y., Park, C., Seok, S., Seo, H. & Kim, H. (2018). Secure IoT framework and 2D architecture for End-To-End security. *Journal of Supercomputing*, 74(8), 3521–3535. https://link.springer.com/article/10.1007/s11227-016-1684-0

Djenna, A., Harous, S. & Saidouni, D.E. (2021). Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure. *Applied sciences,* 11(10), 4580. https://doi.org/10.3390/app11104580

Dovom, E. M., Azmoodeh, A., Dehghantanha, A., Newton, D. E., Parizi, R. M. & Karimipour, H. (2019). Fuzzy pattern tree for edge malware detection and categorization in IoT. *Journal of Systems Architecture,* 97, 1–7. https://doi.org/10.1016/j.sysarc.2019.01.017

Grassi, P., Garcia, M. & Fenton, J. (2017). DRAFT NIST Special Publication 800-63-3 Digital Identity Guidelines. *National Institute of Standards and Technology*, Los Altos, CA. https://doi.org/10.6028/NIST.SP.800-63-3

Halgamuge, M. N. & Niyato, D. (2025). Adaptive edge security framework for dynamic IoT security policies in diverse environments. *Computers & Security,* 148(2),17-38. http://dx.doi.org/10.1016/j.cose.2024.104128

Ismail, Sh., Nouman, M., Dawoud, D. W. & Reza. H. (2024).Towards a lightweight security framework using blockchain and machine learning. *Blockchain: Research and Applications,* 5(1), 1-12. http://dx.doi.org/10.1016/j.bcra.2023.100174

Kamaludeen, N. B. A., Lee, S. P. & Parizi, R. M. (2019, July). Guideline-based approach for IoT home application development. In *2019 international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)* (pp. 929-936). IEEE.

Khan. Y., Su'ud, M.B.M., Alam, M.M., Ahmad, S.F., Salim, N.A. & Khan, N. (2023). Architectural Threats to Security and Privacy: A Challenge for Internet of Things (IoT) Applications. *Electronics (Switzerland),* 12(1), 88-108. https://doi.org/10.3390/electronics12010088

Kirikkayis, Y., Winter, M. & Reichert, M. (2024). A User Study on Modeling IoT-Aware Processes with BPMN 2.0. *Information 2024, 15, 229.*

Krishnamurthy, V., Jothi, S. & Karuppiah, S. V. (2023). HO-DQLN: Hybrid optimization-based deep Q-learning network for optimizing QoS requirements in service oriented model. *Expert Systems with Applications*. 227(12). https://doi.org/10.1016/j.eswa.2023.120188

Li, Y., Shi, L., Cheng, P., Chen, J. & Quevedo, D. E. (2015).Jamming Attacks on Remote State Estimation in Cyber-Physical Systems: A Game-Theoretic Approach. *IEEE Transactions on Automatic Control,* 60(10), 2831–2836. http://dx.doi.org/10.1109/TAC.2015.2461851

Liu, H., Yang, B. & Liu, T. (2014). Efficient Naming, Addressing and Profile Services in Internet-of-Things Sensory Environments. *Ad Hoc Networks*, 18, 85–101. http://dx.doi.org/10.1016/j.adhoc.2013.02.008

Mashal, I., Alsaryrah, O., Chung, TY., Yang, C Z., Kuo, WH. & Agrawal, D. P. (2015). Choices for interaction with things on Internet and underlying issues. *Ad Hoc Networks,* 28, 68–90. https://doi.org/10.1016/j.adhoc.2014.12.006

Mazhar, T., Talpur, D. B., Shloul, T. A., Ghadi, Y.Y., Haq, I., Ullah, I., Ouahada, K. & Hamam, H. (2023). Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence. *Brain Sci.,* 13, 683. https://doi.org/10.3390/brainsci13040683

Ngu, H., Gutierrez, M., Metsis, V., Nepal, S. & Sheng, Q. Z. (2016). IoT Middleware: A Survey on Issues and Enabling Technologies," IEEE Internet of Things Journal, vol. 4, no. 1, pp. 1–20. https://doi.org/10.1109/JIOT.2016.2615180

Paranjothi, A., Tanik, U., Wang, Y. & Khan, M. S. (2019). Hybrid-vehfog: A robust approach for reliable dissemination of critical messages in connected vehicles. *Transactions on Emerging Telecommunications Technologies*, 30(6), 35-55. http://dx.doi.org/10.1002/ett.3595

Puthal, D., Nepal, S., Ranjan, R. & Chen, J. (2016). Threats to networking cloud and edge datacenters in the Internet of Things. *IEEE Cloud Computing*, 3(3), 64–71. http://dx.doi.org/10.1109/MCC.2016.63

Qi, P., Chiaro, D. & Piccialli, F. (2025). Small models, big impact: A review on the power of lightweight Federated Learning. *Future Generation Computer Systems*, 16, 1-15. https://doi.org/10.1016/j.future.2024.107484

Ray, P P. (2018). A Survey on Internet of Things Architectures. *Journal of King Saud University - Computer and Information Sciences,* 30, 291– 319. https://doi.org/10.1016/j.jksuci.2016.10.003

Ren, J., Guo, H., Xu, C. & Zhang, Y. (2017). Serving at the edge: A scalable IoT architecture based on transparent computing. *IEEE Network,* 31(5), 96–105. https://doi.org/10.1109/MNET.2017.1700030

Said, O. & Masud, M. (2013). Towards internet of things: survey and future vision. *International Journal of Computer Networks*, 5(1), 1–17. https://www.researchgate.net/publication/297141894

Sakhnini, J., Karimipour, H., Dehghantanha, A., Parizi, R. M. & Srivastava, G. (2019). Security aspects of internet of things aided smart grids: A bibliometric survey. *Internet of Things,* 14, 1-19. https://doi.org/10.1016/j.IoT.2019.100111

Salah, Kh. & Khan, M. (2018). IoT Security: Review, Blockchain Solutions, and Open Challenges. *Future Generation Computer Systems*, 82, 395–411. http://dx.doi.org/10.1016/j.future.2017.11.022

Santos, J., Rodrigues, J. J., Silva, B. M., Casal, J., Saleem, K. & Denisov, V. (2016). An IoT-Based Mobile Gateway for Intelligent Personal Assistants on Mobile Health Environments. *Journal of Network and Computer Applications*, 71, 194–204. https://doi.org/10.1016/j.jnca.2016.03.014

Sethi, M., Arkko, J. & Keränen, A. (2017). End-to-End Security for Sleepy Smart Object Networks. *Annual IEEE Conference on Local Computer Networks-Workshops*, pp. 964–972. https://doi.org/10.1109/LCNW.2012.6424089

Sethi, P., & Sarangi, S. R. (2017). Internet of things: architectures, protocols, and applications. *Journal of electrical and computer engineering*, *2017*(1), 9324035.

Srivastava, G., Parizi, R. M., Dehghantanha, A. & Choo, K.-K. R. (2019). Data sharing and privacy for patient IoT devices using blockchain. Smart City and Informatization, (iSCI 2019), pp 334–348.

Taherdoost, H. (2023). Security and Internet of Things: Benefits, Challenges, and Future Perspectives. *Electronics,* 12, 1-19. https://doi.org/10.3390/electronics12081901

Wang, D., Ming, J., Chen, T., Zhang, X. & Wang, C. (2018). Cracking IoT Device User Account via Brute-force Attack to SMS Authentication Code. *In Proceedings of the First Workshop on Radical and Experiential Security,* pp. 57–60. http://dx.doi.org/10.1145/3203422.3203426

Wang, H., Wang, Y., & Jin, J. (2024). Application of multimodality perception scene construction based on Internet of Things (IoT) technology in art teaching. *PeerJ Computer Science*, *10*, e2047.

Wu, M., Lu, TJ., Ling, FY., Sun, J. & Du, HY. (2010). Research on the architecture of internet of things," *3rd International Conference on Advanced Computer Theory and Engineering (ICACTE),* 5, 483–507. http://dx.doi.org/10.1109/ICACTE.2010.5579493

Yang, Y., Wu, L., Yin, G., Li, L. & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. *IEEE Internet Things*, 4, 1250–1258. https://doi: 10.1109/JIOT.2017.2694844

Zarca, A. M., Bernal Bernabe, J., Farris, I., Khettab, Y., Taleb, T. & Skarmeta, A. (2018).Enhancing IoT security through network softwarization and virtual security appliances. *International Journal of Network Management*, 28(5), 20-38. https://doi.org/10.1002/nem.2038

Zhang, W., Meng, Y., Liu, Y., Zhang, X., Zhang, Y. & Zhu, H.( 2018). Homonit: Monitoring Smart Home Apps from Encrypted Traffic. *ACM SIGSAC Conference on Computer and Communications Security,* pp. 1074–1088, ACM. https://doi.org/10.1145/3243734.3243820

# Improving the Security of the Three-Tier IoT Cloud Model Using Simon Algorithm and Mutual Authentication

**Mohammad Shirdel**
*Ph.D. Candidate, Department of Information Technology , Faculty of Management, Science and Research Branch, Islamic Azad University, Tehran, Iran*

**Maghsoud Amiri** [*1]
*Prof., Department of Industrial Management, Faculty of Management and Accounting, Allameh Tabataei University, Tehran, Iran*

**Mohamad Ali Afshar Kazemi**
*Associate Prof., Department of Management, Faculty of Management, Central Tehran Branch, Islamic Azad University, Tehran, Iran*

**Mohamad Reza Motadel**
*Assistant Prof., Department of Industrial Management, Faculty of Management, Central Tehran Branch, Islamic Azad University, Tehran, Iran*

## Abstract
With the expansion of the number of smart devices and related applications, a significant volume of data is generated, which plays an important role in automating everyday activities. This big data requires fast processing, secure storage, and reliable transmission through secure channels to protect it from malicious threats and attacks. Privacy protection has always been one of the main challenges in cyberspace, and with the emergence of the Internet of Things (IoT), this challenge has gained wider dimensions. In this paper, an evaluation model based on the three-tier architecture of the Internet of Things, including perception, transmission, and application layers, is presented. Specific performance indicators are defined and applied for each layer. In order to evaluate the system performance, expert opinions are collected and the indicators are prioritized using the fuzzy TOPSIS decision-making method. Also, security models such as Simon lightweight encryption and mutual authentication have been added to each layer separately and their impact on the overall system performance has been analyzed. To implement these algorithms, an STM32F4 microcontroller with an ARM Cortex-M4 processor has been used, which provides adequate processing power and the ability to accurately measure security and performance indicators. The final results show that the proposed model leads to improved security levels and reduced vulnerability to cyber attacks.

**Keywords:** Security architecture, Internet of things, Three-layer model IoT.

1. Corresponding Author: amir@atu.ir