دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

توسعه سیستم پیشنهاددهی فیلم چندوجهی با استفاده از شبکه‌های عصبی گراف و همجوشی ویژگی‌های متنی و تصویری

علی مصدق[1]، دانیال براتی[2] و کیارش فضیلت[3]

[1]دانشجوی ارشد مهندسی کامپیوتر، واحد تهران غرب، دانشگاه آزاد اسلامی، تهران، ایران ali.mosaddegh@yahoo.com

2دانشجوی ارشد مهندسی کامپیوتر، واحد تهران غرب، دانشگاه آزاد اسلامی، تهران، ایران danial.barati1999@gmail.com

3دانشجوی ارشد مهندسی کامپیوتر، واحد تهران غرب، دانشگاه آزاد اسلامی، تهران، ایران kiarashfzl2424@gmail.com

چکیده

این پژوهش به طراحی و توسعه یک سیستم پیشنهاددهی چندوجهی فیلم با استفاده از شبکه‌های عصبی گرافی (GCN) پرداخته است. هدف اصلی این سیستم، بهبود دقت و کیفیت توصیه‌ها از طریق ترکیب اطلاعات چندوجهی شامل ویژگی‌های متنی و تصویری فیلم‌ها بود. در این مدل، گراف تعاملات کاربر-فیلم به‌عنوان ساختار اصلی مورد استفاده قرار گرفت و ارتباطات میان کاربران و فیلم‌ها به کمک گره‌ها و لبه‌های گراف مدل‌سازی شد. ویژگی‌های متنی فیلم‌ها با مدل‌های تعبیه‌سازی و ویژگی‌های تصویری با استفاده از شبکه‌های عصبی پیچشی استخراج و سپس در گره‌های گراف ترکیب شدند. شبکه عصبی گرافی برای یادگیری ویژگی‌های تعاملی و پیش‌بینی ترجیحات کاربران به کار گرفته شد. نتایج آزمایش‌ها نشان داد که مدل پیشنهادی، با وجود نوسانات در مقادیر خطا و میانگین مربعات خطا (MSE)، به بهبود نسبی دقت و همگرایی مدل نسبت به روش‌های پایه دست یافته است. گراف تعاملات نیز نشان‌دهنده تنوع سلایق کاربران و اهمیت برخی فیلم‌های پرتعامل بود. این پژوهش همچنین پیشنهادهایی برای بهبود مدل شامل استفاده از داده‌های واقعی، الگوریتم‌های پیشرفته‌تر همجوشی و بهبود تفسیرپذیری ارائه می‌کند. مدل پیشنهادی می‌تواند مبنایی برای طراحی سیستم‌های توصیه‌گر پیشرفته‌تر و شخصی‌سازی‌شده‌تر باشد.

کلید واژه:

سیستم پیشنهاددهی، شبکه‌های عصبی گرافی، داده‌های چندوجهی، توصیه‌گر فیلم، همجوشی ویژگی‌ها.

مقدمه

در سال‌های اخیر، حجم عظیمی از داده‌های دیجیتال و چندرسانه‌ای مانند فیلم، موسیقی و تصاویر، دسترسی کاربران به محتوا را به‌شدت افزایش داده است[1]. سیستم‌های پیشنهاددهی به‌عنوان راه‌حلی مؤثر برای هدایت کاربران به سمت محتواهای مناسب و افزایش تجربه کاربری مطرح شده‌اند[2]. این سیستم‌ها به کاربران کمک می‌کنند تا از میان حجم عظیم داده‌ها، محتوای مرتبط و متناسب با سلایق شخصی خود را پیدا کنند. با رشد فناوری‌های یادگیری عمیق و پردازش زبان طبیعی، روش‌های مختلفی برای بهبود دقت و شخصی‌سازی پیشنهادها توسعه یافته‌اند[3،4].

بسیاری از تحقیقات اخیر نشان داده‌اند که رویکردهای چندوجهی، که از ترکیب منابع داده‌ای مختلف مانند متون، تصاویر و سایر ویژگی‌های محتوایی استفاده می‌کنند، دقت بیشتری در ارائه پیشنهادهای شخصی‌سازی شده دارند. به‌خصوص در حوزه فیلم و محتوای ویدئویی، ترکیب

ویژگی‌های متنی مانند ژانر و خلاصه داستان و ویژگی‌های تصویری مانند پوستر یا صحنه‌های کلیدی فیلم می‌تواند نقشی مهم در بهبود کیفیت پیشنهادها ایفا کند. روش‌های نوین مانند شبکه‌های عصبی گراف (GNN) و ترانسفورمرها توانایی ویژه‌ای در همجوشی و تحلیل اطلاعات چندوجهی دارند[4]. شبکه‌های عصبی گراف با امکان پردازش داده‌های غیراقلیدسی و استفاده از ساختارهای گرافی مانند ارتباطات کاربر-فیلم، در سیستم‌های پیشنهاددهی جدید به کار گرفته شده‌اند و عملکرد چشمگیری را نشان داده‌اند[3].

با این حال، هنوز چالش‌هایی نظیر چگونگی همگام‌سازی بهینه اطلاعات متنی و تصویری، به‌خصوص در سیستم‌های پیشنهاددهی فیلم، به‌طور کامل حل نشده است[5]. اکثر روش‌های فعلی تمرکز بر روی یک یا دو نوع ویژگی دارند و به ندرت از ترکیب چندوجهی با تمرکز بر روابط گرافی و ساختارهای کاربر-محتوا استفاده می‌کنند. همچنین، تفسیرپذیری پیشنهادها برای کاربران و امکان ارائه توضیحاتی در مورد دلایل هر پیشنهاد از جنبه‌های مهمی است که کمتر به آن توجه شده است[3،5].

در این مقاله، با هدف ارتقای دقت و تنوع پیشنهادها و همچنین بهبود تفسیرپذیری پیشنهادها، یک سیستم پیشنهاددهی فیلم چندوجهی مبتنی بر شبکه‌های عصبی گراف معرفی شده است. این سیستم با استفاده از همجوشی داده‌های متنی و تصویری، به‌گونه‌ای طراحی شده است که امکان اجرای آن با داده‌های شبیه‌سازی شده و در محیط گوگل کولب فراهم باشد. نتایج نشان می‌دهند که ترکیب ویژگی‌های متنی و تصویری از طریق شبکه‌های عصبی گراف می‌تواند به پیشنهادهای شخصی‌سازی‌شده‌تر و دقیق‌تر منجر شود و تجربه کاربری بهتری را فراهم کند.

کارهای گذشته

ژی[1] و همکاران[1]، در مطالعه‌ای با عنوان *Movie Recommendation with Poster Attention via Multi-modal Transformer Feature Fusion* به معرفی سیستمی چندوجهی برای پیشنهاددهی فیلم پرداخته‌اند که از ویژگی‌های پوستر فیلم و توضیحات متنی فیلم برای پیش‌بینی ترجیحات کاربران استفاده می‌کند. در این تحقیق از مدل BERT برای استخراج ویژگی‌های متنی و از مدل ViT برای ویژگی‌های تصویری استفاده شده است. ترکیب این مدل‌ها و استفاده از معماری ترنسفورمر برای همجوشی ویژگی‌ها منجر به افزایش دقت در پیش‌بینی امتیازات کاربران شده است. نتایج این مدل از طریق آزمون بر روی مجموعه داده MovieLens 100K و 1 M اثبات شده است که دقت پیش‌بینی را نسبت به الگوریتم‌های پایه افزایش داده است.

وو[2] و همکاران[2]، در مقاله‌ای با عنوان *Towards Bridging the Cross-modal Semantic Gap for Multi-modal Recommendation* به بررسی چالش‌های مربوط به شکاف معنایی بین مودالیته‌ها در سیستم‌های پیشنهاددهی چندوجهی پرداخته‌اند. این پژوهش با الهام از مدل CLIP، به توسعه چارچوبی به نام CLIPER پرداخته است که با استفاده از هم‌ترازی نمایه‌های مختلف، قابلیت استخراج اطلاعات چندیدگاهی را فراهم می‌آورد. این رویکرد توانسته است عملکرد بهتری نسبت به مدل‌های چندوجهی فعلی در سه مجموعه داده مختلف نشان دهد.

توکال[3] و همکاران[3]، در کنفرانس بین‌المللی مدل‌سازی محاسباتی، شبیه‌سازی و بهینه‌سازی(ICCMSO) ، پژوهشی با عنوان *Enhanced Movie Recommender System Using Deep Learning Techniques* ارائه کردند. در این تحقیق، از تکنیک‌های یادگیری عمیق شامل شبکه‌های عصبی مصنوعی (ANN) برای استخراج ویژگی‌ها از رفتار کاربران و متادیتای فیلم، شبکه‌های عصبی بازگشتی (RNN) برای درک الگوهای زمانی، و شبکه‌های عصبی پیچشی (CNN) برای تحلیل همبستگی‌های مکانی داده‌ها استفاده شده است. هدف این مدل، بهبود دقت پیشنهاددهی از طریق ترکیب ویژگی‌های کوتاه‌مدت و بلندمدت در ترجیحات کاربر است.

مالیتستا[4] و همکاران[4]، در مقاله‌ای با عنوان *Formalizing Multimedia Recommendation through Multimodal Deep Learning* در نشریه ACM، به بررسی سیستم‌های پیشنهاددهی چندرسانه‌ای از طریق یادگیری عمیق چندوجهی پرداخته‌اند. این پژوهش به بررسی چالش‌های مربوط به پیشنهاددهی در حوزه‌هایی مانند مد و موسیقی پرداخته و استفاده از تکنیک‌های چندوجهی را به عنوان راهکاری برای ارائه پیشنهادهای دقیق‌تر معرفی کرده است. محققان در این مطالعه به بازنگری روش‌های چندوجهی در پیشنهاددهی چندرسانه‌ای پرداخته و

[1] Xia
[2] Wu
[3] Tokala
[4] Malitesta

الگوریتم‌های اخیر را در چارچوبی به نام Elliot مورد ارزیابی قرار داده‌اند. این مطالعه با هدف ارائه دستورالعمل‌هایی برای طراحی و پیاده‌سازی نسل بعدی سیستم‌های پیشنهاددهی چندوجهی انجام شده است.

بوراباک[5] و آیکتین[6][5]، در مطالعه‌ای با عنوان *SynerGraph: An Integrated Graph Convolution Network for Multimodal Recommendation* یک رویکرد جدید برای سیستم‌های پیشنهاددهی چندوجهی با تمرکز بر ادغام و پالایش داده‌های چندوجهی معرفی کردند. این پژوهش نشان داده است که استفاده از فیلترهای پالایشی، دقت سیستم‌های چندوجهی را نسبت به مدل‌های تک‌وجهی بهبود می‌بخشد و اطلاعات متنی نقشی کلیدی در افزایش دقت پیشنهاددهی ایفا می‌کند.

مبوروک[7] و همکاران[6]، در مقاله‌ای تحت عنوان *Enhancing Movie Recommendations: A Deep Neural Network Approach with MovieLens Case Study* در کنفرانس IWCMC ، به بررسی بهبود سیستم‌های پیشنهاددهی فیلم با استفاده از شبکه‌های عصبی عمیق پرداخته‌اند. این پژوهش، چالش‌هایی نظیر مسئله شروع سرد، پراکندگی داده‌ها و کمبود بازخورد صریح کاربران را مورد توجه قرار داده و از شبکه‌های عصبی عمیق(DNN) ، شبکه‌های عصبی پیچشی(CNN) ، شبکه‌های عصبی بازگشتی (RNN) و خودرمزگذارها (AEs) بهره برده است. هدف این پژوهش، بهبود عملکرد سیستم‌های پیشنهاددهی است که به بازخوردهای ضمنی کاربران تکیه دارند و این مدل بر اساس معیارهایی مانند نسبت موفقیت و نمرات مربوطه (NDCG) ارزیابی شده است که نشان‌دهنده برتری این روش نسبت به روش‌های قبلی است.

هی[8] و همکاران[7]، در مقاله‌ای با عنوان *Multi-modal Bayesian Recommendation System* که در کنفرانس IMCEC ارائه شد، سیستم پیشنهاددهی چندوجهی با نام MBR را معرفی کرده‌اند که از مدالیت‌های تصویر و متن برای بهبود کیفیت پیشنهادها استفاده می‌کند. این سیستم از شبکه‌های عصبی پیچشی عمیق برای استخراج ویژگی‌های تصویری و از مدل‌های زبان برای تحلیل متنی بهره برده است. آزمایش‌ها بر روی یک مجموعه داده بزرگ‌مقیاس نشان داده که سیستم MBR در ارائه پیشنهادها بهبود یافته است و عملکرد بالایی دارد.

وی[9] و همکاران[8]، در مقاله *Multi-view Sequence Recommendation Model* که در کنفرانس IMCEC ارائه شده است، به بررسی الگوریتم‌های پیشنهاددهی مبتنی بر یادگیری عمیق و آگاه از بافت پرداخته‌اند. این پژوهش، تاثیرات زمینه‌ای مانند زمان، مکان و محیط اجتماعی بر رفتار کاربران را در نظر می‌گیرد و به دنبال توسعه سیستمی است که پروفایل‌های دقیق‌تری از کاربران ارائه دهد. نتایج این مطالعه نشان می‌دهد که استفاده از اطلاعات زمینه‌ای و آگاهی از صحنه می‌تواند به پیشنهادهایی دقیق‌تر و مناسب‌تر منجر شود.

سایت[10] و همکاران[9]، در مقاله *Enhancing Sequence Movie Recommendation System Using Deep Learning and KMeans* که در مجله Applied Sciences منتشر شده است، یک سیستم پیشنهاددهی را معرفی کرده‌اند که با ترکیب یادگیری عمیق و خوشه‌بندی KMeans، به بهبود دقت در توصیه‌های فیلم می‌پردازد. این سیستم با استفاده از اطلاعات کاربران نظیر سن، جنسیت و شغل، کاربران جدید را تحلیل کرده و با کاربران با ترجیحات مشابه مطابقت می‌دهد. مدل پیشنهاددهی با به‌کارگیری شبکه‌های ترنسفورمری و چندلایه ادراکی، دقت پیش‌بینی را افزایش داده و با استفاده از خوشه‌بندی KMeans بر روی ویژگی‌های ژانر فیلم‌ها، تنوع در پیشنهادها را نیز حفظ کرده است. ارزیابی مدل بر روی مجموعه داده MovieLens نشان از برتری آن در مقایسه با مدل‌های پایه دارد.

کیم[11] و همکاران[10]، در مقاله‌ای با عنوان *Multi-Modal Deep Learning Based Metadata Extensions for Video Clipping* که در مجله International Journal on Advanced Science, Engineering & Information Technology منتشر شده، یک مدل توسعه متادیتا برای ویدیوها با استفاده از یادگیری عمیق چندوجهی معرفی کرده‌اند. این مدل با شناسایی اشیا و تبدیل گفتار به متن (STT) متادیتای ویدیوها را گسترش می‌دهد. این توسعه می‌تواند به سیستم‌های جست‌وجو و پیشنهاددهی ویدیو کمک کند تا نتایج نزدیک‌تری به عبارات جست‌وجو و محتوای مرتبط به کاربران ارائه دهند.

[5] Burabak
[6] Aytekin
[7] Mabrouk
[8] He
[9] Wei
[10] Siet
[11] Kim

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

زان[12] و همکاران[11]، در مقاله *Research on Movie Recommendation Algorithm Based on Deep Learning* که در کنفرانس ICICACS ارائه شده، از یادگیری عمیق برای بهبود دقت الگوریتم پیشنهاددهی فیلم استفاده کرده‌اند. این مدل با بهره‌گیری از سیستم عصبی مصنوعی و الگوریتم انتشار پسرو برای بهینه‌سازی پارامترهای شبکه، دقت پیش‌بینی را بهبود بخشیده است. نتایج نشان داده که این مدل می‌تواند نیازهای شخصی‌سازی‌شده کاربران را به خوبی برآورده کند و دقت آن نسبت به الگوریتم‌های سنتی 1.4٪ بهبود یافته است.

پنگ[13] و همکاران[12]، در مقاله *Integration of Deep Reinforcement Learning with Collaborative Filtering for Movie Recommendation Systems* در مجله Applied Sciences ، سیستم پیشنهاددهی فیلم را معرفی کرده‌اند که ترکیبی از یادگیری تقویتی عمیق (DRL) و فیلترگذاری مشارکتی (CF) است. این سیستم با استفاده از الگوریتم DDPG و تحلیل مقدار ویژه(SVD) ، مشکلاتی نظیر کمبود داده و مسئله شروع سرد را بهبود می‌بخشد. ارزیابی مدل با معیارهایی نظیر دقت، بازخوانی و نمره F1 ، نشان از برتری این روش نسبت به مدل‌های مرجع پیشنهاددهی دارد.

لی[14] و همکاران[13]، در مقاله‌ای با عنوان *Graph Neural Networks with Deep Mutual Learning for Designing Multi-modal Recommendation Systems* که در مجله Information Sciences منتشر شده، چارچوبی با نام GNNMR را معرفی کرده‌اند که شبکه‌های عصبی گراف (GNN) را با تکنیک یادگیری متقابل عمیق ترکیب می‌کند. این چارچوب به هر مدالیت خاص یک گراف دوطرفه اختصاص می‌دهد و از این طریق به استخراج روابط معنایی پنهان بین مدالیت‌ها کمک می‌کند. نتایج تجربی نشان‌دهنده برتری این مدل در مقایسه با سایر مدل‌های چندوجهی در وظیفه پیشنهاددهی Top-K است.

جدول 1. خلاصه پیشینه پژوهش

محققان	سال	موضوع	روش	نتیجه
سایت و همکاران	2024	سیستم پیشنهاددهی فیلم با استفاده از یادگیری عمیق و خوشه‌بندی KMeans	ترکیب یادگیری عمیق و خوشه‌بندی KMeans برای بهبود دقت در توصیه‌های فیلم	بهبود دقت در مقایسه با مدل‌های پایه در MovieLens
کیم و همکاران	2024	توسعه متادیتا برای ویدیوها با استفاده از یادگیری عمیق چندوجهی	استفاده از شناسایی اشیا و تبدیل گفتار به متن برای گسترش متادیتا	بهبود جست‌وجو و پیشنهاددهی در سیستم‌های ویدئویی
زان و همکاران	2024	الگوریتم پیشنهاددهی فیلم با استفاده از یادگیری عمیق	استفاده از سیستم عصبی مصنوعی و الگوریتم انتشار پسرو	بهبود 1.4٪ در دقت پیش‌بینی نسبت به روش‌های سنتی
پنگ و همکاران	2024	سیستم پیشنهاددهی فیلم با ترکیب یادگیری تقویتی عمیق و فیلترگذاری مشارکتی	ترکیب یادگیری تقویتی عمیق (DRL)و تحلیل مقدار ویژه (SVD)با فیلترگذاری مشارکتی	افزایش دقت و شخصی‌سازی پیشنهادها در مجموعه MovieLens
لی و همکاران	2024	سیستم پیشنهاددهی چندوجهی با ترکیب شبکه‌های عصبی گراف و یادگیری متقابل عمیق	ترکیب شبکه‌های عصبی گراف با یادگیری متقابل عمیق (GNNMR)	برتری در وظیفه پیشنهاددهی Top-K

[12] Zhan
[13] Peng
[14] Li

نسبت به سایر مدل‌های چندوجهی				
برتری در معیارهای NDCGو نسبت موفقیت در مقایسه با روش‌های قبلی	استفاده از شبکه‌های عصبی عمیق(DNN) ، CNN، RNNو AEs	بهبود سیستم‌های پیشنهاددهی فیلم با شبکه‌های عصبی عمیق	2024	**مبوروک و همکاران**
بهبود عملکرد در ارائه پیشنهادهای بهینه‌تر با استفاده از تصاویر و متن	استفاده از شبکه‌های عصبی پیچشی و مدل‌های زبان برای تحلیل متنی	سیستم پیشنهاددهی چندوجهی با استفاده از شبکه‌های عصبی پیچشی و مدل‌های زبان	2024	**هی و همکاران**
ارائه پروفایل‌های دقیق‌تر کاربران و توصیه‌های دقیق‌تر	توسعه سیستم آگاه از بافت با استفاده از تحلیل زمانی، مکانی و محیط اجتماعی	الگوریتم پیشنهاددهی توالی چنددیدگاهی با یادگیری عمیق آگاه از بافت	2024	**وی و همکاران**
راهنمایی برای طراحی نسل بعدی سیستم‌های پیشنهاددهی چندوجهی	مرور روش‌های چندوجهی و ارزیابی آن‌ها در چارچوبElliot	فرمالیزه کردن پیشنهاددهی چندرسانه‌ای با یادگیری عمیق چندوجهی	2024	**مالیتستا و همکاران**
افزایش دقت پیش‌بینی امتیازات کاربران نسبت به الگوریتم‌های پایه	استفاده از BERT و ViT برای استخراج ویژگی‌های پوستر و متن	پیشنهاددهی فیلم با استفاده از پوستر و ترنسفورمر چندوجهی	2024	**ژی و همکاران**
عملکرد بهتر نسبت به مدل‌های چندوجهی در سه مجموعه داده مختلف	استفاده از چارچوب CLIPER برای کاهش شکاف معنایی بین مدالیت‌ها	سیستم پیشنهاددهی چندوجهی با استفاده از چارچوبCLIPER	2024	**وو و همکاران**
بهبود دقت در ترکیب ویژگی‌های کوتاه‌مدت و بلندمدت کاربران	استفاده ازANN ، CNNو RNNبرای ترکیب ویژگی‌های کوتاه‌مدت و بلندمدت	سیستم پیشنهاددهی فیلم بهبود یافته با تکنیک‌های یادگیری عمیق	2024	**توکال و همکاران**
بهبود ساختار و دقت پیشنهاددهی از طریق نمودارهای کاربر-آیتم	شبکه‌های عصبی گراف برای استخراج روابط در نمودار کاربر-آیتم	شبکه‌های عصبی گراف برای پیشنهاددهی چندوجهی	2024	**مالیتستا**
بهبود دقت پیشنهاددهی و افزایش نقش اطلاعات متنی	ادغام و پالایش داده‌های چندوجهی با فیلترهای پالایشی	سیستم پیشنهاددهی چندوجهی با شبکه گرافی و پالایش داده‌ها	2024	**بوراباک و آیکتین**

بررسی مطالعات انجام‌شده نشان می‌دهد که در سال‌های اخیر رویکردهای مختلفی در زمینه سیستم‌های پیشنهاددهی چندوجهی و مبتنی بر یادگیری عمیق توسعه یافته‌اند. هرچند بسیاری از تحقیقات بر بهبود دقت و شخصی‌سازی پیشنهادها تمرکز کرده‌اند، برخی چالش‌های مهم همچنان به‌طور کامل حل نشده‌اند. برای مثال، پژوهش‌هایی که از روش‌های ترکیبی مانند یادگیری تقویتی عمیق و فیلترگذاری مشارکتی بهره برده‌اند، بیشتر بر افزایش دقت در شرایط کمبود داده و مسئله شروع سرد تمرکز کرده‌اند، در حالی که چالش‌های دیگری نظیر یکپارچه‌سازی کامل داده‌های چندوجهی و بهینه‌سازی کارایی سیستم در زمان واقعی کمتر مورد توجه بوده‌اند. اگرچه روش‌های مختلفی برای پردازش تصاویر

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

پزشکی، مانند شبکه‌های عصبی پیچشی سبک برای تشخیص آلزایمر [15] و معماری‌های U-Net برای بخش‌بندی تصاویرMR [16] پیشنهاد شده‌اند، اما این رویکردها اغلب در مواجهه با داده‌های پویا و چندوجهی، قابلیت انطباق کافی ندارند. علاوه بر این، الگوریتم‌های بهینه‌سازی مانند «انطباق پیش‌رو» کارایی آموزش مدل‌های یادگیری عمیق را بهبود داده‌اند [17]، اما کاربرد آن‌ها در سیستم‌های پیشنهاددهی چندوجهی هنوز مورد بررسی قرار نگرفته است. این مطالعه با ادغام تکنیک‌های پیشرفته بهینه‌سازی و همجوشی داده‌های چندوجهی، به بررسی این شکاف و افزایش دقت پیشنهاددهی می‌پردازد. بسیاری از مطالعات نیز به استفاده از روش‌های پیشرفته‌ای چون شبکه‌های عصبی گراف و یادگیری متقابل عمیق برای بهبود سیستم‌های چندوجهی پرداخته‌اند. اما، موضوعاتی مانند تفسیرپذیری و شفافیت پیشنهادهای ارائه‌شده و چگونگی همجوشی و ترکیب مناسب ویژگی‌های متنی، تصویری و زمانی به‌طور کامل بررسی نشده است. این مسئله به‌خصوص در حوزه‌هایی که کاربران نیازمند فهمیدن دلایل پیشنهادها هستند، اهمیت بیشتری پیدا می‌کند. علاوه بر این، در حالی که برخی تحقیقات از روش‌های جدید مانند مدل‌های ترنسفورمری و شبکه‌های پیچشی استفاده کرده‌اند، کمبود مطالعاتی که به ترکیب این روش‌ها با روش‌های سنتی برای افزایش تنوع پیشنهادها توجه کنند، مشهود است.

روش شناسی

در این مقاله، یک سیستم پیشنهاددهی چندوجهی فیلم مبتنی بر شبکه‌های عصبی گراف (GNN) ارائه می‌شود که داده‌های متنی (مانند ژانر و خلاصه داستان) و داده‌های تصویری (مانند پوستر فیلم) را برای ارائه پیشنهادهای شخصی‌سازی‌شده ترکیب می‌کند. این روش شامل مراحل اصلی زیر است: پیش‌پردازش داده‌ها، استخراج ویژگی‌های چندوجهی، ساختاردهی گراف و استفاده از شبکه عصبی گرافی برای پردازش و همجوشی داده‌ها.

۱. پیش‌پردازش داده‌ها

داده‌های متنی، شامل ژانر و توضیحات کوتاه فیلم، ابتدا به توکن‌های متنی تبدیل شده و با استفاده از مدل تعبیه‌سازی متن BERT به بردارهای ویژگی تبدیل می‌شوند. داده‌های تصویری، مانند پوستر فیلم، به شبکه‌های عصبی پیچشی (CNN) داده می‌شوند تا ویژگی‌های تصویری مهم استخراج شوند.

۲. ساختاردهی گراف

در این مرحله، شبکه‌ای گرافی تشکیل می‌شود که گره‌های آن نشان‌دهنده کاربران و فیلم‌ها است. لبه‌های گراف نمایانگر تعاملات کاربران و فیلم‌ها (مانند امتیازها یا بازدیدها) هستند. همچنین، ویژگی‌های استخراج شده از داده‌های متنی و تصویری به گره‌های فیلم افزوده می‌شود تا همجوشی داده‌ها تسهیل شود.

۳. مدل شبکه عصبی گراف(GNN)

در این روش از شبکه‌های عصبی گراف برای پردازش داده‌های گراف استفاده می‌شود. مدل پیشنهادی با استفاده از لایه گراف کانولوشن (GCN) یا گراف آَتنشن(GAT) ، ویژگی‌های هر گره را از همسایگان خود می‌آموزد و اطلاعات را در طول گراف به‌روزرسانی می‌کند. معادلات زیر برای به‌روزرسانی و انتشار ویژگی‌ها در گراف به کار می‌روند:

1. لایه گراف کانولوشن(GCN)

(1)

$$H^{(t+1)} = \sigma\left(D^{\frac{1}{2}}AD^{-\frac{1}{2}}H^{(l)}W^{(l)}\right)$$

در این معادله:

- A ماتریس مجاورت گراف است.
- D ماتریس درجه است که مقدار لبه‌های مرتبط با هر گره را نشان می‌دهد.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

- $H^{(l)}$ ویژگی‌های گره‌ها در لایه l است.
- $W^{(l)}$ وزن‌های قابل یادگیری مدل در لایه l است.
- σ تابع فعال‌سازی مانند $ReLU$ است.

2. گراف اَتِنشن(GAT) : برای بهبود اهمیت ارتباطات میان گره‌ها، مدل GAT از مکانیزم توجه استفاده می‌کند:

(2)

$$h_i' = \sigma\left(\sum_{j \in N(i)} a_{ij} W h_j\right)$$

که در آن:

- a_{ij} مقدار توجه بین گره i و j است که با توجه به ویژگی‌های گره‌ها محاسبه می‌شود.
- W ماتریس وزن قابل یادگیری است.

3. ادغام ویژگی‌های چندوجهی (همجوشی) برای همجوشی ویژگی‌های متنی و تصویری با گره‌های گراف، از ترکیب ویژگی‌ها استفاده می‌شود. بردار ویژگی نهایی فیلم به شکل زیر تعریف می‌شود:

(3)

$$h_{movie} = [h_{text}; h_{image}]$$

که در آن:

- h_{text} و h_{image} به ترتیب ویژگی‌های متنی و تصویری فیلم هستند.

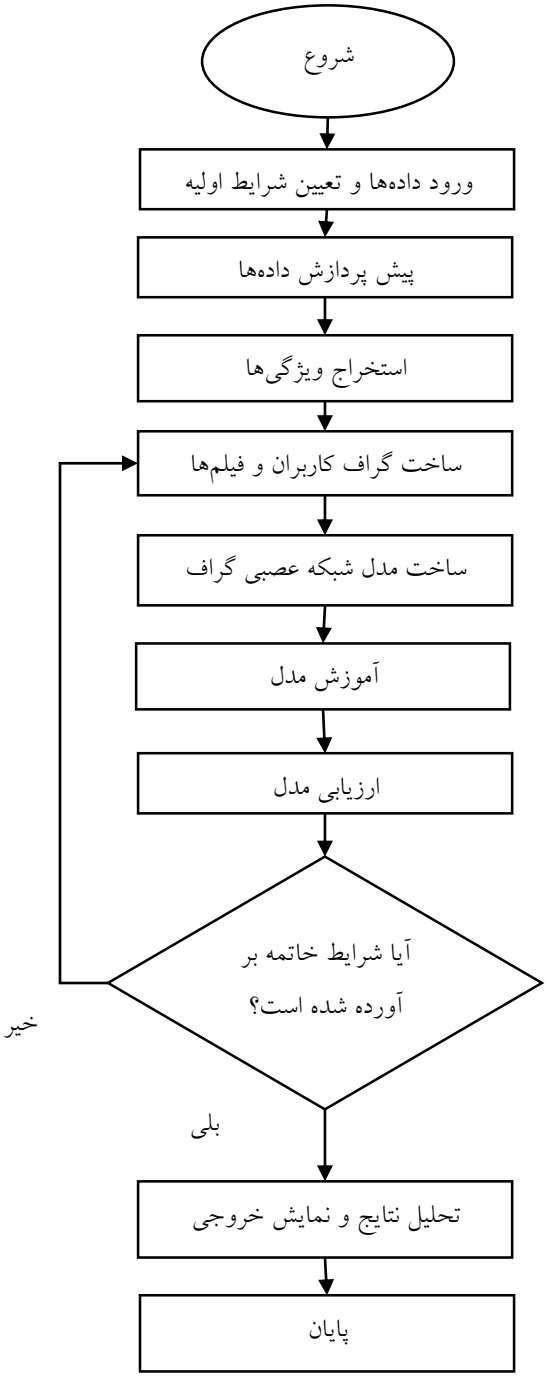
4. آموزش و بهینه‌سازی

مدل پیشنهادی با استفاده از تابع زیان میانگین مربعات خطا (MSE) و تابع زیان متقابل (Cross-Entropy) برای ارزیابی دقت پیشنهادها آموزش داده می‌شود. در نهایت، مدل به گونه‌ای بهینه‌سازی می‌شود که خطای پیش‌بینی‌های آن کمینه شود.

۵. ارزیابی مدل

برای ارزیابی مدل، از معیارهای مختلفی مانند دقت(Precision) ، بازخوانی (Recall) و نمره F1 استفاده می‌شود تا عملکرد مدل در ارائه پیشنهادها بررسی شود. همچنین، عملکرد مدل پیشنهادی با مدل‌های پایه مقایسه می‌شود تا میزان بهبود دقت و تنوع پیشنهادها ارزیابی شود.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055



شکل-1 فلوچارت روش پژوهش

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

نتایج و بحث

در این بخش، مدل پیشنهادی با استفاده از داده‌های شبیه‌سازی شده و ارزیابی معیارهای مختلف مورد بررسی قرار می‌گیرد.

برای این منظور، از مجموعه داده Movie Lens (نسخه‌های 100 Kو M1) استفاده می‌شود که به دلیل ساختار مناسب و تنوع داده‌ها، گزینه خوبی برای آزمایش سیستم‌های پیشنهاددهی به‌شمار می‌رود. علاوه بر این، برخی از داده‌ها به‌صورت شبیه‌سازی شده ایجاد می‌شوند تا ویژگی‌های متنی و تصویری فیلم‌ها (مانند ژانر، خلاصه، پوستر) و تعاملات کاربران شبیه‌سازی شوند. در شبیه‌سازی، از داده‌های متنی و تصویری فرضی به عنوان ورودی‌های گره‌های فیلم و از مشخصات کاربران برای گره‌های کاربر استفاده می‌شود. داده‌های متنی از طریق مدل‌های تعبیه‌سازی مانند BERTبه بردارهای عددی تبدیل می‌شوند و داده‌های تصویری با استفاده از مدل‌های پیچشی پردازش می‌شوند. برای ارزیابی عملکرد مدل پیشنهادی، از معیارهای دقت(Precision) ، بازخوانی(Recall) ، نمره F1 و خطای میانگین مربعات(MSE) استفاده می‌شود. این معیارها به ما امکان می‌دهند که عملکرد مدل در ارائه پیشنهادهای شخصی‌سازی شده و کاهش خطای پیش‌بینی را اندازه‌گیری کنیم. برای اطمینان از کارایی مدل، عملکرد آن با مدل‌های پایه مقایسه می‌شود.

پارامترهای شبیه‌سازی به نحوی تنظیم شده‌اند که شرایط واقعی سیستم‌های پیشنهاددهی را بازسازی کنند. در جدول -2، پارامترهای اصلی شبیه‌سازی و مقادیر آنها ارائه شده است:

جدول -2 پارامترهای شبیه سازی روش پیشنهادی

پارامتر	مقدار
تعداد فیلم‌ها	1000
تعداد کاربران	500
تعداد تعاملات کاربر-فیلم	10000
طول بردار متنی	256
طول بردار تصویری	128
تعداد لایه‌هایGCN	2
نرخ یادگیری	0.001
تعداد اپوک‌ها	100

این مقادیر با توجه به نیازهای سیستم پیشنهاددهی تنظیم شده‌اند تا بهینه‌سازی و دقت مدل به‌طور موثری انجام شود.

مدل پیشنهادی ابتدا با استفاده از داده‌های شبیه‌سازی شده آموزش می‌بیند و سپس بر روی مجموعه داده آزمون ارزیابی می‌شود. نتایج نشان می‌دهند که ترکیب ویژگی‌های متنی و تصویری در یک ساختار گرافی، عملکرد بهتری نسبت به مدل‌های صرفاً متنی یا تصویری ارائه می‌دهد. این ارزیابی نشان می‌دهد که روش پیشنهادی با استفاده از همجوشی داده‌ها و بهره‌گیری از شبکه‌های عصبی گرافی، می‌تواند پیشنهادهای دقیق‌تر و کاربرپسندتری ارائه دهد.

جدول -3 نتایج مقادیر خطا (Loss) را در پایان هر ۱۰ دوره نشان می‌دهد. با بررسی این نتایج، می‌توان موارد زیر را استنباط کرد:

جدول -3: نتایج ارزیابی مدل در بازه‌های ۱۰ دوره‌ای

دوره(Epoch)	مقدار خطا(Loss)
10	1.134210
20	0.996586
30	1.318439
40	1.144770
50	0.714058
60	1.043826
70	1.008833
80	1.342521
90	0.898000
100	1.122035

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

1. نوسانات خطا: مقادیر خطا در طول دوره‌های مختلف تا حدی نوسان دارد و این امر نشان می‌دهد که مدل در مراحل مختلف به درجات مختلفی از دقت دست یافته است.
2. کاهش تدریجی خطا: به‌طور کلی، در طول ۱۰۰ دوره، مقادیر خطا به سمت کاهش میل می‌کنند، به‌خصوص از دوره ۵۰ تا ۱۰۰ که مقدار خطا بیشتر به سمت تثبیت گرایش پیدا می‌کند.
3. افزایش دقت در اواخر دوره‌ها: با نزدیک شدن به ۱۰۰ دوره، مقدار خطا تقریباً به میزان ۱،۱۲ می‌رسد که نسبت به مقدار ابتدایی بهبود یافته است. این نشان می‌دهد که مدل در حال همگرایی و بهبود دقت است.

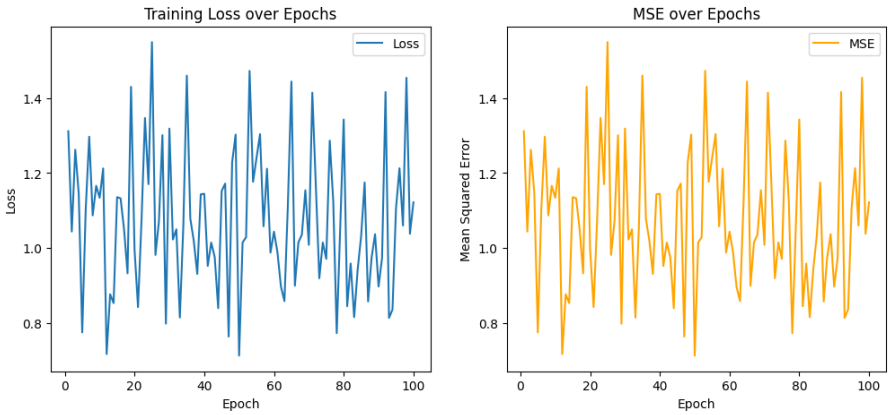
جدول-4: نتایج ارزیابی مدل در ۱۰ دوره ابتدایی

دوره(Epoch)	مقدار خطا(Loss)	میانگین مربعات خطا(MSE)
1	1.311481	1.311481
2	1.044312	1.044312
3	1.262064	1.262064
4	1.144806	1.144806
5	0.775845	0.775845
6	1.103355	1.103355
7	1.296755	1.296755
8	1.087321	1.087321
9	1.166090	1.166090
10	1.134210	1.134210

جدول-4، مقادیر خطا و میانگین مربعات خطا را در ۱۰ دوره اول آموزش مدل نشان می‌دهد. تحلیل این نتایج شامل نکات زیر است:

1. نوسانات ابتدایی در مقدار خطا: در دوره‌های ابتدایی، مقادیر خطا و MSE به صورت متناوب کاهش و افزایش داشته‌اند که به دلیل شروع فرآیند یادگیری مدل و تنظیم وزن‌ها طبیعی است.
2. بهبود تدریجی دقت: به تدریج از دوره ۴ به بعد، مقادیر خطا و MSE بهبود پیدا کرده و مقادیر پایین‌تری را نشان می‌دهند. این روند نشان می‌دهد که مدل در حال یادگیری الگوهای بهتر و نزدیک‌تر شدن به نتایج هدف است.
3. ثبات بیشتر در دوره‌های بعدی: در دوره‌های بعدی، خطا به سمت ثبات بیشتر میل می‌کند که نشان‌دهنده همگرایی مدل است.

نتایج نشان می‌دهند که مدل با گذر زمان و دوره‌های آموزشی به تدریج به بهبود دقت دست یافته و به سمت مقدار خطای پایین‌تر و ثبات بیشتر در ارزیابی‌های نهایی نزدیک شده است. این نتایج نشان‌دهنده کارایی مدل در یادگیری الگوهای پیشنهادی و کاهش خطای پیش‌بینی برای توصیه‌ها است.

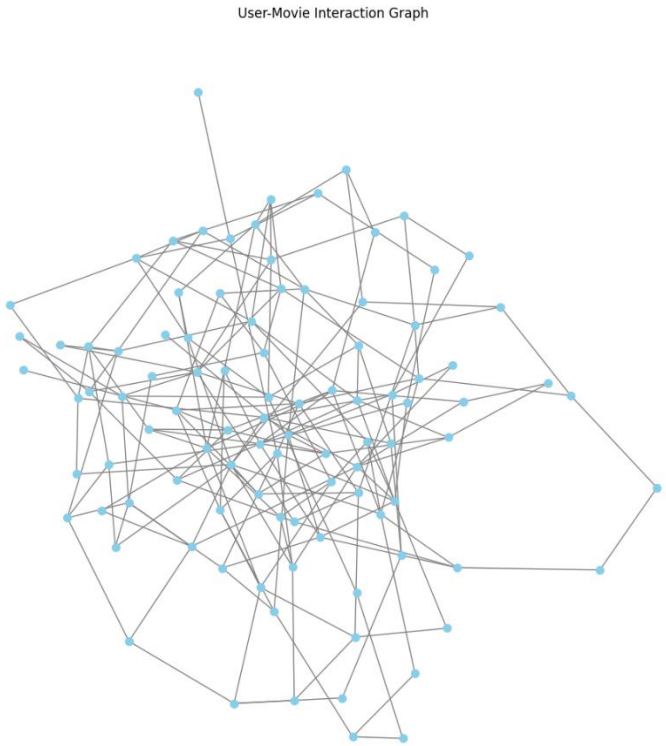


شکل-2 نمودارهای Training Loss و MSE در طول دوره‌ها

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

دو نمودار شکل-2، تغییرات خطا (Loss) و میانگین مربعات خطا (MSE) را در طول دوره‌های آموزشی مدل نشان می‌دهند.

- نمودارTraining Loss over Epochs : این نمودار، مقدار خطا را در طول ۱۰۰ دوره آموزشی نمایش می‌دهد. همان‌طور که مشاهده می‌شود، مقدار خطا دارای نوسانات زیادی است و به‌طور کامل تثبیت نشده است. این نوسانات به دلیل تنظیمات اولیه مدل و فرآیند یادگیری رخ می‌دهد.
- نمودارMSE over Epochs : این نمودار میانگین مربعات خطا را در طول دوره‌ها نمایش می‌دهد. MSE نیز دارای نوسانات مشابه خطا است و نشان می‌دهد که مدل در حال یادگیری و تنظیم وزن‌ها است.
- نوسانات زیاد: مقدار خطا و MSE در دوره‌های مختلف دچار نوسانات زیادی می‌شوند که ممکن است نشان‌دهنده عدم همگرایی کامل مدل باشد. این نوسانات به دلایل مختلفی از جمله تنظیمات اولیه وزن‌ها، نرخ یادگیری، و تعداد داده‌های آموزشی ممکن است رخ دهد.
- کاهش نسبی خطا وMSE : در کل، با وجود نوسانات، می‌توان دید که مدل در طول دوره‌ها به سمت کاهش خطا و MSE حرکت می‌کند. این نشان‌دهنده بهبود نسبی دقت مدل و کاهش خطاهای پیش‌بینی است.
- عدم تثبیت کامل خطا: با وجود کاهش خطا، این نمودارها نشان می‌دهند که مدل هنوز به تثبیت کامل نرسیده است. این امر ممکن است با افزایش تعداد دوره‌ها و بهینه‌سازی بیشتر مدل بهبود یابد.



شکل -3 گراف تعاملات کاربر-فیلم

شکل-3، گراف تعاملات کاربران و فیلم‌ها را نشان می‌دهد. در این گراف، گره‌ها نمایانگر کاربران و فیلم‌ها هستند و لبه‌ها تعاملات میان آن‌ها را نشان می‌دهند. این گراف به ما کمک می‌کند تا روابط میان کاربران و فیلم‌ها را به‌صورت بصری مشاهده کنیم. گراف تعاملات به‌طور طبیعی دارای ساختاری متراکم است که نشان‌دهنده تنوع سلایق کاربران و تمایل آن‌ها به تعامل با فیلم‌های مختلف است.

- تراکم روابط: تمرکز روابط در مرکز گراف نشان می‌دهد که برخی کاربران و فیلم‌ها دارای تعاملات بیشتری هستند که ممکن است نشان‌دهنده جذابیت بالای این فیلم‌ها باشد.
- توزیع پراکنده: برخی گره‌ها در اطراف گراف قرار دارند که نشان‌دهنده تعاملات کمتر آن‌ها است؛ این امر می‌تواند به دلایلی همچون جدید بودن کاربران یا فیلم‌ها یا عدم جذابیت آن‌ها باشد.

تحلیل نتایج نشان می‌دهند که مدل در حال یادگیری است و به تدریج به دقت بالاتری دست می‌یابد، اما همچنان نیاز به بهینه‌سازی بیشتری برای دستیابی به نتایج باثبات‌تر دارد. در پژوهش‌های آتی می‌توان پارامترهای یادگیری مدل (مانند نرخ یادگیری و تعداد دوره‌ها) بررسی و بهینه شوند تا مدل به همگرایی و تثبیت بیشتری دست یابد.

نتیجه‌گیری

در این پژوهش، یک مدل پیشنهاددهی چندوجهی مبتنی بر شبکه‌های عصبی گرافی برای بهبود دقت و کارایی سیستم‌های توصیه‌گر فیلم ارائه شد. هدف اصلی این مدل، ترکیب ویژگی‌های متنی و تصویری فیلم‌ها با استفاده از شبکه‌های عصبی گرافی (GCN) بود تا بتواند الگوهای پنهان در روابط بین کاربران و فیلم‌ها را استخراج کرده و توصیه‌های بهتری ارائه دهد. با توجه به پیچیدگی‌های داده‌های چندوجهی، استفاده از یک ساختار گرافی برای مدل‌سازی تعاملات میان کاربران و آیتم‌ها کمک شایانی به افزایش دقت و شخصی‌سازی پیشنهادها کرد.

در فرآیند آموزش مدل، گراف تعاملات کاربر-فیلم به‌عنوان ساختار داده‌ای اصلی استفاده شد که شامل ویژگی‌های متنی و تصویری به‌عنوان ورودی‌های مدل بود. نتایج نشان دادند که مدل پیشنهادی با وجود نوسانات اولیه، به مرور زمان به دقت بیشتری دست یافت. با این حال، نمودارهای خطا و MSE همچنان نوساناتی داشتند که نشان‌دهنده این است که مدل به‌طور کامل به همگرایی و ثبات نرسیده است. این موضوع می‌تواند ناشی از تعداد محدود دوره‌های آموزشی یا تنظیمات بهینه‌سازی باشد.

تحلیل نتایج همچنین نشان داد که گراف تعاملات کاربر-فیلم، به‌ویژه در بخش‌هایی که تراکم بیشتری دارد، نشان‌دهنده تعاملات پربسامد میان کاربران و فیلم‌ها است. این گره‌ها احتمالاً نمایانگر فیلم‌های محبوب یا کاربران فعال‌تر هستند که تأثیر زیادی بر توصیه‌های سیستم دارند. این یافته‌ها با اصول پایه‌ای سیستم‌های توصیه‌گر هماهنگ است؛ به این معنا که فیلم‌های پربیننده و کاربران پرفعالیت، وزن بیشتری در آموزش مدل دارند و می‌توانند دقت مدل را بهبود دهند.

نکته دیگری که از نتایج قابل برداشت است، کارایی بالای روش‌های گرافی در پردازش داده‌های چندوجهی است. شبکه‌های عصبی گرافی قابلیت استخراج ویژگی‌های پیچیده از داده‌های غیرساختاریافته را دارند و این ویژگی به‌خصوص در سیستم‌های توصیه‌گر که با داده‌های چندوجهی متنی، تصویری و تعاملی سروکار دارند، می‌تواند بسیار مؤثر باشد. به علاوه، ترکیب اطلاعات مختلف و همجوشی ویژگی‌های چندوجهی منجر به ایجاد نمایه‌های دقیق‌تری از فیلم‌ها و کاربران می‌شود و این امر توصیه‌های شخصی‌سازی‌شده‌تر و دقیق‌تری را ممکن می‌سازد.

با توجه به نتایج به‌دست‌آمده و محدودیت‌های موجود، پیشنهادهای زیر برای بهبود و توسعه مدل در تحقیقات آینده ارائه می‌شود:

1. افزایش تعداد دوره‌های آموزشی و بهبود تنظیمات بهینه‌سازی: با توجه به اینکه نمودارهای خطا و MSE همچنان دارای نوساناتی هستند، می‌توان در تحقیقات آتی، تعداد دوره‌های آموزشی را افزایش داده و تنظیمات بهینه‌سازی مانند نرخ یادگیری و الگوریتم بهینه‌سازی را بررسی کرد تا مدل به همگرایی و تثبیت بیشتری برسد.
2. استفاده از تکنیک‌های پیشرفته‌تر همجوشی ویژگی‌ها: در این پژوهش، همجوشی ویژگی‌های متنی و تصویری با استفاده از روش‌های ساده‌تری انجام شد. در مطالعات آتی، می‌توان از تکنیک‌های پیچیده‌تر همجوشی مانند توجه چندگانه (Multi-head Attention) یا شبکه‌های خودتوجهی (Self-attention) برای بهبود دقت مدل استفاده کرد. این روش‌ها می‌توانند همبستگی‌های بیشتری بین ویژگی‌های متنی و تصویری را در نظر گرفته و مدل‌سازی دقیق‌تری انجام دهند.
3. استفاده از داده‌های واقعی و مقیاس‌پذیر: در این پژوهش، از داده‌های شبیه‌سازی شده برای آزمایش مدل استفاده شد. برای بررسی کاربرد مدل در شرایط واقعی، پیشنهاد می‌شود از مجموعه داده‌های واقعی و بزرگ‌تری مانند مجموعه داده‌های MovieLens با مقیاس بالاتر استفاده شود. داده‌های واقعی با تنوع بیشتر می‌توانند چالش‌های جدیدی را برای مدل به همراه داشته باشند و موجب افزایش قابلیت تعمیم‌دهی مدل شوند.

4. ترکیب شبکه‌های عصبی گرافی با مدل‌های دیگر: استفاده از ترکیبی از مدل‌های شبکه‌های عصبی گرافی (GCN) با سایر مدل‌های یادگیری عمیق مانند شبکه‌های عصبی بازگشتی (RNN) یا مدل‌های ترنسفورمر می‌تواند عملکرد مدل را بهبود بخشد. به‌ویژه، استفاده از مدل‌های ترنسفورمری می‌تواند با توجه به قابلیت آن‌ها در استخراج ویژگی‌های پیچیده‌تر، دقت سیستم‌های پیشنهاددهی را افزایش دهد.

5. توجه به قابلیت تفسیرپذیری مدل: یکی از چالش‌های سیستم‌های توصیه‌گر، توضیح دلایل پیشنهادها است. در تحقیقات آتی، می‌توان از مدل‌هایی با تفسیرپذیری بیشتر استفاده کرد تا کاربران بتوانند دلایل پیشنهادها را بهتر درک کنند. این امر می‌تواند اعتماد کاربران به سیستم پیشنهاددهی را افزایش دهد.

6. ارزیابی با معیارهای متنوع‌تر: در این پژوهش، معیارهای خطا و MSE به عنوان معیارهای ارزیابی استفاده شدند. برای ارزیابی جامع‌تر مدل، پیشنهاد می‌شود از معیارهای دیگری مانند دقت (Precision)، بازخوانی (Recall) و نرخ کلیک (Click-Through Rate) استفاده شود. این معیارها می‌توانند عملکرد مدل را از جنبه‌های مختلف بررسی کرده و نقاط ضعف و قوت آن را دقیق‌تر شناسایی کنند.

این پژوهش نشان داد که استفاده از شبکه‌های عصبی گرافی در سیستم‌های توصیه‌گر فیلم می‌تواند کارایی و دقت توصیه‌ها را بهبود دهد. با این حال، همچنان نیاز به بهینه‌سازی و آزمایش‌های بیشتر برای رسیدن به مدلی پایدار و باثبات وجود دارد. ترکیب ویژگی‌های چندوجهی با شبکه‌های عصبی گرافی، نتایج امیدوارکننده‌ای ارائه داد و می‌تواند به‌عنوان مبنایی برای توسعه بیشتر مدل‌های توصیه‌گر استفاده شود.

در نهایت، توسعه این مدل‌ها و بهبود روش‌های همجوشی ویژگی‌ها در سیستم‌های پیشنهاددهی می‌تواند منجر به ارائه پیشنهادهای دقیق‌تر و شخصی‌سازی‌شده‌تر برای کاربران شود و تجربه کاربری بهتری را در محیط‌های دیجیتال به ارمغان آورد.

تشکر و قدردانی

این پژوهش بدون حمایت یا مشارکت از سوی مؤسسات، افراد یا سازمان‌های خاص انجام شده است.

فهرست منابع

[1]. Xia, L., Yang, Y., Chen, Z., Yang, Z., & Zhu, S. (2024). Movie Recommendation with Poster Attention via Multi-modal Transformer Feature Fusion. *arXiv preprint arXiv:2407.09157*.
[2]. Wu, X., Huang, A., Yang, H., He, H., Tai, Y., & Zhang, W. (2024). Towards Bridging the Cross-modal Semantic Gap for Multi-modal Recommendation. *arXiv preprint arXiv:2407.05420*.
[3]. Tokala, S., Nagaram, J., Enduri, M. K., & Lakshmi, T. J. (2024, June). Enhanced Movie Recommender system using Deep Learning Techniques. In *2024 3rd International Conference on Computational Modelling, Simulation and Optimization (ICCMSO)* (pp. 71-75). IEEE.
[4]. Malitesta, D. (2024). Graph neural networks for recommendation leveraging multimodal information.
[5]. Burabak, M., & Aytekin, T. (2024). SynerGraph: An Integrated Graph Convolution Network for Multimodal Recommendation. *arXiv preprint arXiv:2405.19031*.
[6]. Mouhiha, M., Oualhaj, O. A., & Mabrouk, A. (2024, May). Enhancing Movie Recommendations: A Deep Neural Network Approach with MovieLens Case Study. In *2024 International Wireless Communications and Mobile Computing (IWCMC)* (pp. 1303-1308). IEEE.
[7]. He, J., Zhang, L., Cao, W., Yang, M., Li, M., Zhao, Z., & Leung, M. F. (2024, May). Multi-modal Bayesian Recommendation System. In *2024 IEEE 6th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)* (Vol. 6, pp. 141-145). IEEE.
[8]. Wei, X., Dou, J., Wang, S., Zhang, Y., Hou, B., & Wang, F. (2024, May). Multi-view Sequence Recommendation Model. In *2024 IEEE 6th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)* (Vol. 6, pp. 645-648). IEEE.
[9]. Malitesta, D., Cornacchia, G., Pomo, C., Merra, F. A., Di Noia, T., & Di Sciascio, E. (2018). Formalizing multimedia recommendation through multimodal deep learning. *ACM Transactions on Recommender Systems*.
[10]. Siet, S., Peng, S., Ilkhomjon, S., Kang, M., & Park, D. S. (2024). Enhancing sequence movie recommendation system using deep learning and kmeans. *Applied Sciences*, *14*(6), 2505.

[11]. Kim, W. H., Kim, G. W., & Kim, J. C. (2024). Multi-Modal Deep Learning based Metadata Extensions for Video Clipping. *International Journal on Advanced Science, Engineering & Information Technology*, *14*(1).
[12]. Zhan, Y., Xie, H., Huan, H., & Che, S. (2024, February). Research on Movie Recommendation Algorithm based on Deep Learning. In *2024 International Conference on Integrated Circuits and Communication Systems (ICICACS)* (pp. 1-6). IEEE.
[13]. Peng, S., Siet, S., Ilkhomjon, S., Kim, D. Y., & Park, D. S. (2024). Integration of deep reinforcement learning with collaborative filtering for movie recommendation systems. *Applied Sciences*, *14*(3), 1155.
[14]. Li, J., Yang, C., Ye, G., & Nguyen, Q. V. H. (2024). Graph neural networks with deep mutual learning for designing multi-modal recommendation systems. *Information Sciences*, *654*, 119815.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

تشخیص حمله کانال جانبی بر اساس ماشین بردار پشتیبان بهبودیافته

دانیال جعفری[1]

[1]دانشجو کارشناسی ارشد نرم افزار، دانشگاه امام رضا،jafaridaniel18@gmail.com

چکیده:

در حوزه تشخیص حملات کانال جانبی، استفاده از تکنیک‌های یادگیری ماشین به‌ویژه ماشین بردار پشتیبان (SVM) به‌عنوان یکی از روش‌های موثر مورد توجه قرار گرفته است. در تحقیقات اخیر، بهبود عملکرد SVM با بهره‌گیری از الگوریتم بازپخت شبیه‌سازی‌شده به‌منظور تنظیم بهینه پارامترها بررسی شده است. تنظیم مناسب پارامترهایSVM ، که یکی از چالش‌های کلیدی در این زمینه محسوب می‌شود، یک مسئله NP-Hardاست بنابراین استفاده از روش‌های فراابتکاری برای حل آن پیشنهاد می‌شود. در این پژوهش، الگوریتم فراابتکاری یوزپلنگ که دارای قدرت همگرایی بالاتری نسبت به سایر روش‌های بهینه‌سازی مانند بازپخت شبیه‌سازی‌شده است، برای اولین‌بار به‌منظور بهبود عملکرد SVM در تشخیص حملات کانال جانبی به کار گرفته شده است. نتایج شبیه‌سازی روی مجموعه داده DPA Contest v4 نشان می‌دهد که روش پیشنهادی توانسته دقت تشخیص را در مقایسه با SVM استاندارد و نسخه بهبودیافته آن با الگوریتم بازپخت شبیه‌سازی‌شده، به میزان 1 درصد افزایش دهد. این بهبود عملکرد نشان‌دهنده ظرفیت بالای الگوریتم یوزپلنگ در بهینه‌سازی مسائل پیچیده و حساس مانند تشخیص حملات کانال جانبی است.

مقدمه:

هنگامی که الگوریتم‌های رمزنگاری بر روی دستگاه‌های الکتریکی پیاده سازی می‌شوند، مدار سخت‌افزاری، اطلاعات فیزیکی مرتبط مانند: زمان [1]، تابش الکترومغناطیسی [2]، مصرف انرژی، اپتیک [3]، آکوستیک [4] و غیره را به صورت غیر مستقیم افشا می‌کنند. تجزیه و تحلیل کانال جانبی (SCA) بدون نیاز به تحلیل مستقیم خود الگوریتم رمزنگاری، از این اطلاعات فیزیکی نشت کرده استفاده می‌کند. تجزیه و تحلیل کانال جانبی معمولاً کلید اصلی را به چند کلید فرعی تقسیم می‌کند و اطلاعات فیزیکی لو رفته را مهاجم می‌تواند ضبط کند. در نهایت مهاجم با ترکیب این اطلاعات و استفاده از دانش مرتبط، کلید اصلی را بازیابی می کند.

زمانی که پل کوچر اولین حمله کانال جانبی شناخته شده عمومی (حمله کانال جانبی) را بر روی چندین سیستم رمزنگاری[5] منتشر کرد، جذابیت زیادی در جامعه امنیتی برای بردارهای حمله فیزیکی مانند زمان بندی، مصرف انرژی[6]، تشعشعات الکترومغناطیسی (EM) [7] و صدا [8] ایجاد شد. در مقابل تحلیل های رمزنگاری سنتی که به شناسایی ضعف های نظری در ساختار الگوریتم های رمزنگاری می پردازند، حملات کانال جانبی بر شناسایی نقاط ضعف در پیاده سازی واقعی الگوریتم ها، در بخش نرم افزار و سخت افزار متمرکز هستند. این نوع حملات با بهره گیری از اطلاعات فیزیکی یا اجرایی نشت کرده، تلاش می کنند تا کلید مخفی را بازیابی کنند.

اگرچه بیشتر مطالعات در زمینه حملات کانال جانبی بر نفوذ به سیستم‌های رمزنگاری متمرکز شده‌اند، تحقیقات نشان داده است که اصول اساسی این نوع حملات می‌توانند انواع دیگری از تهدیدات را نیز به وجود آورند. برای مثال، حملات صوتی به صفحه‌کلید می‌توانند متن تایپ‌شده

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

را افشا کنند [9]، یا تجزیه و تحلیل توان مصرفی پردازنده‌های تعبیه‌شده می‌تواند اطلاعاتی درباره دستورالعمل‌های اجراشده را بازیابی کنند [10].

در تنظیمات رایج این نوع حملات، از روش‌هایی مانند بازرسی بصری آثار فیزیکی، تحلیل‌های آماری و تئوری اطلاعات استفاده می‌شود. حملات کانال جانبی مبتنی بر توان مصرفی را می‌توان به دو دسته اصلی تقسیم کرد: حملات غیر پروفایل (مانند: تجزیه و تحلیل توان ساده یا دیفرانسیلی [6]) و حملات پروفایل (شامل حملات مبتنی بر الگو یا رویکردهای تصادفی[11]) تقسیم کرد.

این دسته‌بندی نشان‌دهنده تنوع تکنیک‌ها و روش‌های موجود برای بهره‌برداری از اطلاعات فیزیکی نشت‌کرده در سیستم‌های محاسباتی است.

سیستم‌های یادگیری ماشین به طور کلی با افزایش تجربه در یک وظیفه خاص، عملکرد خود را بهبود می‌بخشند [12]. در مسائل طبقه‌بندی، این سیستم‌ها معمولاً با نمونه‌های آموزشی متشکل از بردارهای داده‌های ورودی (ویژگی‌ها) و خروجی‌های مرتبط (برچسب‌ها) آموزش داده می‌شوند،که این رویکرد به‌عنوان یادگیری نظارت‌شده شناخته می‌شود. در فرآیند آموزش، الگوریتم بر اساس داده‌های ورودی، پیش‌بینی‌هایی انجام می‌دهد و در صورت تطابق نداشتن این پیش‌بینی‌ها با برچسب‌های مورد انتظار، پارامترهای مدل اصلاح می‌شوند. هدف نهایی، ایجاد مدلی است که بتواند به طور مؤثر روی داده‌های دیده‌نشده تعمیم یابد؛ به این معنا که پیش‌بینی‌های دقیقی برای ورودی‌هایی که در داده‌های آموزشی حضور نداشته‌اند ارائه کند.

در مقابل، یادگیری بدون نظارت به وظایفی اشاره دارد که در آن برچسب‌های نتیجه در دسترس نیستند. در این حالت، الگوریتم سعی می‌کند ساختارهای زیربنایی یا ویژگی‌های پنهان مجموعه داده‌های ورودی را شناسایی کند، مثلاً با خوشه‌بندی داده‌ها به گروه‌های مختلف این کار را انجام می دهد.

یادگیری نیمه‌نظارت‌شده بین این دو دسته قرار می‌گیرد و حالتی را توصیف می‌کند که در آن برچسب‌های خروجی تنها برای بخشی از نمونه‌های آموزشی موجود است. این رویکرد تلاش می‌کند تا از ترکیب داده‌های برچسب‌دار و بدون برچسب برای بهبود عملکرد مدل بهره گیرد و ساختاری بهینه برای تحلیل مجموعه داده‌های ناقص ارائه دهد.

یادگیری ماشین به طور گسترده در بسیاری از حوزه‌ها مانند پردازش زبان طبیعی، تشخیص تصویر یا روباتیک استفاده می‌شود و اهمیت بیشتری برای سیستم‌های خودمختار آینده پیدا می‌کند [13]. علاوه بر این، تعداد زیادی مقاله نیز در سال‌های گذشته ارائه شده است که تکنیک‌های یادگیری ماشین را با تحلیل حملات کانال جانبی ترکیب کرده اند. جاپ و همکاران در یک بررسی، بخشی از تحقیقات مرتبط را که به کاربرد یادگیری ماشین در تحلیل توان مصرفی یا کانال‌های جانبی تشعشعات الکترومغناطیسی در پیاده‌سازی‌های رمزنگاری پرداخته‌اند، خلاصه کردند [14].

آنها خاطرنشان کردند که یک تشابه قوی بین مشکلات یادگیری ماشین نظارت شده و حمله‌های کانال جانبی نمایه شده و همچنین بین یادگیری ماشین بدون نظارت و حمله‌های کانال جانبی بدون پروفایل وجود دارد. در یکی از آخرین مقالات این حوزه [15] یک سیستم تحلیل کانال جانبی پیشنهاد شده است که در آن از روش بازپخت شبیه‌سازی‌شده و روش ماشین بردار پشتیبان برای تشخیص استفاده کرده است.

در این مقاله با توجه به عملکرد مناسب ماشین بردار پشتیبان در حمله کانال جانبی به ارائه روشی جدید از این روش یادگیری ماشین با تنظیم پارامترهای آن پرداخته شده است. تنظیم پارامتر ماشین بردار پشتیبان با روش بهینه‌سازی یورپلنگ [16] انجام می‌شود رویکردی که تاکنون

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

مورد استفاده قرار نگرفته است. دلیل انتخاب الگوریتم بهینه‌سازی یوزپلنگ، توانایی بالای آن در همگرایی به نقطه بهینه حتی در مسائلی با ابعاد بالا است. این ویژگی باعث می‌شود که مدل پیشنهادی بتواند مقادیر دقیق و بهینه‌ای را برای پارامترهای ماشین بردار پشتیبان پیدا کند، که به طور مستقیم بر دقت و کارایی سیستم تشخیص حملات کانال جانبی تأثیر می‌گذارد.

الگوریتم بهینه‌ساز یوزپلنگ [16] در سال 2022 معرفی شده است، بر اساس رفتار طبیعی یوزپلنگ در شکار طراحی شده و به عنوان الگوریتمی با قدرت جست‌وجوی بالا شناخته شده است. مطالعات نشان داده‌اند که این الگوریتم در آزمایش‌های انجام‌شده بر روی توابع تست، از نظر دقت همگرایی عملکرد بهتری نسبت به سایر روش‌ها داشته است. بر همین اساس، به نظر می‌رسد جایگزینی الگوریتم یوزپلنگ به جای روش بازپخت شبیه‌سازی‌شده که در مقاله [15] استفاده شده بود، می‌تواند منجر به افزایش صحت تشخیص در سیستم‌های تحلیل کانال جانبی شود. این ویژگی به خصوص در مسائل پیچیده‌ای که نیازمند جست‌وجوی دقیق و همگرایی سریع هستند، اهمیت بیشتری پیدا می‌کند.

بنابراین، با توجه به اینکه از روش ماشین بردار پشتیبان برای تشخیص حملات کانال جانبی استفاده شده است و همچنین به این نکته اشاره شده که تنظیم بهینه پارامترهای این روش می‌تواند تأثیر زیادی بر عملکرد آن داشته باشد، لازم به ذکر است که تاکنون چنین بهبودی در استفاده از ماشین بردار پشتیبان برای تشخیص حملات کانال جانبی صورت نگرفته است. به همین دلیل، در این پژوهش با هدف افزایش دقت تشخیص نفوذ، از طریق بهبود عملکرد ماشین بردار پشتیبان با استفاده از الگوریتم بهینه‌ساز یوزپلنگ، یک رویکرد جدید برای تشخیص نفوذ در شبکه‌های اینترنت اشیا ارائه می‌شود. این رویکرد می‌تواند به بهبود دقت و کارایی سیستم‌های تشخیص نفوذ کمک کند و در نهایت، تهدیدات امنیتی را در این شبکه‌ها کاهش دهد.

1. مرور ادبیات:

یکی از اولین مقالاتی که به کاربرد تکنیک‌های یادگیری ماشین در حمله‌های کانال جانبی پیاده سازی رمزنگاری می‌پردازد توسط هوسپودر و همکاران ارائه شد [17]. آنها از یک نوع ماشین بردار پشتیبان به نام ماشین بردار پشتیبانی حداقل مربع (LS-SVM) برای تشخیص رد قدرت یک نرم افزار محافظت نشده استفاده کردند. آنها نشان دادند که انتخاب پارامترهای LS-SVM به طور قابل توجهی بر عملکرد طبقه بندی تأثیر می‌گذارد، در حالی که اندازه مجموعه آموزشی اهمیت کمتری دارد.

هوسر و زونر نیز اولین کسانی بودند که از طبقه‌بندی چند کلاسه ماشین بردار پشتیبان برای تحلیل وزن های همینگ HW[15] یک بایت در پیاده‌سازی استاندارد رمزگذاری پیشرفته AES[16] که روی میکروکنترلر ATMega اجرا می‌شود، استفاده کردند [18]. آنها نشان دادند که حمله ماشین بردار پشتیبان نسبت به حمله الگو برای ردیابی قدرت با سطح نویز بالا مناسب‌تر است، زیرا این فرض را که داده‌ها زیربنای یک توزیع گاوسی چند متغیره هستند، راحت‌تر می‌کند. این مبنای کار بارتکوویتز و لمکه-راست یک سال بعد را فراهم کرد، که ماشین‌های بردار پشتیبانی احتمالی چند کلاسه را به همان روشی که در حملات الگو مشابه انجام می‌شد طراحی کنند [19]. همچنین در مقاله [20] مقادیر مطلق بردار وزن w تعیین می‌کند که آیا یک ویژگی متناظر تأثیر قابل توجهی بر عملکرد طبقه بندی دارد یا خیر؟ بنابراین، مقادیر وزنی با مقدار مطلق

[15] Hamming Weight
[16] advanced encryption standard

کوچک برای نادیده گرفتن ویژگی‌های بی‌اهمیت روی صفر تنظیم می‌شوند. کارایی روش بر اساس به اصطلاح آنتروپی حدس کلیدی (KGE) اندازه‌گیری شد، تکنیکی که دشواری بازیابی مقدار صحیح یک کلید را با توجه به تعداد مورد نیاز ردیابی کمیت می‌کند. آنها مشاهده کردند که هسته خطی در حملات قالب مبتنی بر ماشین بردار پشتیبان عملکرد مناسبی ندارد زیرا مشکل طبقه‌بندی خطی را ایجاد می‌کند، در حالی که هسته RBF برای مسائل غیرخطی مناسب‌تر است.

بانکو و همکاران چندین طبقه‌بندی کننده را در زمینه حملات تک ردیابی بررسی کردند [3]. این نوع حملات دشمنی را فرض می‌کنند که تنها به یک رد حمله دسترسی دارد. هنگام هدف قرار دادن رمزهای متقارن، حملات باید دارای تحمل خطا باشند به این معنا که اطلاعات نشت کانال جانبی برای یک مقدار میانی می‌تواند مجموعه‌ای از مقادیر ممکن باشد. نمونه‌هایی از ادبیات آنالیز توان ساده عمل‌گرایانه [21] است که مجموعه‌ای از پنج حدس وزن همینگ را تحمل می‌کند، در حالی که حمله‌های کانال جانبی جبری [22] به سه مقدار وزن همینگ ممکن محدود می‌شوند. در این مطالعه، الگوها، ماشین بردار پشتیبان، شبکه عصبی، درخت تصمیم و جنگل تصادفی برای خروجی فهرست رتبه‌بندی وزن‌های همینگ با توجه به ردپای مصرف انرژی به‌دست‌آمده از اجرای استاندارد رمزگذاری پیشرفته در حال اجرا بر روی دو پلتفرم آزمایشی در نظر گرفته شدند.

در [23] یک مطالعه اضافی اهمیت تنظیم پارامترهای مناسب را هنگام استفاده از تکنیک‌های یادگیری ماشین (قابل پارامترسازی) برای تجزیه و تحلیل کانال جانبی نشان داد. از مجموعه طبقه‌بندی‌کننده‌های نظارت‌شده، بررسی‌شده بهترین نتایج (از نظر دقت طبقه‌بندی با استفاده از اعتبارسنجی متقاطع ده‌برابر) از طریق تنظیم پارامتر برای ماشین بردار پشتیبان به‌دست آمد. با این حال، جنگل تصادفی با تنظیمات بهینه خود فقط کمی بدتر عمل کردند، اما نسبت به تغییرات مقدار پارامتر بسیار قوی‌تر بودند. علاوه بر این نشان داده شده است که یک الگوریتم با دقت تنظیم شده قادر است به دقت نسبتاً بالایی (بیش از 70٪ در هنگام داشتن نویز کم) برسد، حتی اگر فقط تعداد کمی از ویژگی‌های مرتبط استفاده شود (در اینجا 20٪).

در تحقیق [24] با عنوان یک سیستم تشخیص حمله کانال جانبی با استفاده از رویدادهای هسته پردازشگر و یک ماشین بردار پشتیبان به این موضوع اشاره دارد که توانسته روشی برای تشخیص و سرکوب حملات کانال باند جانبی با استفاده از یادگیری ماشین و رویدادهای هسته پردازشگر پیشنهاد کند. یک مدل یادگیری نظارت شده در پیاده‌سازی یک سیستم مبتنی بر شمارنده‌های رویداد سخت‌افزاری برای شناسایی اکسپلویت‌های مخرب مانند انواع SPECTER که در یک فرآیند و در یک سیستم مبتنی بر لینوکس -که به عنوان یک دستگاه محاسباتی Edge اجرا می‌شوند-، استفاده می‌شود. این رویکرد از سخت‌افزار موجود بر روی تراشه به منظور شناسایی انواع سوءاستفاده‌های مخرب در میان سایر فرآیندهای برنامه و تعلیق فرآیند متخلف استفاده می‌کند. در این تحقیق انواع مختلف حمله کانال جانبی تجزیه و تحلیل شده و نشان داده می شود که چگونه در سیستم تشخیص، برای شناسایی و واکنش همزمان چندین حمله به طور همزمان آموزش داده می‌شود و چگونه از تکنیک‌های کاهش ابعاد و تکنیک‌های انتخاب ویژگی از مجموعه بزرگی از داده‌های شمارنده برای بهبود نتایج عملکرد استفاده شده است؟

در تحقیق [25] با عنوان یادگیری ماشینی برای حملات کانال جانبی پین بر اساس حسگرهای حرکتی گوشی‌های هوشمند، به این موضوع اشاره دارد که حسگرهای حرکتی در تمام دستگاه‌های تلفن همراه ادغام شده‌اند و اطلاعات مفیدی را برای اهداف مختلف ارائه می‌دهند. با این حال، این داده‌های حسگر را می‌توان توسط هر برنامه و وب‌سایتی که از طریق مرورگر قابل دسترسی باشد، بدون نیاز به مجوزهای امنیتی خواند. در این مقاله، نشان داده شده است که اطلاعات مربوط به حرکات تلفن هوشمند می‌تواند منجر به شناسایی شماره شخصی تایپ شده توسط کاربر شود. برای کاهش میزان داده‌های لو رفته، از رویکرد رویداد محور استفاده می‌کند که در آن حسگرهای حرکتی فقط زمانی که یک کلید

فشار داده می‌شود نمونه‌برداری می‌شوند. داده‌های به‌دست‌آمده برای آموزش الگوریتم یادگیری ماشین برای طبقه‌بندی ضربه‌های کلید به شیوه‌ای تحت نظارت استفاده می‌شوند. همچنین کاربران هر بار که احراز هویت مورد نیاز است، پین یکسانی را وارد می‌کنند که منجر به اطلاعات بیشتر کانال جانبی در دسترس مهاجم می‌شود. نتایج عددی امکان‌پذیری حملات سایبری پین را بر اساس حسگرهای حرکتی، بدون محدودیت در طول پین و ترکیب‌های رقمی ممکن، نشان می‌دهد.

در تحقیق [26] با عنوان تشخیص نفوذ در محیط‌های IoT از طریق تکنیک‌های کانال جانبی و یادگیری ماشین با اشاره به این موضوع که ظهور فناوری اینترنت اشیا (IoT) در دهه گذشته منجر به کاربردهای متعدد در زمینه‌های مختلف شده است. برخی از داده‌های پردازش شده با استفاده از این فناوری می‌توانند حساس بوده و دستگاه‌های درگیر می‌توانند مستعد حملات سایبری باشند، که منجر به افزایش علاقه به حوزه امنیت اطلاعات اعمال شده در اینترنت اشیا شده است. این مطالعه روشی را برای تجزیه و تحلیل یک شبکه اینترنت اشیا برای شناسایی حملات با استفاده از تکنیک‌های کانال جانبی ارائه می‌کند که نظارت مصرف برق دستگاه‌ها را بر عهده دارد و نشان می‌دهدکه می‌توان از یک سیستم مانیتورینگ مجهز به یادگیری ماشین برای تشخیص نفوذ بدون تداخل با رفتار عادی دستگاه‌ها استفاده کرد. آزمایش‌ها تحت سناریوهای مختلف، مانند استفاده از مجموعه داده‌های سفارشی، شناسایی حملات جدیدی که مدل با آن‌ها آموزش ندیده است، یا شناسایی حملاتی که به صورت زنده اتفاق می‌افتند، نتایج مثبتی را به همراه دارد. مزایای اصلی سیستم پیشنهادی سادگی، تکرارپذیری آن (هم کد و هم داده در دسترس هستند) و قابل حمل بودن است، زیرا می‌توان آن را در بسیاری از دستگاه‌ها مستقر کرد و نیاز زیادی به منابع ندارد. با توجه به ساختار شبکه اینترنت اشیا و محدودیت‌های قدرت دستگاه‌ها، استراتژی‌های استقرار مختلفی را پیشنهاد می‌کند.

در تحقیق [27] با عنوان سیستم تشخیص نفوذ کانال جانبی برای وسایل نقلیه هوایی بدون سرنشین حیاتی ماموریت، به این موضوع اشاره می کند که تروجان‌های سخت افزاری به تدریج در حال تبدیل شدن به یک تهدید رو به رشد در چشم انداز اینترنت اشیا هستند. این نوع حمله می‌تواند منجر به حوادث فاجعه بار برای وسایل نقلیه هوایی بدون سرنشین شود. نمونه‌هایی از این حوادث می‌تواند نشت اطلاعات، نقص در عملکرد پهپاد، که منجر به سقوط می‌شود و مسائل مربوط به یکپارچگی داده‌ها در اطلاعات جمع آوری شده توسط حسگرها باشد. مقالات دیگر سعی کرده‌اند این مشکل را با تمرکز بر تقویت رمزگذاری و سخت‌تر کردن ویژگی‌های فیزیکی دستگاه برای محدود کردن نشت اطلاعات حل کنند. با این حال، هدف این تحقیق نشان دادن اثربخشی تکنیک تشخیص نفوذ مبتنی بر کانال جانبی است و نشان می‌دهد که چگونه این تکنیک سیستم تشخیص نفوذ به طور موثر حوادث مربوط به اجرای وسایل نقلیه هوایی بدون سرنشین در پهپادها را شناسایی می‌کند و اختلافات در امپدانس سیستم را تحلیل می‌کند.

در تحقیق [28] با عنوان یک رویکرد چند هدفه برای تشخیص تروجان سخت افزاری مبتنی بر کانال جانبی با استفاده از ردیابی قدرت، به این موضوع اشاره می کند که شناسایی تروجان‌های سخت افزاری در گذشته به طور گسترده مورد مطالعه قرار گرفته است. در این مقاله، یک تکنیک تحلیل کانال جانبی پیشنهاد می‌شود که از تکنیک انتخاب ویژگی مبتنی بر پوشش برای تشخیص تروجان سخت‌افزاری استفاده می‌کند. الگوریتم بهینه‌سازی نهنگ برای استخراج دقیق بهترین زیرمجموعه ویژگی‌ها اصلاح شده است. هدف تکنیک پیشنهادی چند هدفه است: بهبود دقت و به حداقل رساندن تعداد ویژگی‌ها. تثبیت کننده روش انتخاب ویژگی به ایجاد یک مبادله متقابل بین پارامترهای دقت و فراخوان کمک می‌کند و در نتیجه تعداد منفی‌های کاذب را به حداقل می‌رساند.

همانطور که اشاره شد کوچر و همکاران [29] حمله مصرف برق را پیشنهاد کردند. این شاخه‌ای از حملات کانال جانبی است که دستگاه‌ها را با اندازه گیری مصرف انرژی مورد هدف قرار می‌دهد. آنان پیشنهاد کردند که تحلیل توان دیفرانسیل کلاسیک با موفقیت کلید الگوریتم را شکسته است و دریافتند که بین مصرف انرژی و داده‌ها هنگام رمزگذاری دستگاه ارتباط وجود دارد. علاوه بر این، این رابطه حاوی داده‌های کلید دستگاه رمزگذاری شده است که می‌تواند برای شکستن کلید استفاده شود. با تجزیه و تحلیل مصرف برق یک دستگاه در هنگام رمزگذاری یا رمزگشایی،

می‌توان کلید استفاده شده را استنباط کرد. برای انجام این نوع حمله، یک کامپیوتر از یک دستگاه رمزگذاری استفاده و مجموعه‌ای از متن‌های ساده شناخته شده را برای رمزگذاری به دستگاه وارد می‌کند. همانطور که دستگاه، رمزگذاری را انجام می‌دهد، یک اسیلوسکوپ میزان مصرف انرژی را اندازه گیری می‌کند و در نتیجه ردیابی نیرو را به دست می‌آورد. به دنبال این رویکرد، روش‌های حمله تحلیل قدرت بیشتری توسعه یافتند که می‌توان آن‌ها را به طور کلی به عنوان حملات پروفایل و حملات غیرپروفایل طبقه‌بندی کرد. حملات غیرپروفایل شامل تجزیه و تحلیل اطلاعات متقابل [30] و حملات برخوردی [31] و تجزیه و تحلیل توان همبستگی [32] و حملات پروفایل شامل حملات قالب [33] و حملات کانال جانبی مبتنی بر یادگیری ماشینی، مانند پرسپترون چندلایه [34]، جنگل‌های تصادفی [35] و روش نزدیک‌ترین همسایگان [36] ، شبکه‌های عصبی کانولوشن [37] و ماشین‌های بردار پشتیبان [38-41] است.

حملات غیرپروفایل ساده در برابر تداخل محیطی آسیب پذیر هستند. در مقابل، تکنیک‌های حمله پروفایل در برابر نویزهای محیطی انعطاف‌پذیرتر هستند، زیرا به کنترل کامل دستگاهی که مشابه دستگاه هدف است نیاز دارند. مهاجم از دستگاه متعلق به خود برای ایجاد یک مدل نشت کانال جانبی بر اساس تعداد زیادی نمونه استفاده می‌کند که با استفاده از این حمله، امکان شکستن کلید آسان‌تر روی دستگاه مورد نظر را فراهم می‌کند. هوسپودار و همکاران [38] برای اولین‌بار مدل LS-SVM را در حملات تجزیه و تحلیل مصرف انرژی اعمال کردند. یافته‌ها نشان داد که انتخاب پارامتر یادگیری ماشین تأثیر قابل‌توجهی بر عملکرد طبقه‌بندی دارد. هوسر و زونر و همکاران [39] با در نظر گرفتن مقادیر میانی برای طبقه‌بندی پروفایل‌های مصرف برق و کاهش پیچیدگی فضایی، مدل بیت را به مدل وزن همینگ گسترش و نشان دادند که حملات مبتنی بر ماشین بردار پشتیبان حملات قالب‌های معمولی را در موقعیت‌های نویز بالا شکست می‌دهند. هوو و همکاران [40] از یک ماشین بردار پشتیبان مبتنی بر هسته موجک برای بازیابی مقادیر افست و کلیدهای یک الگوریتم AES پوشانده استفاده کرده و نشان دادند که ماشین‌های بردار هسته موجک ماشین‌های بردار هسته گاوسی را شکست می‌دهند. پیک و هوسر و همکاران [41] از الگوریتم SMOTE برای رسیدگی به مشکل داده‌های نامتعادل در طول آموزش ماشین بردار پشتیبان استفاده کردند. این روش قادر به استخراج ویژگی‌هایی است که مهم‌ترین اطلاعات را از ردیابی نیرو حفظ می‌کند و در عین حال نویز را کاهش می‌دهد که پس از آن برای طبقه‌بندی ماشین بردار پشتیبان استفاده می‌شود. مشارکت‌های بالا نشان می‌دهد که ماشین بردار پشتیبان‌ها از سایر روش‌های یادگیری ماشین بهتر عمل می‌کند. با این حال، مشکل انتخاب پارامتر در ماشین بردار پشتیبان‌ها هنوز با روش‌های آنها حل نشده باقی مانده است.

بهینه‌سازی هایپرپارامتر با مسئله انتخاب مدل نیز مرتبط است. این به فرآیند یافتن تنظیمات پارامتر بهینه برای یک الگوریتم در نظر گرفته شده اشاره دارد که دقت آن را به حداکثر می‌رساند. از نظر یک شبکه عصبی، به عنوان مثال، تعداد لایه‌های پنهان یا نوع تابع فعال‌سازی مورد استفاده برای نورون‌های یک لایه مشخص است. متغیرهایی مانند موارد فوق معمولاً تأثیر زیادی بر ظرفیت بازنمایی یک تکنیک یادگیری ماشین دارند. با این حال، اهمیت این مرحله توسط همه نویسندگان مقالات بررسی شده تشخیص داده نشده (یا برای گزارش آن مهم تلقی نشده است). به طور خاص، تنها دو مشارکت وجود دارد که به صراحت تأثیر تنظیم پارامترهای مناسب را بر اثربخشی حمله‌های کانال جانبی بررسی کردند [43]. با این حال، دامنه تکنیک‌های مورد استفاده، از استفاده از مقادیر استاندارد برگرفته از ادبیات [44] در جستجوی شبکه [17] تا روش‌های پیشرفته مانند گروه ذرات [45] و الگوریتم‌های ژنتیک [46] پیش می‌رود. هنگام انتخاب یک الگوریتم مناسب، باید این نکته را نیز در نظر گرفت که الگوریتم‌های ساده‌تر یادگیری ماشین یا ابزارهای تحلیل کانال جانبی استاندارد به سربار بهینه‌سازی کمتری نیاز دارند.

الگوریتم‌های ابتکاری به طور گسترده در مسائل بهینه‌سازی استفاده می‌شود. چندین محقق از الگوریتم‌های اکتشافی برای استخراج این ویژگی استفاده کرده‌اند. وانگ و همکاران [47] چارچوبی از GA-CPA را پیشنهاد کردند که الگوریتم‌های ژنتیک و CPA را ترکیب می‌کرد. این چارچوب از الگوریتم‌های ژنتیک برای استخراج مقادیر مشخصه و به دنبال آن یک حمله CPA استفاده می‌کند. وانگ و همکاران [48] یک الگوریتم شبکه عصبی را توصیف کردند که از بهینه‌سازی ازدحام ذرات (PSO) برای شناسایی تروجان‌های سخت افزاری استفاده می‌کند. نتایج تجربی نشان می‌دهد که دقت تشخیص روش شبکه عصبی مبتنی بر گروه ذرات از روش‌های شبکه عصبی با روش پس انتشارخطای معمولی پیشی می‌گیرد.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

چندین محقق از الگوریتم‌های اکتشافی برای بهینه‌سازی پارامتر استفاده کرده‌اند که با روش‌های حل دقیق سنتی در اولویت‌بندی جستجو در فضای حل تقریبی متفاوت است. چندین الگوریتم اکتشافی برای بهینه‌سازی پارامترهای ماشین بردار پشتیبان مورد مطالعه قرار گرفته است، مانند الگوریتم‌های ژنتیک [49]، بهینه‌سازی ازدحام ذرات [50]، بهینه‌سازی کلونی مورچه‌ها [51] و بازپخت شبیه‌سازی‌شده [52]. این مطالعات، دقت طبقه بندی بهبود یافته را در مقایسه با روش‌های دیگر مانند جستجوی شبکه‌ای نشان داده‌اند. الگوریتم ژنتیک، نزدیک به بهترین راه حل است، اما رمزگذاری مسئله و سپس رمزگشایی راه حل دشوار است. الگوریتم گروه ذرات دارای متغیرهای کمتری برای تغییر دادن و یک اصل ساده است، اما قابلیت جستجوی محلی ضعیف و دقت جستجوی کافی ندارد. روش کلونی مورچگان به آرامی همگرا می‌شود و تمایل دارد به بهینه محلی بیفتد. علاوه بر این، کلونی مورچگان نمی‌تواند مسائل بهینه‌سازی مداوم فضا را مدیریت کند و فقط برای مسائل گسسته مناسب است. بازپخت شبیه‌سازی‌شده کشف مقادیر حداکثر یا حداقل را با امکان انتخاب تصادفی راه حل‌های زیر بهینه امکان پذیر و فرار از بهینه محلی را آسان‌تر می‌کند.

در مطالعه [15]، روش بازپخت شبیه‌سازی‌شده و ماشین بردار پشتیبان برای ایجاد یک مدل SA-SVM ترکیب شدند، که ایجاد و برای تحلیل توان کانال جانبی اعمال شد. آزمایش بر روی مجموعه داده عمومی DPA انجام شد. ابتدا ضریب پیرسون برای انتخاب مقادیر ویژه مجموعه داده ردپای قدرت به کار گرفته شد سپس مدل HW به عنوان برچسب برای مدل SA-SVM مورد استفاده قرار گرفت. مدل SA-SVM از احتمال معینی برای پذیرش افزایش‌های منفی استفاده می‌کند تا از بهینه محلی خارج شود و پارامترهای بهینه را راحت‌تر پیدا کند. اما روش بازپخت شبیه‌سازی‌شده در ابعاد بالای مسائل بهینه‌سازی دارای دقت بالایی نیست زیرا فرایند اکتشاف در این الگوریتم ضعیف است. پیشنهاد این طرح نامه و پروپوزال مبنی بر استفاده از الگوریتم یوزپلنگ برای ماشین بردار پشتیبان یک راهکار باقدرت اکتشاف و استخراج بالا است که می‌تواند در ابعاد بالای مسئله با دقت همگرا شود.

2. روش پیشنهادی:

روش پیشنهادی در این مقاله، ماشین بردار پشتیبان بهبودیافته با الگوریتم بهینه‌سازی یوزپلنگ است. از چالش‌های روش پیشنهادی این است که چگونه می‌توان تشخیص حملات کانال جانبی را با دقت بالاتری انجام داد و چگونه روش ماشین بردار پشتیبان بهبود یافته به کمک الگوریتم بهینه ساز یوزپلنگ، در تشخیص حملات کانال جانبی می‌تواند نسبت به روش ماشین بردار پشتیبان استاندارد بوده و نسخه بهبودیافته آن با روش بازپخت شبیه‌سازی‌شده دقت بالاتری داشته باشد.

بنابراین هدف روش پیشنهادی در تشخیص حملات کانال جانبی، بالا بردن صحت تشخیص حملات است و این هدف با این مفروضات تحقیق شده است که الگوریتم بهینه‌سازی یوزپلنگ نسبت به الگوریتم بازپخت شبیه‌سازی‌شده دارای دقت بهینه‌سازی بالاتری است. همچنین روش ماشین بردار پشتیبان در صورتی که با الگوریتم بهینه‌سازی یوزپلنگ در حوزه تشخیص حملات کانال جانبی بهبود داده شود می‌تواند به دقت بالاتری دست پیدا کند.

چارچوب تشخیص حملات کانال جانبی شامل سه قسمت است:

1. ماژول جمع آوری داده‌ها
2. ماژول آموزش طبقه بند
3. ماژول تست

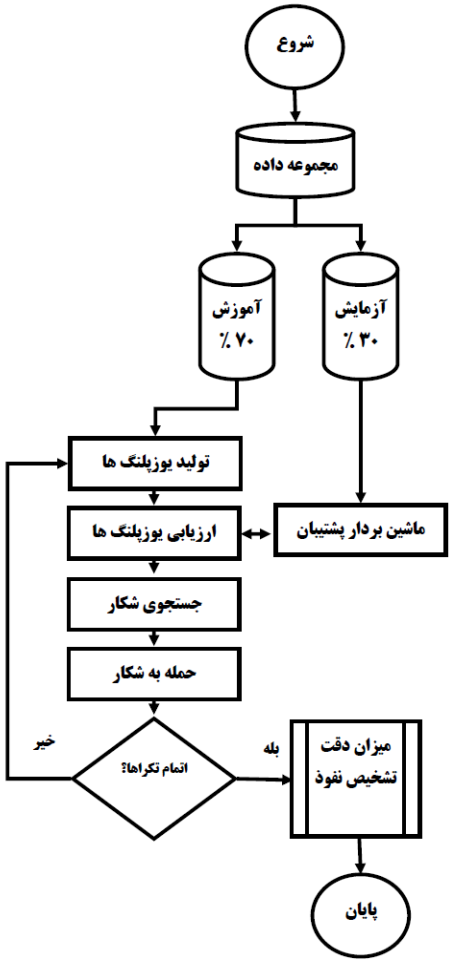
دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

1. ماژول جمع‌آوری داده‌ها: در این ماژول، مجموعه داده‌ها استخراج شده از DPA Contest v4 آماده سازی می‌شود.

2. ماژول تشخیص با آموزش طبقه بند: داده‌ها به عنوان ورودی برای طبقه بند ماشین بردار پشتیبان کار می‌کنند. ماشین بردار پشتیبان در این ماژول آموزش دیده تا الگوی داده‌ها را یاد بگیرد.

3. ماژول تست: از داده‌های تست روی مدل برای ارزیابی عملکرد مدل برای تشخیص حملات کانال جانبی استفاده شده و میزان صحت تشخیص حملات بررسی می‌شود.

مراحل کلی روش پیشنهادی در فلوچارت شکل 1 آمده است:



شکل 1: مراحل تنظیم پارامتر ماشین بردار پشتیبان با الگوریتم یوزپلنگ

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

در ماژول آموزش طبقه بند (SVM-CO) ماشین بردار پشتیبان با استفاده از داده‌های نرمال و مخرب، آموزش داده می‌شود. داده‌ها به بخش‌های آموزشی و آزمایشی تقسیم می‌شوند. بهبود روش ماشین بردار پشتیبان با استفاده از الگوریتم یوزپلنگ به این صورت است که در الگوریتم یوزپلنگ، هر یوزپلنگ (جواب ممکن) یک مقدار تصادفی برای متغیر C و w در روش ماشین بردار پشتیبان در معادله 1 تولید می‌شود، پارامتر C تنظیم‌کننده حاشیه است که وظیفه آن برقراری تعادل بین حداکثر کردن حاشیه و حداقل کردن خطای دسته‌بندی بوده و همواره بزرگ‌تر از صفر است و پارامتر w هم وزن است به علت آنکه در روش ماشین بردار پشتیبان به‌صورت تصادفی تولید می‌شود و ممکن است در بهترین مقدار خود قرار نگیرد، ازاین‌رو به دست آوردن مقدار مناسب C و w در روش ماشین بردار پشتیبان یک مسئله بهینه‌سازی است که الگوریتم یوزپلنگ بهترین مقدار را برای آن به دست می‌آورد. در ماشین بردار پشتیبان پیدا کردن بهترین w وC با کمینه‌سازی معادله 1 محقق می‌شود:

$$\min \frac{1}{2} \|w\|^2 + C \sum_i \varepsilon_i \quad (1)$$

که در بهینه‌سازی آن باید شرط معادله 2 در نظر گرفته شود:

$$y_i(<w.x_i>+b) \geq 1-\varepsilon_i \, , \varepsilon_i \geq 0 \;\; \forall i \quad (2)$$

در معادله 2 پارامتر b بایاس، x_i ویژگی داده و y_i کلاس داده است. در الگوریتم یوزپلنگ با استفاده از اپراتورهای خود، هر جواب ممکن (مقداری برای پارامتر C وw) را می‌یابد تا درنهایت به بهترین مقدار این پارامترها دست یابد. برای محاسبه برازندگی هر جواب در این الگوریتم از تابع برازندگی میزان صحت طبقه‌بندی از معادله 3 استفاده می‌شود.

$$accuracy = \frac{TN+TP}{TN+FN+TP+FP} \quad (3)$$

هر یک از عناصر ماتریس به شرح ذیل است:

TN: بیانگر تعداد رکوردهایی است که دسته واقعی آن‌ها منفی بوده و الگوریتم دسته بندی نیز دسته آن‌ها را به‌درستی منفی تشخیص داده است.

TP: بیانگر تعداد رکوردهایی است که دسته واقعی آن‌ها مثبت بوده و الگوریتم دسته بندی نیز دسته آن‌ها را به‌درستی مثبت تشخیص داده است.

FP: بیانگر تعداد رکوردهایی است که دسته واقعی آن‌ها منفی بوده و الگوریتم دسته بندی دسته آن‌ها را به اشتباه مثبت تشخیص داده است.

FN: بیانگر تعداد رکوردهایی است که دسته واقعی آن‌ها مثبت بوده و الگوریتم دسته بندی دسته آن‌ها را به اشتباه منفی تشخیص داده است.

در مسئله تنظیم پارامترهای ماشین بردار پشتیبان، هر جواب ممکن در الگوریتم بهینه‌سازی یک ارایه به‌صورت حقیقی است که نشان دهنده مقدار عددی برای دو پارامتر W وC در ماشین بردار پشتیبان است:

C	W
0.45	0.74

شکل 2: ساختار یک یوزپلنگ در تنظیم پارامترهای ماشین بردار پشتیبان

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

در شکل 2 هر یوزپلنگ نشان دهنده دو پارامتر اصلی در ماشین بردار پشتیبان است. به‌علت آنکه اعداد حقیقی هستند دیگر نیاز به تبدیل همانند انتخاب ویژگی نیست. میزان برازندگی هر یوزپلنگ با استفاده از دقت ماشین بردار پشتیبان که در معادله 3 به ازاء پارامترها است.

حرکات یوزپلنگ در الگوریتم بهینه‌سازی یوزپلنگ شامل:

- جستجوکردن: یوزپلنگ‌ها برای یافتن طعمه خود نیاز به جستجو دارند از جمله اسکن یا جستجوی فعال در قلمرو خود (فضای جستجو) یا اطراف آن.
- نشستن و انتظار: پس از شناسایی طعمه، اما وضعیت مناسب، یوزپلنگ‌ها ممکن است بنشینند و منتظر نزدیک شدن طعمه یا بهتر شدن وضعیت باشند.
- هجوم بردن: این استراتژی دو مرحله اساسی دارد:
  - عجله: زمانی که یوزپلنگ تصمیم به حمله می‌گیرد، با حداکثر سرعت به سمت طعمه می‌شتابد.
  - گرفتن: یوزپلنگ از سرعت و انعطاف پذیری برای گرفتن طعمه با نزدیک شدن به طعمه استفاده می‌کند.
- شکار را رها کند و به خانه برگردد: برای این استراتژی دو حالت در نظر گرفته شده است. (1) اگر یوزپلنگ در شکار طعمه ناموفق باشد، باید موقعیت خود را تغییر دهد یا به قلمرو خود بازگردد. (2) در مواردی که شکار موفقی در یک بازه زمانی انجام نشود، موقعیت خود را به آخرین شکار کشف شده ببرد و جستجو را در اطراف آن انجام دهد.

استراتژی جستجو: یوزپلنگ‌ها از دو طریق به دنبال طعمه می‌گردند: در حالت نشسته یا ایستاده محیط را پایش و یا به طور فعال در اطراف آن گشت زنی می‌کنند. حالت پایش زمانی مناسب‌تر است که طعمه در حال راه رفتن در دشت متراکم و چرا باشد. از طرفی انتخاب حالت فعال که نیاز به انرژی بیشتری نسبت به حالت پایش دارد در صورتیکه طعمه پراکنده و فعال باشد بهتر است. بنابراین، در طول دوره شکار، با توجه به وضعیت طعمه، پوشش منطقه و وضعیت خود یوزپلنگ‌ها، زنجیره‌ای از این دو حالت جستجو است. معادله جستجوی تصادفی برای به روزرسانی موقعیت جدید یوزپلنگ در معادله 4 آمده است که موقعیت فعلی با گام حرکتی شکل می گیرد:

$$X_{i,j}^{t+1} = X_{i,j}^{t} + \hat{r}_{i,j}^{-1}.\alpha_{i,j}^{t} \qquad (4)$$

در معادله 4 $X_{i,j}^{t+1}$ موقعیت بعدی یوزپلنگ و $X_{i,j}^{t}$ موقعیت فعلی آن است و $\hat{r}_{i,j}^{-1}$ پارامتر تصادفی با توزیع نرمال استاندارد است و $\alpha_{i,j}^{t}$ طول گام برای حرکت است و بیشتر از 0 است و حالت پیش فرض آن $0.001 \times \frac{t}{T}$ است به این معنی که یوزپلنگ در حال جستجوی آهسته است. همچنین ممکن است در مواجهه با شکارها و یا دشمنان دیگر، به سرعت حرکت کرده و تغییر جهت حرکت داشته باشد. $\alpha_{i,j}^{t}$ حرکتی بین یوزپلنگ و دیگر همسایه ها و یا رهبر است. رهبر به بهترین جواب پیدا شده در هر تکرار بهینه‌سازی گفته می‌شود.

استراتژی نشستن و منتظر ماندن: در طول حالت جستجو، طعمه ممکن است در میدان دید یوزپلنگ قرار گیرد. در این شرایط هر حرکت یوزپلنگ ممکن است طعمه را از حضور خود آگاه کند و منجر به فرار طعمه شود. برای جلوگیری از این نگرانی، یوزپلنگ ممکن است تصمیم بگیرد (با دراز کشیدن روی زمین یا پنهان شدن در میان بوته‌ها) کمین کند تا به اندازه کافی به طعمه نزدیک شود. بنابراین، در این حالت، یوزپلنگ در موقعیت خود باقی می‌ماند و منتظر می‌شود تا طعمه نزدیک‌تر شود، معادله 5 برای این منظور در نظر گرفته شده است:

$$X_{i,j}^{t+1} = X_{i,j}^{t} \qquad (5)$$

در معادله 5 $X_{i,j}^{t+1}$ موقعیت بعدی یوزپلنگ و $X_{i,j}^{t}$ موقعیت فعلی آن است و در واقع به‌روزرسانی در موقعیت یوزپلنگ‌ها رخ نمی‌دهد.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

استراتژی حمله: یوزپلنگ‌ها از دو عامل مهم برای حمله به طعمه خود استفاده می‌کنند: سرعت و انعطاف پذیری. وقتی یوزپلنگ تصمیم به حمله می‌گیرد، با سرعت تمام به سمت طعمه می‌رود. پس از مدتی طعمه متوجه حمله یوزپلنگ می‌شود و شروع به فرار می کند. به عبارت دیگر، یوزپلنگ موقعیت شکار را دنبال و جهت حرکت خود را به گونه‌ای تنظیم می‌کند که در یک نقطه راه شکار را مسدود می سازد. از آنجایی که یوزپلنگ با حداکثر سرعت به فاصله کمی از طعمه رسیده است، طعمه باید فرار کند و موقعیت خود را به طور ناگهانی تغییر دهد تا زنده بماند. یعنی موقعیت بعدی یوزپلنگ نزدیک آخرین موقعیت شکار است.

در معادله 6 استراتژی حمله آمده است:

$$X_{i,j}^{t+1} = X_{B,j}^{t} + \check{r}_{i,j}.\beta_{i,j}^{t} \quad (6)$$

که در آن $X_{B,j}^{t}$ موقعیت فعلی شکار است و در واقع بهترین موقعیت فعلی در الگوریتم است. $\check{r}_{i,j}$ عامل چرخش و $\beta_{i,j}^{t}$ برعامل همکنش یوزپلنگ است. $X_{B,j}^{t}$ برای نزدیک شدن به طعمه که در واقع بهترین جواب مسئله است در نظر گرفته شده و $\beta_{i,j}^{t}$ نشان دهنده تعامل یوزپلنگ‌ها با دیگر یوزپلنگ‌ها و یا رهبر است. $\check{r}_{i,j}$ عامل چرخش نیز یک حرکت تصادفی با معادله 7 است که در آن $r_{i,j}$ توزیع نرمال استاندارد است.

$$\check{r}_{i,j} = |r_{i,j}|^{\exp(\frac{r_{i,j}}{2})} sin(2\pi r_{i,j}) \quad (7)$$

در این الگوریتم برای حرکت‌های تصادفی از پارامترهای تصادفی r و همچنین مقدار H با معادله 8 استفاده می‌شود که در آن r_1 یک عدد تصادفی یکنواخت بین $[0و1]$ است.

$$H = e^{2\left(1-\frac{t}{T}\right)}(2r_1 - 1) \quad (8)$$

شبه کد روش پیشنهادی به‌صورت زیر است:

1- تعریف مسئله با تابع برازندگی (معادله 1)، مشخص کردن ابعاد مسئله (2 بعد برای دو پارامتر W و Cg) تعیین تعداد جمعیت اولیه یوزپلنگ‌ها
2- ارزیابی هر یوزپلنگ با تابع برازندگی تولید جمعیت اولیه با معادله 1

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

3- مشخص کردن یوزپلنگ‌ها، رهبر و طعمه با توجه به برازندگی آنها

4- بیشترین تکرارهای الگوریتم تعیین شود و مشخص کردن مقدار T تا وقتیکه به تکرار نهایی نرسیده است مراحل زیر انجام شود:

4-2-1- انتخاب تعداد تصادفی یوزپلنگ‌ها و برای هر یوزپلنگ مراحل زیر انجام شود

4-2-2- مشخص کردن همسایه‌های هر یوزپلنگ

4-2-2-1- انجام عملگرهای حرکتی در هر بعد یوزپلنگ‌ها

4-2-2-2- محاسبه H و $\alpha, \beta, \hat{r}, \check{r},$

4-2-2-3- به‌صورت تولید تصادفی توزیع غیریکنواخت بین 0 و 1 r_2, r_3

4-2-2-4- **اگر** $r_2 \leq r_3$

4-2-2-5- تولید تصادفی توزیع غیریکنواخت بین 0 و 3 برای r_4 و **اگر** $H \geq r_4$

انجام جستجو توسط هر یوزپلنگ با معادله 4 در غیر این صورت انجام حرکت حمله به سمت شکار با معادله 6

4-2-2-6- **اگر** $H < r_4$ منتظر ماندن و حرکت نکردن با معادله 5

4-2-3- به‌روزرسانی رهبر

4-2-4- شماره t یک عدد اضافه شود و اگر $t > rand \times T$ آنگاه رها کردن شکار و برگشت به خانه

5- برگشت رهبر به‌عنوان بهترین عامل جستجو و جواب مسئله (بهترین مقادیر برای دو پارامتر W و C)

نتایج:

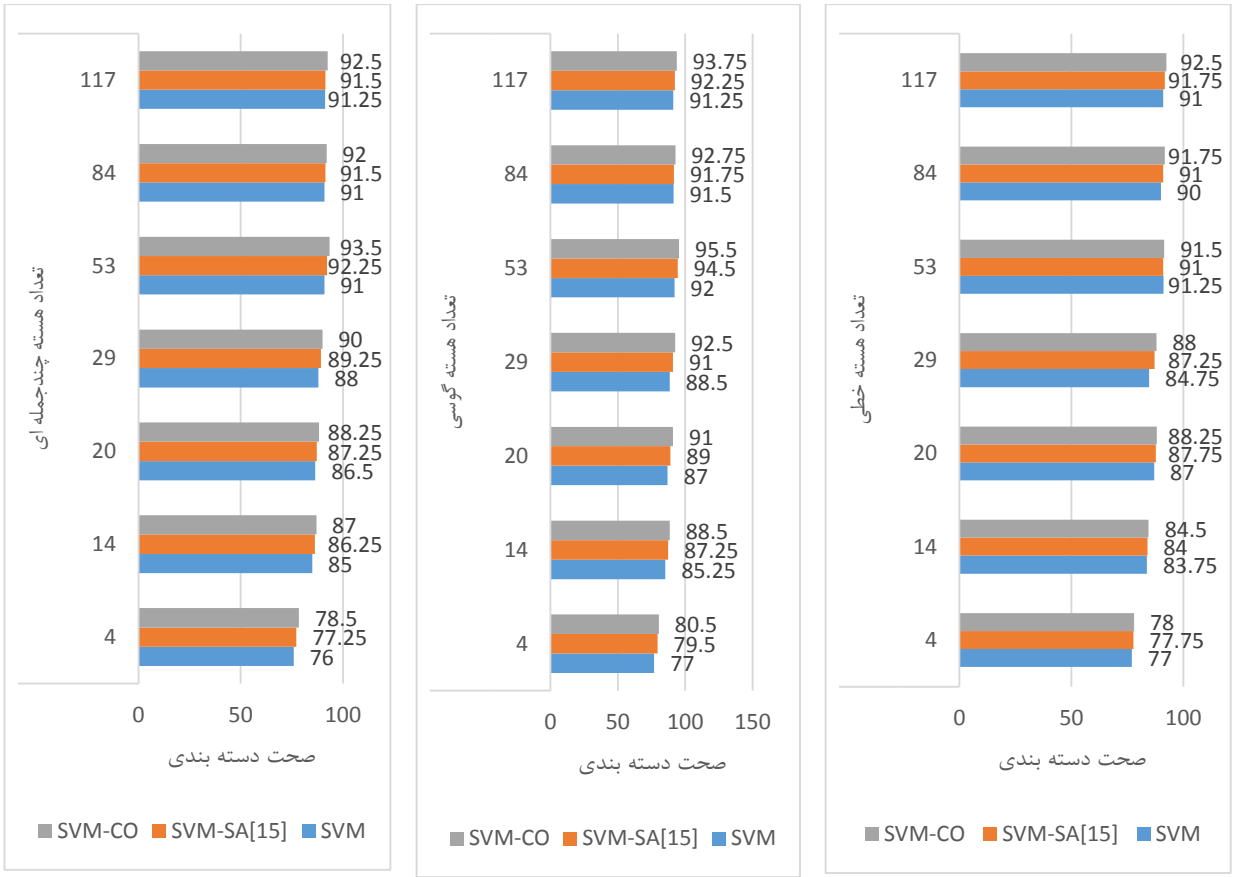
مجموعه داده آزمایشات از مسابقه DPA در زمینه امنیت رمزنگاری و آخرین نسخه آن DPA Contest v4 است [53]. از آنجایی که در این آزمایش از رمزگذاری کامل استفاده نشده نسخه DPA Contest v 4.1 به عنوان مجموعه داده انتخاب شده است که مشترک بین تحقیق حاضر و تحقیق [15] است. برای مقایسه پذیر بودن روش پیشنهادی، شبیه‌سازی بر روی مجموعه داده کامل انجام شد که شامل 1000 نمونه با 435000 ویژگی در هر نمونه است.

نتایج صحت تشخیص حمله با معیارصحت دسته بندی معادله 3 برای سه روش مبتنی بر ماشین بردار پشتیبان آمده است، که شامل:

- آزمایش با ماشین بردار پشتیبان با هسته گوسی، چندجمله ای و خطی
- آزمایش با ماشین بردار پشتیبان بهبود یافته با روش بازپخت شبیه‌سازی‌شده [15] با هسته گوسی، چندجمله ای و خطی
- آزمایش با ماشین بردار پشتیبان بهبود یافته با روش یوزپلنگ با هسته گوسی، چندجمله ای و خطی

در شکل 3 نتایج سه روش مبتنی بر ماشین بردار پشتیبان با تغییر تعداد هسته‌های مختلف آمده است.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055



شکل 3: نتایج صحت دسته بندی در هسته‌های مختلف ماشین بردار پشتیبان

Svm : ماشین بردار پشتیبان، Svm-Sa : ماشین بردار پشتیبان بهبودیافته با روش بازپخت شبیه‌سازی‌شده [15]، Svm-Co : ماشین بردار پشتیبان بهبودیافته با روش یوزپلنگ

همانطور که از شکل 3 مشخص است بیشترین مقدار صحت دسته بندی مربوط به روش ماشین بردار پشتیبان بهبودیافته با روش یوزپلنگ و سپس روش ماشین بردار پشتیبان بهبودیافته با روش بازپخت شبیه‌سازی‌شده [15] است. در شکل 4 میزان بهبود نتایج در روش پیشنهادی و روش مقاله [15] آمده است. بالاترین میزان صحت نتایج عدد 95. درصد با هسته گوسی در روش ماشین بردار پشتیبان بهبودیافته با روش یوزپلنگ است.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

شکل 4: میزان بهبود نتایج در مقایسه با روش پیشنهادی (SVM-CO) و روش (SVM-SA) [15]

همانطور که از شکل 4 مشخص است بیشترین میزان بهبود نتایج 2.25 درصد و کمترین آن 0.32 است. بطور میانگین در آزمایشات انجام شده میزان بهبود نتایج روش پیشنهادی (SVM-CO) و روش مقاله(SVM-SA) [15] در شکل 5 آمده است.

شکل 5: میانگین میزان بهبود نتایج در مقایسه با روش پیشنهادی (SVM-CO) و روش (SVM-SA) [15] در هسته‌های مختلف

همانطور که از شکل 5 مشخص است، بیشترین مقدار بهبود در هسته گوسی بوده است و در حالت کلی روش پیشنهادی توانسته در مجموعه آزمایشات نسبت به روش مقاله [15] نتایج بالاتری داشته باشد. نتایج نشان می‌دهد که ماشین بردار پشتیبان با هسته گوسی بهترین عملکرد را در روش پیشنهادی داشته است و توانسته به بهبود 1.48 درصدی نسبت به روش مقاله(SVM-SA)

[15] برسد، ولی در هسته خطی و چندجمله ای این میزان بهبود مشاهده نشده است. درواقع تاثیر الگوریتم بهینه‌سازی یوزپلنگ نسبت به الگوریتم بازپخت شبیه‌سازی‌شده در بهبود ماشین بردار پشتیبان وقتیکه هسته گوسی انتخاب شده باشد، بیشتر است زیرا خط جداساز در هسته گوسی وابستگی بیشتری به تنظیم پارامتر W و C در ماشین بردار پشتیبان دارد ولی در هسته خطی این تاثیر کمتر است زیرا در هسته خطی، خط جداساز مانند هسته چندجمله ای و گوسی قدرت خمیدگی و جداسازی کلاس‌ها را ندارد.

نتیجه گیری:

تحقیقات در زمینه تشخیص حمله‌های کانال جانبی به منظور جلوگیری از شکستن سیستم‌های رمزنگاری انجام می‌شود. حمله‌های کانال جانبی مبتنی بر قدرت شامل حملات غیرپروفایل، از جمله تجزیه و تحلیل توان ساده/دیفرانسیل، و حملات پروفایل، از جمله حملات الگو و رویکردهای تصادفی می‌شوند. تشخیص این حملات با استفاده از روش‌های یادگیری ماشین انجام شده است که یکی از روش‌های کارا در این زمینه، ماشین بردار پشتیبان (SVM) است. با توجه به اینکه ماشین بردار پشتیبان یک راهکار مناسب برای تشخیص حملات کانال جانبی محسوب می‌شود ولی پارامترهای آن به‌خوبی تنظیم نشده است و این مسئله بر صحت دسته‌بندی آن تأثیر می‌گذارد.

در این مقاله، با توجه به عملکرد مناسب ماشین بردار پشتیبان در تشخیص حمله کانال جانبی، به ارائه روشی جدید از این روش یادگیری ماشین با تنظیم پارامترهای آن با استفاده از روش فراابتکاری یوزپلنگ پرداخته شده است. نتایج بر روی مجموعه داده استخراج‌شده از DPA Contest v4در مقایسه با دو روش دیگر از ماشین بردار پشتیبان با هسته‌های مختلف ارزیابی شد. نتایج نشان داد که بهترین نتیجه با استفاده از هسته گوسی به‌دست آمده است، در حالی که تنظیم پارامترها با روش بازپخت شبیه‌سازی‌شده در بهترین حالت 94.5 درصد صحت دسته‌بندی را به همراه داشت، تنظیم پارامترها با استفاده از روش یوزپلنگ 95.5 درصد صحت دسته‌بندی را بهبود بخشید.

بعنوان اقدامات آینده، می‌توان به استفاده از الگوریتم‌های فراابتکاری برای تنظیم تعداد هسته‌های ماشین بردار پشتیبان اشاره کرد. نتایج نشان می‌دهند که با تغییر هسته‌های ماشین بردار پشتیبان، نتایج صحت دسته‌بندی تغییر می‌کند، بنابراین، تعیین دقیق تعداد هسته‌ها یک مسئله بهینه‌سازی است که می‌تواند با استفاده از الگوریتم‌های بهینه‌سازی بهبود یابد.

منابع:

[1] Kocher, P.C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In Proceedings of the 16th Annual International Cryptology Conference (CRYPTO 96), Santa Barbara, CA, USA, 18–22 August 1996; pp. 104–113.
[2] Wang, R.; Wang, H.; Dubrova, E. Far Field EM Side-Channel Attack on AES Using Deep Learning. In Proceedings of the 4th ACM Workshop on Attacks and Solutions in Hardware Security, online, 13 November 2020; pp. 35–44.
[3] Ferrigno, J.; Hlavá˘c, M. When AES Blinks: Introducing Optical Side Channel. IET Inf. Secur. 2008, 2, 94.
[4] Genkin, D.; Shamir, A.; Tromer, E. Acoustic Cryptanalysis. J. Cryptol. 2017, 30, 392–443.
[5] Kocher, P.C.: Timing attacks on implementations of DiffieHellman, RSA, DSS, and other systems. Advances in Cryptology– CRYPTO '96: 16th Annual International Cryptology Conference Santa Barbara. California, USA August 18–22, 1996 Proceedings, pp. 104–113. Springer, Berlin (1996)
[6] Kocher, P., Jaffe, J., Jun, B.: Differential power analysis. Advances in Cryptology–CRYPTO' 99: 19th Annual International Cryptology Conference Santa Barbara, California, USA, August 15–19, 1999. Proceedings, pp. 388–397. Springer, Berlin (1999)

[7] Quisquater, J.J., Samyde, D.: Electromagnetic analysis (EMA): measures and counter-measures for smart cards. Smart Card Programming and Security: International Conference on Research in Smart Cards, E-smart 2001 Cannes, France, September 19–21, 2001. Proceedings, pp. 200–210. Springer, Berlin (2001)
[8] Genkin, D., Shamir, A., Tromer, E.: Acoustic cryptanalysis. J. Cryptol. 30(2), 392–443 (2017)
[9] Zhuang, L., Zhou, F., Tygar, J.D.: Keyboard acoustic emanations revisited. ACM Trans. Inf. Syst. Secur. 13(1), 3:1–3:26 (2009)
[10] Eisenbarth, T., Paar, C., Weghenkel, B.: Building a side channel based disassembler. Transactions on Computational Science X: Special Issue on Security in Computing, Part I, pp. 78–99. Springer, Berlin (2010)
[11] chindler, W., Lemke, K., Paar, C.: A stochastic model for differential side channel cryptanalysis. In: Rao, J.R., Sunar, B. (eds.) Cryptographic Hardware and Embedded Systems—CHES 2005: 7th International Workshop, Edinburgh, UK, August 29– September 1, 2005. Proceedings, pp. 30–46. Springer, Berlin (2005)
[12] Hastie, T., Tibshirani, R., Friedman, J.: The Elements of Statistical Learning: Data Mining, Inference and Prediction, 2nd edn. Springer, Berlin (2009)
[13] Jordan, M.I., Mitchell, T.M.: Machine learning: trends, perspectives, and prospects. Science 349(6245), 255–26
[14] Jap, D., Breier, J.: Overview of machine learning based sidechannel analysis methods. In: 2014 International Symposium on Integrated Circuits (ISIC), pp. 38–41 (2014)
[15] *Ying Zhang , Pengfei He , Han Gan , Hongxin Zhang ,Pengfei Fan: Side-Channel Power Analysis Based on SA-SVM.in:2023 applted sciences* 3:1–3:26 (2023)
[16] *Mohammad Amin Akbari, Mohsen Zare, Rasoul Azizipanah-abarghooee,Seyedali Mirjalil & Mohamed Deriche1 . (2022). The cheetah optimizer:a nature.inspired metaheuristic algorithm for large.scale optimization problems . Scientific Reports.10953.*
[17] Hospodar, G., Gierlichs, B., De Mulder, E., Verbauwhede, I., Vandewalle, J.: Machine learning in side-channel analysis: a first study. J. Cryptogr. Eng. 1(4), 293 (2011)
[18] Heuser, A., Zohner, M.: Intelligent machine homicide. In: Schindler, W., Huss, S.A. (eds.) Constructive Side-Channel Analysis and Secure Design: Third International Workshop, COSADE 2012, Darmstadt, Germany, May 3–4, 2012. Proceedings. Springer, Berlin (2012)
[19] Bartkewitz, T., Lemke-Rust, K.: Efficient template attacks based on probabilistic multi-class support vector machines. In: Mangard, S. (ed.) Smart Card Research and Advanced Applications: 11th International Conference, CARDIS 2012, Graz, Austria, November 28–30, 2012, Revised Selected Papers, pp. 263–276. Springer, Berlin (2013)
[20] Standaert, F.X., Malkin, T.G., Yung, M.: A unified framework for the analysis of side-channel key recovery attacks. In: Joux, A. (ed.) Advances in Cryptology—EUROCRYPT 2009: 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26–30, 2009. Proceedings. Springer, Berlin (2009)
[21] Mangard, S.: A simple power-analysis (SPA) attack on implementations of the AES key expansion. In: Lee, P.J., Lim, C.H. (eds.) Information Security and Cryptology—ICISC 2002: 5th International Conference Seoul, Korea, November 28–29, 2002. Revised Papers, pp. 343–358. Springer, Berlin (2003)
[22] Renauld, M., Standaert, F.X.: Algebraic side-channel attacks. In: Bao, F., Yung, M., Lin, D., Jing, J. (eds.) Information Security and Cryptology: 5th International Conference, Inscrypt 2009, Beijing, China, December 12–15, 2009. Revised Selected Papers, pp. 393– 410. Springer, Berlin (2010)
[23] Picek, S., Heuser, A., Jovic, A., Ludwig, S.A., Guilley, S., Jakobovic, D., Mentens, N.: Side-channel analysis and machine learning: A practical perspective. In: 2017 International Joint Conference on Neural Networks (IJCNN), pp. 4095–4102 (2017)
[24] *Rob Oshana.: A Side Channel Attack Detection System Using Processor Core Events and a Support Vector Machine. In:2022 Mediterranean Conference on Embedded Computing (MECO).* (2022)
[25] *MATTEO NERINI.: Machine Learning for PIN Side-Channel Attacks Based on Smartphone Motion Sensors. In: IEEE Access.* (2023)
[26] *ALEJANDRO DOMÍNGUEZ CAMPOS.: Intrusion detection on IoT environments through side-channel and Machine Learning techniques. In: IEEE Access.* (2024)
[27] *Alejandro Almeida, Muneeba Asif.: Side-Channel-Driven Intrusion Detection System for Mission Critical Unmanned Aerial Vehicles. In: IEEE Access.* (2023)

[28] *PRIYADHARSHINI MOHANRAJ .: A Multiobjective Approach for Side-Channel Based Hardware Trojan Detection Using Power Traces In IEICE TRANS.* (2024)
[29] Goos, G.; Hartmanis, J.; van Leeuwen, J.; Kocher, P.; Jaffe, J.; Jun, B. Differential Power Analysis. In Proceedings of the 19th Annual International Cryptology Conference (CRYPTO 99), Santa Barbara, CA, USA, 15–19 August 1999; pp. 388–397.
[30] Gierlichs, B.; Batina, L.; Tuyls, P.; Preneel, B. Mutual Information Analysis. In Cryptographic Hardware and Embedded Systems— CHES 2008; Oswald, E., Rohatgi, P., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2008; Volume 5154, pp. 426–442. ISBN 978-3-540-85052-6.
[31] Niu, Y.; Zhang, J.; Wang, A.; Chen, C. An Efficient Collision Power Attack on AES Encryption in Edge Computing. IEEE Access 2019, 7, 18734–18748.
[32] Han, J.; Kim, Y.-J.; Kim, S.-J.; Sim, B.-Y.; Han, D.-G. Improved Correlation Power Analysis on Bitslice Block Ciphers. IEEE Access 2022, 10, 39387–39396.
[33] Choudary, M.O.; Kuhn, M.G. Efficient, Portable Template Attacks. IEEE Trans. Inf. Forensic Secur. 2018, 13, 490–501
[34] Golder, A.; Das, D.; Danial, J.; Ghosh, S.; Sen, S.; Raychowdhury, A. Practical Approaches Toward Deep-Learning-Based Cross-Device Power Side-Channel Attack. IEEE Trans. VLSI Syst. 2019, 27, 2720–2733.
[35] Picek, S.; Heuser, A.; Jovic, A.; Legay, A. Climbing Down the Hierarchy: Hierarchical Classification for Machine Learning Side-Channel Attacks. In Proceedings of the 9th International Conference on Cryptology in Africa (AFRICACRYPT 2017), Dakar, Senegal, 24–26 May 2017; pp. 61–78.
[36] Liu, J.; Zhang, S.; Luo, Y.; Cao, L. Machine Learning-Based Similarity Attacks for Chaos-Based Cryptosystems. IEEE Trans. Emerg. Top. Comput. 2021, 10, 824–837
[37] Martinasek, Z.; Hajny, J.; Malina, L. Optimization of Power Analysis Using Neural Network. In Proceedings of the 10th IFIP WG 8.8/11.2 International Conference (CARDIS 2011), Leuven, Belgium, 14–16 September 2011; pp. 94–107.
[38] Hospodar, G.; Gierlichs, B.; De Mulder, E.; Verbauwhede, I.; Vandewalle, J. Machine Learning in Side-Channel Analysis: A First Study. J. Cryptogr. Eng. 2011, 1, 293–302.
[39] Heuser, A.; Zohner, M. Intelligent Machine Homicide. In Proceedings of the 10th International Workshop, COSADE 2019, Darmstadt, Germany, 3–5 April 2019; pp. 249–264.
[40] Hou, S.; Zhou, Y.; Liu, H.; Zhu, N. Wavelet Support Vector Machine Algorithm in Power Analysis Attacks. Radioengineering 2017, 26, 890–902.
[41] Picek, S.; Heuser, A.; Jovic, A.; Bhasin, S.; Regazzoni, F. The Curse of Class Imbalance and Conflicting Metrics with Machine Learning for Side-Channel Evaluations. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2018, 2019, 209–237
[42] Tran, N.Q.; Hur, J.; Nguyen, H.M. Effective Feature Extraction Method for SVM-Based Profiled Attacks. Comput. Inf. 2021, 40, 1108–1135.
[43] Martinasek, Z., Zeman, V., Malina, L., Martinasek, J.: k-Nearest neighbors algorithm in profiling power analysis attacks. Radioengineering 25(2), 365–382 (2016
[44] Lerman, L., Bontempi, G., Markowitch, O.: A machine learning approach against a masked AES. J. Cryptogr. Eng. 5(2), 123–139 (2015)
[45] Duan, L., Hongxin, Z., Qiang, L., Xinjie, Z., Pengfei, H.: Electromagnetic side-channel attack based on PSO directed acyclic graph SVM. J. China Univ. Posts Telecommun. 22(5), 10–15 (2015)
[46] Maghrebi, H., Portigliatti, T., Prouff, E.: Breaking cryptographic implementations using deep learning techniques. In: Carlet, C., Hasan, M.A., Saraswat, V. (eds.) Security, Privacy, and Applied Cryptography Engineering: 6th International Conference, SPACE 2016, Hyderabad, India, December 14–18, 2016. Proceedings, pp. 3–26. Springer, Cham (2016)
[47] Wang, A.; Li, Y.; Ding, Y.; Zhu, L.; Wang, Y. Efficient Framework for Genetic Algorithm-Based Correlation Power Analysis. IEEE Trans. Inf. Forensics Secur. 2021, 16, 4882–4894.
[48] Wang, C.X.; Zhao, S.Y.; Wang, X.S.; Luo, M.; Yang, M. A Neural Network Trojan Detection Method Based on Particle Swarm Optimization. In Proceedings of the 14th International Conference on Solid-State and Integrated Circuit Technology (ICSICT), Qingdao, China, 31 October–3 November 2018; pp. 1–3.
[49] Huang, C.-L.; Wang, C.-J. A GA-Based Feature Selection and Parameters Optimizationfor Support Vector Machines. Expert Syst. Appl. 2006, 31, 231–240.

[50] Lin, S.-W.; Ying, K.-C.; Chen, S.-C.; Lee, Z.-J. Particle Swarm Optimization for Parameter Determination and Feature Selection of Support Vector Machines. Expert Syst. Appl. 2008, 35, 1817–1824.
[51] Zhang, X.; Chen, X.; He, Z. An ACO-Based Algorithm for Parameter Optimization of Support Vector Machines. Expert Syst. Appl. 2010, 37, 6618–6628.
[52] Sartakhti, J.S.; Afrabandpey, H.; Saraee, M. Simulated Annealing Least Squares Twin Support Vector Machine (SA-LSTSVM) for Pattern Classification. Soft Comput. 2017, 21, 4361–4373.
[53] Yin, Z.; Zheng, J.; Huang, L.; Gao, Y.; Peng, H.; Yin, L. SA-SVM-Based Locomotion Pattern Recognition for Exoskeleton Robot. Appl. Sci. 2021, 11, 5573.
[54] DPA Contest V4. Available online: https://www.dpacontest.org/v4/rsm_doc.php (accessed on 20 March 2023).

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

به‌نام‌خدا

بررسی استفاده از فایربیس Firebase در توسعه اپلیکیشن‌های اندرویدی

خانم دکتر پریسا دانشجو[1]، سیدمحمد میرشریفی[2]

[1]دانشیار،دانشکده فنی مهندسی،دانشگاه آزاد اسلامی- واحد تهران غرب،تهران،ایران، Daneshjoo.p@wtiau.acir
[2]دانشجوی کارشناسی ارشد، واحدالکترونیکی دانشگاه آزاد اسلامی، seyyedstar2097@gmail.com

چکیده

در دنیای توسعه نرم افزارهای کاربردی تلفن همراه، استفاده از فناوری‌های ابری به عنوان راهکاری برای ساده‌سازی فرآیند توسعه و افزایش کارایی سیستم‌ها مورد توجه ویژه قرار گرفته است. فایربیس که توسط شرکت گوگل ارائه شده است، یکی از ابزارهای پیشرفته و پرکاربرد در این حوزه محسوب می‌شود. این پلتفرم(سکو) با ارائه خدمات مختلف نظیر پایگاه داده بلادرنگ، احراز هویت کاربران، اعلان‌های فوری نیز تحلیل رفتار کاربر توانسته است جایگاه ویژه‌ای در بین توسعه‌دهندگان اپلیکیشن‌های اندرویدی پیدا کند.

هدف از این پژوهش، بررسی جامع فایربیس، تحلیل نقاط قوت و ضعف آن همچنین شناسایی کاربردهای آن در توسعه اپلیکیشن‌های اندرویدی است. در این تحقیق از روش کیفی برای جمع‌آوری داده‌ها و تحلیل محتوا استفاده شده است. نتایج نشان می‌دهد که فایربیس می‌تواند به کاهش زمان و هزینه توسعه کمک کرده و در عین حال بهره‌وری سیستم‌ها را افزایش دهد. با این حال، محدودیت‌هایی همچون وابستگی به زیرساخت‌های گوگل و مقیاس‌پذیری در پروژه‌های بزرگ، از جمله چالش‌های اصلی استفاده از این ابزار به شمار می‌رود.

این مقاله می‌تواند به توسعه‌دهندگان و تصمیم‌گیران حوزه فناوری اطلاعات کمک کند تا در انتخاب ابزارهای مناسب برای توسعه اپلیکیشن‌ها (نرم افزارهای کاربردی)، تصمیم‌های بهتری اتخاذ کنند.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

1. مقدمه

با گسترش روزافزون استفاده از تلفن‌های هوشمند و اپلیکیشن‌های موبایلی، نیاز به استفاده از ابزارها و پلتفرم‌های مناسب برای توسعه اپلیکیشن‌ها به یک ضرورت تبدیل شده است. در این راستا فایربیس به عنوان یکی از قدرتمندترین پلتفرم‌های ارائه‌شده توسط گوگل، به توسعه‌دهندگان امکان می‌دهد تا به جای صرف زمان و هزینه برای طراحی زیرساخت‌های پیچیده از جمله هزینه های سرور، از خدمات آماده و جامع آن بهره‌مند شوند.(Smith & Johnson, 2020)

این پلتفرم در سال 2011 توسط شرکت Firebase تأسیس و در سال 2014 توسط گوگل خریداری شد. از آن زمان تاکنون، فایربیس به یکی از ابزارهای پیشرو در توسعه اپلیکیشن‌های موبایلی تبدیل شده است. خدماتی همچون پایگاه داده بلادرنگ، فضای ذخیره‌سازی ابری، تحلیل رفتار کاربر و احراز هویت، از جمله امکاناتی هستند که این پلتفرم در اختیار توسعه‌دهندگان قرار می‌دهد.(Brown et al., 2021)

در این مقاله، پس از معرفی کامل خدمات فایربیس، به بررسی کاربردها، مزایا و معایب آن پرداخته خواهد شد. همچنین رخی از چالش‌های استفاده از این ابزار و راهکارهای مقابله با آن‌ها نیز مورد بحث قرار می‌گیرد.

ضرورت تحقیق در این است که فایربیس به یکی از ابزارهای کلیدی برای توسعه‌دهندگان موبایل تبدیل شده است و بررسی جامع‌تر ویژگی‌ها، مزایا و معایب آن می‌تواند به توسعه‌دهندگان و محققان در انتخاب آگاهانه این پلتفرم کمک کند.

اهداف تحقیق شامل شناسایی کاربردهای اصلی فایربیس، تحلیل مزایا و محدودیت‌های آن و ارائه راهکارهایی برای مقابله با چالش‌های موجود است. در این مقاله، ضمن بررسی خدمات فایربیس، تأثیرات آن بر فرآیند توسعه نرم‌افزار تحلیل می‌شود و راهکارهایی برای بهینه‌سازی استفاده از این ابزار ارائه خواهد شد.

2. مواد و روش‌ها

2.1.روش تحقیق

این تحقیق از روش کیفی برای جمع‌آوری داده‌ها و تحلیل محتوا استفاده کرده است. منابع مورد استفاده شامل مستندات رسمی گوگل، مقالات علمی و پروژه‌های موفق در حوزه توسعه اپلیکیشن‌های اندرویدی بوده‌اند. روش تحقیق بر پایه تحلیل کاربردها و مقایسه ابزارهای مشابه انجام شده است.

2 . 2 سوالات تحقیق

1. فایربیس چه خدماتی برای توسعه اپلیکیشن‌های اندرویدی ارائه می‌دهد؟
2. مزایا و محدودیت‌های استفاده از فایربیس در پروژه‌های اندرویدی چیست؟
3. چگونه می‌توان از فایربیس برای کاهش هزینه‌ها و افزایش کارایی اپلیکیشن‌ها استفاده کرد؟

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

4. چالش‌های اصلی استفاده از فایربیس چیست و چگونه می‌توان آن‌ها را مدیریت کرد؟

2 . 3 جامعه آماری و نمونه

جامعه آماری این تحقیق شامل اپلیکیشن‌های اندرویدی است که از خدمات فایربیس استفاده کرده‌اند. نمونه‌های بررسی‌شده شامل 3 اپلیکیشن موفق بوده که در حوزه‌های مختلف نظیر پیام‌رسانی، مدیریت پروژه می‌کنند.

اپلیکیشن‌های پیاده شده:

1.سیستم جامع مدیریت پارکینگ:

این سیستم به‌طور واقعی و اجرا شده برای وجود فضای پارک کردن در مراکز خرید پیاده شد. این سیستم تماما از زیرساخت فایربیس استفاده کرد که به موارد مورد استفاده از این زیرساخت می‌پردازیم.

1.1-استفاده از حسگر (سنسور)های متصل به فایربیس برای جمع‌آوری داده مثلا پر یا خالی بودن جای پارک.

2.1-استفاده از Firebase Real Time Database ذخیره‌سازی و نمایش درلحظه وضعیت پر یا خالی بودن پارکینگ ها.

3.1-استفاده از سیستم Cloud Messaging برای آگاه‌سازی کاربر با نوتیفیکیشن(اعلان).

4.1-استفاده از سیستم Firebase Authentication برای ساخت حساب کاربری و ذخیره رفتار های کاربر.

5.1-استفاده از سیستم Cloud Storage برای ذخیره‌سازی طولانی مدت و کوئری پذیر SQL

6.1-استفاده از سیستم Firebase Analytics برای خطایابی و گزارش‌گیری از پروژه.

2.فروشگاه اینترنتی:

این سیستم به‌طور واقعی و اجرا شده برای پیاده‌سازی فروشگاه اینترنتی پوشاک از زیرساخت فایربیس استفاده‌کرده که به موارد مورد استفاده از این زیرساخت می‌پردازیم.

1.2- استفاده از Firebase Real Time Database ذخیره‌سازی و نمایش درلحظه وضعیت موجودی محصولات.

2.2- استفاده از سیستم Cloud Messaging برای آگاه‌سازی کاربر با نوتیفیکیشن مانند آگاه‌سازی درصورت موجودشدن محصول، محصولات جدید، تخفیفات.

3.2- استفاده از سیستم Firebase Authentication برای ساخت حساب کاربری و ذخیره رفتار های کاربر.

4.2-استفاده از سیستم Cloud Storage برای ذخیره‌سازی طولانی مدت و کوئری پذیر SQL.

5.2-استفاده از سیستم Firebase Analytics برای خطایابی و گزارش‌گیری از پروژه.

3.پیامرسان:

1.3- استفاده از Firebase Real Time Database ذخیره‌سازی و نمایش درلحظه پیام‌های ارسالی و دریافتی بین خود و مخاطبان.

2.3- استفاده از سیستم Cloud Messaging برای آگاه‌سازی پیام های دریافت شده.

3.3- استفاده از سیستم Firebase Authentication برای ساخت حساب کاربری.

4.3-استفاده از سیستم Firebase Analytics برای خطایابی و گزارش‌گیری از پروژه.

(Amrulloh & Marcos, 2024, p. X)و (Napitupulu, 2023) و (Shelke, Patil, Pinjari, & Budaragade, 2024)

2 . 4 فرآیند تحقیق

فرآیند تحقیق شامل مراحل زیر بوده است:

1. مطالعه مستندات رسمی فایربیس برای شناسایی خدمات و ویژگی‌های آن.(Firebase Documentation, 2023)
2. بررسی پروژه‌های موفق و تحلیل نحوه استفاده از فایربیس در آن‌ها
3. شناسایی مزایا، معایب، و چالش‌های فایربیس در پروژه‌های اندرویدی

2 . 5 ابزار تحقیق

برای این تحقیق از ابزارهای زیر استفاده شده است:

- مستندات رسمی گوگل
- نرم‌افزارهای تحلیل داده
- بررسی اپلیکیشن‌های موفق

3 . یافته‌ها و بحث

3 . 1 خدمات اصلی فایربیس

فایربیس مجموعه‌ای از ابزارها و خدمات را در اختیار توسعه‌دهندگان قرار می‌دهد که عبارتند از:

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

1. **پایگاه داده بلادرنگ (Realtime Database):** این پایگاه داده به توسعه‌دهندگان امکان می‌دهد تا داده‌ها را به‌صورت لحظه‌ای ذخیره و بازیابی کنند. این ویژگی برای اپلیکیشن‌های تعاملی مانند پیام‌رسان‌ها بسیار مفید است مانند تلگرام زمانی‌که در چت(گپ) وضعیت آنلاینی(برخط بودن) یا آفلاینی(برون خط بودن) شخص مشاهده می‌شود یا می‌توان در لحظه و آنلاین(برخط) فیلم ها را مشاهده کرد یا بدون رفرش کردن(راه‌اندازی مجدد) صفحه پیام‌ها دریافت و ارسال میشود.(Johnson, 2021)
2. **Cloud Messaging:** برای آگاه‌سازی نوتیفیکیشن کاربران.
3. **ذخیره‌سازی ابری (Cloud Storage):** فایربیس امکان ذخیره امن فایل‌های چندرسانه‌ای را فراهم می‌کند و به توسعه‌دهندگان اجازه می‌دهد تا به‌سادگی فایل‌ها را مدیریت کنند(Anderson, 2020) .
4. **احراز هویت کاربران (Authentication):** این سرویس از روش‌های متنوعی برای احراز هویت کاربران، مانند ایمیل، شماره تلفن و شبکه‌های اجتماعی پشتیبانی می‌کند و حساب‌کاربری افراد به‌طور یکپارچه در گوگل ذخیره می‌شود.
5. **تحلیل رفتار کاربر (Firebase Analytics):** این ابزار امکان تحلیل دقیق رفتار کاربران را فراهم و به توسعه‌دهندگان کمک می‌کند تا تجربه کاربری را بهبود بخشند، این سرویس امکان رصد خطاهای طرح و پروژه و رصد مدل تلفن همراه و موقعیت مکانی حدودی درحد شهر و کشور را به توسعه دهنده می‌دهد و از لحاظ آمارگیری کاربرد دارد. (Smith, 2022)

3 . 2 مزایا

فایربیس مزایای متعددی دارد که می‌تواند فرآیند توسعه را بهبود بخشد:

1. **کاهش هزینه و زمان توسعه:** استفاده از خدمات آماده فایربیس باعث کاهش هزینه‌های زیرساختی و کاهش زمان توسعه می‌شود و نیازی به هزینه های برنامه‌نویس سرور و حتی خود سرور نیست(Brown et al., 2021) .
2. **یکپارچگی خدمات:** ابزارهای مختلف فایربیس به‌خوبی با یکدیگر یکپارچه هستند و این ویژگی فرآیند توسعه را ساده‌تر می‌کند.
3. **پشتیبانی از پلتفرم‌های مختلف:** ایربیس نه تنها برای اندروید، بلکه برای iOS و وب نیز خدمات ارائه می‌دهد.

3 . 3 محدودیت‌ها و چالش‌ها

1. **وابستگی به گوگل:** وابستگی کامل به زیرساخت‌های گوگل به دلیل تغییر مداوم مستندات ممکن است برای برخی توسعه‌دهندگان مشکل‌ساز باشد. (Anderson, 2020)
2. **محدودیت در مقیاس‌پذیری:** در پروژه‌های بزرگ، محدودیت‌های مربوط به تعداد درخواست‌ها و حجم داده‌ها ممکن است عملکرد سیستم را تحت تأثیر قرار دهد مانند علی بابا(فروش بلیط قطار، هواپیما) که مجبور به تغییر ساختار سروری شد.
3. **پیچیدگی معماری:** استفاده از فایربیس در پروژه‌های بزرگ نیازمند برنامه‌ریزی دقیق و مهارت‌های فنی پیشرفته است.
4. **جایگزین های مناسب درصورت عملکرد نادرست:**

B4A Back For App:Realtime Database

B4A Back For App :Cloud Storage

Matrix, push pole, poshe:Cloud Messaging

Yandex App Metrica : Firebase Analytics

4 . نتیجه‌گیری

فایربیس به عنوان یک پلتفرم و سکوی جامع و پیشرفته، می‌تواند به توسعه‌دهندگان کمک کند تا با کاهش هزینه‌ها و زمان توسعه، اپلیکیشن‌ها و نرم افزارهای کاربردی بهتری تولید کنند. با این حال، توسعه‌دهندگان باید محدودیت‌های آن را در نظر بگیرند و با توجه به نیازهای پروژه، از این ابزار استفاده کنند. در پروژه‌های بزرگ، ممکن است نیاز به ترکیب فایربیس با ابزارهای دیگر باشد.

منابع

- Anderson, P. (2020). Cloud-Based Solutions for Mobile App Development. *Journal of Software Engineering*, 18(3), 34-47.
- Brown, T., Smith, J., & Johnson, R. (2021). Firebase: Revolutionizing Mobile App Development. *Journal of Cloud Computing*, 19(2), 56-78.
- Firebase Documentation. (2023). Official Documentation. Google Inc.
- Johnson, R. (2021). Real-Time Database Management in Mobile Apps. *Database Systems Journal*, 7(3), 89-102.
- Smith, J., & Johnson, R. (2020). Benefits and Challenges of Firebase in Mobile Applications. *International Journal of Mobile Computing*, 15(2), 45-60.
- Amrulloh, N. A., & Marcos, H. (2024). *Perancangan aplikasi data penjualan batik berbasis Android menggunakan database Firebase*. Program Studi Informatika, Fakultas Ilmu Komputer Universitas Amikom Purwokerto.
- Napitupulu, H. Y. P. (2023). *Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia, Depok, Indonesia*.
- Shelke, A., Patil, K., Pinjari, S., & Budaragade, A. P. (2024). *Connecting communities: An Android social networking application with Firebase & Java*. D.Y. Patil College of Engineering & Technology, Kolhapur, Maharashtra, India.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

بررسی مدیریت دسترسی مقیاس پذیر در اینترنت اشیا با استفاده از بلاکچین

دکتر پریسا دانشجو[1]، لیلا کیومرثی[2]

[1]دانشیار،دانشکده فنی مهندسی،دانشگاه آزاد اسلامی- واحد تهران غرب،تهران،ایران، Daneshjoo.p@wtiau.acir

[2]کارشناسی ارشد، گروه مهندسی کامپیوتر، واحد الکترونیکی، دانشگاه آزاد اسلامی، واحد علوم تحقیقات

چکیده

ظهور اینترنت اشیا (IOT) مستلزم چالش‌های فنی جدیدی مانند مدیریت تعداد زیادی از دستگاه های اینترنت اشیا است. با وجود این واقعیت که در حال حاضر انواع چارچوب های مدیریت ایمن برای اینترنت اشیا وجود دارد، آنها بر مدل‌هایی متمرکز هستند که کاربرد آنها را در سناریوهایی با تعداد زیاد دستگاه اینترنت اشیا محدود می کند. تمرکز مدیریت به عنوان نقطه شکست قلمداد می شود و در اشیاء تجاری با مشکل مواجه می شود. مدیریت متمرکز برای اشیاء پویا مانند ماشین‌های زنجیره تامین چالش برانگیز است. به منظور غلبه بر این محدودیت ها، یک سیستم مدیریت توزیع شده اینترنت اشیا مبتنی بر بلاکچین تعریف شد. در این روش موجودیت هایی که مدیر نامیده می‌شوند مسئول مدیریت مجوزهای کنترل دسترسی مجموعه‌ای از دستگاه های اینترنت اشیا هستند. خط مشی مدیریت در بلاکچین ذخیره و تعاملات مدیریتی با اشیا از طریق بلاکچین انجام می‌شود. بلاکچین یک دفتر کل دیجیتال غیرمتمرکز است که برای مدیریت نیازی به یک مرکز کنترل برای همه ندارد(مانند سیستم دسترسی بانک‌ها) علاوه بر این، بلاکچین دارای تکنولوژی ضد دستکاری بوده و امن است. مقیاس پذیری راه حل پیشنهادی (مدیریت دسترسی به صورت غیر متمرکز) با راه حل های مدیریت دسترسی متمرکز در اینترنت اشیا مورد بررسی و نتایج مورد ارزیابی قرار گرفت. طبق نتایج حاصل شده، مقیاس پذیری در سیستم های متمرکز بسیار بالا بوده ولی دستاورهای مدیریت غیر متمرکز قابل توجه است.

کلید واژه- اینترنت اشیا(IOT) ، بلاکچین ، قرارداد هوشمند(Smart Contract) ، مدیریت دسترسی ، مقیاس پذیری

مقدمه:

اینترنت اشیا(IOT) به اتصال دستگاه هایی با قابلیت های محدود به اینترنت اشاره دارد. یکی از جنبه های اصلی اینترنت اشیا تسهیل به اشتراک گذاری منابع دستگاه های محدود شده با سایر نهادها است. برای محقق شدن این موضوع، دستگاه ها(IOT) باید بتوانند مدیریت کنند که چه کسی به منابع آن ها دسترسی داشته باشد. این دستگاه ها در ذخیره و پردازش اطلاعات جهت مدیریت دسترسی به منابع خودشان محدودیت هایی دارند و این موضوع زمانی مهم تر می‌شود که در سناریوهای پویا مرتب دستگاه های اینترنت اشیا در شبکه اضافه وکم می شوند و این باعث می شود دستگاه فرستنده به‌طور دائم سیاست های خود را تغییر دهد. بر همین اساس، راه حل هایی بر اساس آیین نامه‌های محدوده شده مانند پروتکل اپلیکیشن‌های محدود شده (CoAP) ارائه شده است[۱].این آیین نامه‌ها دستگاه های اینترنت اشیاء را به صورت متمرکز و از طریق یک سرور مدیریت می کنند و چون در یک نقطه متمرکز شده است، به عنوان نقطه شکست قلمداد می شود و در اشیاء تجاری نیز در زمینه مقیاس پذیری مشکلاتی به‌وجود می آید. این معماری متمرکز برای مدیریت اشیایی که توسط یک حوزه مدیریت کنترل می شوند ممکن است پاسخگو باشد ولی برای اشیاء پویا مانند ماشین های زنجیره

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

تامین که ممکن است حوزه های مدیریتی متفاوت داشته باشند چالش برانگیز است. رویکرد های زیادی درباره مدیریت دسترسی به اینترنت اشیا وجود دارد؛ اولین رویکرد که توسط کارگروه مهندسی اینترنت، توسعه پیدا کرد، رابط مدیریتی CoAP نامیده می شود(CoMI). رویکرد دیگر LwM2M (یک پروتکل مدیریت دستگاه‌ها است که برای دستگاه‌های محدود و نیازهای محیط ماشین به ماشین M2Mطراحی شده است.)که توسط کمپانی Open Mobile Alliance توسعه پیدا کرد.

فناوری بلاکچین:

از زمان معرفی بیت کوین توسط ساتوشی ناکاموتو در سال۲۰۰۹، بلاکچین محبوبیت خود را افزایش داد[۲]. به این ترتیب، بلاکچین در مناطقی غیر از ارزهای رمز پایه اعمال شده است، زیرا پتانسیل(ظرفیت) آن فراتر از بیت کوین است. از سو ی دیگر، نقاط قوت آن باعث شده است که به یک جزء ایده آل برای راه حل های اینترنت اشیا تبدیل شود. اهداف طراحی ساختار بلاکچین شامل: ممانعت از قوانین سیستم توسط مقامات مرکزی، اطلاعات ذخیره شده قابل ممیزی و قابل استفاده برای همه همتایان است، تراکنش ها توسط همتایان تایید می شود و سیستم، قابل دستکاری توسط عوامل مخرب نیست و با اجماع همتایان، تغییرات انجام می شود. بلاکچین یک دفتر دیجیتال از تراکنش های گذشته است. تراکنش، تبادل اطلاعات بین نهادهای مختلف است که به شبکه پخش می شود[۳].

تراکنش ها به ترتیب زمانی در بلوک ها ذخیره می شوند و هر بلوک حاوی یک هش از بلوک قبلی است که زنجیره ای از بلوک ها را ایجاد می‌کند. اولین بلوک در زنجیره به نام بلوک پیدایش، تنها بلوکی است که حاوی هش بلوک قبلی نیست. بلوک ها نه تنها تراکنش ها را ذخیره می کنند، بلکه می توانند انواع دیگری از اطلاعات دیجیتال مانند قرارداد های هوشمند را نیز ذخیره کنند. قرارداد هوشمند یک قرارداد تراکنش کامپیوتری است. بلاکچین به هیچ مرجع متمرکزی متکی نیست و با فرض غیر قابل اعتماد بودن گره های داخل شبکه از طریق اجماع همتایان برای تایید اطلاعات و توافق متکی است. الگوریتم های اجماع PoW (اثبات کار) - PoS (اثبات سهام) - PoB : (اثبات سوختگی) - PoC (امکانات ذخیره سازی)در بلاکچین مورد استفاده قرار می گیرد.

توابع هش یا درهم ساز: تابعی که یک ورودی دیجیتال با طول دلخواه می گیرد و یک خروجی با طول ثابت نگاشت می کند. طول ورودی هیچ اثری بر روی خروجی نداشته و سایز خروجی ثابت است. تابع هش، یکطرفه و به هیچ عنوان قابل تبدیل به مقدار اولیه نخواهد بود. هش های بیتکوین از نوع sha256 است که یا به صورت ۲۵۶ بیت بوده و یا ۶۴ کاراکتر هگزا دسیمال است.

کاربرد هش در بلاکچین: صحت داده حفظ می‌شود و کوچکترین تغییر در ورودی باعث تغییرات چشمگیر در خروجی می‌شود. برای امنیت بالا کلمات عبور هش شده نگهداری می‌شود. آدرس کیف پول(Account Address) در بلاکچین از هش کلید عمومی کاربران تولید می‌شود.

تراکنش‌ها: تراکنش انتقال مبلغ بین فرستنده و گیرنده است. فرستنده برای ارسال باید نشانی گیرنده که همان کلید عمومی هش شده را دارد وارد کند. وقتی تراکنش ارسال می‌شود، گیرنده کلید عمومی را با کلید خصوصی مطابقت داده و می‌تواند به اطلاعات دست پیدا کند. برای اطمینان از صحت اطلاعات، تمام اطلاعات داخل بلاک هش و با هش بلاک قبلی(Parent) نیز دوباره هش می شود. طبق مدل هش

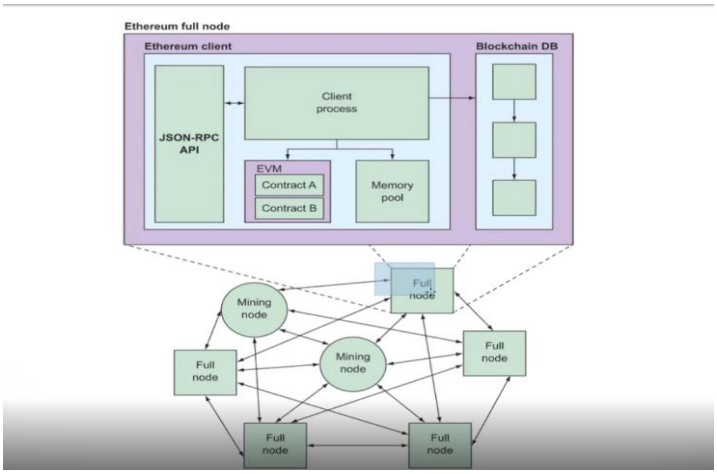
دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

درخت مرکل، تمامی تراکنش ها هش و سپس هش آنها نیز دو به دو با یکدیگر هش می‌شوند. در صورت تغییر در یکی از تراکنش‌ها هش درخت مرکل به‌هم ریخته و زمانی که بلاک در شبکه ارسال می‌شود، تمام نودها باخبر شده و در صورتی که نود خاطی اطلاعات را اصلاح نکند در شبکه کنار گذاشته می‌شود.

بلاکچین و Decentralized : با ورود یک تراکنش نود ها برای پردازش آن اعلام آمادگی کرده و با طرح یک مسئله پیچیده توسط بلاکچین و حل توسط سریع ترین نود، آن نود انتخاب می‌شود. بلاکچین یک سیستم توزیع شده است و اطلاعات ثبت شده در آن تغییر ناپذیر است. دارای یک ماژول به اسم لجر(Ledger) نظیر به نظیر (P2P) توزیع شده(DLT) هر نود از شبکه یک نسخه کامل (کپی محلی) از دیتا بیس را دارد و این کپی در همه گره ها یکسان است. نود ها به طور مرتب کپی محلی خودشان را به‌روزرسانی می کنند. هر تراکنش وقتی معتبر خواهد بود که اکثریت نود های شبکه آن را بپذیرند(۵۱٪).

وقتی بلاک جدیدی تولید می‌شود در شبکه Broadcast می شود. با اجرا و راه اندازی client هر سیستمی یک نود از شبکه بلاکچین می شود. توسط اتریوم، انتقال هر گونه ارزشی (اعم از توکن، مالکیت و...) بین نود های شبکه امکان پذیر است.

اتریوم یک بلاکچین، EVM compatible است، پس از راه اندازی نود در شبکه اتریوم یک ماشین مجازی بر روی سیستم ایجاد می شود و هر سیستم عاملی می‌تواند به شبکه متصل گردد. وقتی یک سیستم فول نود می‌شود و می‌تواند برنامه های قراردادهای هوشمند را که کامپایل شده است، بر روی خود اجرا کند، قرارداد هوشمند بر روی همه نود ها قرار می‌گیرد. قراردادهای هوشمند، نرم افزار های واسطی بین دیتای بلاکچین و Applicationهای نوشته شده هستند[۴].



در این مقاله با استفاده از امکانات بلاکچین روشی برای مدیریت غیر متمرکز دسترسی اینترنت اشیا پیشنهاد می شود.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

روش پیشنهادی:

شکل زیر، نمای کلی از معماری مدیریت دسترسی غیر متمرکز و اجزای آن را نشان می دهد[۵] . نقش یک مدیر گروه عامل را می توان با توجه به موارد استفاده مختلف توسط بازیگران مختلف بازی کرد. (به جز شبکه های حسگر بی سیم و نودهای مدیریت هاب).

تمام شبکه های حسگر بی سیم به منظور تعامل با بلاکچین به گره های مدیریت هاب متصل هستند.

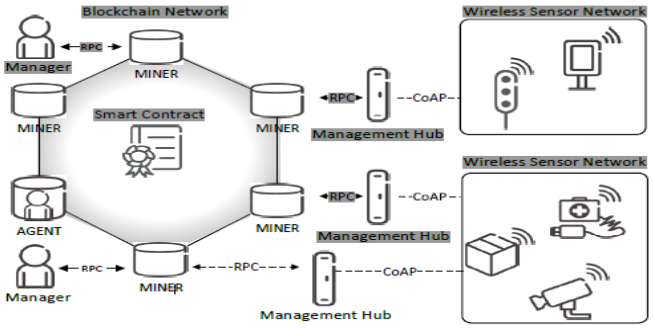


Fig. 2: Decentralized Management System

شبکه های حسگرا بی سیم (WSN) : شبکه حسگر بی سیم شبکه ای از دستگاه های اینترنت اشیا است که امکان اتصال محدود در برنامه‌های کاربردی باتوان محدود و منابع محاسبات را دارد. دستگاه های اینترنت اشیا مرتبط با WSNها به دلیل حافظه محدود، قدرت محاسباتی و یا در دسترس بودن انرژی به بلاکچین تعلق ندارند و با پروتوکل CoAP (از یک مدل پیاده سازی امن)بین آنها با مدیریت هاب ارتباط برقرار می‌کنند و در بلاکچین با یک کلید عمومی شناخته می شوند.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

مدیران: مدیر مسئول مدیریت دسترسی و کنترل مجوزهای مجموعه ای از دستگاه های اینترنت اشیا است. مدیران تعلق به WSNها ندارند و مالک دستگاه های موجود در آن هستند. مدیران به جای اشیا با بلاکچین تعامل دارند و مجوز های دسترسی به آنها را کنترل می کنند. دستگاه ها امکان ارتباط با قرارداد هوشمند را ندارند و یک شی فقط می تواند توسط یک مدیر ثبت شود.

نود عامل: یک نود پاسخگو به استقرار قرارداد هوشمند بوده و قرارداد را در تمام شبکه توسط نشانی آن انتشار می دهد.

قرارداد هوشمند: سیستم مدیریتی که در این تحقیق مد نظر است یک عملیات تعریف شده در یک قرارداد هوشمند واحد است.

Name	Method	Description
Register Manager	Tx	Registers a Manager into the system.
Register Device	Tx	Registers a Device into the system.
Add Manager to Device	Tx	Registers a Device under a Manager's control.
Remove Manager to Device	Tx	De-registers a Device from a Manager's control.
Add Rule	Tx	Adds an access control rule under a device.
De-register Manager	Tx	De-registers a Manager from the system. The manager should not manage any device before being remove from the system.
De-register Device	Tx	De-registers a Device from the system.
Revoke Permission	Tx	Deletes a policy rule from the system.
Query Manager	Call	Checks if a node is a Manager.
Query Permission	Call	Checks if a Device can access the resources of another Device.

TABLE I: Operations of the Smart Contract

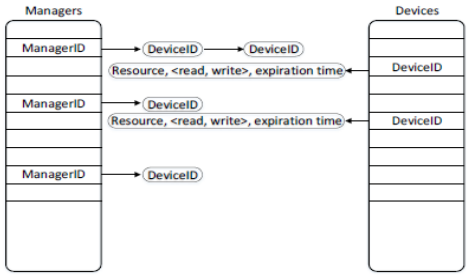


Fig. 3: Data Structure in the Smart Contract

همانطور که در شکل جدول I مشخص است، دو نوع عملیات در یک قرارداد هوشمند وجود دارد. یکی عملیاتی که توسط تراکنش های بلاکچین آغاز می شود و دیگری عملیاتی که بلاکچین را پرس و جو می‌کند. اولی باید توسط ماینرها انجام شود در حالی در دومی نیازی نیست و بدون هزینه است. طبق شکل ۳ : اطلاعات محدود دستگاه ها، مدیران و سیاست های مدیریت دسترسی با دو ساختار متفاوت در قرارداد های هوشمند ذخیره می شوند. علاوه بر آن، مدیران تنها موجوداتی هستند که امکان تعامل با قراداد هوشمند را از طریق تراکنش برای ثبت نام و لغو ثبت و تعریف سیاست های جدید در سامانه را دارند. هاب های مدیریت فقط از طریق فراخوان می‌توانند اطلاعات دسترسی ها را از بلاکچین ها به‌دست آورند.

شبکه بلاکچین: شبکه ای که برای اجرای مفهوم کار ما انتخاب شده، اتریوم است که یک Platform با قابلیت توسعه برنامه هایی با زبان Solidity برای ایجاد قرارداد های هوشمند به شمار می رود.

ماینرها در شبکه امنیت و پایداری شبکه را از طریق تایید تراکنش‌ها و ذخیره در بلاکچین تامین می کنند.

هاب های مدیریت: این هاب ها در لبه WSN's قرار دارند، یک رابط کاربری جاوا اسکریپتی هستند که اطلاعات کدگذاری شده در پیام CoAP توسط اینترنت اشیا را به پیام RPC ترجمه می کنند. هاب مدیریت به یک نود از شبکه بلاکچین متصل است. این واسط کاربری از WEB 3 Javascript API برای ارتباط با نود های اتریوم با فراخوانی RPC و همچنین از سمتی دیگر از طریق

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

WEB3 JAVA Script Library با اشیا ارتباط برقرار می‌کند. هاب مدیریت فقط عملیات Query permission را از قرارداد هوشمند اجرا می‌کند و اشیا می توانند اطلاعات دسترسی را توسط هاب مدیریت از بلاکچین بدون هیچ هزینه ای دریافت کنند و نیازی به تایید ماینرها نیست و زمان پاسخگویی بالا است. چندین شبکه حسگرا به یک هاب مدیریت و چندین هاب مدیریت می‌توانند به یک نود متصل شوند که مقیاس پذیری را تا حدود زیادی بالا می برد. در صورت خرابی یک نود هاب مدیریت به طور خودکار به نود دیگری وصل می شود. در صورت خرابی یک هاب مدیریت اشیاء به طور خودکار به یک هاب مدیریت دیگر متصل می شوند.

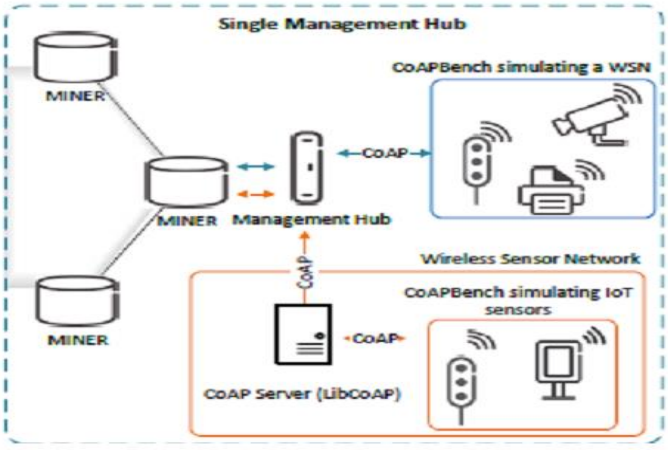
انجام آزمایش و مقایسه عملکرد : برای انجام این آزمایش از یک دسکتاپ با سیستم عامل اوبونتو استفاده شده و برای اندازه گیری و ارسال درخواست‌ها از ابزار CoAP Bench استفاده شد تا قادر به ارسال پیام‌های PUT ، POSTو DELETE باشد، همچنین قادر به تشخیص داده درخواستی بوده و عملیات ثبت در LwM2M را پشتیبانی کند. برای پیاده سازی ایجاد پیام از کتابخانه CoAP-Lib در یک سروری در همان ماشین استفاده شد. برای پیاده سازی شبکه بلاکچین توسط نرم افزار داکر یک نسخه از اتریوم نصب شد. پیاده سازی Wakaama و Leshan (دو سرور پیشرفته جاوایی)از پروتکل مدیریتی LwM2M سرور را در اختیار داریم.

در این تحقیق، به‌وسیله ابزار CoAP Becnch درخواست‌هایی را به عنوان مشتری به Leshan وWakaama ارسال و مشتریان مجازی، از ۱ به ۱۰۰۰۰ افزایش داده شد. پس از ثبت نام مشتریان، به روز رسانی اطلاعات بر روی سرور LwM2M در مدت ۳۰ ثانیه ترافیک ایجاد شد. در اینجا چون درحالت آزمایشی غیر متمرکز در حالت اولیه بود، فقط اشیاء شبیه سازی شده و هاب ها درگیر بودند و بقیه عملیات مربوط به قرارداد هوشمند است که از طریق تراکنش ها در بلاکچین توسط ماینر ها با تاخیر انجام می شود و در این مقطع درگیر نبودند.

به همین علت ارزیابی سیستم غیر متمرکز با دو سناریو انجام پذیرفت:

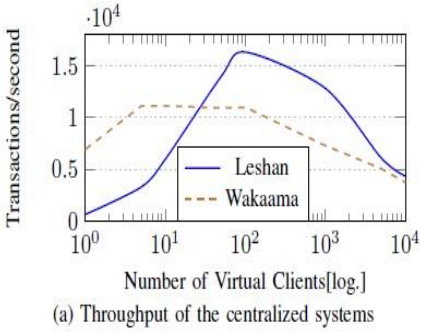
در سناریوی اول شبیه سازی تغییر اندازه شبکه در یکWSN متصل به یک هاب مدیریت را انجام دادیم؛ جایی که client های مجازی ترافیک درخواست دسترسی به یک منبع خاص را به مدیریت هاب ارسال می کنند.

در سناریوی دوم شبیه‌سازی، تعداد متنوعی از درخواست‌های همزمان دستگاه‌های اینترنت اشیا از منبعی که توسط یک دستگاه اینترنت اشیای دیگر ارائه می‌شود، دریافت می‌گردد. در سناریوی دوم، درخواست کنترل دسترسی از طرف اشیا از بلاکچین و سپس از طریق هاب مدیریت به اشیا ارسال می‌شود.

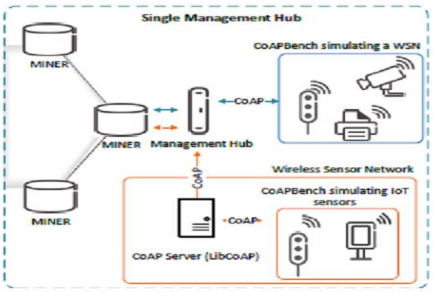


دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

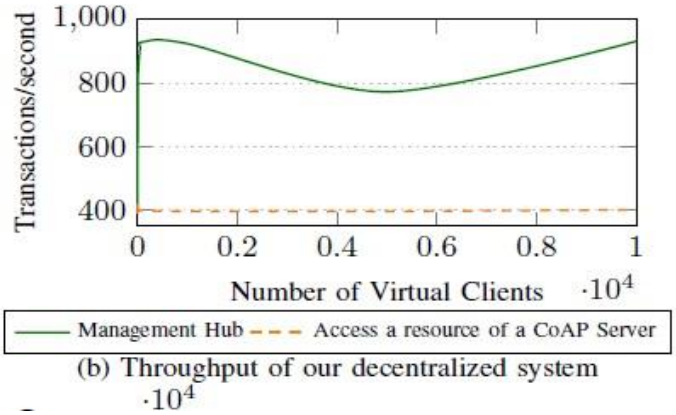
هدف ما در اینجا، به‌دست آوردن درک درستی از مقیاس پذیری سیستم های موجود با یک سرور متمرکز با روش تحقیق ما از یک سیستم غیر متمرکز و با چندین هاب مدیریت و تعداد نامحدودی گره در شبکه بلاکچین است. در هر دو سناریو، ارسال درخواست‌ها از مشتری مجازی از یک طیفی از ۱ تا ۱۰۰۰۰به یک هاب مدیریت واحد ارسال می شود.



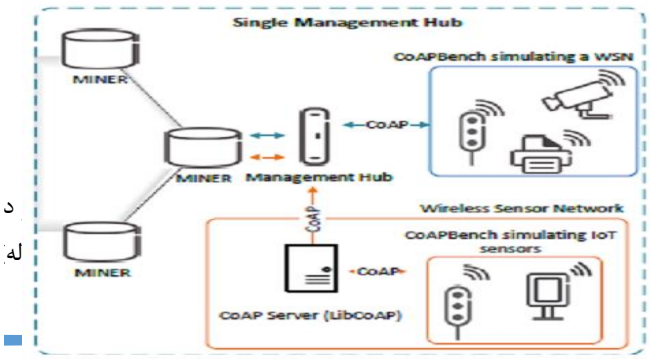
(a) Throughput of the centralized systems



ابتدا ما توان عملیاتی Wakaama و Leshan و پیاده سازی خود را ارزیابی کردیم. طبق شکل a- Leshan حداکثر عملکرد ۱۶۰۰۰ هزار درخواست در ثانیه را از ۱۰۰ مشتری همزمان داشته است. Wakaama برعکس Leshan به حداکثر توان خود با ۱۲۰۰۰ درخواست برای ۵ مشتری همزمان زودتر رسیده است. اما عملکرد آن در ابتدا از ۱ تا ۵۰ مشتری همزمان بالاتر از Leshan بوده و توان خود را تا ۱۰۰ مشتری همزمان نیز حفظ کرده است. در یک نقطه توان هر دو سرور به طور ثابل توجهی کاهش پیدا کرده و به ۴۰۰۰ هزار درخواست در ثانیه از ۱۰۰۰۰ مشتری مجازی رسیده است. در حقیقت thread های سیستم عامل ما بعد از ۱۱۰۰۰ درخواست تمام شده است. در این لحظه Leshan متوقف ولی wakaama هنوز با ۱۱۰۰۰ کلاینت مجازی به کار خود ادامه می دهد.



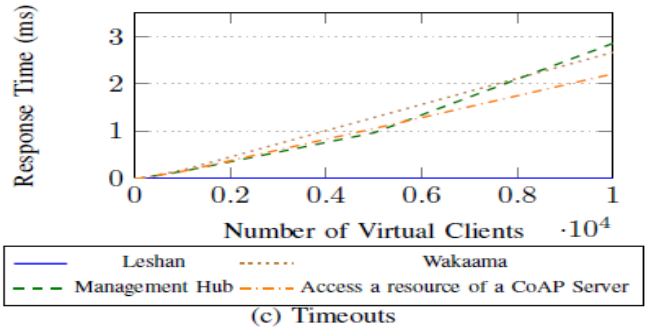
(b) Throughput of our decentralized system
·10^4



قوانین کلی نشریه به شرح زیر است:

پیاده سازی تحقیق ما (غیر متمرکز) در شکل b عملکرد ضعیف تری را در مقابل سیستم های متمرکز نشان می دهد. عملکرد زمانی که اندازه WSN از ۱ به ۱۰۰۰۰ مشتری تغییر کرد، تنها در حدود ۷۹۰ درخواست در ثانیه است.

در سناریوی دوم که در آن تعداد متنوعی از مشتریان به طور پیوسته اطلاعات یک دستگاه IOT را درخواست می‌کنند، با وجود تعداد مشتریان اینترنت اشیا که درخواست اعلام می کنند به طور ثابت در ۳۹۰ درخواست در ثانیه است.



(c) Timeouts

شکل c تعداد درخواست های timeout شده در ۳۰ ثانیه از انجام تست را نشان می دهد. Timeoutبرای همه سیستم ها به جز Leshan افزایش یافته است. او با وجود اینکه در مرز ۱۰۰۰۰ مشتری مجازی متوالی به دلیل کمبود حافظه متوقف شد توانست تمام درخواست‌ها را با timeout نزدیک به صفر پاسخگو باشد. در مقایسه راه حل های پیشرفته(سرور های جاوایی) ، پیاده سازی ما در یک مرتبه پایین تری قرار گرفت و عامل محدود کننده اصلی، تاثیر تاخیر پیام‌های RPC بین هاب مدیریت و بلاکچین است.

مقیاس پذیری: در بحث مقیاس پذیری، همانگونه که نتایج قبلی هم نشان داده مدیریت دسترسی سنتی (متمرکز)از پیاده سازی ما از نظر توان عملیاتی بهتر بود. با این حال، هدف ما رسیدن به یک سیستم متمرکز بهینه سازی شده نبود و در عوض، ما از مقیاس پذیری افقی در حالیکه WSN ها به چندین هاب مدیریت متصل هستند حمایت می کنیم.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

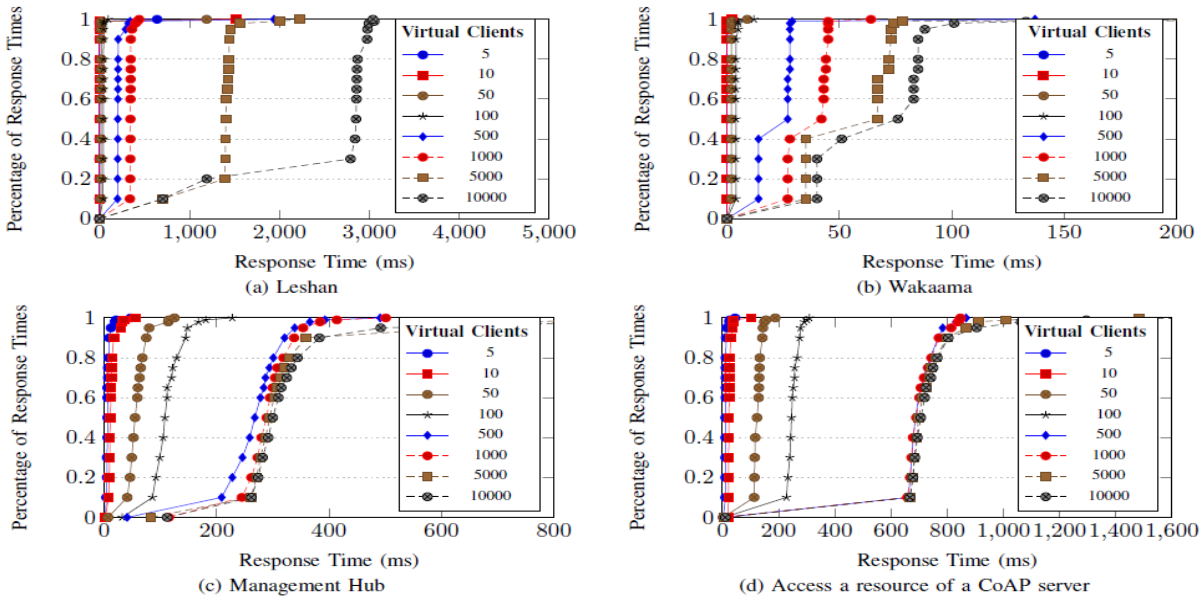
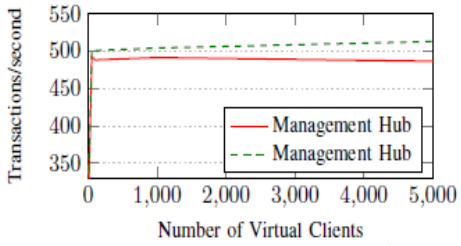


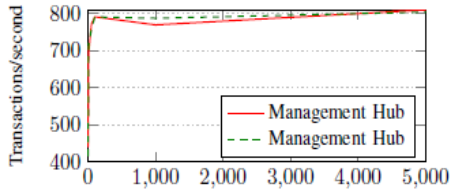
Fig. 6: Latency

تاخیرات: طبق شکل ۶، تاخیر Leshan در حالی‌که برای ۱۰۰۰ مشتری مجازی کم بود، برای ۱۰۰۰۰ مشتری همزمان تا ۳ ثانیه افزایش یافت. Wakaama به شکل چشمگیری برای مشتریان مجازی، تاخیرات را پایین نگه داشت. در پیاده سازی روش ما، عملیات در ارتباط مستقیم با هاب مدیریت ، نسبت به عملیاتی که از Access a resource of CoAP server انجام می‌شود ۵۰ درصد عملکرد بهتری دارد، در حالی‌که سیستم ما دارای عملکرد بالاتری نسبت به Leshan برای مشتریان بالای ۱۰۰۰ است. با اینکه عملکرد کلی سیستم ما پایین بود، عملکرد کلی wakaama قابل قبول بوده و نشانگر این است که عملکرد در یک سیستم متمرکز بهتر از عملکرد در روش ما از نظر مقیاس پذیری در شرایط یک هاب مدیریت بود.

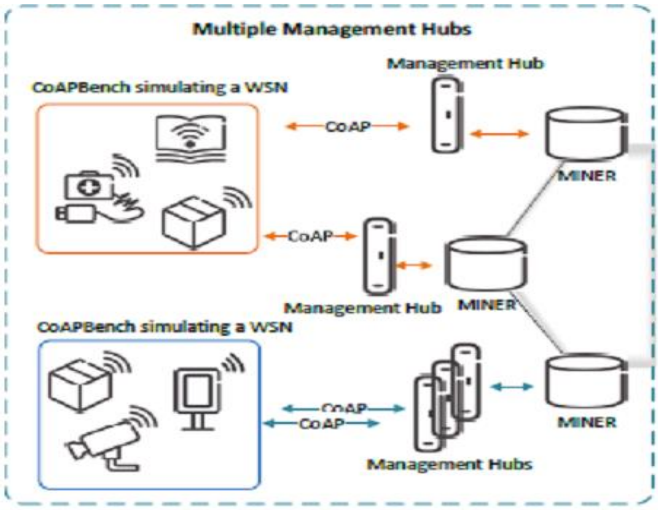
دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055



(a) Two Management Hubs connected to one blockchain node



(b) Two Management Hubs connected to two different blockchain nodes



ارزیابی سناریوی چند هاب مدیریت : در بخش شکل ۴ : در سناریوی اول به طور همزمان دو هاب مدیریت را به یک نود از بلاکچین متصل تا عملکرد آن را بررسی و در سناریوی دوم دو هاب مدیریت را به دو نود بلاکچین به طور جداگانه متصل می‌کنیم. دستگاه های WSN به طور مساوی به هریک از هاب های مدیریت وصل می شوند.

شکل a توان مدیریتی هر یک از هاب های مدیریتی را نشان می دهد. در اینجا خروجی توان عملیاتی هر هاب مدیریت نصف خروجی توان یک هاب مدیریت در نمودار b است که به یک نود بلاکچین متصل شده است.(با توجه به شکل b) در این سناریو، کاهش شدید عملکرد وجود دارد و اتصال چند هاب به یک نود بلاکچین خروجی مطلق نود را بین هاب ها تقسیم می کند. از طرفی وقتی دو هاب را به دو نود مختلف بلاکچین وصل می‌کنیم، خروجی ها با خروجی شکل b برابر است. به عبارتی دیگر سیستم طوری طراحی شده که بهترین عملکرد را زمانی که چندین هاب مدیریتی به نودهای مختلف بلاکچین وصل می شود داشته باشد، به طوری‌که عملکرد ۲۰ هاب مدیریتی در مناطق مختلف جغرافیایی با WSN های متفاوت، عملکرد بهتری نسبت به Leshanو wakaama داشته اند. در نظر داشته باشید که آزمایش با ۵۰۰۰ مشتری مجازی به جای ۱۰۰۰۰ انجام گرفت که این به‌دلیل شرایط CoAP Bench بود که با جاوا پیاده سازی شده بود و برای افزایش به ۱۰۰۰۰ عدد و افزایش thread باید از ماشین های مجازی استفاده می‌شد که این خود به‌دلیل تاخیر در شبکه ماشین های مجازی بر نتایج ما تاثیر منفی می گذاشت.

نتیجه گیری: این مقاله، یک معماری اثبات مفهوم را ارائه می‌کند که از فن آوری بلاکچین به منظور پیاده سازی سیستم مدیریت دسترسی برای اینترنت اشیا استفاده می کند و در آن اعتبار ها و مجوز ها برای دسترسی به منابع مختلف اینترنت اشیا در سطح جهانی در زنجیره بلاکچین ذخیره می شود. یکی از تفاوت‌های اصلی روش ما با روش های موجود، طراحی غیر متمرکز آن است که در آن، سیاست های کل سیستم در یک بلاکچین ذخیره می شود. همچنین، این مقاله پیشرفته ترین سیستم های مدیریت دسترسی در IOT را در برابر راه حل ما ارزیابی می‌کند. هدف از این مطالعه به‌دست آوردن درک درستی از تاثیر عملکرد و مقیاس پذیری توزیع اطلاعات کنترل دسترسی به دستگاه های اینترنت اشیا در برابر سیستم های مدیریت دسترسی فعلی اینترنت اشیا است. طبق یافته های این مطالعه، راه حل ما عملکرد بهتری نسبت به سیستم های متمرکز IOT بهینه شده در مورد یک مرکز مدیریت ندارد؛ با این حال، ارزیابی نشان می دهد که پیاده سازی ما نسبت به سناریو های متمرکز زمانی که بار را بین شبکه های بلاکچین توزیع می کنیم، مزایای مقیاس پذیر قابل توجهی دارد.

به طور خلاصه راه حل ارائه شده در تحقیق، به گونه‌ای طراحی شده که مقیاس پذیری افقی را در جایی که WSN ها به چندین هاب مدیریت متصل هستند مورد توجه قرار می دهد و اثر بخشی طراحی ما را در برخی از سناریو های خاص اینترنت اشیا اثبات می کند.

مراجع

[1] S. Wallin, "Automating Network and Service Configuration Using NETCONF and YANG."

[2] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Business & information systems engineering,* vol. 59, pp. 183-187, 2017.

[3] S. M. B. A Ouriat, S Khandan Alamdari, "Application, Pros and Cons of Blockchain Networks," *International Journal of Finance & Managerial Accounting,* 2024.

[4] Y. C. Hu, T. T. Lee, D. Chatzopoulos, and P. Hui, "Analyzing smart contract interactions and contract level state consensus," *Concurrency and Computation: Practice and Experience,* vol. 32, no. 12, p. e5228, 2020.

[5] O. Novo, "Scalable access management in IoT using blockchain: A performance evaluation," *IEEE Internet of Things Journal,* vol. 6, no. 3, pp. 4694-4701, 2018.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

چالش های امنیتی در حوزه رایانش ابری

کیارش محمودنهرانی[1]، محسن حیدری[2] و محمد بغدادی[3]

[1]دانشجوی کارشناسی ارشد،دانشکده فنی مهندسی،دانشگاه آزاد اسلامی- واحد تهران غرب،تهران،ایران

[2]دانشجوی کارشناسی ارشد،دانشکده فنی مهندسی،دانشگاه آزاد اسلامی- واحد تهران غرب،تهران،ایران

[3]دانشجوی کارشناسی ارشد،دانشکده فنی مهندسی،دانشگاه آزاد اسلامی- واحد تهران غرب،تهران،ایران

چکیده:

به‌موازات رشد و گسترش تکنولوژی اطلاعات، مقوله امنیت در شبکه‌های ابری، به‌طور چشمگیری مورد توجه قرار گرفته است. امروزه امنیت به‌عنوان یکی از مهمترین چالش‌های فناوری رایانش ابری، مورد مطالعه محققان است. مهمترین گام در تامین امنیت، تشخیص تهدیدات احتمالی و ارایه فرایند امنیتی و محافظتی لازم است.در این فناوری، ابر، ابزاری است برای برون سپاری خدمات و باعث فراهم آمدن امکان استفاده تخصصی تر و کاراتر از منابع می‌شود. این مقاله چالش‌های امنیتی در بستر رایانش ابری را مورد بررسی قرار داد و نشان داد که احراز هویت کاربران یک گام حیاتی برای افزایش امنیت در ابر است. تکنیک‌های موجود برای احراز هویت کاربران شامل روش‌های سنتی مانند رمزهای عبور و پین‌ها هستند که به دانش کاربر متکی‌اند. روش‌های امن‌تر مانند احراز هویت چندعاملی چندین شکل تاییدیه از جمله رمزهای عبور، کارت‌های هوشمند و بیومتریک را ترکیب می‌کنند. علاوه بر این، روش‌هایی مانند رمزهای یک‌بار مصرف و تحلیل ضربه‌های کلید با تولید کدهای زمان‌دار و تحلیل الگوهای تایپ، امنیت را افزایش می‌دهند. تکنیک‌هایی مانند ماژول قابل اعتماد موبایل با توابع هش و رمزنگاری نامتقارن، احراز هویت چندعاملی با الگوریتم‌های رمزنگاری فازی هش و تحلیل ضربه‌های کلید با الگوریتم‌های خوشه‌بندی k-means نیز به کار می‌روند. همچنین، احراز هویت یک‌باره با پروتکل OTP و احراز هویت بیومتریک با سیستم احراز هویت استاتیک ارائه شده‌اند.

کلمات کلیدی: رایانش ابری، چالش‌های امنیتی رایانش ابری، احراز هویت، کنترل دسترسی، Cloud API

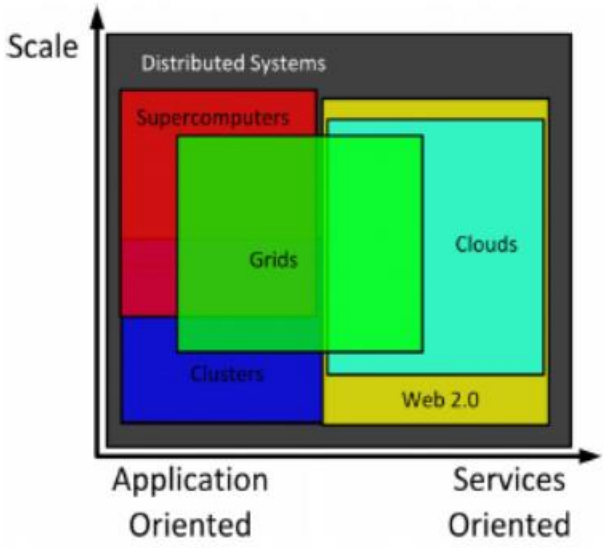
1. مقدمه

رایانش ابری یک مدل قوی است که به کاربران و سازمان‌ها اجازه می‌دهد خدمات مورد نیاز خود را براساس نیاز خود خریداری کنند. این مدل، خدمات بسیاری مانند ذخیره‌سازی، پلتفرم‌های استقرار، دسترسی راحت به سرویس‌های وب و غیره را ارایه می‌دهد. تعادل بار یک مشکل رایج در فضای ابری است که حفظ عملکرد برنامه‌های کاربردی مجاور اندازه‌گیری کیفیت خدمات(QoS[17]) و پیروی از سند توافقنامه سطح سرویس(SLA[18]) را که از سوی ارایه‌دهندگان ابری به شرکت‌ها نیاز است، دشوار می‌کند. هدف ارایه‌دهندگان

[17] Quality of Service
[18] Service Level Agreement

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

ابر، توزیع بار کاری برابر بین سرورها است[1]. ویژگی‌های رایانش ابری با بسیاری از فناوری‌های موجود دیگر مانند رایانش شبکه‌ای، رایانش کاربردی، رایانش خوشه‌ای و رایانش توزیع‌شده به طور کلی همپوشانی دارد. در واقع، رایانش ابری از رایانش شبکه‌ای تکامل یافته و به عنوان عضو اصلی و پشتیبانی زیرساختی به آن متکی است. این تکامل، نتیجه تغییر در تمرکز از زیرساختی که منابع ذخیره‌سازی و محاسباتی ارائه می‌دهد (مانند مورد در شبکه‌ها) به زیرساختی است که بر اساس اقتصاد طراحی شده و هدف آن ارائه منابع و خدمات انتزاعی‌تر است (مانند مورد در ابرها). اما در مورد رایانش کاربردی، این یک الگوی جدید زیرساخت رایانشی نیست؛ بلکه یک مدل تجاری است که در آن منابع رایانشی، مانند محاسبات و ذخیره‌سازی، به‌صورت خدمات اندازه‌گیری‌شده و بسته‌بندی‌شده مشابه یک خدمت عمومی فیزیکی، مانند برق یا شبکه تلفن عمومی ارائه می‌شوند. رایانش کاربردی معمولاً با استفاده از سایر زیرساخت‌های رایانشی (مثلاً شبکه‌ها) با خدمات اضافی حسابداری و نظارت پیاده‌سازی می‌شود. یک زیرساخت ابری می‌تواند به صورت داخلی توسط یک شرکت استفاده شود یا به عنوان رایانش کاربردی به عموم عرضه شود. شکل 1، نمای کلی از رابطه بین ابرها و حوزه‌های دیگر را که با آن‌ها همپوشانی دارند، نشان می‌دهد. وب 2.0 تقریباً تمام طیف برنامه‌های خدمات‌محور را پوشش می‌دهد که در آن رایانش ابری در سمت مقیاس بزرگ قرار دارد. ابررایانه‌ها و رایانش خوشه‌ای بیشتر بر برنامه‌های غیرخدماتی سنتی متمرکز شده‌اند. رایانش شبکه نیز با همه این زمینه‌ها همپوشانی دارد که به طور کلی در مقیاس کمتری نسبت به ابررایانه‌ها و ابرها در نظر گرفته می‌شود [2].

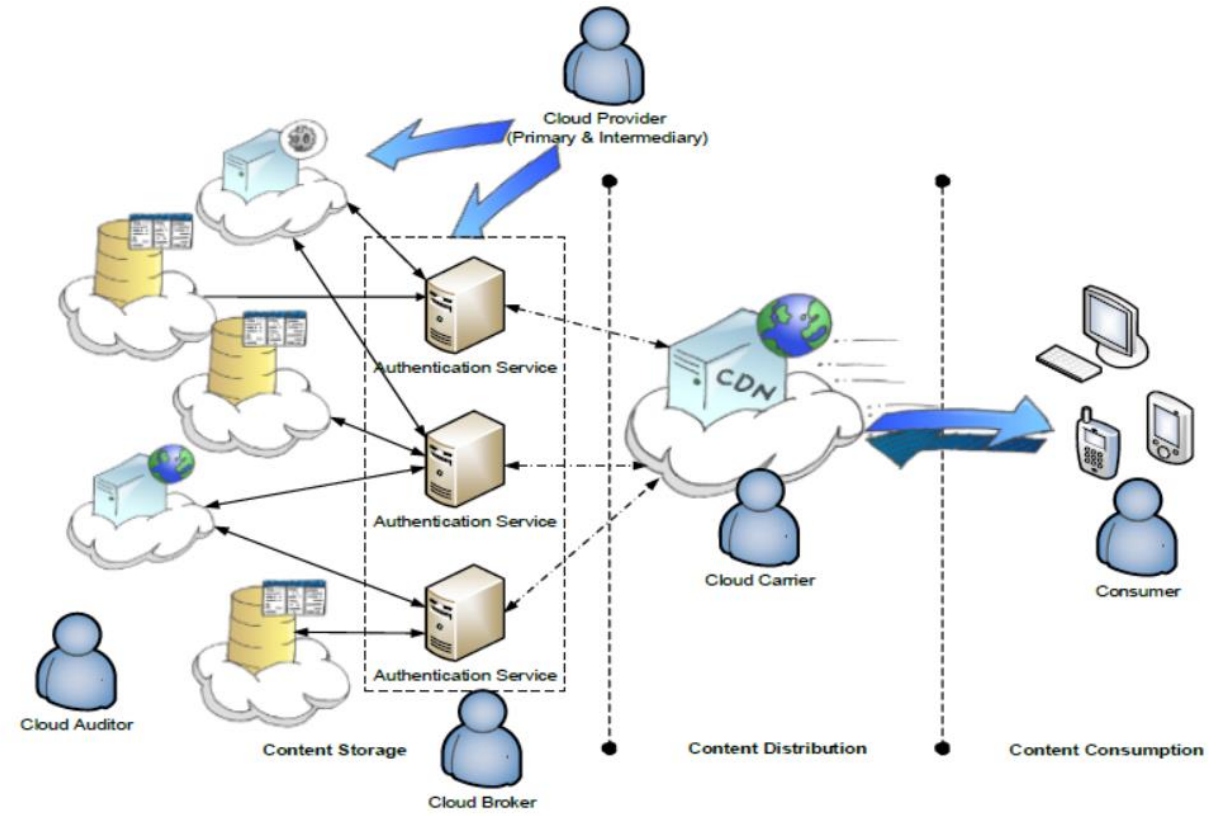


شکل 1. نمایی از شبکه‌ها و ابرها

ماهیت توزیع‌شده‌ی محیط ابری چالش‌هایی را در مدیریت هویت کاربران، احراز هویت و مجوزدهی ایجاد می‌کند. ارائه‌دهندگان خدمات ابری به اطلاعات ذخیره‌شده توسط کاربران برای احراز هویت دسترسی دارند که این موضوع مشکلات حریم خصوصی را به

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

دنبال دارد. کاربران برای اطمینان از اجرای صحیح قوانین توافق‌نامه سطح خدمات (SLA[19]) با مشکل مواجه هستند، زیرا شفافیت کافی برای پایش(مانیتورینگ) اطلاعات خود در ابر وجود ندارد. علاوه بر این، کاربران که اطلاعات را در قالب چندین سرویس ابری مشترک به اشتراک گذاشته‌اند، باید رمزهای عبور را در هر سرویس برای احراز هویت ذخیره کنند. در نتیجه، داده‌های احراز هویت در چندین ابر تکرار می‌شوند که این مساله ممکن است امنیت را به خطر بیندازد. ارائه‌دهندگان خدمات ابری، مدیریت و احراز هویت کاربران را به طور فزاینده‌ای پیچیده می‌دانند که بر اعتماد کاربران تأثیر می‌گذارد. برای حل این مشکلات، راه‌حل‌هایی مانند امنیت به‌عنوان یک سرویس (SEaaS[20]) و احراز هویت به‌عنوان یک سرویس (AaaS[21]) پدید آمده‌اند که اقدامات امنیتی مبتنی بر ابر را ارائه می‌دهند. در شکل (2)، تمامی ذی‌نفعان در فرآیند احراز هویت سرویس ابری نشان داده شده است [3].



شکل 2. ذی‌نفعان در احراز هویت سرویس ابری

خدمات ابری به راحتی با داشتن یک مرورگر و اتصال به اینترنت قابل دسترسی هستند و از سرویس‌های محبوب مانند جیمیل، فیسبوک و دراپ‌باکس در دستگاه‌های مختلف پشتیبانی می‌کنند. یکی از مزایای مهم رایانش ابری این است که زیرساخت و نگهداری

[19] Service Level Agreement
[20] Security-as-a-Service
[21] Authentication-as-a-Service

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

آن توسط ارائه‌دهندگان شخص ثالث مدیریت می‌شود. با این حال، رایانش ابری با تهدیدات امنیتی روبروست، از جمله حملات انکار سرویس توزیع‌شده (DDoS[۲۲]) که می‌توانند خدمات را با ارسال درخواست‌های کاذب به سرورها مختل کنند و آن‌ها را برای کاربران قانونی غیرقابل دسترسی کنند. علی‌رغم مزایا، اطمینان از اجرای تدابیر امنیتی قوی برای حفاظت از داده‌ها و حفظ قابلیت اطمینان خدمات بسیار حیاتی است[4]. از مهمترین چالش‌های امنیتی در بستر ابر می توان به نفوذ داده‌ها، انطباق با مقررات قانونی و پاسخ‌گویی پیچیده به برخی رویدادها اشاره کرد. نفوذ داده‌ها می‌تواند به دلیل تدابیر امنیتی ناکافی یا آسیب‌پذیری‌های زیرساخت ابری رخ دهد که به از دست دادن اطلاعات حساس و ضرر مالی منجر می‌شود. انطباق با قوانین حفاظت از داده‌ها، پیچیده و پرهزینه است. علاوه بر این، کاربران مشترک چندین سرویس ابری با داده‌های احراز هویت تکراری در ابرهای مختلف مواجه می‌شوند که خطرات امنیتی را افزایش می‌دهد. پرداختن به این چالش‌ها برای حفاظت از داده‌ها و حفظ اعتماد در محیط‌های رایانش ابری بسیار حیاتی است[3] . از این رو، در این مقاله تلاش می شود به بررسی چالش‌های امنیتی در حوزه رایانش ابری پرداخته شود. درک این چالش‌ها به توسعه تدابیر امنیتی قوی برای حفاظت از اطلاعات حساس، حفظ اعتماد کاربران و اطمینان از انطباق قانونی کمک می‌کند.

2. الزامات دسترسی به محیط ابری

محیط ابری یک فضای چندکاربر و ناهمگون است که در آن ارائه‌دهندگان خدمات ابری (CSPها[۲۳]) خدمات متنوعی را به صورت همزمان به بسیاری از مشتریان یا کاربران ارائه می‌دهند. این پارادایم مزایای قابل توجهی دارد، اما به این معنی است که الزامات کنترل دسترسی با آنچه معمولاً در شبکه‌های سازمانی عمومی استفاده می‌شود متفاوت است. عوامل کلیدی که باید در محیط ابری مورد توجه قرار گیرند شامل مکانیزم‌های کنترل دسترسی ویژه برای مدیریت نیازهای متنوع کاربران و اطمینان از ارائه خدمات امن و کارآمد می شوند. این الزامات در جدول 1 خلاصه شده اند [2]:

جدول1. الزامات دسترسی به محیط ابری

الزامات	توضیح
مستاجر[۲۴]	مشتریان مختلف یک برنامه مدیریت ارتباط با مشتری ارائه‌شده توسط Salesforce.com ، مانند خدمات MRF ، BIT Mesra و بیمارستان‌های آپولو، به عنوان مستاجر محسوب می‌شوند. هر سازمان می‌تواند تعداد زیادی کاربر داشته باشد.
کاربر	کارمندان هر مستاجر که از برنامه‌های مختلف ابری استفاده می‌کنند.
وظیفه	ساده‌ترین یا اساسی‌ترین واحد، یک فرآیند کسب و کار به حساب می‌اید.
اشیاء	منابع مختلفی که کاربران مایل به دسترسی به آن‌ها هستند.

[22] Distributed Denial of service
[23] Cloud Service Providers
[24] Tenant

نقش	به هر کاربر در یک سازمان، بر اساس فعالیت‌هایی که مجاز به انجام آن‌ها است، اختصاص داده می‌شود
مجوز	منظور، مجوز انجام یک عملیات خاص بر روی یک شیء است
جلسه	منظور، نقشه کاربر به نقش‌های مختلف اختصاص داده شده به آن است.
مکان	مجوزهای دسترسی آگاه به مکان را در خود جای داده است.
قوانین کسب و کار	عملکردهای استاندارد یک سازمان که کاربران آن دنبال می‌کنند. این قوانین می‌توانند از یک سازمان به سازمان دیگر متفاوت باشند. این قوانین شامل کمترین دسترسی، کمترین جداسازی وظیفه، و تفویض وظایف است.

3. چالش‌های امنیتی رایانش ابری

در دنیای به هم پیوسته امروزی، فناوری ابری به عنوان عاملی حیاتی برای نوآوری صنعت فناوری اطلاعات در نظر گرفته می‌شود. این فناوری، مدلی است که خدمات مختلف بر اساس تقاضا و دسترسی شبکه به پایگاه‌های داده مشترک منابع فیزیکی مانند محاسبات و ذخیره‌سازی را در اختیار مصرف‌کنندگان قرار می‌دهد. به این ترتیب، مشتریان دیگر نیازی به خرید سخت افزار گران قیمت برای دسترسی به این خدمات ندارند. حال آن‌که، می‌توانند از سخت‌افزار کالایی (مانند لپ‌تاپ) متصل به اینترنت استفاده کنند و ابزاری با هدف توسعه راه‌حل‌هایی برای مشکلات پیچیده در اختیارشان بگذارند. علاوه بر این، رایانش ابری، کاربران را قادر می‌سازد تا از راه دور به منابع از هر مکانی دسترسی داشته باشند و امکان همکاری مجازی را فراهم می‌کند. این بستر مجموعه‌ای از خدمات مانند نرم افزار به عنوان سرویس(SaaS) ، پلتفرم به عنوان سرویس (PaaS) و زیرساخت به عنوان سرویس (IaaS) را ارائه می‌دهد. علاوه بر این، خدمات ابری مقیاس‌پذیر، انعطاف‌پذیر و قابل اعتماد برای کاربران در صورت تقاضا هستند [5]. از آنجا که میزان جرایم سایبری در اینترنت در حال افزایش است، امنیت رایانش ابری نیز به دلایل زیادی تحت تاثیر قرار گرفته است. به منظور محافظت از تمام خدمات و مزایای ارائه شده توسط رایانش ابری و اینترنت، امنیت داده ها ضروری است. محرمانه بودن داده‌ها را می‌توان در سراسر شبکه با استفاده از فناوری رمزنگاری-که رمزگذاری و رمزگشایی است- به دست آورد. از مهمترین دلایل ارزیابی امنیت در بستر ابری می‌توان به موارد جدول (2) اشاره کرد [6]:

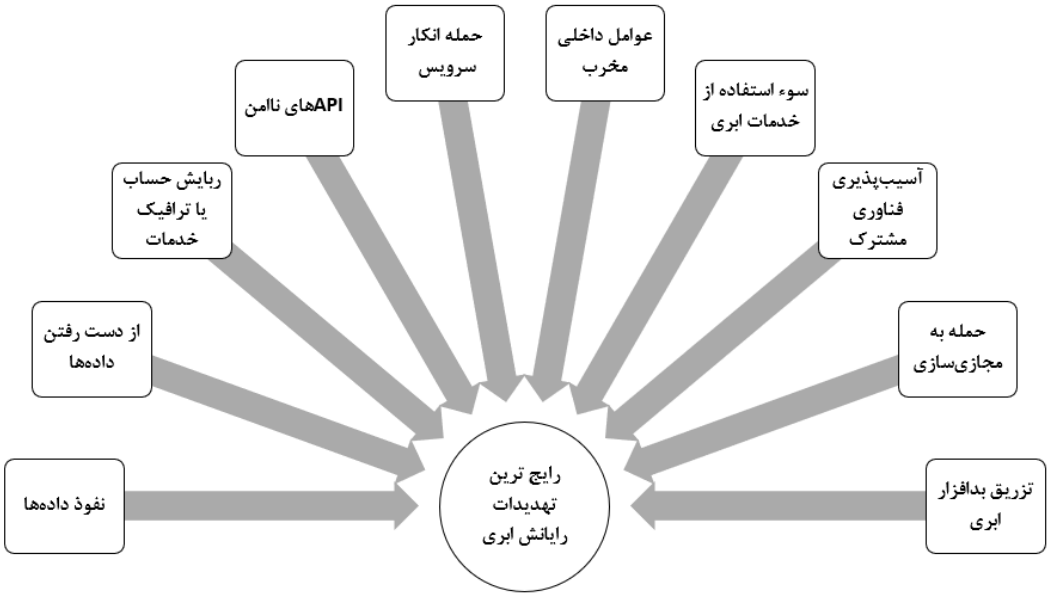
جدول2. اهمیت امنیت در بستر ابری

عامل	تعریف
احراز هویت	هویت فرستنده و گیرنده باید قبل از ارسال پیام تأیید شود.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

محرمانه بودن	فقط کاربران مجاز می‌توانند پیام را تفسیر کنند و هیچ کس دیگری نمی‌تواند از آن استفاده کند.
یکپارچگی	اطمینان از اینکه محتوای داده‌های ارسالی حاوی هیچ‌گونه تغییری نیست.
قابلیت اطمینان و در دسترس بودن سرویس	از آنجایی که مزاحمان بر دسترسی کاربران به خدمات تأثیر می‌گذارند، این فناوری باید کیفیت خدمات مورد انتظار را برای کاربران فراهم کند.
امنیت دسترسی به داده ها و محرمانگی	با ذخیره کردن پرونده‌های محرمانه امنیتی توسط سرویسی مثل Google docs بسیار می‌توان از امن ماندن و عدم دسترسی‌های غیر مجاز اطمینان حاصل کرد
مفقود شدن و از بین رفتن داده‌ها	با توجه به اینکه تعداد کمی از کاربران از داده‌های خود Back up می‌گیرند در صورتی که مشکلی برای cloud پیش بیاید کل داده‌ها از دست خواهد رفت.

اگرچه رایانش ابری یک پیشرفت در چندین سرویس وب موجود است، اما با تهدیدات امنیتی مشابه و متفاوت بسیاری روبه‌رو است که به سایر سرویس‌های وب مرتبط است. برخی از تهدیدات اصلی رایانش ابری در شکل 3 ارائه شده و در اینجا مورد بحث قرار گرفته‌اند[7] .



شکل 3. مهمترین تهدیدهای رایانش ابری

1.3 نفوذ داده‌ها

در رایانش ابری، داده‌ها از کاربران و سازمان‌های مختلف در محیط ابری ذخیره می‌شود و هرگونه نفوذ به این محیط یک حمله بالقوه به داده‌های همه کاربران ابر است. بنابراین، داده‌هایی که در محیط ابری ذخیره، پردازش یا به اشتراک گذاشته می‌شوند، هدف بسیار ارزنده‌ای هستند. این شامل نفوذهایی به دلیل غفلت یا خطای انسانی، حملات مخرب هدفمند، آسیب‌پذیری‌های مربوط به برنامه‌های ابری و سایر نواقص سیاست‌های امنیتی در تشخیص تهدیدات، کاهش آسیب‌پذیری‌ها، هوش امنیتی و بسیاری موارد دیگر است[7] .

2.3 از دست رفتن داده‌ها

یکی از خطرات بزرگ مرتبط با استفاده از ابر، از دست رفتن داده‌ها است. داده‌ها می‌توانند به روش‌های مختلفی به خطر بیفتند، از جمله حذف و تغییر محتوای اصلی. از دست رفتن داده‌ها به دلیل ویروس یا بدافزار که به سخت‌افزار، ذخیره‌سازی پشتیبان و بازیابی داده‌ها آسیب می‌رساند، در محیط ابری بسیار مشکل‌ساز است. این خطر همچنین می‌تواند به دلیل بلایای طبیعی، قطعی برق، خطای انسانی و خرابی هارد دیسک رخ دهد[7].

3.3 ربایش حساب یا ترافیک خدمات[۲۵]

هک کردن اطلاعات حساس مربوط به حساب‌ها و خدمات توسط مجرمان سایبری یا هکرها دارای همان خطراتی است که بسیاری از خدمات دیگر وب با آن مواجه هستند. اطلاعات خصوصی مانند سوابق مالی، تصاویر، شماره کارت‌های اعتباری و غیره می‌توانند توسط هکرها منتشر، استفاده یا به فروش برسند. همچنین این تهدید شامل حملات مرد میانی[۲۶]، دستکاری‌های مهندسی اجتماعی[۲۷]، استراق سمع فعالیت‌ها[۲۸] و نفوذ بدافزارها/جاسوس‌افزارها است[7].

4.3 رابط‌ها و واسط‌های برنامه‌نویسی کاربردی (API[۲۹]) ناامن

رابط‌ها وAPI های ناامن و ماشین‌های مجازی (VM[۳۰]) نیز یک تهدید بالقوه برای محیط رایانش ابری محسوب می‌شوند. API ها، VMها و سایر واسط‌های نرم‌افزاری توسط کاربر برای دسترسی به خدمات ابری استفاده می‌شوند. این نقاط تماس اجزای مرکزی هستند زیرا نظارت بر فعالیت‌ها، مدیریت و تأمین منابع را فراهم می‌کنند. بنابراین، نقایص امنیتی در این نقاط منجر به کنترل‌های دسترسی نادرست، احراز هویت غیرقانونی، نقض رمزنگاری و غیره می‌شود. این خطرات به دلیل ضعف در اعتبارنامه‌هایAPI ، نارسایی در مدیریت کلیدها، اشکالات در سیستم عامل، نرم‌افزارهای بدون پچ و خطاهای هایپروایزر[۳۱] به‌وجود می‌آیند[7].

[25] Account or service traffic hijacking
[26] Man-in-the-middle attack
[27] Social engineering manipulations
[28] Eavesdropping on activities
[29] Application programme interfaces
[30] Virtual machines
[31] Hypervisor

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

5.3 حمله انکار سرویس (DoS)

در یک حمله DoS، شبکه توسط اسپم‌های مهاجم غرق می‌شود که ترافیک بی‌فایده‌ای با هدف استفاده از منابع ایجاد می‌کند. این وضعیت می‌تواند منجر به عدم دسترسی منابع و خدمات برای کاربران معتبر شود. این حمله به دلیل معماری ضعیف امنیت شبکه، برنامه‌های آسیب‌پذیر، پروتکل‌های شبکه ناامن و غیره رخ می‌دهد[7].

6.3 عوامل داخلی مخرب

همچنین تهدیدات امنیتی می‌توانند داخلی باشند و این نوع تهدیدها کمی سخت‌تر قابل پیشگیری هستند. هر اطلاعات حساسی می‌تواند توسط هر داخلی/کارمندی که دسترسی مدیریتی دارد به یک دستگاه ذخیره‌سازی کپی شود. اطلاعات می‌توانند توسط هر کارمند سابق ناراضی، مدیر سیستم، شریک تجاری یا پیمانکار شخص ثالث به سرقت بروند. چنین ریسک‌هایی می‌توانند با انجام بررسی‌های پیش‌زمینه‌ای مناسب و محدود کردن دسترسی به داده‌های محرمانه کاهش یابند [7].

7.3 سوء استفاده از خدمات ابری

ابر به کاربران خود توهم قابلیت نامحدود محاسباتی، منابع شبکه و ظرفیت ذخیره‌سازی را ارائه می‌دهد. اسپمرها، نویسندگان کد مخرب، هکرها و سایر مجرمان سایبری می‌توانند از این قابلیت‌ها به طور ناعادلانه برای شکستن رمز عبور یا کلید رمزنگاری، ایجاد گلوگاه در شبکه، میزبانی داده‌های مخرب و بسیاری موارد دیگر استفاده کنند. این تهدید می‌تواند به دلیل نبود نظارت مناسب و توافق‌نامه سطح خدمات در محیط ابری بروز کند [7].

8.3 آسیب‌پذیری‌های فناوری مشترک

رایانش ابری یک فناوری مقیاس‌پذیر برای به اشتراک‌گذاری زیرساخت، فناوری و منابع است. این پلتفرم چندکاربری از هایپروایزر برای تسهیل دسترسی به سیستم‌عامل‌های میهمان استفاده می‌کند. با این حال، کمبودهای مجوزدهی و محدودیت‌های هایپروایزر می‌توانند به نفوذگران دسترسی و کنترل نامناسب را فراهم کنند. همچنین این تهدید می‌تواند به دلیل آسیب‌پذیری‌های مرتبط با ماشین‌های مجازی و سوییچینگ شخص ثالث بروز کند [7].

9.3 حمله مجازی‌سازی[32]

معماری مجازی‌سازی داخلی نیاز به سخت‌افزار مستقل دارد و بهترین مجازی‌سازی با استفاده از معماری لایه‌ای برنامه‌ریزی شده است. با وجود ناهنجاری‌ها و دشمنان در سیستم‌عامل‌های امروزی، می‌توان آسیب‌پذیری‌هایی را برای کنترل مخرب سیستم‌عامل میزبان راه‌اندازی کرد. به محض اینکه مهاجم توانایی کنترل سیستم‌عامل میزبان را به دست آورد، هایپروایزر به عنوان ناهنجاری

[32] Virtualisation attack

مشخص می‌شود. بنابراین، حقوق مدیریتی فرمان هایپروایزر به مهاجم اجازه می‌دهد تا هر اقدام مخربی را بر روی هر یک از ماشین‌های مجازی که توسط هایپروایزر میزبانی می‌شوند انجام دهد [7].

10.3 تزریق بدافزار ابری

حملات تزریق بدافزار ابری (CMIA[33]) برای دسترسی به داده‌های کاربر که در ابر ذخیره و پردازش می‌شوند صورت می گیرند. برخی از تهدیدات CMIA که به طور گسترده اعمال می‌شوند شامل حملات اسکریپت‌نویسی سایت و حملات تزریق زبان پرس و جو ساخت‌یافته (SQL[34]) هستند. چنین حملاتی ممکن است به دلیل ارائه‌دهندگان خدمات ابری آسیب‌پذیر مانند پلتفرم ابری OpenStack رخ دهند. با کمک یک کد مخرب، دشمنان می‌توانند به راحتی اطلاعات رمزگذاری شده را از بافر از طریق سوء استفاده از نقص طراحی در رایانه‌های اصلی امروزی ارسال کنند[7].

4. امنیت به عنوان یک سرویس (SaaS[35])

یکی از انواع خدمات ابری امنیت به عنوان سرویس (SaaS) است که راه‌حل‌های امنیتی ابری مانند تشخیص نفوذ، آنتی‌ویروس و مدیریت فایروال را از طریق اینترنت به کاربران ارائه می‌دهد. این رویکرد به سازمان‌ها اجازه می‌دهد نیازهای امنیتی خود را به ارائه‌دهندگان ابری متخصص واگذار کنند و از مقیاس‌پذیری، انعطاف‌پذیری و هزینه‌های کمتر رایانش ابری بهره‌مند شوند. SaaS می‌تواند با سیستم‌های داخلی موجود ادغام شود و نظارت مداوم و تشخیص تهدیدات در زمان واقعی را فراهم کند. این ادغام زیرساخت امنیتی کلی را تقویت می‌کند و به سازمان‌ها کمک می‌کند تا به‌طور کارآمدتری به الزامات انطباق دست یابند و با چشم‌انداز تهدیدات سایبری متغیر سازگار شوند[8]. یکی از انواع این نوع خدمات، احراز هویت به عنوان سرویس (AaaS) است. AaaS فرمی از احراز هویت کاربر است که از طریق آن خطر از دست دادن داده‌های محرمانه از ابر کاهش می‌یابد. هنگامی که یک کاربر خدمات ابری می‌خواهد به چندین سرویس موجود در ابر دسترسی پیدا کند، باید رمز عبور خود را در چندین ابر ذخیره کند که این موضوع مشکلات حریم خصوصی را برای مشتری و ارائه‌دهنده به همراه دارد [9].

تکنیک‌های احراز هویت مختلفی وجود دارد که برای ایمن‌سازی داده‌ها و احراز هویت کاربران قانونی اعمال می‌شوند. از مهمترین الزامات این نوع سرویس‌ها می توان به موارد زیر اشاره نمود:

- تکنیک امنیتی از نوعی باید اعمال شود که داده‌ها بدون گرفتن اجازه از شخص معتبر قابل تغییر نباشند.
- سیستمی امنیتی باید انتخاب شود که کاربران بتوانند به ایمنی و حفظ حریم خصوصی آن داده‌ها اعتماد کنند.
- داده‌ها باید همیشه در زمانی که به آن ها نیاز است در دسترس باشند.

[33] Cloud malware injection attacks
[34] Structured query language
[35] Security-as-a-Service

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

- معمولاً احراز هویت یا تنها برای یک طرف است یا دسترسی باز است، ارائه‌دهنده خدمات ابری بستر مناسبی برای احراز هویت چندگانه رابط کاربری ندارد و این منجر به دسترسی غیرمجاز یا ضعیف به فضای ابری می‌شود [9].

1.4 تکنیک‌های موجود برای احراز هویت کاربر

تکنیک‌های موجود برای احراز هویت کاربران شامل روش‌های سنتی مانند رمزهای عبور و پین‌ها است که به چیزی که کاربر می‌داند متکی هستند. تکنیک‌های امن‌تر مانند احراز هویت چندعاملی (MFA[36]) چندین شکل تاییدیه را ترکیب می‌کند، از جمله رمزهای عبور، کارت‌های هوشمند و بیومتریک. علاوه بر این، روش‌هایی مانند رمزهای یک‌بار مصرف (OTP[37]) و تحلیل ضربه‌های کلید امنیت را با تولید کدهای زمان‌دار و تحلیل الگوهای تایپ افزایش می‌دهند. در جدول 3، تکنیک‌های موجود برای احراز هویت کاربر ارائه شده است [9].

جدول 3. تکنیک‌های موجود برای احراز هویت کاربر

تکنیک	الگوریتم/روش/ابزار	نتایج
ماژول قابل اعتماد موبایل	توابع هش، طرح‌های امضا، رمزنگاری نامتقارن	جنبه امنیتی مورد استفاده در تلفن‌های همراه
احراز هویت چندعاملی (MFA)	الگوریتم‌های رمزنگاری فازی هش	اعتبارسنجی کاربران معتبر و شناسایی متقلبان در مجموعه داده‌ها
تحلیل ضربه‌های کلید	الگوریتم‌های خوشه‌بندیk-means	نشان‌دادن قابلیت احراز هویت کاربران نهایی
احراز هویت یک‌باره	پروتکلOTP	پروتکل در برابر حملات رمز یک‌بار مصرف امن است
احراز هویت بیومتریک	سیستم احراز هویت استاتیک	احراز هویت هویت کاربران از طریق دستگاه‌های اسکن ویژه
رمزهای عبور برای احراز هویت کاربران عمومی	پنجرهVisual Crypto-Pass ، عبور گرافیکی	قابلیت استفاده و امنیت

همچنین در ادامه توضیح مختصری در مورد هر یک از تکنیک‌ها آورده شده است.

1.1.4 ماژول قابل اعتماد تلفن همراه[38]

[36] Multi-factor Authentication
[37] One-Time Password
[38] Mobile trusted module

ماژول قابل اعتماد موبایل (MTM[39]) یک تکنیک پیشرفته احراز هویت کاربر است که برای بهبود امنیت دستگاه‌های موبایل طراحی شده است. این تکنیک از روش‌های رمزنگاری مانند توابع هش، طرح‌های امضا و رمزنگاری نامتقارن برای حفاظت از داده‌ها و تایید هویت کاربران استفاده می‌کند. MTM یک محیط امن برای عملیات حساس از جمله تولید کلید و ذخیره اعتبارنامه‌ها فراهم می‌کند و با جداسازی عملکردهای امنیتی حیاتی از آسیب‌پذیری‌های نرم‌افزاری ممکن، خطر دسترسی غیرمجاز و نقض داده‌ها را کاهش می‌دهد. این تکنیک از احراز هویت چندعاملی پشتیبانی می‌کند و عوامل اضافی مانند بیومتریک را برای افزایش امنیت اضافه می‌کند. MTM به صورت یکپارچه با سیستم‌عامل‌های تلفن همراه ادغام می‌شود و فرایندهای احراز هویت کارامد و کاربرپسند را تضمین می‌کند و همزمان خطر دسترسی غیرمجاز و نقض داده‌ها را کاهش می‌دهد [10].

2.1.4 احراز هویت چندعاملی (MFA[40])

احراز هویت چندعاملی (MFA) یک تکنیک امنیتی است که نیاز به چندین شکل شناسایی دارد و شامل موردی که کاربر می‌داند (مانند رمز عبور)، موردی که کاربر دارد (مانند گوشی هوشمند)، و موردی که کاربر است (مانند بیومتریک) می‌شود. این رویکرد لایه‌ای خطر دسترسی غیرمجاز را به طور قابل توجهی کاهش می‌دهد و دسترسی به سیستم‌ها را برای مهاجمان بسیار سخت‌تر می‌کند. با ارائه یک لایه امنیتی اضافی، MFA کمک می‌کند تا اطلاعات حساس و سیستم‌های بحرانی محافظت شوند و خطرات مرتبط با احراز هویت تنها با رمز عبور مانند فیشینگ و سرقت رمز عبور کاهش یابد. این تکنیک به طور گسترده در صنایع مختلف برای افزایش امنیت و اعتماد در تراکنش‌های دیجیتال پذیرفته شده است [11].

3.1.4 تحلیل ضربه‌های کلید[41]

تحلیل ضربه‌های کلید یک تکنیک احراز هویت کاربر است که از الگوهای تایپ منحصر به فرد افراد برای تایید هویت آن‌ها استفاده می‌کند. با اندازه‌گیری ریتم، سرعت و فشار اعمال‌شده هنگام تایپ، یک "امضای ضربه‌کلید" متمایز برای هر کاربر ایجاد می‌شود. این روش بیومتریک، با استفاده از الگوریتم‌هایی مانند خوشه‌بندی K-means، امنیت را افزایش می‌دهد و تقلید یا جعل الگوهای تایپ را برای مهاجمان دشوار می‌کند. تحلیل ضربه‌های کلید احراز هویت مداوم را ارائه می‌دهد و حتی پس از ورود اولیه نیز تاییدیه مداوم را فراهم می‌کند و در محیط‌های با امنیت بالا بسیار مفید است. این روش، یک فرایند احراز هویت بی‌درز و نامحسوس را ارائه می‌دهد که تجربه کاربری را بهبود می‌بخشد و نیاز به سخت‌افزار اضافی ندارد[12].

4.1.4 احراز هویت یک‌باره (OTA[42])

احراز هویت یک‌باره (OTA) یک مکانیزم امنیتی است که برای هر جلسه ورود یک کد منحصر به فرد و زمان‌دار تولید می‌کند و امنیت را با اطمینان از اینکه هر جلسه نیاز به یک کد متفاوت دارد افزایش می‌دهد. این روش که به‌طور معمول از طریق پروتکل‌های

[39] Mobile Trusted Module
[40] Multi-factor Authentication
[41] Key stroke Analysis
[42] One time Authentication

رمز یک‌بار مصرف (OTP[43]) پیاده‌سازی می‌شود، یک کد منحصر به فرد را برای هر تلاش ورود به دستگاه ثبت‌شده کاربر ارسال می‌کند که فقط برای یک مدت کوتاه معتبر است. OTA با دشوار کردن استفاده مجدد از اعتبارنامه‌های دزدیده شده برای مهاجمان، خطر دسترسی غیرمجاز را به طور قابل توجهی کاهش می‌دهد. این روش به ویژه در محافظت از حساب‌های حساس و تراکنش‌های مالی مؤثر است و امنیت قوی و راحتی کاربر را حفظ می‌کند[13].

5.1.4 احراز هویت بیومتریک

احراز هویت بیومتریک از ویژگی‌های فیزیکی یا رفتاری منحصر به فرد مانند اثر انگشت، تشخیص چهره، اسکن عنبیه یا تشخیص صدا برای تأیید هویت کاربر استفاده می‌کند. این روش بسیار ایمن بوده، تقلید یا جعل آن سخت است و محافظت قوی در برابر دسترسی غیرمجاز فراهم می‌کند. سیستم‌های بیومتریک تجربه کاربری را با حذف نیاز به رمزهای عبور پیچیده و دستگاه‌های احراز هویت اضافی ساده می‌کنند. احراز هویت بیومتریک به طور گسترده در بخش‌های مختلف پذیرفته شده و اطمینان می‌دهد که تنها افراد مجاز می‌توانند به اطلاعات حساس دسترسی پیدا کنند و امنیت و راحتی را افزایش می‌دهد[14].

6.1.4 رمزهای عبور برای احراز هویت کاربران عمومی

رمزهای عبور برای احراز هویت کاربران عمومی یک روش گسترده است که شامل ایجاد یک رشته مخفی از کاراکترها برای دسترسی کاربران به سیستم‌ها و خدمات می‌شود. رمزهای عبور به دلیل سادگی و سهولت استفاده، محبوب هستند اما اثربخشی آن‌ها به پیچیدگی رمز عبور و پیروی از روش‌های امنیتی خوب بستگی دارد. با این حال، رمزهای عبور دارای آسیب‌پذیری‌های ذاتی هستندکه از جمله آنها، حساسیت به حملات فیشینگ، حملات جست‌وجوی فراگیر و سرقت است. برای افزایش امنیت، اقدامات اضافی مانند احراز هویت چندعاملی (MFA) توصیه می‌شود که رمزهای عبور را با اشکال دیگر تأییدیه ترکیب می‌کند. این رویکرد به محافظت از اطلاعات حساس کمک می‌کند و اطمینان می‌دهد که رمزهای عبور همچنان گزینه‌ای مناسب هستند در حالی که به محدودیت‌های آن‌ها رسیدگی می‌شود[15].

5. کارهای پیشین

گانجام و همکاران [2] به بررسی امنیت APIهای ابری که یکی از تهدیدات عمده در رایانش ابری است، پرداختند. مدل پیشنهادی علاوه بر استفاده از احراز هویت مبتنی بر شناسه و رمز عبور برای کاربران قانونی، سیاست‌های کنترل دسترسی را نیز به کار می‌گیرد تا از دسترسی غیرمجاز به قابلیت‌های APIهای ابری جلوگیری کند. لیم و همکاران [3] به‌طور انتقادی، راهبردها و چارچوب‌های مختلف احراز هویت برای خدمات ابری را مورد بررسی قرار دادند، مزایا و معایب آن‌ها را بحث کردند و طبقه‌بندی احراز هویت خدمات ابری پیشرفته را ارائه دادند. این مقاله با بررسی مسائل باز، چالش‌های اصلی و جهت‌های آینده در این زمینه را بررسی نموده است. شاهیل و همکاران [4] ریسک‌های حملات انکار سرویس توزیع شده (DDOS) را که می‌توانند با ارسال هزاران درخواست مخرب به

[43] One-Time Password

شبکه سرور یا بهره‌برداری از آسیب‌پذیری‌های نرم‌افزاری، سایت تولیدی را غیرقابل استفاده کنند، مورد بررسی قرار داده اند. این مقاله دو راهبرد پیشگیرانه یعنی فیلتر کردن ورودی و خروجی شبکه (NEIF)- که به جلوگیری از حملات DDOS از ابر کمک می‌کند- و تکنیک هانی‌پات را- که با ضبط فعالیت‌های مهاجم، حملات و مهاجمان را شناسایی می‌کند-، پیشنهاد نموده است. در این مقاله تأکید شده است که اگرچه این راهبردها مؤثر هستند، اما به دلیل خطرات ذاتی، نیاز به بهبود بیشتر دارند. الجمعه و همکاران [7] تهدیدات مختلف رایانش ابری را بررسی و مکانیزم‌های دفاعی در برابر این تهدیدات را مشخص کرده‌اند. بر اساس این مقاله، تهدید بزرگی که شناسایی شده، مربوط به نقض داده‌ها است که به دلیل عدم درک مدیریت از خدمات رایانش ابری و مکانیزم‌های دفاعی آن‌ها رخ می‌دهد. همچنین، این مطالعه سوء استفاده از خدمات رایانش ابری را نیز مطرح می‌کند که می‌تواند علاوه بر داده‌های حساس سازمان، هویت و اطلاعات شخصی کاربران را نیز به خطر بیندازد. شارما و همکاران [9] نتیجه گرفتند که برای پیاده‌سازی احراز هویت چندمرحله‌ای در محیط‌های ابری می توان از تکنیک‌هایی مانند دسترسی بیومتریک و سیستم‌های احراز هویت یک‌بار مصرف یا موبایلی استفاده نمود. این مطالعه بیان کرد که جامعه پژوهش علمی به طور گسترده‌ای تکنیک‌های احراز هویت موجود در محیط رایانش ابری را مورد بررسی قرار نداده است. این مطالعه فناوری‌ها و تکنیک‌های مختلف را نشان داده و مقایسه می‌کند و نیاز به تحقیقات بیشتر در مورد روش‌های احراز هویت کاربران و راهبردهای پیشگیری در محیط رایانش ابری را مورد تاکید قرار می‌دهد. آدی و همکاران [16] یک مدل امنیت داده پویا چهار مرحله‌ای برای رایانش ابری ارائه دادند که از رمزنگاری و استگانوگرافی استفاده می‌کند. این مدل شامل رمزگذاری، استگانوگرافی، پشتیبان‌گیری و بازیابی داده‌ها و نیز به اشتراک‌گذاری داده‌ها است. ثابیت و همکاران [17] یک الگوریتم رمزگذاری سبک وزن را برای بهبود امنیت داده‌ها در رایانش ابری پیشنهاد دادند که با استفاده از روش‌های معماری Feistal و عملیات منطقی امنیت قوی‌تری را فراهم می‌کند. لی و همکاران [18] یک سیستم تولید هوشمند با استفاده از رایانش لبه‌ای و بلاکچین طراحی کردند که می‌تواند زمان پردازش را بهبود بخشد و انتقال داده‌ها و معاملات خدمات تولیدی را تسهیل کند.

در جدول 4 خلاصه این مطالعات آورده شده است:

جدول 4. خلاصه پژوهش های پیشین

مرجع	هدف	راهکار پیشنهادی در زمینه امنیت ابری	نتیجه
گانجام و همکاران[2]	بررسی امنیتAPI های ابری	احراز هویت مبتنی بر شناسه و رمز عبور و استفاده از سیاست‌های کنترل دسترسی	سیاست‌های کنترل دسترسی از دسترسی غیرمجاز به APIهای ابری جلوگیری می‌کند

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

لیم و همکاران[3]	بررسی راهبردها و چارچوب‌های احراز هویت برای خدمات ابری	طبقه‌بندی سیستم های احراز هویت بر اساس هدف و کاربرد	نیاز به بررسی مسائل باز، چالش‌ها و جهت‌های آینده در احراز هویت خدمات ابری
شاهیل و همکاران[4]	بررسی ریسک‌های حملات DDOS	فیلتر کردن ورودی و خروجی شبکه (NEIF) و تکنیک هانی‌پات	این راهبردها مؤثر هستند اما نیاز به بهبود بیشتر دارند.
الجمعه و همکاران[7]	بررسی تهدیدات رایانش ابری و مکانیزم‌های دفاعی	شناسایی نقض داده‌ها به دلیل عدم درک مدیریت و سوء استفاده از خدمات ابری	تهدیدات می‌توانند داده‌های حساس سازمان و هویت کاربران را به خطر بیندازند.
شارما و همکاران[9]	پیاده‌سازی احراز هویت چندمرحله‌ای در محیط‌های ابری	استفاده از دسترسی بیومتریک و سیستم‌های احراز هویت یک‌بار مصرف یا موبایلی	نیاز به تحقیقات بیشتر در مورد روش‌های احراز هویت کاربران و راهبردهای پیشگیری در محیط رایانش ابری تأکید می‌شود.
آدی و همکاران[16]	ارائه مدل امنیت داده پویا چهار مرحله‌ای	رمزنگاری و استگانوگرافی شامل رمزگذاری، پشتیبان‌گیری، بازیابی داده‌ها و به اشتراک‌گذاری داده‌ها	مدل ارائه‌شده امنیت، حریم خصوصی و یکپارچگی داده‌ها را در برابر مهاجمان تضمین می‌کند.
ثابیت و همکاران[17]	بهبود امنیت داده‌ها در رایانش ابری	الگوریتم رمزگذاری سبک وزن با استفاده از روش‌های معماری Feistal و عملیات منطقی	الگوریتم پیشنهادی امنیت قوی‌تری را فراهم می‌کند
لی و همکاران[18]	طراحی سیستم تولید هوشمند با رایانش لبه‌ای و بلاکچین	استفاده از رایانش لبه‌ای برای کاهش زمان پردازش و بلاکچین برای تسهیل انتقال داده‌ها و معاملات خدمات تولیدی	سیستم پیشنهاد شده زمان پردازش را بهبود می‌بخشد و انتقال داده‌ها و معاملات خدمات تولیدی را تسهیل می‌کند.

6. نتیجه گیری

با پیشرفت فناوری اطلاعات، نیاز به انجام کارهای محاسباتی در هر زمان و مکان افزایش یافته و همچنین نیاز به انجام محاسبات سنگین بدون نیاز به سخت‌افزارها و نرم‌افزارهای گران‌قیمت به وجود آمده است. رایانش ابری به عنوان آخرین پاسخ فناوری به این نیازها، به میلیون‌ها کاربر امکان می‌دهد داده‌های خود را در فضای عظیم ابری ذخیره کنند. با این حال، این راحتی همراه با خطراتی نظیر دسترسی غیرمجاز و از دست دادن داده‌ها است که امنیت را به چالشی بسیار مهم تبدیل می‌کند. رایانش ابری می‌تواند با استفاده از ماشین‌های مجازی شبکه‌ای به طور پویا مراکز داده جدید ایجاد کند و توسعه نرم‌افزارها به عنوان یک سرویس قابل دسترس برای میلیون‌ها نفر را تسهیل کند. تهدیدات امنیتی در رایانش ابری به دو دسته داخلی و خارجی تقسیم می‌شوند: تهدیدات خارجی شامل آسیب‌پذیری‌های مراکز داده بزرگ و تهدیدات داخلی شامل نیاز به حفاظت کاربران از یکدیگر است. رایانش ابری به کسب‌وکارها امکان کاهش هزینه‌ها از طریق برون‌سپاری خدمات مورد نیازشان را می‌دهد، اما چالش‌های جدیدی در حفاظت از داده‌ها، قابلیت اطمینان، یکپارچگی و محرمانه بودن را معرفی می‌کند. در نتیجه، امنیت ابری به یک تمایز کلیدی و مزیت رقابتی بین ارائه‌دهندگان ابر تبدیل شده است. با توجه به افزایش جرایم سایبری، امنیت رایانش ابری به دلایل مختلف به‌طور قابل‌توجهی تحت تأثیر قرار گرفته است. امنیت داده‌ها برای محافظت از تمامی خدمات و مزایای ارائه‌شده توسط رایانش ابری و اینترنت بسیار حائز اهمیت است. محرمانه بودن داده‌ها را می‌توان با استفاده از فناوری‌های رمزنگاری برای رمزگذاری و رمزگشایی در سراسر شبکه حفظ کرد. دلایل اصلی برای ارزیابی امنیت در بستر ابری شامل احراز هویت، اطمینان از اینکه فقط کاربران مجاز قادر به تفسیر پیام‌ها هستند؛ محرمانه بودن، حفظ یکپارچگی داده‌ها در برابر تغییرات غیرمجاز؛ قابلیت اطمینان و در دسترس بودن سرویس، تضمین کیفیت خدمات مورد انتظار با وجود تداخل‌ها؛ امنیت دسترسی به داده‌ها و محرمانگی، اطمینان از امن ماندن و عدم دسترسی غیرمجاز به فایل‌های محرمانه ذخیره‌شده در خدماتی مانند Google Docs؛ و پیشگیری از نابودی یا از دست دادن داده‌ها، با توجه به اینکه تعداد کمی از کاربران، از داده‌های خود نسخه پشتیبان تهیه می‌کنند و در صورت بروز مشکل برای ابر، کل داده‌ها از دست خواهند رفت. در این مقاله به بررسی چالش های امنیتی در بستر ابری پرداخته شد. نتایج نشان داد؛ احراز هویت کاربران یک گام کلیدی در افزایش امنیت ابر است. همچنین تکنیک‌های موجود برای احراز هویت کاربران شامل روش‌های سنتی مانند رمزهای عبور و پین‌ها است که به چیزی که کاربر می‌داند متکی هستند. تکنیک‌های امن‌تر مانند احراز هویت چندعاملی چندین شکل تاییدیه، از جمله رمزهای عبور، کارت‌های هوشمند و بیومتریک را ترکیب می‌کند. علاوه بر این، روش‌هایی مانند رمزهای یک‌بار مصرف و تحلیل ضربه‌های کلید امنیت را با تولید کدهای زمان‌دار و تحلیل الگوهای تایپ افزایش می‌دهند. در این میان، تکنیک‌هایی مانند ماژول قابل اعتماد تلفن همراه با توابع هش و رمزنگاری نامتقارن، احراز هویت چندعاملی با الگوریتم‌های رمزنگاری فازی هش و تحلیل ضربه‌های کلید با الگوریتم‌های خوشه‌بندی k-means نیز استفاده می‌شوند. همچنین، احراز هویت یک‌باره با پروتکل OTP و احراز هویت بیومتریک با سیستم احراز هویت استاتیک ارائه شده‌اند.

منابع

[1] Shafiq DA, Jhanjhi NZ, Abdullah A. Load balancing techniques in cloud computing environment: A review. Journal of King Saud University-Computer and Information Sciences. 2022 Jul 1;34(7):3910-33.

[2] Gunjan K, Tiwari RK, Sahoo G. Towards securing APIs in cloud computing. arXiv preprint arXiv:1307.6649. 2013 Jul 25.

[3] Lim SY, Kiah MM, Ang TF. Security issues and future challenges of cloud service authentication. Acta Polytechnica Hungarica. 2017 May;14(2):69-89.

[4] Shahil UM, Deekshitha M, Anam M N, Basthikodi M. Ddos attacks in cloud computing and its preventions. JETIR-International Journal of Emerging Technologies and Innovative Research (www. jetir. org), ISSN. 2019 May 5:2349-5162.

[5] Rahman A, Islam MJ, Band SS, Muhammad G, Hasan K, Tiwari P. Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT. Digital Communications and Networks. 2023 Apr 1;9(2):411-21.

[6] Thabit F, Can O, Alhomdy S, Al-Gaphari GH, Jagtap S. A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing. International Journal of intelligent networks. 2022 Jan 1;3:16-30.

[7] Aljumah A, Ahanger TA. Cyber security threats, challenges and defence mechanisms in cloud computing. IET communications. 2020 Apr;14(7):1185-91.

[8] Senk C. Adoption of security as a service. Journal of Internet Services and Applications. 2013 Dec;4:1-6.

[9] Sharma A, Keshwani B, Dadheech P. Authentication issues and techniques in cloud computing security: A review. InProceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India 2019 Feb 26.

[10] Gan Q, Wang X, Fang X. Efficient and secure auditing scheme for outsourced big data with dynamicity in cloud. Science China Information Sciences. 2018 Dec;61(12):122104.

[11] Liu W, Uluagac AS, Beyah R. MACA: A privacy-preserving multi-factor cloud authentication system utilizing big data. In2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) 2014 Apr 27 (pp. 518-523). IEEE.

[12] Bhattasali T, Saeed K. Two factor remote authentication in healthcare. In2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI) 2014 Sep 24 (pp. 380-386). IEEE.

[13] Castiglione A, De Santis A, Castiglione A, Palmieri F. An efficient and transparent one-time authentication protocol with non-interactive key scheduling and update. In2014 IEEE 28th International Conference on Advanced Information Networking and Applications 2014 May 13 (pp. 351-358). IEEE.

[14] Mahalakshmi B, Suseendran G. An analysis of cloud computing issues on data integrity, privacy and its current solutions. InData Management, Analytics and Innovation: Proceedings of ICDMAI 2018, Volume 2 2019 (pp. 467-482). Springer Singapore.

[15] Nandgaonkar SV, Raut AB. A comprehensive study on cloud computing. International Journal of Computer Science and Mobile Computing. 2014 Apr;3(4):733-8.

[16] Adee R, Mouratidis H. A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. Sensors. 2022 Feb 1;22(3):1109.

[17] Thabit F, Alhomdy S, Al-Ahdal AH, Jagtap S. A new lightweight cryptographic algorithm for enhancing data security in cloud computing. Global Transitions Proceedings. 2021 Jun 1;2(1):91-9.

[18] Lee CK, Huo YZ, Zhang SZ, Ng KK. Design of a smart manufacturing system with the application of multi-access edge computing and blockchain technology. IEEE access. 2020 Feb 7;8:28659-67.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

مسیریابی کارآمد و افزایش طول عمر، در عملکرد شبکه حسگر بی سیم با استفاده از الگوریتم کلنی زنبورعسل مصنوعی و الگوریتم خواب و بیدار

سیده مهساحسینی کیا[1] ، محمدمهدی شیرمحمدی[2]

[1] گروه کامپیوتر، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران mahsahosseinikia@gmail.com
[2] گروه کامپیوتر، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران Mmshirmohammadi@gmail.com

چکیده :

برای افزایش طول عمر شبکه‌های حسگر بی‌سیم (WSN)، نیاز به پروتکل‌های مسیریابی کارآمد وجود دارد تا کانال‌های ارتباطی بین منبع و مقصد ایجاد کنند. از آنجا که گره‌ها به‌طور تصادفی در محیط‌های نسبتاً ناامن پراکنده می‌شوند، این پروتکل‌های مسیریابی در معرض انواع مختلفی از حملات قرار دارند. برای شبکه‌های حسگر بی‌سیم، پروتکل‌های مسیریابی مبتنی بر اعتماد طراحی شده‌اند که به جای سریع‌ترین مسیر، از مسیرهای قابل‌اعتماد استفاده می‌کنند تا از این حملات جلوگیری کنند. برای کاهش مصرف انرژی گره‌ها از تکنیک خوشه‌بندی مبتنی بر کلونی زنبورعسل artificial bee colony-based (ABC) که مصرف انرژی را در شبکه حسگر به‌صورت مساوی تقسیم می‌کند و الگوریتم خواب و بیدار Sleep-Wake Algorithm (SWA) که تنها بخشی از گره ها را در هر لحظه فعال نگه می دارد استفاده شده است. الگوریتم پیشنهادی ABC- SWA بر اساس تحلیل شبیه‌سازی با دیگر پروتکل‌های مقایسه شده است و نشان می‌دهد که عملکرد آن در زمینه کاهش مصرف انرژی، تعداد گره‌های فعال و طول عمر شبکه بهتر است.

کلمات کلیدی : WSN, ABC, SWA, TEER, Clustering, Efficient Routing, Lifetime

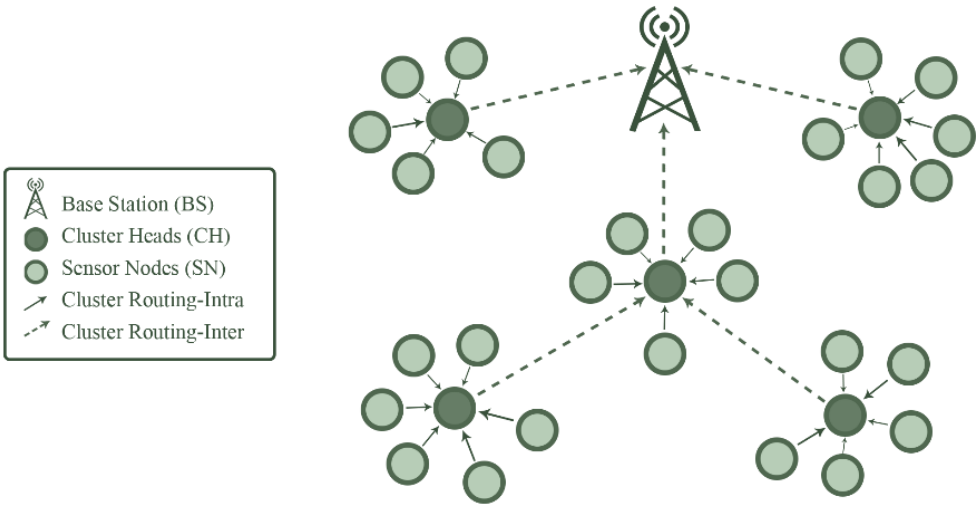
1. مقدمه :

دو توپولوژی مختلف برای ارتباطات بی‌سیم وجود دارد. اولین توپولوژی مرکزی‌شده نام دارد و به آن ساختاریافته نیز می‌گویند، در حالی که دومین توپولوژی، ناساختاریافته و غیرمتمرکز است. در شبکه‌های ارتباطات بی‌سیم، ایده اصلی این است که صدا و داده‌ها به‌طور مشترک از طریق همان زیرساخت شبکه سلولی انتقال یابند. چالش اصلی در این توپولوژی‌ها، جابه‌جایی بین ایستگاه‌های پایه بدون افت یا تأخیر در اطلاعات است. در شبکه‌های بی‌سیم خودمختار (WANET)، که در آن چندین گره متحرک برای ارتباط از یک کانال بی‌سیم مشترک استفاده می‌کنند، از توپولوژی توزیع‌شده استفاده می‌شود. در WANET، گره‌ها می‌توانند به‌طور مستقیم ارتباط برقرار کنند، مشروط بر اینکه در محدوده ارتباطی یکدیگر قرار داشته باشند. این گره‌ها می‌توانند داده‌ها را از طریق مسیریابی چندمرحله‌ای به گره‌های مقصد دورتر ارسال کنند.

اینترنت اشیا (IoT) با ترکیب حسگرها و دستگاه‌های مختلف به بهبود عملکرد WSN کمک و اتصال قوی‌تری را فراهم می‌کند. به این ترتیب، مفهوم آینده‌ای با " هوشمندی محیطی "، که در آن دستگاه‌های متعددی اطلاعات را از محیط جمع‌آوری، تحلیل و با کاربران تعامل می‌کنند، به تحقق پیوسته است.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

در سال‌های اخیر، نوع جدیدی از شبکه‌ها به نام شبکه‌های حسگر بی‌سیم (WSN) معرفی شده‌اند که هر گره در این شبکه‌ها می‌تواند محیط را حس کند و یک یا چند پارامتر فیزیکی را تغییر دهد. از آنجا که یک گره به‌تنهایی نمی‌تواند وظیفه حسگری را به‌طور کامل انجام دهد، گره‌های حسگر از طریق ارتباطات بی‌سیم با یکدیگر همکاری می‌کنند. شایان ذکر است که کاربردهای واقعی متنوعی مانند نظامی، بهداشت، نظارت و امنیت می‌توانند از شبکه‌های حسگر بی‌سیم بهره‌مند شوند. به‌دلیل کاربرد گسترده این شبکه‌ها در بخش‌های نظامی و غیرنظامی مانند پایش آب‌وهوا، نظارت بر حیات‌وحش، و مدیریت بلایا، این شبکه‌ها در سال‌های اخیر توجه بسیاری را به خود جلب کرده‌اند. در این کاربردها، تعداد زیادی گره حسگر به‌صورت تصادفی در محیط‌های سخت و بدون کنترل پخش می‌شوند و به‌دلیل فقدان یک ناظر مرکزی، در معرض انواع مختلفی از حملات احتمالی قرار دارند. از جمله چالش‌های اصلی که شبکه‌های حسگر بی‌سیم با آن مواجه هستند، امنیت است که تأثیر زیادی بر عملکرد شبکه دارد. شکل1 نمونه ای از شبکه حسگر بی سیم-که شامل یک ایستگاه پایه (BS) و چندین نود (SN) بوده و بصورت تصادفی در محیط پراکنده شده اند- و نودهایی را که بصورت رندوم بعنوان سرخوشه (CH) انتخاب می شوند، به نمایش می گذارد.



شکل 1. یک نمونه ساده شبکه حسگر بی سیم

مطالعات انجام‌شده در زمینه پروتکل‌های مسیریابی مبتنی بر اعتماد و تکنیک‌های خوشه‌بندی مبتنی بر کلونی زنبور عسل، مزایایی در بهینه‌سازی شبکه‌های حسگر بی‌سیم از نظر امنیت و مصرف انرژی دارند. با این حال، مطالعاتی که به‌طور جهانی بهینه‌سازی طول عمر شبکه‌های حسگر بی‌سیم را مورد بررسی قرار داده‌اند، کمبودهایی دارند. ضمن اینکه در بخش کارهای انجام شده در گذشته، به تعدادی از الگوریتم های بهبود وضعیت شبکه اشاره دارد. از این رو، در بخش روش پیشنهادی، ایده الگوریتم خواب و بیدار را بر روی الگوریتم خوشه‌بندی مبتنی بر کلونی زنبورعسل پیاده سازی کرده‌ایم. در بخش تجزیه و تحلیل، جزئیات مربوط به شبیه سازی و مقایسه روش پیشنهادی خواب و بیدار بر روی خوشه‌بندی مبتنی بر کلونی زنبور عسل را با روش های پیشین انجام داده و در بخش آخر به نتیجه گیری پرداخته ایم.

2. کارهای انجام شده :

در گذشته، روش‌های متنوعی برای بهینه‌سازی مصرف انرژی در WSNها بررسی شده است؛ از جمله: الگوریتم مورچگان (ACO) برای مسیریابی چندگانه، الگوریتم ازدحام ذرات (PSO) برای خوشه‌بندی حسگرها، کلونی زنبور عسل (ABC) که مصرف انرژی را کاهش می دهد. الگوریتم‌های

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

SWA برای مدیریت مصرف انرژی و بسیاری از الگوریتم های دیگری که سبب افزایش طول عمر شبکه هستند. این مقاله با ادغام دو الگوریتم ABC و SWA کارایی شبکه را ارتقا داده و آن ها را برای طراحی پروتکل‌های مسیریابی کارامد در WSN استفاده می‌کند.

با بررسی هایی که پژوهشگران با اعمال الگوریتم های بهینه مانند الگوریتم ABC بر روی الگوریتم های TEER انجام داده اند، نشان داده شده است که ادغام الگوریتم ها می تواند در افزایش طول عمر شبکه های حسگر بی سیم (WSN) بسیار موثر واقع شوند. از این رو جدول1 به مقایسه دو الگوریتم TEER و ABC-TEER پرداخته است.

جدول1. مقایسه دو الگوریتم TEER و ABC-TEER

ویژگی	TEER	ABC-TEER
1.نوع بهینه‌سازی	روش‌های پایه و غیرهوشمند برای مسیریابی و خوشه‌بندی.	از الگوریتم مصنوعی زنبور عسل (ABC) برای بهینه‌سازی مسیرها و خوشه‌بندی استفاده می‌کند.
2.انتخاب سرخوشه	معیارهای ساده مانند انرژی باقی‌مانده و موقعیت.	انتخاب بهینه با استفاده از معیارهای چندگانه (انرژی، اعتماد، موقعیت) با کمک الگوریتم ABC .
3.مصرف انرژی	مصرف نامتعادل انرژی و احتمال تخلیه سریع انرژی برخی گره‌ها.	مصرف بهینه و توزیع متوازن انرژی در سراسر شبکه.
4.طول عمر شبکه	طول عمر کوتاه‌تر به دلیل بهینه‌سازی ضعیف انرژی.	طول عمر شبکه بیشتر به دلیل مدیریت بهتر انرژی و انتخاب بهینه CH .
5.تعادل بار ترافیکی	احتمال عدم تعادل در بار ترافیکی و فشار بر گره‌های خاص.	تعادل مناسب بار ترافیکی به دلیل انتخاب بهینه مسیرها و خوشه‌ها.
6.توان عملیاتی	نرخ انتقال داده استاندارد و متوسط.	بهبود 9.5% در نرخ انتقال داده (Throughput) نسبت به TEER .
7.پیچیدگی محاسباتی	پیچیدگی پایین اما کارایی کمتر.	پیچیدگی بالاتر به دلیل استفاده ازABC ، اما کارایی بهتر.
8.مقاومت در برابر خرابی	آسیب‌پذیر در برابر تخلیه انرژی و خرابی گره‌ها.	مقاومت بیشتر به دلیل توزیع متوازن انرژی و انتخاب مسیرهای پایدار.

3. روش پیشنهادی :

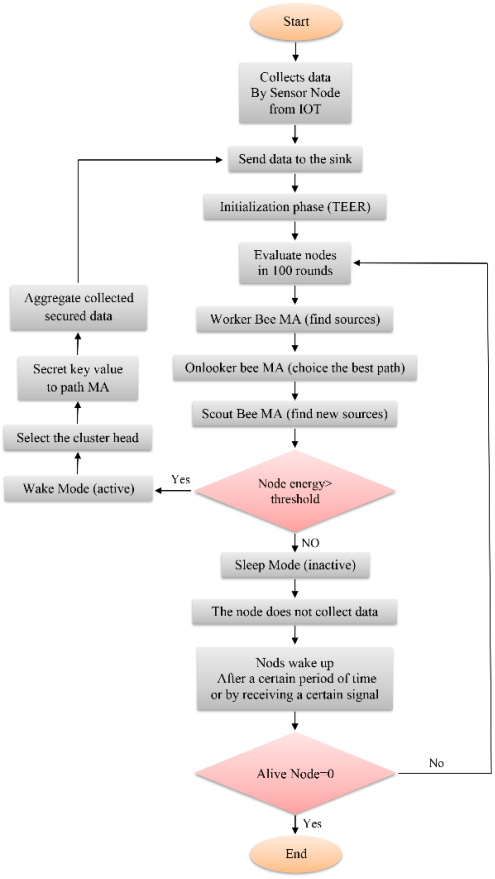
خوشه‌بندی یکی از تکنیک‌های مهم در شبکه‌های حسگر بی‌سیم است که امکان صرفه‌جویی در توان مصرفی گره‌های حسگر و مقیاس‌پذیری شبکه را فراهم می‌کند. روش خوشه‌بندی، حسگرها را بر اساس موقعیت و سطح انرژی گره‌ها به چندین خوشه تقسیم می‌کند. هر خوشه از این روش برای انتقال داده‌های جمع‌آوری شده از حسگرهای خود به یک نقطه مشترک به نام سرخوشه استفاده می‌کند که از میان گره‌های خوشه با توجه به معیارهای تعریف‌شده انتخاب می‌شود. در نتیجه، سرخوشه معمولاً گره‌ای است که دارای امنیت بالاتر و در عین حال مصرف انرژی کمتر است. این سرخوشه وظیفه دارد که اطلاعات را در درون خوشه ارسال کرده و همزمان آن را به سمت مقصد (Sink) هدایت کند. در هر تکرار از الگوریتم‌های خوشه‌بندی، یک سرخوشه جدید انتخاب می‌شود که این انتخاب ممکن است به‌صورت تصادفی یا بر اساس معیارهایی مانند انرژی باقی‌مانده، مقدار آستانه، پوشش و غیره باشد.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

برای افزایش طول عمر شبکه، یک پروتکل مسیریابی قابل‌اعتماد و کم‌مصرف با نام ABC- SWA طراحی شده است. این پروتکل در چرخه‌هایی اجرا می‌شود که هر چرخه شامل مرحله انتخاب سرخوشه و مرحله انتقال داده است. گره مقصد (sink) به‌عنوان مرجع ارزیابی اعتماد برای همه گره‌های دیگر عمل می‌کند و یک نسخه از مقدار اعتماد هر گره را نیز در خود نگهداری می‌کند. در مرحله اول، گره‌های حسگر یک رهبر برای خوشه انتخاب می‌کنند. در مرحله دوم، سرخوشه‌ها برای هر گره در خوشه یک بازه زمانی برای انتقال داده‌ها بر اساس زمان‌بندی SWA تعیین می‌کنند. حسگرهای خوشه، اطلاعات خود را به سرخوشه ارسال می‌کنند و سپس سرخوشه اطلاعات را مستقیماً به گره مقصد می‌رساند. برای توزیع متوازن بار ترافیک و مصرف انرژی، فرآیند انتخاب سرخوشه‌ها در هر دور چندین بار تکرار می‌شود.

الگوریتم ABC از مقداردهی اولیه با جمعیتی از زنبورهای کارگر به‌صورت تصادفی آغاز می‌شود. در مرحله بعد زنبورهای کارگر به جست‌وجوی منابع (جست‌وجوی محلی) می‌پردازند و اطلاعات کیفیت منابع را جمع‌آوری می‌کنند. سپس در مرحله بهبود، زنبورهای ناظر اطلاعات زنبورهای کارگر را بررسی و بهترین منابع را انتخاب می‌کنند. در مرحله کاوش، اگر زنبوری نتواند بهبود یابد، به‌عنوان زنبور کاوشگر عمل کرده و به جست‌وجوی منابع جدید می‌پردازد. و در نهایت، در مرحله تکرار، این مراحل بارها تکرار می‌شود تا به یک راه‌حل بهینه نزدیک‌تر شوند. الگوریتم‌های **خواب و بیدار (**SWA**)** در شبکه‌های حسگر بی‌سیم (WSN) یکی از مهم‌ترین مکانیزم‌ها برای مدیریت مصرف انرژی و افزایش طول عمر شبکه محسوب می شوند. در شبکه‌های حسگر بی‌سیم، حسگرها معمولاً باتری‌محور هستند و تعویض یا شارژ باتری آنها دشوار است، بنابراین کاهش مصرف انرژی اهمیت حیاتی دارد. این الگوریتم‌ها با زمان‌بندی دقیق وضعیت حسگرها بین دو حالت کار می‌کنند: 1-**حالت خواب(Sleep Mode)** ؛ که حسگر در این حالت مصرف انرژی بسیار کمی دارد و تنها بخشی از سخت‌افزار آن فعال است (مانند تایمر). حسگر در این حالت داده‌ای ارسال یا دریافت نمی‌کند. 2-**حالت بیدار(Active Mode)** ؛ که حسگر در این حالت فعال است، داده‌ها را حس می‌کند، پردازش می‌کند و با دیگر حسگرها یا ایستگاه اصلی ارتباط برقرار می‌کند.ترکیب **الگوریتم زنبور عسل مصنوعی (ABC)** و **الگوریتم خواب و بیدار (SWA)** می‌تواند یک رویکرد ترکیبی و بهینه برای حل مسائل **مدیریت انرژی** و **بهینه‌سازی مسیر** در **شبکه‌های حسگر بی‌سیم (WSN)**ارائه دهد. این ترکیب با هدف افزایش طول عمر شبکه و کاهش مصرف انرژی انجام می‌شود. الگوریتم ABC از رفتار طبیعی زنبورها الهام گرفته شده است و برای حل مسائل بهینه‌سازی به کار می‌رود. در این الگوریتم، **زنبورهای کارگر**، **ناظر** و **پیشاهنگ** به دنبال منابع غذایی (راه‌حل‌های بهینه) می‌گردند. در زمینه WSN ، ABC برای انتخاب بهینه **سرخوشه‌ها** و مسیرهای کم‌مصرف برای انتقال داده استفاده می‌شود. SWA چرخه های **خواب** و **بیدار** را برای گره‌های شبکه مدیریت می‌کند. در زمان خواب، گره‌ها خاموش می‌شوند تا انرژی ذخیره کنند و در زمان بیدار، وظایف خود مانند انتقال داده را انجام می‌دهند. این فرایند، فشار روی گره‌ها را کاهش داده و از مصرف غیرضروری انرژی جلوگیری می‌کند. در شکل 2 ، مراحل این چرخه را مشاهده می کنید.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055



شکل 2. الگوریتم ABC- SWA

در رویکرد ترکیبی، برای انتخاب سرخوشه‌ها و مسیریابی بهینه از ABC استفاده می‌شود، در حالی که SWA برای مدیریت چرخه خواب و بیدار گره‌ها به کار می‌رود. این ترکیب به این شیوه عمل می‌کند: فاز1 انتخاب سرخوشه، ابتدا گره‌ها توسط الگوریتم ABC بر اساس انرژی باقی‌مانده، فاصله و اعتماد بهینه‌ترین سرخوشه‌ها را انتخاب می‌کنند. فاز2 مدیریت خواب و بیدار. گره‌های غیرسرخوشه که وظایف حیاتی ندارند، توسط SWA وارد حالت خواب می‌شوند تا انرژی خود را ذخیره کنند.گره‌های سرخوشه و گره‌های مهم در حالت بیدار باقی می‌مانند تا فرایند انتقال داده‌ها به درستی انجام شود. فاز3 مسیریابی بهینه داده. داده‌ها از طریق مسیرهای انتخاب‌شده توسط ABC از گره‌ها به سرخوشه‌ها و سپس به ایستگاه پایه (Sink) منتقل می‌شوند. در این فرایند، انرژی مصرف‌شده برای انتقال داده به حداقل می‌رسد. فاز4 بازیابی انرژی و تغییر چرخه. چرخه خواب و بیدار به طور دوره‌ای و پویا تنظیم می‌شود تا گره‌ها به تناوب بین خواب و بیدار تغییر وضعیت دهند. این فرایند فشار کاری را بین گره‌ها به صورت متعادل توزیع می‌کند. در جدول2 ویژگی های **الگوریتم ABC** و **الگوریتم خواب و بیدار SWA** ارائه شده است.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

جدول2. ویژگی های **الگوریتم ABC** و **الگوریتم خواب و بیدار SWA**

ویژگی	الگوریتم زنبور عسل مصنوعی ABC	الگوریتم خواب و بیدار SWA
هدف اصلی	بهینه‌سازی مسیرها و انتخاب سرخوشه‌ها برای کاهش مصرف انرژی	مدیریت چرخه خواب و بیدار گره‌ها برای کاهش مصرف انرژی.
مکانیزم عملکرد	بر اساس هوش ازدحامی و رفتار زنبورهای عسل (شامل کارگر، دیده‌بان و جست‌جوگر)	بر اساس خاموش و روشن کردن گره‌ها به صورت برنامه‌ریزی‌شده یا تصادفی
مصرف انرژی	کاهش مصرف انرژی از طریق انتخاب بهینه مسیر و سرخوشه‌ها	کاهش مصرف انرژی با خاموش نگه داشتن گره‌های غیرضروری در زمان‌های مشخص
تعادل بار ترافیکی	توزیع مناسب بار ترافیکی بین گره‌ها و مسیرها	کاهش بار گره‌ها با جلوگیری از فعالیت غیرضروری گره‌های اضافی
پیچیدگی محاسباتی	پیچیدگی محاسباتی متوسط به دلیل استفاده از الگوریتم بهینه‌سازی ABC	پیچیدگی کمتر در محاسبه زمان خواب و بیداری گره‌ها
الگوریتم بهینه‌سازی	استفاده از هوش مصنوعی (ABC) برای یافتن مسیرهای بهینه	استفاده از زمان‌بندی خواب و بیداری برای کاهش انرژی مصرفی
کاربردها	بهینه‌سازی مسیر در شبکه‌های حسگر بی‌سیم و انتخاب سرخوشه	مدیریت انرژی و افزایش طول عمر شبکه‌های حسگر بی‌سیم (WSN)
مقاومت در برابر خرابی گره‌ها	انتخاب مسیرهای پایدار و توزیع انرژی مانع از خرابی سریع گره‌ها می‌شود	با مدیریت خواب و بیداری، فشار کمتری بر گره‌های فعال وارد می‌شود
طول عمر شبکه	طول عمر شبکه با بهینه‌سازی مسیرها و مدیریت انرژی افزایش می‌یابد	افزایش طول عمر شبکه با کاهش فعالیت گره‌های غیرضروری

4. نتایج و تحلیل‌ها :

یک محیط آزمایشی شامل پیاده‌سازی شبکه حسگر بی‌سیم با استفاده از گره‌هایی که از پروتکل‌های مسیریابی مبتنی بر اعتماد و تکنیک‌های خوشه‌بندی مبتنی بر کلونی زنبور عسل استفاده می‌کنند، فراهم شد. در این محیط، گره‌ها به‌طور تصادفی توزیع شده‌اند و دستگاه‌های اینترنت اشیا نیز برای جمع‌آوری داده‌ها یکپارچه شده‌اند. معیارهای کارایی از جمله طول عمر شبکه، مصرف انرژی و بازدهی مورد بررسی قرار گرفتند. پروتکل ABC از طریق شبیه‌سازی ارزیابی شد و عملکرد آن با پروتکل ترکیبی ABC-**SWA** پیشنهادی مقایسه گردید و بر معیارهایی مانند تعداد گره‌های فعال و تعداد دورها و به حداقل رساندن مصرف انرژی تمرکز شد.

4.1. نسبت تحویل بسته (Packet Delivery Ratio - PDR) : نشان‌دهنده نسبت تعداد بسته‌های ارسالی به بسته‌های دریافتی است. این نسبت یکی از عوامل کلیدی موفقیت در شبکه‌های بی‌سیم محسوب می‌شود و موفقیت انتقال بسته‌ها را تعیین می‌کند.

$$PDR = \frac{Recieved\ Packet\ Count}{Delivered\ Packet\ Count}$$

4.2. بازدهی (Throughput) : بازدهی شبکه به معنای سرعت ارسال موفقیت‌آمیز داده‌ها از گره فرستنده به گره دریافت‌کننده است.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

$$Throughput = \frac{Foreaded\ data}{Transmission\ time}$$

4.3. **فرمول (ABC-SWA)**: فرمول کلی بهینه‌سازی انرژی و مسیر را می‌توان به صورت زیر ترکیب کرد.

$$E_{\text{total}} = \sum_{i=1}^{N} [W_i \cdot \text{ABC}_{\text{opt}}(E_i, D_i) + (1 - W_i) \cdot \text{SWA}_{\text{opt}}(S_i, T_i)]$$

توضیح متغیرها :

- E_{total} : انرژی کل مصرف‌شده در شبکه.
- N : تعداد گره‌های شبکه.
- W_i : وزن عملکرد الگوریتم (بین 0 و 1) برای تنظیم میزان تأثیر الگوریتم **ABC** و **SWA** .
- $\mathbf{ABC_{opt}(E_i,D_i)}$: انرژی بهینه‌شده برای انتخاب سرخوشه و مسیریابی توسط **ABC** .
- $\mathbf{E_i}$: انرژی باقی‌مانده گره i .
- $\mathbf{D_i}$: فاصله گره i تا سرخوشه یا ایستگاه پایه.
- $\mathbf{SWA_{opt}(S_i,T_i)}$: انرژی ذخیره‌شده با مدیریت چرخه خواب و بیدار توسط **SWA** .
- $\mathbf{S_i}$: زمان خواب گره i .
- $\mathbf{T_i}$: زمان بیداری گره i .

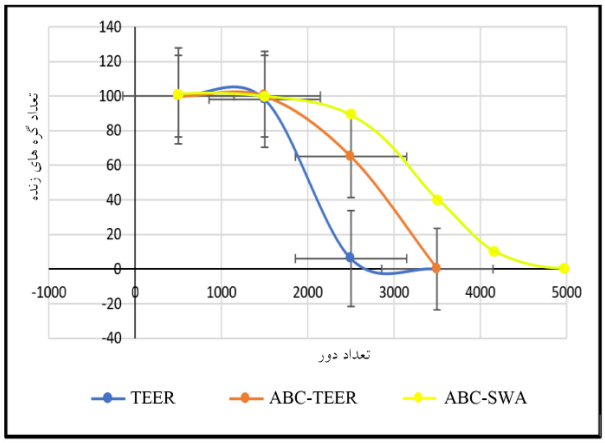
4.4. طول عمر شبکه (Network Lifetime) نیازهای انرژی سنجش (جمع آوری داده)، انتقال و دریافت گره ها طول عمر WSN را مشخص می کند. طول عمر شبکه بر اساس تعداد گره های فعال فعلی، انرژی باقیمانده گره ها و بازده انرژی کلی شبکه محاسبه می شود. پارامتر های شبیه سازی در جدول 3 ، مقایسه بین TEER، طرح اولیه **ABC** و طرح پیشنهادی **ABC-SWA** را نشان می دهد.
در این طرح ها پارامترها به این شیوه است. تعداد گره‌های حسگر (100)، ابعاد میدان (100*100متر)، انرژی اولیه هر گره (2 ژول)، موقعیت ایستگاه پایه (50.50)، حداکثر تعداد تکرار برای هر سه الگوریتم (5000 دور).

جدول 3. عملکرد روش TEER ، ABC و ABC-SWA در هر دور

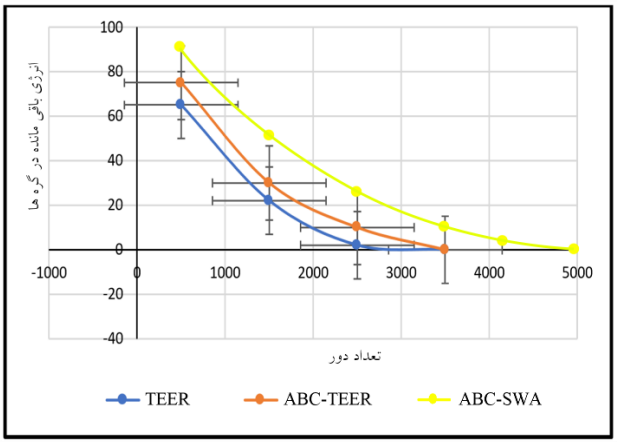
تعداد دور	تعداد گره های زنده			انرژی باقی مانده		
	TEER	**ABC**	**ABC-SWA**	TEER	**ABC**	**ABC-SWA**
500	100	100	100	65	75	90
1500	98	100	100	22	30	50
2500	6	65	90	2	10	28
3500	0	0	40	0	0	10
4000	0	0	10	0	0	5
4500	0	0	4	0	0	1
5000	0	0	0	0	0	0

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

نتایج شبیه‌سازی در نمودارهای شکل 3 ، نشان دهنده تعداد گره های زنده و شکل 4 ، نشان دهنده میزان انرژی باقی مانده در گره‌ها نشان داد که پروتکل **ABC-SWA** به‌طور کلی عملکرد بهتری نسبت به پروتکل‌های TEER و **ABC** دارد و با بهینه‌سازی انتخاب سرخوشه و با به حداقل رساندن مصرف انرژی گره‌ها توانسته است تعداد گره‌های فعال را افزایش دهد و طول عمر شبکه را بهبود بخشد. همچنین در بررسی‌های انجام‌شده، بازدهی شبکه **ABC-SWA** در مقایسه با **ABC**, افزایش چشمگیری داشته است.

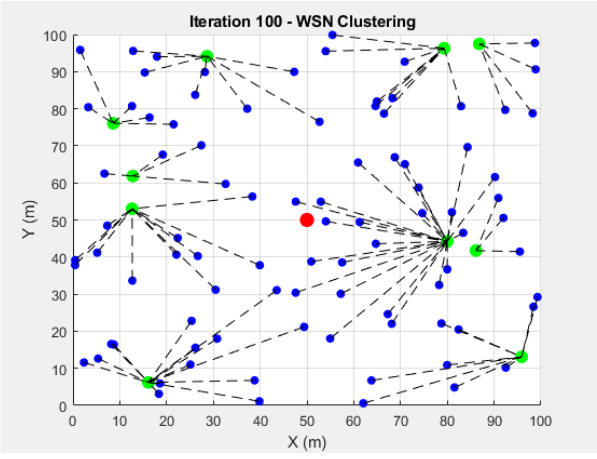


شکل 3. نمودار تعداد گره های زنده در شبکه، با سه الگوریتم

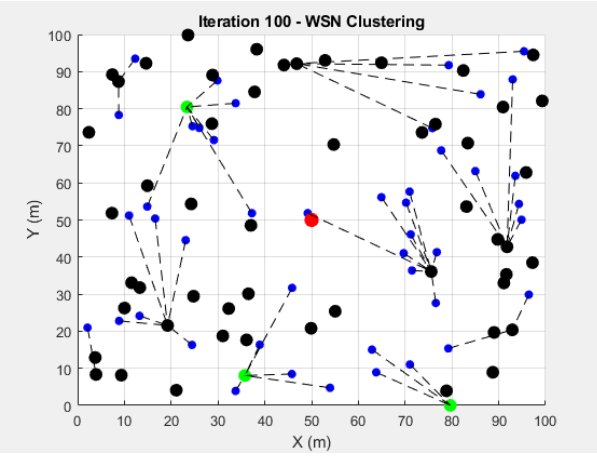


شکل 4. نمودار انرژی باقی مانده در شبکه، با سه الگوریتم

همانطور که در شکل 5 مشاهده می کنید، نمایی کلی از الگوریتم **ABC** در دور صدم WSN، با انتخاب سرخوشه های مناسب با توجه به معیارهای گفته شده، نشان داده شده است، همچنین شکل 6 نمایی کلی از الگوریتم **ABC-SWA** در دور صدم WSN، به خواب و بیدار بودن گره ها اشاره دارد که در آن گره های خاکستری به‌عنوان گره های خواب (غیرفعال)، در هر دور جای خود را با گره های بیدار (فعال) برای حفظ انرژی شبکه جابه‌جا می کنند.



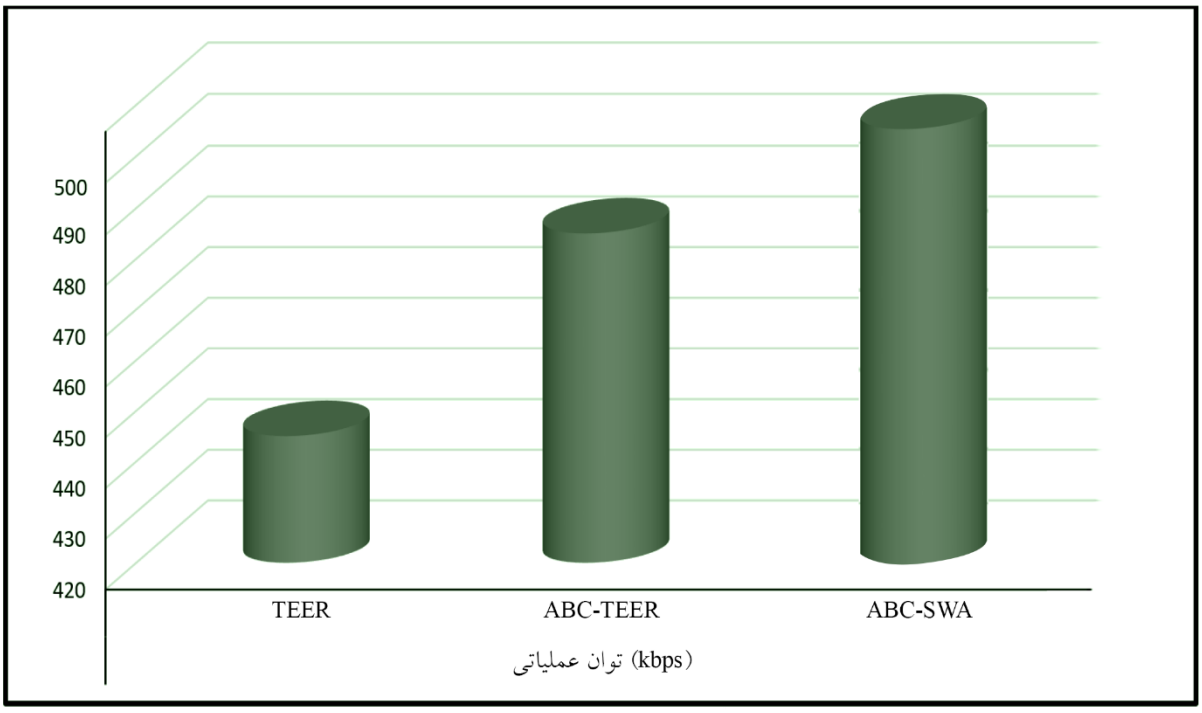
شکل 5. نمایی از الگوریتم **ABC** در دور صدم در WSN



شکل 6. نمایی از الگوریتم **ABC-SWA** در دور صدم در WSN

توان عملیاتی که مقدار انتقال داده در واحد زمان است، در سه الگوریتم معرفی شده، در شکل 7 به وضوح مشخص است.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055



شکل 7. توان عملیاتی سه الگوریتم

5. جمع بندی

برای اینکه WSN ها دوام بیشتری داشته باشند، ایجاد کانال های ارتباطی بین منابع و سینک با استفاده از پروتکل های مسیریابی موثر مهم است. هنگامی که گره ها به طور دلخواه در یک محیط غیر ایمن قرار می گیرند، چندین نوع مختلف حمله می تواند علیه این پروتکل های مسیریابی راه اندازی شود. تکنیک‌های مسیریابی مبتنی بر اعتماد برای WSN طراحی شده‌اند که ترجیح می‌دهند یک مسیر شناخته شده و امن را به جای کوتاه‌ترین مسیر موجود برای خنثی کردن چنین حملاتی انتخاب کنند. با استفاده از MATLAB، پروتکل ABC را بررسی کردیم و بر اساس الگوریتم **ABC-SWA** برای مسیریابی مطمئن و کم انرژی، پروتکل‌ها را از نظر درصد گره‌های زنده و مقدار انرژی باقی‌مانده پس از هر دور مقایسه کردیم. از مقایسه پروتکل‌های ABC و **ABC-SWA** ، تحلیل‌های توان عملیاتی و نرخ تلفات بسته، به دست آمد. تجزیه و تحلیل توان عملیاتی و نرخ تلفات بسته و همچنین طول عمر، همگی برای پروتکل **ABC-SWA** در شبیه سازی ها نتایج بهتری را به همراه داشتند.

منابع :

[1] O. Kaiwartya, A. H. Abdullah, Y. Cao et al., “Virtualization in wireless sensor networks: fault tolerant embedding for Internet of things,” IEEE Internet of Things Journal, vol. 5, no. 2, pp. 571–580, 2018.
[2] P. K. Shukla et al., “Network Physical Address Based Encryption Technique Using Digital Logic”, International Journal of Scientific & Technology Research, Vol. 9, No. 4, 2020, Pp no.- 3119-3122.
[3] O. Kaiwartya, A. H. Abdullah, Y. Cao, et al., “Internet of vehicles: motivation, layered architecture, network model, challenges, and future aspects,” IEEE Access, vol. 4, pp. 5356–5373, 2016.

[4] V. Roy. "An Improved Image Encryption Consuming Fusion Transmutation and Edge Operator." Journal of Cybersecurity and Information Management, Vol. 8, No. 1, 2021, PP. 42-52.
[5] L. Farhan, R. Kharel, O. Kaiwartya, M. Hammoudeh, and B. Adebisi, "Towards green computing for Internet of things: energy-oriented path and message scheduling approach," Sustainable Cities and Society, vol. 38, pp. 195–204, 2018.
[6] V. Roy. " Breast cancer Classification with Multi-Fusion Technique and Correlation Analysis" Fusion: Practice & Applications, Vol. 9, No. 2, 2023, PP. 48-61.
[7] Roy, V., Shukla, P. K., Gupta, A. K., Goel, V., Shukla, P. K., & Shukla, S. (2021). Taxonomy on EEG Artifacts Removal Methods, Issues, and Healthcare Applications. Journal of Organizational and End User Computing (JOEUC), 33(1), 19-46. http://doi.org/10.4018/JOEUC.2021010102.
[8] O. Kaiwartya, A. H. Abdullah, Y. Cao et al., "Internet of vehicles: motivation, layered architecture, network model, challenges, and future aspects," IEEE Access, vol. 4, pp. 5356–5373, 2016.
[9] A. Khatri, S. Kumar, O. Kaiwartya, and A. H. Abdullah, "Green computing for wireless sensor networks: optimization and Huffman coding approach," Peer-to-Peer Networking and Applications, vol. 10, no. 3, pp. 592–609, 2017.
[10] P. Kumar, A. Baliyan, K. R. Prasad, N. Sreekanth, P. Jawarkar, V. Roy, E. T. Amoatey, "Machine Learning Enabled Techniques for Protecting Wireless Sensor Networks by Estimating Attack Prevalence and Device Deployment Strategy for 5G Networks", Wireless Communications and Mobile Computing, vol. 2022, Article ID 5713092, 15 pages, 2022. https://doi.org/10.1155/2022/5713092
[11] Saranya, V., Shankar, S., & Kanagachidambaresan, G. R. (2018). Energy efficient clustering scheme (EECS) for wireless sensor network with mobile sink. Wireless Personal Communications, 100(4), 1553–1567. https://doi.org/10.1007/s11277-018-5653-1
[12] Roy, S., Mazumdar, N., & Pamula, R. (2021). An energy and coverage sensitive approach to hierarchical data collection for mobile sink-based wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, 12(1), 1267–1291.
[13] Nabil M. AbdelAziz,Hassan H. Mohammed,Khalid A. Eldrandaly, An effective Decision making model through Fusion Optimization and risk associated with flash flood hazards: A case study Asyut, Egypt, Journal of Fusion: Practice and Applications, Vol. 12 , No. 1 , (2023) : 64-94 (Doi : https://doi.org/10.54216/FPA.120105)
[14] Yalcin, S., & Erdem, E. (2019). Bacteria interactive cost and balanced-compromised approach to clustering and transmission boundary-range cognitive routing in mobile heterogeneous wireless sensor networks. Sensors. https://doi.org/10.3390/s19040867
[15] Fotohi, R., & Bari, S. F. (2020). A novel countermeasure technique to protect WSN against denial-ofsleep attacks using Firefly and Hopfield neural network (HNN) algorithms. Journal of Supercomputing, 76(6), 6860–6886. https://doi.org/10.1007/s11227-019-03131-x
[16] Sharmin, N., Karmaker, A., Lambert, W. L., Alam, M. S., & Shawkat, M. S. T. S. A. (2020). Minimizing the energy hole problem in wireless sensor networks: A Wedge Merging Approach. Sensors.
[17] Zahra, M., Wang, Y., & Ding, W. J. (2019). Cross-layer routing for a mobility support protocol based on handover mechanism in cluster-based wireless sensor networks with mobile sink. Sensors.
[18] Basumatary, H., Debnath, A., Barma, M. K. D., & Bhattacharyya, B. K. (2020). Centroid-based routing protocol with moving sink node for uniform and non-uniform distribution of wireless sensor nodes. Journal of Supercomputing, 77(4), 3727–3751.
[19] Zhang, J., Tang, J., Wang, Z. H., Wang, F., & Yu, G. (2020). Load-balancing rendezvous approach for mobility-enabled adaptive energy-efficient data collection in WSNs. KSII Transactions on Internet and Information Systems, 14(3), 1204–1227.
[20] Theodorou, T., & Mamatas, L. (2021). SD-MIoT: A software-defined networking solution for mobile internet of things. IEEE Internet Things, 8(6), 4604–4617.
[21] Maruthupandi, J., Prasanna, S., Jayalakshmi, P., Mareeswari, V., Kumar, B. S., & Sanjeevi, P. (2021). Route manipulation aware software-defined networks for effective routing in SDN controlled MANET by Disney routing protocol. Microprocessors and Microsystems.

[22] Guo, W. J., Yan, C. R., & Lu, T. (2019). Optimizing the lifetime of wireless sensor networks via reinforcement-learning-based routing. International Journal of Distributed Sensor Networks.
[23] Alghamdi, T. A. (2020). Energy efficient protocol in wireless sensor network: Optimized cluster head selection model. Telecommunication Systems, 74(3), 331–345. https://doi.org/10.1007/s11235-020-00659-9
[24] Balamurugan, A., Priya, M. D., Janakiraman, S., & Malar, A. C. J. (2021). Hybrid stochastic ranking and opposite differential evolution-based enhanced Firefly Optimization Algorithm for extending network lifetime through efficient clustering in WSNs. Journal of Network and Systems Management, 29(3), 1–31.
[25] Baradaran, A. A., & Navi, K. (2020). HQCA-WSN: High-quality clustering algorithm and optimal cluster head selection using fuzzy logic in wireless sensor networks. Fuzzy Sets and Systems, 389(1), 114–144.
[26] Mohd Zainal Abidin Ab Kadir , Mhmed Algrnaodi , Ahmed N. Al-Masri, Optimal Algorithm for Shared Network Communication Bandwidth in IoT Applications, International Journal of Wireless and Ad Hoc Communication, Vol. 2 , No. 1 , (2021) : 33-48 (Doi : https://doi.org/10.54216/IJWAC.020103)
[27] Muhammad Edmerdash, Waleed khedr, Ehab Rushdy, An Overview of Cloud-Based Secure Services for Enterprise Drug–Drug Interaction Systems, International Journal of Wireless and Ad Hoc Communication, Vol. 2 , No. 2 , (2021) : 49-58 (Doi : https://doi.org/10.54216/IJWAC.020201)
[28] Andino Maseleno, Design of Optimal Machine Learning based Cybersecurity Intrusion Detection Systems, Journal of Cybersecurity and Information Management, Vol. 0 , No. 1 , (2019) : 32-43 (Doi : https://doi.org/10.54216/JCIM.000103).
[29] Ahmed Abdelhafeez, Hoda K. Mohamed, Skin Cancer Detection using Neutrosophic c-means and Fuzzy c-means Clustering Algorithms, Journal of Intelligent Systems and Internet of Things, Vol. 8 , No. 1 , (2023) : 33-42 (Doi : https://doi.org/10.54216/JISIoT.080103)
[30] Lobna Osman, Olutosin Taiwo, Ahmed Elashry, Absalom E. Ezugwu, Intelligent Edge Computing for IoT: Enhancing Security and Privacy, Journal of Intelligent Systems and Internet of Things, Vol. 8, No. 1, (2023): 55-65 (Doi : https://doi.org/10.54216/JISIoT.080105