Electronic & Cyber Defense
Vol. 13, No. 4, 2026 (Serial No. 52). pp. 157- 177
ISSN: 2322-4347, E-ISSN: 2980-8979

Fuzzy-Enhanced Deep Kronecker Stacked Autoencoder for Robust Attack Detection in Social Internet of Things

Mohammad Hassan Nataj Solhdar

PhD student.Department of Shohadaye hoveyzeh Campus of technology, Shahid Chamran University of Ahvaz, Ahvaz, Iran (Correspondence: *????*)

ARTICLE INFO

Article history:

Article Type: Research paper

Receive: *09* October 2025
Revise: 03 December 2025
Accept: 04 January 202*6*
Available online: 22 December 2025

Keywords:
Social Internet of Things – SIoT
Fuzzy Logic
Deep Kronecker Network
Stacked Autoencoder
Intrusion Detection

ABSTRACT

Abstract

This paper proposes a novel hybrid model, the Fuzzy Deep Kronecker Stacked Autoencoder (FDKSAE), addressing the increasing complexity and dynamism of attacks in Social Internet of Things (SIoT) environments. Initially, raw network data were scaled using Z-score normalization. Subsequently, a deep neural network enhanced with the Gower similarity metric was employed for feature integration. In the detection phase, the deep Kronecker network architecture was combined with a multi-layer autoencoder and fuzzy logic to dynamically react to diverse attack patterns and varying network conditions. For performance evaluation, the N-BaIoT dataset, comprising over seven million samples and ten diverse attack classes, was utilized. Experimental results demonstrated that the proposed model achieved superior performance with simultaneous improvements in accuracy (92%) , F1-score (91%) , and prediction precision (91%) , compared to conventional methods such as GAN, MH CNN AM, TM MLA, and HAD. These achievements underscore that the integration of fuzzy logic with deep architectures can effectively manage uncertainties associated with network traffic and attack patterns.

Cite this article: Hassan Nataj Solhdar, M. Fuzzy-Enhanced Deep Kronecker Stacked Autoencoder for Robust Attack Detection in Social Internet of Things. *Electronic and Cyber Defense*, 2025; 13(4): 153- 173

DOI: https://doi.org/10.47176/ECDJ.2025

«پدافند الکترونیکی و سایبری»
سال سیزدهم، شماره ۴، زمستان ۱۴۰۴، ص ۱۵۷- ۱۷۷
شاپا الکترونیکی: ۴۳۴۷ -۲۳۲۲ شاپا چاپی: ۸۹۷۹- ۲۹۸۰

رمزگذار خودکار پشته‌ای کرونکر عمیق بهبودیافته با منطق فازی برای تشخیص مقاوم حملات در اینترنت اشیا اجتماعی

محمدحسن نتاج صلح دار
دانشجوی دکتری،پردیس صنعتی شهدای هویزه، دانشگاه شهید چمران اهواز، اهواز، ایران (نویسنده مسئول: n.solhdar@scu.ac.ir)

چکیده

در این مقاله، باتوجه‌به پیچیدگی و پویایی روزافزون حملات در محیط‌های اینترنت اشیا اجتماعی، یک مدل ترکیبی نوین به نام خود رمزگذار پشته‌ای کرونکر عمیق فازی پیشنهاد شده است. ابتدا داده‌های خام شبکه با استفاده از نرمال‌سازی Z-Score به مقیاس یکسان رسانده شدند و سپس از یک شبکه عصبی عمیق تقویت‌شده با معیار شباهت گوور برای ادغام ویژگی‌ها بهره گرفته شد. در فاز تشخیص، ساختار شبکه کرونکر عمیق با رمزگذار خودکار چندلایه همراه با منطق فازی ترکیب شد تا به‌صورت پویا نسبت به الگوهای متفاوت حمله و شرایط متغیر شبکه واکنش نشان دهد. برای سنجش عملکرد، مجموعه‌داده‌ی *N-BaIoT* با بیش از هفت میلیون نمونه و ده کلاس حمله متنوع مورداستفاده قرار گرفت. نتایج تجربی نشان داد که مدل پیشنهادی با بهبود هم‌زمان دقت (۹۲٪)، معیار *F1* (۹۱٪) و دقت پیش‌بینی (۹۱٪)، نسبت به روش‌های مرسوم مانند *GAN* ، *MH-CNN-AM*، *TM-MLA* و *HAD* برتری دارد. این دستاوردها تأکید می‌کنند که ادغام منطق فازی با معماری‌های عمیق می‌تواند عدم قطعیت‌های مرتبط با ترافیک شبکه و الگوهای حمله را به طور مؤثری مدیریت کند.

مشخصات مقاله

تاریخچه مقاله:
نوع مقاله: علمی- پژوهشی

دریافت: 1404/07/17
بازنگری: 1404/09/12
پذیرش: 1404/10/14
ارائه آنلاین: 1404/10/23

کلیدواژه‌ها:
اینترنت اشیا اجتماعی
منطق فازی
شبکه کرونکر عمیق
رمزگذار خودکار پشته‌ای
تشخیص نفوذ

استناد: حسن نتاج صلحدار, محمد. رمزگذار خودکار پشته‌ای کرونکر عمیق بهبودیافته با منطق فازی برای تشخیص مقاوم حملات در اینترنت اشیاء اجتماعی .پدافند الکترونیکی و سایبری. ۱۴۰۴؛ ۱۳ (۴): ۱۵۳-۱۷۳. DOI: https://doi.org/10.47176/ECDJ.2025

1. مقدمه

اینترنت اشیا اجتماعی[1](SIoT) ، فناوری اینترنت اشیا (IoT) را با اصول شبکه‌های اجتماعی ادغام می‌کند و اتصال‌پذیری و تجربیات کاربران را بهبود می‌بخشد. این چارچوب نوآورانه به دستگاه‌ها اجازه می‌دهد تا به شیوه‌ای آگاهانه اجتماعی تعامل داشته باشند، اطلاعات را به اشتراک بگذارند و بر اساس زمینه اجتماعی خود همکاری کنند. انواع مختلف دستگاه‌های عادی می‌توانند داده و اطلاعات را تبادل کنند. اطلاعات به‌صورت یکپارچه با تجهیز دستگاه‌ها به حسگرها، پردازنده‌ها و نرم‌افزار (مبادله می‌شوند). SIoT دستگاه‌ها را قادر می‌سازد تا در تبادلات انسان به انسان شرکت کنند. این فناوری یک سامانه فعال را توسعه می‌دهد که اشتراک اطلاعات شبکه و مشارکت جامعه را افزایش می‌دهد [۱].

SIoT به شبکه‌ای از اشیا هوشمند اشاره دارد که نه‌تنها قادر به تعامل با محیط فیزیکی هستند (مانند IoT سنتی)، بلکه می‌توانند روابط اجتماعی با یکدیگر، با انسان‌ها و با محیط‌های مجازی برقرار کنند. این روابط بر اساس معیارهایی مانند مالکیت، همکاری، هم‌مکانی، و خویشاوندی تعریف می‌شوند.

ویژگی‌های SIoT به شرح زیر است:

تعامل اجتماعی: دستگاه‌ها می‌توانند اطلاعات را به اشتراک بگذارند و بر اساس زمینه اجتماعی خود همکاری کنند. این شامل توانایی تبادل داده و اطلاعات بین انواع مختلف دستگاه‌های عادی است.

پویایی و پیچیدگی: به دلیل روابط متغیر و تعاملات پویا بین اشیا و کاربران، SIoT ذاتاً پیچیده و پویا است. این پویایی ناشی از تغییر مداوم در وضعیت، موقعیت و ارتباطات دستگاه‌ها و کاربران است.

مقیاس‌پذیری: تعداد فزاینده دستگاه‌ها و تعاملات، چالش‌های مقیاس‌پذیری را ایجاد می‌کند، زیرا مدیریت حجم عظیم‌داده‌ها و روابط نیازمند زیرساخت‌های قوی است.

·تنوع داده: داده‌ها می‌توانند از انواع حسگرها، دستگاه‌ها، و تعاملات اجتماعی باشند که شامل داده‌های عددی و دسته‌بندی شده[2] است. این تنوع، پردازش و تحلیل داده‌ها را پیچیده‌تر می‌کند.

تفاوت با IoT سنتی: درحالی‌که IoT بر اتصال فیزیکی و جمع‌آوری داده تمرکز دارد، SIoT یک‌لایه "آگاهی اجتماعی" اضافه می‌کند. این لایه امکان "تبادلات انسان به انسان" را از طریق دستگاه‌ها فراهم می‌کند و "اشتراک اطلاعات شبکه و مشارکت جامعه را افزایش می‌دهد". این بعد اجتماعی، SIoT را از IoT صرف متمایز می‌سازد و به آن قابلیت‌های جدیدی می‌بخشد.

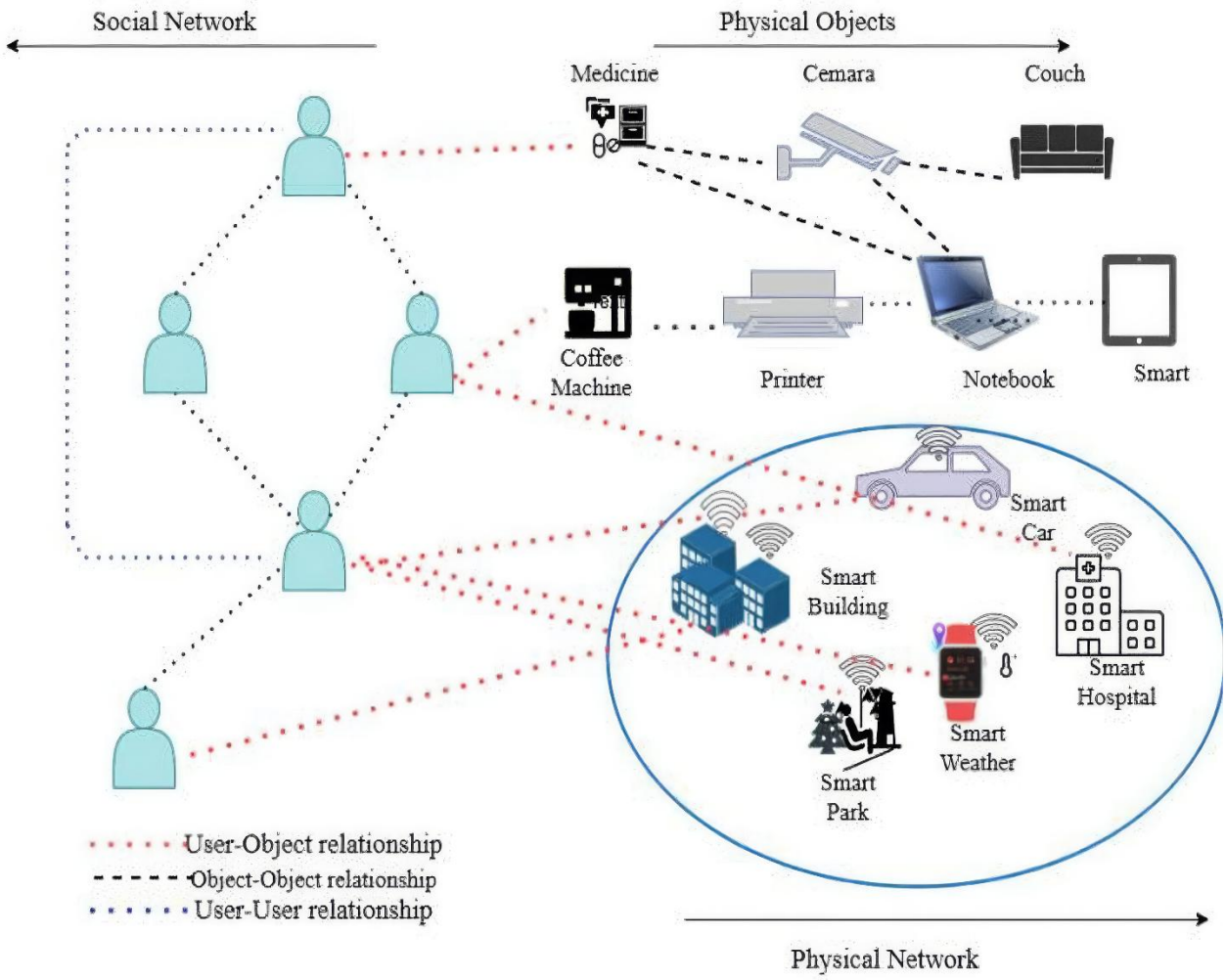
SIoT در حوزه‌های متنوعی مانند حسگری محیطی، نظارت بر سلامت، شهرهای هوشمند، حمل‌ونقل هوشمند، اتوماسیون خانگی، و دستگاه‌های توصیه‌گر اجتماعی کاربرد دارد.

افزایش محبوبیت دستگاه‌های IoT منجر به حملات پیچیده‌تری شده است که به دلیل افزایش‌پذیرش دستگاه‌های IoT تشدید شده‌اند و نیازهای امنیتی را پیشرفته‌تر می‌سازند. این سامانه نیازمند استانداردهای امنیتی بهبودیافته‌ای است که فراتر از رویه‌های عملیاتی استاندارد حرکت می‌کنند. روش‌های سنتی و مطالعات اخیر بر ادغام مکانیسم‌های هوشمند مانند یادگیری ماشین و تشخیص ناهنجاری در اقدامات به‌روز شده برای مقابله با چالش‌های امنیتی که به‌تدریج در محیط‌های SIoT تغییر می‌کنند، تأکید دارند [۲]. کمبود منابع در شبکه‌های پویای IoT منجر به عملکرد ناکارآمد روش‌های تشخیص تهدید مبتنی بر امضا و مبتنی بر ناهنجاری می‌شود. توسعه سریع روش‌های حمله باعث می‌شود این روش‌های تشخیص به پروتکل‌های پیچیده‌تری برای کشف تهدیدات امنیتی جدید نیاز داشته باشند، بنابراین حملات شبکه توزیع خدمات IoT را مختل می‌کنند [۳]. عملکرد مؤثر سامانه‌های امنیتی پیشگیرانه نیازمند پیاده‌سازی سامانه‌های تشخیص حمله برای رفع نقاط ضعف فعلی آنهاست. سامانه‌های تشخیص امنیت بر اساس نشانه‌های شناخته شده یا رفتار خاص سامانه عمل می‌کنند. انتشار داده برای حفظ دردسترس‌بودن خدمات حیاتی است و کاربردهای مختلف IoT مانند حسگری محیطی و نظارت بر سلامت را امکان‌پذیر می‌سازد. این یکی از خدمات IoT است که بیشترین تأثیر را می‌پذیرد و اهمیت حریم خصوصی و امنیت داده را برای شبکه برجسته می‌کند. امنیت در دستیابی به یک سامانه و محیط امن حیاتی است، زیرا به کاهش خطرات قابل‌توجه کمک می‌کند [۴].

در زمینهIoT ، درخواست‌کننده به‌عنوان اعتمادکننده عمل می‌کند و باید به ارائه‌دهنده که خدمت موردنیاز را ارائه خواهد داد، یعنی مورداعتماد، تکیه کند. بااین‌حال، دستگاه‌های خاصی ممکن است برای منفعت خود در فعالیت‌های مخرب علیه سایر

[1] Social Internet of Things
[2] mixed-type data

گره‌های IoT شرکت کنند. آنها ممکن است خدمات دروغین یا توصیه‌های گمراه‌کننده ارائه دهند و می‌توانند به‌تنهایی عمل کنند یا با دستگاه‌های دیگر همکاری کنند تا بر یک دسته خدمات خاص مسلط شوند. اگر به این حملات و اختلالات به‌اندازه کافی رسیدگی نشود، می‌توانند مزایای IoT را تضعیف کنند [۵]. یک مهاجم می‌تواند با تسلط بر یک ابزار IoT و استفاده از آن برای اهداف مخرب، لایه شبکه را به خطر بیندازد. سپس این دستگاه به خطر افتاده می‌تواند سایر دستگاه‌های متصل را تحت‌تأثیر قرار دهد و آنها را در برابر حملات بعدی مانند تبانی، ایمیل‌های مخرب و حملات انکار سرویس (DoS) بی‌دفاع کند. در نتیجه، حملات شبکه یک مانع قابل‌توجه در پذیرش گسترده‌تر خدمات IoT هستند که در لایه شبکه در معماری IoT قابل‌تشخیص است [۶]. اقدامات امنیتی پیشگیرانه اغلب دارای نقص در طراحی و پیاده‌سازی هستند که مکانیسم‌های تشخیص حمله را ضروری می‌سازد. اگرچه رویکرد مبتنی بر امضا به دلیل دقت بالا و نرخ هشدار کاذب حداقل به طور گسترده‌ای استفاده می‌شود، اما به دلیل عدم توانایی آن در تشخیص حملات جدید و ناشناخته مورد اعتراض است [۷].



شکل 1: معماری اینترنت اشیا اجتماعی مبتنی بر روابط میان اشیا و کاربران در محیط

در سطح سامانه، تضمین دسترس‌پذیری عملیات به پیاده‌سازی اقدامات امنیتی مؤثر برای ارزیابی رفتار فیزیکی افراد و کمک به تصمیم‌گیری‌ها بستگی دارد. باتوجه‌به اینکه تهدید همیشه وجود دارد، باید اقداماتی برای شناسایی و کاهش اثرات حملات احتمالی در نظر گرفته شود [۸]. روش‌های سنتی برای تشخیص حملات در سامانه‌های IoT با چندین مانع از جمله تأخیر، محدودیت منابع و مسائل مقیاس‌پذیری مواجه هستند. فن‌های یادگیری ماشین با مشاهده فعالیت‌های شبکه و به‌روزرسانی مداوم اطلاعات

تهدید[1]، اطمینان‌پذیری اینترنت اشیا اجتماعی را افزایش می‌دهند [۹]. معماری اینترنت اشیا اجتماعی از برچسب‌های RFID و دستگاه‌های هوشمند برای ترویج تعاملات اجتماعی بین اشیا و انسان‌ها استفاده می‌کند. این معماری به طور مؤثری شکاف بین حوزه‌های فیزیکی و مجازی را پر می‌کند [۱۰] و امکان ارائه خدمات کارآمد را از طریق شبکه‌ای از موجودیت‌های هوشمند متصل‌به‌هم فراهم می‌سازد. موجودیت‌های مجازی (VEs) داده‌ها را از راه دور جمع‌آوری کرده و الگوهای شبکه‌های اجتماعی را تجزیه‌وتحلیل می‌کنند تا ویژگی‌های شبکه را تأیید نمایند [۱۱].

جدول ۱ مدل‌های پیشرفته مختلفی را برای تشخیص حملات IoT برجسته می‌کند، از جمله GANs، CNNs، مدیریت اعتماد[2] و رویکردهای یادگیری عمیق هیبریدی. بیشتر مدل‌ها به‌دقت تشخیص و سازگاری بهبودیافته‌ای دست یافتند، بااین‌حال با چالش‌هایی مانند بیش برازش[3]، مصرف منابع و پیاده‌سازی بلادرنگ محدود مواجه بودند. شکل ۱ معماری اینترنت اشیا اجتماعی (SIoT) را نشان می‌دهد.

با افزایش محبوبیت دستگاه‌های IoT منجر به حملات پیچیده‌تری شده است که نیازهای امنیتی پیشرفته‌تری را ایجاد می‌کند. این گسترش، نقاط ورود بیشتری را برای مهاجمان فراهم می‌آورد.

حملات مبتنی بر اعتماد(Trust-based attacks) : درSIoT ، اعتماد بین دستگاه‌ها و کاربران حیاتی است. مهاجمان می‌توانند با ارائه "خدمات دروغین یا توصیه‌های گمراه‌کننده" یا "تسلط بر یک ابزار IoT و استفاده از آن برای اهداف مخرب" به سامانه اعتماد حمله کنند. این شامل حملات تبانی، سیبیل[4] و حملات انکار سرویس[5] می‌شود. جنبه "اجتماعیSIoT "، بردار حمله جدیدی را باز می‌کند که در آن دست‌کاری اعتماد، تبانی بین دستگاه‌ها، یا انتشار اطلاعات غلط از طریق روابط اجتماعی می‌تواند منجر به آسیب‌های جدی شود.

حریم خصوصی و امنیت داده: تبادل اطلاعات یکپارچه در SIoT اهمیت حریم خصوصی و امنیت داده را برجسته می‌کند. نقض حریم خصوصی در SIoT می‌تواند پیامدهای جدی برای کاربران و سازمان‌ها داشته باشد، زیرا داده‌های حساس از طریق تعاملات اجتماعی به اشتراک گذاشته می‌شوند.

پویایی و عدم قطعیت: محیط‌های SIoT به دلیل تغییرات مداوم در روابط و رفتار دستگاه‌ها، ذاتاً پویا و دارای عدم قطعیت هستند. روش‌های سنتی تشخیص تهدید مبتنی بر امضا و ناهنجاری، اغلب در این محیط‌های پویا ناکارآمد هستند و نمی‌توانند به‌سرعت با الگوهای جدید حمله سازگار شوند.

محدودیت منابع: بسیاری از دستگاه‌های IoT در SIoT دارای منابع محاسباتی و انرژی محدودی هستند که پیاده‌سازی سامانه‌های امنیتی پیچیده و سنگین را دشوار می‌کند. ۱ این محدودیت‌ها نیازمند راهکارهای امنیتی کارآمد و بهینه‌سازی شده هستند.

مهم‌ترین مباحث این مقاله عبارت‌اند از:

- توسعه یک تکنیک مؤثر برای تشخیص حملات در SIoT با ایجاد یک روش یادگیری عمیق هیبریدی، به نام خود رمزگذار پشته‌ای کرونکر عمیق فازی[6]، از طریق ترکیب شبکه کرونکر عمیق[7] (DKN)، خود رمزگذار پشته‌ای عمیق (DSA) و مفهوم فازی.
- ابداع یک تکنیک جدید برای ترکیب ویژگی‌ها با شبکه عصبی عمیق[8] (DNN) همراه با معیار شباهت Gower برای کاهش پیچیدگی محاسباتی.
- یکپارچه‌سازی منطق فازی[9] به مدیریت عدم قطعیت در تشخیص نفوذ کمک می‌کند.

برتری Fuzzy-DKSA نه‌تنها در تشخیص حملات عمومی IoT است، بلکه به طور خاص در توانایی آن برای مدیریت عدم قطعیت و پیچیدگی ناشی از جنبه‌های اجتماعی SIoT نهفته است.

مدیریت عدم قطعیت با منطق فازی: منطق فازی[10] به مدل اجازه می‌دهد تا "عدم قطعیت‌های مرتبط با ترافیک شبکه و الگوهای حمله را به طور مؤثری مدیریت کند". این ویژگی برای محیط‌های SIoT که در آن‌ها رفتار عادی و مخرب اغلب مرزهای

[1] threat intelligence
[2] trust management
[3] overfitting
[4] Sybil attacks
[5] DoS

[6] Fuzzy Deep Kronecker Stacked Auto encoder
[7] Deep Kronecker Network
[8] Deep Neural Network
[9] Fuzzy Logic Integration
[10] Fuzzy Logic

مشخصی ندارند و داده‌ها ممکن است مبهم یا ناقص باشند، حیاتی است. منطق فازی با اجازه‌دادن به "درجات حقیقت" به‌جای "درست/غلط" مطلق، تصمیم‌گیری‌های ظریف‌تر و انطباق‌پذیرتری را ممکن می‌سازد. این امر به‌ویژه در تشخیص حملات نوین و ناشناخته[1] که امضای مشخصی ندارند، مفید است و مقاومت مدل را در برابر تهدیدات تکامل‌یافته افزایش می‌دهد.

یادگیری ویژگی‌های پیچیده با DKN : DKN از "حاصل‌ضرب‌های کرونکر" برای یادگیری ویژگی‌ها استفاده می‌کند. این قابلیت به DKN اجازه می‌دهد تا روابط پیچیده و سلسله‌مراتبی را در داده‌های شبکهSIoT که اغلب دارای ابعاد بالا و ارتباطات متقابل هستند، به طور مؤثر استخراج کند. این توانایی در استخراج ویژگی‌های غنی، برای شناسایی الگوهای حمله پنهان در ترافیک SIoT ضروری است و به مدل امکان می‌دهد تا الگوهای پیچیده و غیرخطی ناشی از تعاملات اجتماعی را بهتر یاد بگیرد.

بازنمایی قوی داده با DSA : DSA با ساختار رمزگذار - رمزگشا[2] خود، قادر به یادگیری بازنمایی‌های فشرده و درعین‌حال غنی از داده‌های ورودی است. این امر به کاهش ابعاد داده‌ها کمک می‌کند و درعین‌حال اطلاعات حیاتی برای تشخیص حمله را حفظ می‌نماید. این بازنمایی قوی، مدل را در برابر نویز و تغییرات جزئی در داده‌ها مقاوم‌تر می‌سازد که در محیط‌های SIoT با داده‌های پرنویز و متغیر، اهمیت بالایی دارد.

ترکیب ویژگی‌ها با DNN و معیار شباهتGower : استفاده از شبکه عصبی عمیق (DNN) همراه با معیار شباهت Gower یک گام مهم در مدیریت "داده‌های با نوع مختلط[3]" است که در SIoTرایج است. این ترکیب، نمایش ویژگی‌ها را بهبود می‌بخشد و به مدل اجازه می‌دهد تا اطلاعات را از ویژگی‌های عددی و دسته‌بندی شده به طور مؤثر ادغام کند که برای تشخیص دقیق در یک محیط ناهمگن SIoT ضروری است.

افزایش مقاومت در برابر حملات: ترکیب هوشمندانه این مؤلفه‌ها (DKN برای یادگیری ویژگی‌های عمیق، DSA برای بازنمایی مقاوم، و منطق فازی برای مدیریت عدم قطعیت) یک سامانه تشخیص نفوذ هیبریدی ایجاد می‌کند که می‌تواند "به‌صورت پویا نسبت به الگوهای متفاوت حمله و شرایط متغیر شبکه واکنش نشان دهد". این انعطاف‌پذیری و توانایی انطباق، منجر به تشخیص "مقاوم" حملات در محیط‌های پیچیده و در حال تحول SIoT می‌شود.

این مقاله به شرح زیر ساختاریافته است: بخش دوم کارهای مرتبط و بخش سوم روش‌شناسی پیشنهادی را تشریح می‌کند. بخش چهارم یافته‌های تجربی را ارائه می‌دهد و بخش پنجم نتیجه‌گیری مطالعه را بیان می‌کند.

2. کارهای مرتبط

در مقاله [۱۲] بر مدل‌های یادگیری ماشین هیبریدی برای تشخیص نفوذ در IoT تأکید دارد که با رویکرد هیبریدی Fuzzy-DKSA همسو است. این مقاله به‌دقت بالا (۹۳٪) و F1-score(۹۲٪) برای DNN در Edge-IIoTset اشاره می‌کند و اهمیت انتخاب ویژگی و رویکردهای ترکیبی را برجسته می‌سازد. این مقاله به‌عنوان یک کار جدید در زمینه مدل‌های هیبریدی است و از DKN و منطق فازی در Fuzzy-DKSA برای مدیریت عدم قطعیت استفاده می‌کند.

در مقاله [۱۳] یک بررسی سیستماتیک بسیار معتبر است که وضعیت هنر درIDS های مبتنی بر ML/DL در IoT را نشان می‌دهد. این مقاله به استفاده از Autoencoder و DNN اشاره می‌کند و چالش‌هایی مانند محدودیت منابع، داده‌های نامتوازن و نیاز به یادگیری افزایشی[4] برای محیط‌های پویا را برجسته می‌سازد.

در مقاله [۱۴] به طور خاص بر استفاده از منطق فازی برای تشخیص ناهنجاری در امنیت شبکه تمرکز دارد و کارایی آن را در مدیریت عدم قطعیت و بهبود دقت نشان می‌دهد (Precision ۲0.95, Recall 0.97, F1-Score 0.96). این امر به طور مستقیم از نوآوری شما در ادغام منطق فازی حمایت می‌کند.

در مقاله [۱۵] یک سامانه IDS مبتنی بر یادگیری ماشین پشته‌ای (stacked ML) را برای وسایل نقلیه هوشمند (نوعی IoT) پیشنهاد می‌کند و به‌دقت بسیار بالا و زمان تشخیص سریع دست می‌یابد. این یک روش نوین و با عملکرد بالا است.

در مقاله [۱۶] یک رویکرد سبک‌وزن مبتنی بر رمزگذار خودکار[5] برای تشخیص نفوذ در IIoT پیشنهاد می‌کند و به‌دقت بالادست

[1] zero-day attacks
[2] encoder-decoder
[3] mixed-type data
[4] incremental learning
[5] autoencoder

می‌یابد. این مقاله نیز از رمزگذار خودکار استفاده می‌کند و بر روی دستگاه‌های با منابع محدود تمرکز دارد.

جدول ۱ روش‌های کلیدی مورداستفاده در مطالعات مرتبط برای شناسایی حملات در سامانه‌های اینترنت اشیا را خلاصه می‌کند و به بیان دستاوردها و محدودیت‌های آن‌ها می‌پردازد. این جدول شکاف‌هایی مانند نیاز بالا به منابع، حساسیت نسبت به رفتار مهاجم، و فقدان یکپارچگی بلادرنگ را نشان می‌دهد که توسعه مدل Fuzzy-DKSA را توجیه می‌کنند.

جدول 1: مروری بر کارهای اخیر

منبع	روش/مدل استفاده‌شده	مشارکت‌های کلیدی	محدودیت‌ها
Nie و همکاران [۱۷]	GAN	شناسایی انواع حملات اخیر با نرخ هشدار کاذب کاهش‌یافته	فاقد راهبُردهای استخراج ویژگی
Das و همکاران [۱۸]	MH-CNN-AM	نرخ پیش‌بینی بالا در شناسایی دستگاه‌های گمراه‌کننده	افزایش هزینه به دلیل ارتباط زیاد بین دستگاه‌ها
Marche و همکاران [۱۹]	مدل مدیریت اعتماد	کاهش دودلی در انتخاب تأمین‌کنندگان قابل‌اعتماد و شناسایی اقدامات پویا	عملکرد نسبتاً ضعیف در مواجهه با حملات مزاحمت ساده
Oliveira و همکاران [۲۰]	مکانیزم ELECTRON	دست‌یابی به کشسانی و سازگاری برای محیط‌های استقرار متنوع	حساسیت به تغییرات رفتار مهاجم که باعث کاهش عملکرد می‌شود
Hankare و همکاران [۲۱]	TM-MLA	شناسایی دستگاه‌های مخرب و تخصیص اعتماد وظیفه‌ای در زمان واقعی	مستعد بیش برازش (overfitting) و سربار تجربی زیاد
Mekala و همکاران [۲۲]	HAD	تضمین حفاظت مبتنی بر شاخص اعتماد در برابر حملات فعال و غیرفعال	نیاز به منابع زیاد و مشکلات مقیاس‌پذیری در تراکم بالای گره‌ها
Babu و همکاران [۲۳]	DBN with NMR-LA	همگرایی بهتر و کاهش مثبت‌های کاذب	عدم یکپارچگی برای کاربردهای هم‌زمان در زمان واقعی
Diro و همکاران [۲۴]	یادگیری عمیق توزیع‌شده	جلوگیری از رسیدن به مینیمم‌های محلی حین آموزش و عملکرد برجسته در داده‌های آزمایشی مخفی	چشم‌پوشی از جنبه‌های تحویل داده و عدم توانایی در شناسایی برخی الگوهای نفوذ بحرانی

3. روش پیشنهادی

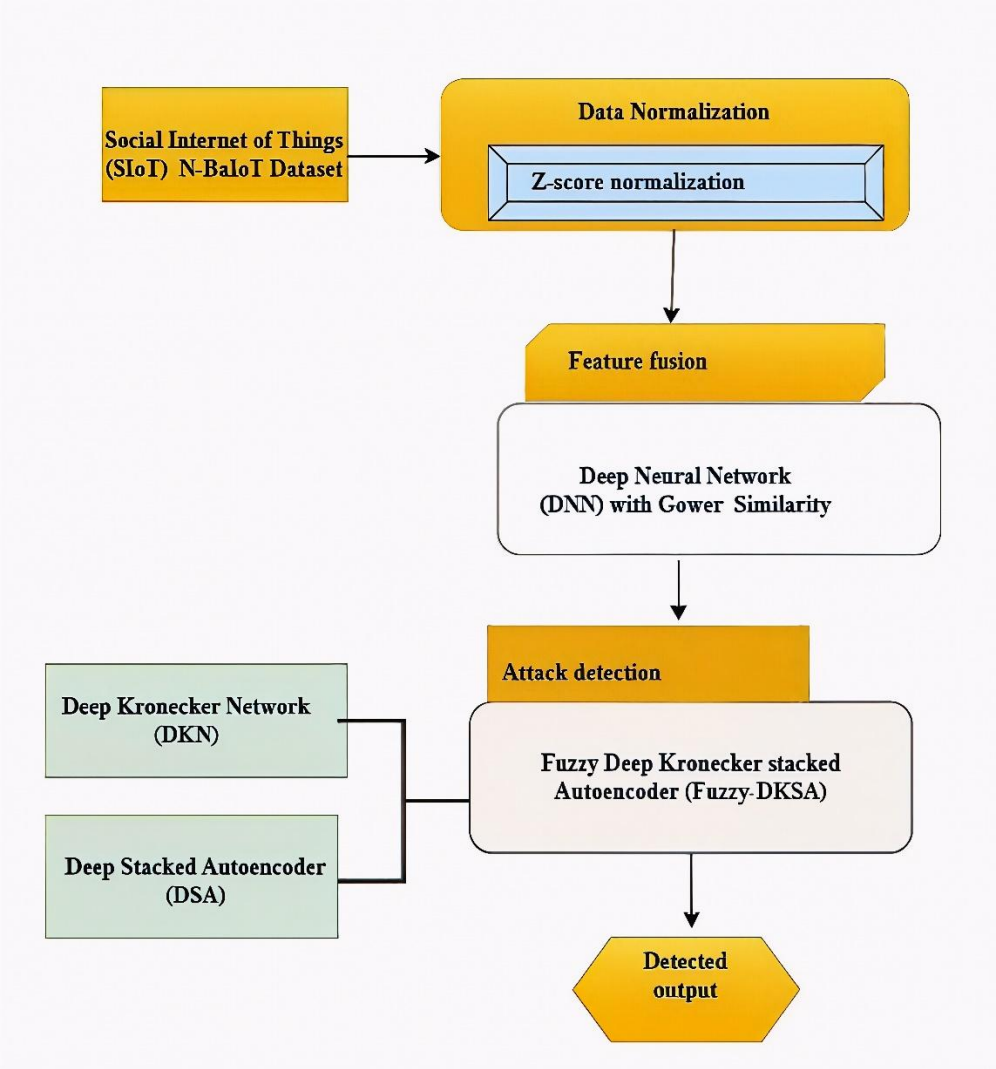
ابتدا، داده‌های اینترنت اشیا اجتماعی از مجموعه‌داده دریافت می‌شوند. سپس، داده‌های دریافت شده به مرحله نرمال‌سازی داده وارد می‌شوند. نرمال‌سازی داده با استفاده از نرمال‌سازی Z-score [25] انجام می‌شود تا اطلاعات به شیوه‌ای ساختاریافته تبدیل شوند (نرمال‌سازی Z-score روشی رایج برای مقیاس‌بندی داده‌ها بر اساس میانگین و انحراف معیار است).

سپس، خروجی مرحله نرمال‌سازی به ماژول ترکیب ویژگی‌ها وارد می‌شود، جایی که ترکیب ویژگی‌ها با استفاده از شبکه عصبی عمیق (DNN) [۲۶] همراه با معیار شباهت Gower [27] برقرار می‌شود (شباهت Gower معیاری است که برای اندازه‌گیری شباهت بین نمونه‌های داده با انواع مختلف ویژگی‌ها به کار می‌رود).

نهایتاً، خروجی ماژول ترکیب ویژگی‌ها به ماژول تشخیص حمله ارسال خواهد شد. در اینجا، تشخیص حمله با استفاده از روش پیشنهادی Fuzzy-DKSA که از ترکیب DKN [23]، DSA [24] و مفهوم فازی ایجاد شده است، انجام می‌شود، جایی که لایه‌ها اصلاح خواهند شد (منظور از اصلاح لایه‌ها، احتمالاً ادغام منطق فازی در ساختار شبکه برای پردازش داده‌ها و تصمیم‌گیری است).

روش Fuzzy-DKSA برای تشخیص حملات در اینترنت اشیا اجتماعی با استفاده از نرم‌افزار MATLAB و مجموعه‌داده N-BaIoT پیاده‌سازی خواهد شد. معیارهایی مانند پرسیژن (Precision)، امتیاز F1 (F1-score) و دقت (Accuracy) برای ارزیابی عملکرد استفاده خواهند شد. کارایی این فرایند نیز با فن‌های کنونی مقایسه خواهد شد تا مزایای آن برجسته شود. شکل ۲ معماری پیشنهادی سامانه Fuzzy-DKSA را برای تشخیص حملات در اینترنت اشیا اجتماعی به نمایش می‌گذارد.

در جدول ۲ چالش‌های امنیتی SIoT و راهکارهای مدل پیشنهادی برای حل این چالش‌ها رو بیان شده است.



شکل 2: معماری سامانه پیشنهادی Fuzzy-DKSA برای تشخیص حملات در اینترنت اشیا اجتماعی

جدول ۲: چالش‌های امنیتی SIoT و راهکارهای Fuzzy-DKSA

چالش امنیتی SIoT	راهکار Fuzzy-DKSA	توضیح چگونگی رفع چالش
عدم قطعیت و ابهام در رفتار شبکه	منطق فازی (Fuzzy Logic)	مدیریت عدم قطعیت با درجات حقیقت به‌جای تصمیم‌گیری باینری، امکان تشخیص الگوهای مبهم و حملات ناشناخته را فراهم می‌کند.
داده‌های ناهمگن (Mixed-type data)	ترکیب ویژگی‌ها با DNN و معیار شباهت Gower	Gower شباهت را برای ویژگی‌های عددی و دسته‌بندی شده محاسبه می‌کند و DNN این اطلاعات را برای بازنمایی یکپارچه پردازش می‌کند.
ابعاد بالای داده و پیچیدگی روابط	شبکه کرونکر عمیق (DKN)	DKN با استفاده از حاصل‌ضرب‌های کرونکر، قادر به یادگیری روابط پیچیده و سلسله‌مراتبی در داده‌های با ابعاد بالا است.

نویز در داده‌ها و نیاز به بازنمایی مقاوم	رمزگذار خودکار پشته‌ای (DSA)	DSA با یادگیری بازنمایی‌های فشرده و مقاوم، نویز را کاهش داده و ویژگی‌های مهم را حتی در داده‌های ناقص حفظ می‌کند.
پویایی شبکه و الگوهای حمله متغیر	ادغام منطق فازی و معماری‌های عمیق	مدل به‌صورت پویا نسبت به الگوهای متفاوت حمله و شرایط متغیر شبکه واکنش نشان می‌دهد و انطباق‌پذیری بالایی دارد.
حملات مبتنی بر اعتماد و تبانی	یادگیری ویژگی‌های عمیق و مدیریت عدم قطعیت	توانایی DKN در کشف الگوهای پیچیده و منطق فازی در مدیریت ابهام، به شناسایی رفتارهای غیرعادی ناشی از دست‌کاری اعتماد کمک می‌کند.
محدودیت منابع (در تشخیص)	بازنمایی فشرده DSA	با کاهش ابعاد داده‌ها و حفظ اطلاعات کلیدی، DSA به کاهش سربار محاسباتی در فاز تشخیص کمک می‌کند.

3.1. شرح مجموعه‌داده

مجموعه‌داده N-BaIoT [25] یک مجموعه‌داده جامع و با ابعاد بالا است که برای تشخیص حملات سایبری در محیط‌های اینترنت اشیا طراحی شده است. این مجموعه شامل ۷,۱۶۲,۶۰۷ نمونه داده ترتیبی است که هر یک نشان‌دهنده ویژگی‌های مختلف صفات کامپیوتری جمع‌آوری شده در یک محیط واقعی هستند.

هر نمونه داده شامل ۱۱۵ ویژگی متمایز است که رفتار دستگاه‌های IoT را منعکس می‌کنند و امکان تحلیل جزئیات فعالیت شبکه را فراهم می‌سازند. این صفات الگوهای زمانی و آماری را ثبت می‌کنند که می‌توانند توسط مدل‌های یادگیری ماشین برای تشخیص مؤثر ناهنجاری مورداستفاده قرار گیرند. این مجموعه‌داده هم ترافیک عادی[1] و هم ترافیک مخرب[2] را در بر می‌گیرد که ترافیک مخرب از طریق ۱۰ نوع حمله سایبری متنوع اجرا شده توسط دو بات‌نت معروف ایجاد شده است. این حملات از حملات انکار سرویس توزیع شده[3] تا سرقت اطلاعات و حملات دسترسی از راه دور را شامل می‌شوند که این مجموعه‌داده را برای وظایف طبقه‌بندی چند کلاسه[4] مناسب می‌سازد. باوجود ۱۰ کلاس حمله با برچسب‌گذاری متمایز، پژوهشگران می‌توانند اثربخشی روش‌های مختلف تشخیص نفوذ را بررسی کنند، به‌ویژه در زمینه‌های داده‌های چند کلاسه و نامتوازن[5].

[1] benign
[2] malicious
[3] Distributed Denial-of-Service - DDoS
[4] multi-class classification
[5] imbalanced data

x_i نشان‌دهنده یک نمونه تکی از مجموعه‌داده با اندازه N است. این یک نمونه از مجموعه‌داده است که در آن $i=1,2,3,\dots,N$.

$$D=\{x_1, x_2, x_3, \dots, x_N\} \quad (1)$$

مجموعه‌داده حاوی چندین ویژگی ورودی است که مربوط به تشخیص حمله می‌شوند. بردار x_i از چندین ویژگی تشکیل شده است که می‌توان آن را به‌صورت زیر نوشت:

$$x_i = \{f_1, f2, f_3, \dots, f_m\} \quad (2)$$

که در آن f_j نشان‌دهنده ویژگی j ام در مجموعه‌داده ارائه شده است. تعداد کل ویژگی‌ها به‌ازای هر نمونه با m نشان داده می‌شود. مجموعه‌داده به دلیل ساختار خود به‌صورت یک ماتریس وجود دارد که می‌توان آن را به‌صورت زیر بیان کرد:

$$D = \{x_1, x_2, \dots, x_N\} \in R_{N\times m} \quad (3)$$

D نشان‌دهنده مجموعه داده‌ای است که حاوی N نمونه همراه با m ویژگی است که کل مجموعه به‌صورت ماتریسی با ابعاد $N\times m$ است.

3.2. پیش‌پردازش داده‌های ناهمگن SIoT

3.2.1. نرمال‌سازی Z-score

اولین گام در روش پیشنهادی، پردازش داده‌های خام SIoT از طریق نرمال‌سازی Z-score است. این روش داده‌ها را بر اساس میانگین (μ) و انحراف معیار (σ) مقیاس‌بندی می‌کند. فرمول آن به‌صورت $X' = \frac{X-\mu}{\sigma}$ بیان می‌شود که در آن X' مقادیر نرمال شده، X نقطه داده اصلی، μ میانگین ویژگی، و σ انحراف معیار است.

اهمیت برای SIoT: این فرایند باعث می‌شود که ویژگی‌ها در یک مقیاس قابل‌اندازه‌گیری قرار گیرند و از تسلط ویژگی‌های با مقادیر بزرگ‌تر بر فرایند آموزش جلوگیری شود که "کارایی عملیاتی مدل‌های یادگیری عمیق را افزایش می‌دهد". در محیط‌های SIoT، داده‌ها از منابع بسیار متنوعی با دامنه‌های مقداری متفاوت جمع‌آوری می‌شوند (مثلاً تعداد پکت‌ها، زمان تأخیر، نوع پروتکل). Z-score به یکسان‌سازی این مقیاس‌ها کمک کرده و از سوگیری مدل به سمت ویژگی‌های با مقادیر بزرگ‌تر جلوگیری می‌کند که برای عملکرد بهینه مدل‌های یادگیری عمیق ضروری است.

$$X' = \frac{X-\mu}{\sigma} \qquad (۴)$$

3.2.2. ترکیب ویژگی‌ها با DNN و معیار شباهت Gower

پس از نرمال‌سازی، داده‌های پردازش شده وارد ماژول ترکیب ویژگی‌ها می‌شوند. در این مرحله، ترکیب ویژگی‌ها با استفاده از شبکه عصبی عمیق (DNN) همراه با معیار شباهت Gower انجام می‌شود. این مرحله برای مدیریت "داده‌های با نوع مختلط" که شامل ویژگی‌های عددی و دسته‌بندی شده هستند، حیاتی است.

معیار شباهت :Gower معیار Gower برای اندازه‌گیری شباهت بین نمونه‌های داده با انواع مختلف ویژگی‌ها به کار می‌رود. محاسبه شباهت بین دو بردار x_i و x_j به شرح زیر انجام می‌شود:

$$S_{ij} = \frac{1}{p}\sum_{k=1}^{p} S_{ijk} \qquad (۵)$$

که در آن S_{ijk} نشان‌دهنده شباهت ویژگی منفرد است، p تعداد کل ویژگی‌هاست.

برای ویژگی‌های عددی(X_K) :

$$S_{ijk} = 1 - \frac{|x_{ik} - x_{jk}|}{R_k} \qquad (۶)$$

دامنه ویژگی k دارای مقدار R_k است.

ویژگی‌های دسته‌بندی شده(CK) :

$$S_{ijk} = \begin{cases} 1, & \text{if } x_{ik} = x_{jk} \\ 0, & \text{otherwise} \end{cases} \qquad (۷)$$

شبکه عصبی عمیق (DNN) شباهت Gower را به‌عنوان ورودی خود برای انجام تبدیل‌ها می‌پذیرد.

$$h(l)=f(W(l)h(l-1) +b(l)) \qquad (8)$$

که در آن، $h(l)$فعال‌سازی لایه l را نشان می‌دهد، $W(l)$ و $b(l)$ به ترتیب وزن‌ها و بایاس‌های خاص لایه را نشان می‌دهند، $f(\cdot)$ تابع فعال‌سازی را نشان می‌دهد.DKN از حاصل‌ضرب‌های کرونکر (Kronecker products - حاصل‌ضرب تنسوری ماتریس‌ها) برای یادگیری ویژگی‌ها استفاده می‌کند:

$$h(l)=\sigma\,(W(l)\otimes h(l-1) + b(l)) \qquad (9)$$

که در آن $\otimes$ حاصل‌ضرب کرونکر را نشان می‌دهد. DSA از یک ساختار رمزگذار - رمزگشا[1] پیروی می‌کند:

لایه رمزگذار:

$$h = f\,(W_e\ X + b_e) \qquad (10)$$

لایه رمزگشا

$$X' = f\,(W_d\ h + b_d) \qquad (11)$$

که در آن، W_e و W_d به ترتیب ماتریس‌های وزن رمزگذار و رمزگشا هستند، b_e و b_d جملات بایاس[2] هستند.

نوآوری: برجسته‌سازی این ترکیب به‌عنوان یک نوآوری در مدیریت داده‌های ناهمگن SIoT و بهبود "بازنمایی ویژگی‌ها". این رویکرد نشان‌دهنده درک عمیق از ماهیت داده‌های SIoT است که اغلب شامل ترکیبی از انواع داده‌ها هستند.

3.3. معماری Fuzzy-DKSA و نوآوری اصلی (ادغام منطق فازی)

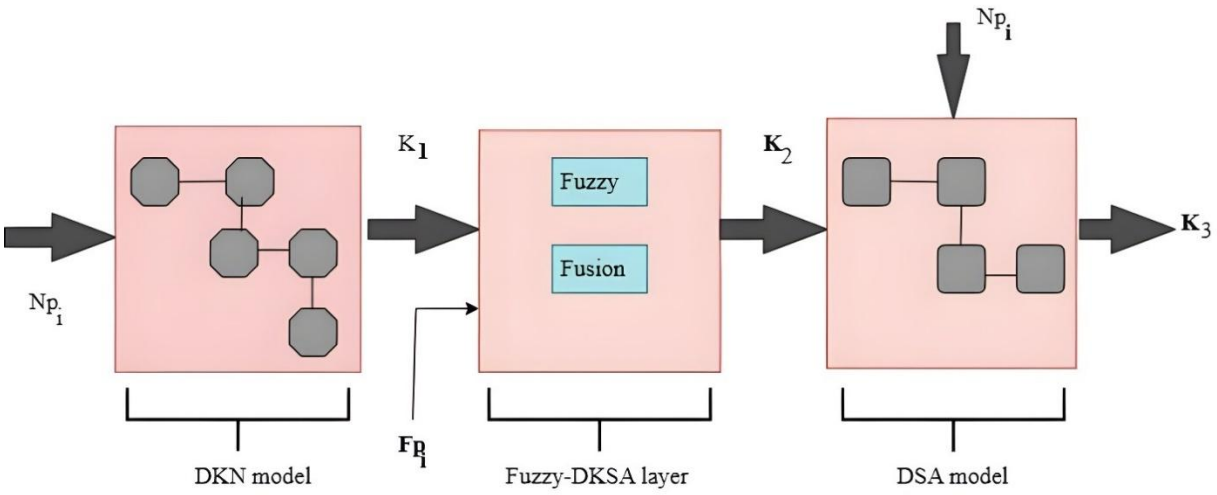
خروجی ماژول ترکیب ویژگی‌ها به ماژول تشخیص حمله ارسال می‌شود، جایی که روش پیشنهادی Fuzzy-DKSA تشخیص حمله را انجام می‌دهد. Fuzzy-DKSA از ترکیب شبکه کرونکر عمیق (DKN)، رمزگذار خودکار پشته‌ای (DSA) و مفاهیم منطق فازی ایجاد شده است.

این مدل منطق فازی را برای مدیریت نمایش‌های داده‌ای نامطمئن یکپارچه می‌کند. یک تابع عضویت فازی استفاده می‌شود:

$$\mu_{A(x)} = \frac{1}{1+e^{-\beta(x-c)}} \qquad (۱۲)$$

که در آن، β پارامتر فازی‌سازی[3]، c مرکز عضویت است.

[1] encoder-decoder
[2] bias terms
[3] fuzzification



شکل 3:طراحی شبکه Fuzzy-DKSA

تابع تصمیم‌گیری به‌صورت زیر است:

$$y = \sum_{i=1}^{N} w_i \cdot \mu_A(x_i) \qquad (۱۳)$$

که در آن wiپارامترهای وزن هستند که از طریق آموزش آموخته شده‌اند. مدل حمله را با استفاده از فعال‌سازی سیگموئید [1] طبقه‌بندی می‌کند:

$$\hat{y} = \frac{1}{1+e^{-(w_o h+b_0)}} \qquad (۱۴)$$

که در آن، W_oو b_oبه ترتیب وزن‌ها و بایاس لایه خروجی هستند.

بهینه‌سازی از تابع زیان Cross-Entropy دودویی[۲] پیروی می‌کند که به‌صورت زیر نشان داده می‌شود:

$$L = -\sum_{i=1}^{n}[y_i \log(\hat{y}_i) + (1 - y_i) \log(1-\hat{y}_i)] \qquad (۱۵)$$

که در آن، y_iبرچسب‌های واقعی را نشان می‌دهد و $\hat{y}_i$ احتمال‌های پیش‌بینی شده را نشان می‌دهد.

4. تشخیص حمله با استفاده از Fuzzy-DKSA

تغییرات قابل‌توجهی در زندگی روزمره با پیاده‌سازی گسترده‌تر اینترنت اشیا (IoT) رخ‌داده است. استقرار سریع IoT منجر به انواع مختلفی از تهدیدات سایبری شده است؛ بنابراین، تشخیص و پیشگیری از این نوع حملات بالقوه به یک حوزه موردتوجه اصلی در ارزیابی‌های پژوهشی اخیر تبدیل شده است. در این ارزیابی، یک مدل fuzzy-DKSA برای تشخیص حملات در IoT به کار گرفته شده است. مدل سامانه تشخیص شامل سه سطح است: مدلDKN ، Fuzzy-DKSA و DSA . در ابتدا، ورودی نرمال شده Npiبه DKN داده می‌شود. در اینجا، ورودی پردازش شده و به‌عنوان خروجی K_1 تولید می‌شود. این به‌عنوان ورودی به Fuzzy-DKSA و ویژگی استخراج شده F_{pi}داده می‌شود. لایه Fuzzy-DKSA حاوی گره‌های فازی و ترکیب (fusion)است که یک خروجی ترکیب شده K_2 از Fuzzy-DKSAتولید می‌کنند. K2 به DSA و داده‌های نرمال شده وارد می‌شود و منجر به نتیجه تشخیص‌داده‌شده K_3 می‌گردد. شکل ۳ طراحی شبکه Fuzzy-DKSA را نشان می‌دهد.

5. ارزیابی

این بخش سامانه پیشنهادی Fuzzy-DKSA را با ارزیابی معیارهای عملکرد مکانیزم تشخیص پیاده‌سازی شده اعتبارسنجی می‌کند. متعاقباً، تحلیل آن با سایر روش‌های تشخیص حمله تثبیت شده مقایسه می‌شود. رویکرد تازه طراحی شده-Fuzzy DKSAبا موفقیت با استفاده از نرم‌افزار MATLAB اعتبارسنجی شده است.

[1] sigmoid activation

[2] Binary Cross-Entropy Loss

5.1. معیارهای عملکرد

معیارهای اصلی در نظر گرفته شده برای ارزیابی Fuzzy-DKSA عبارت‌اند از دقت[1]، امتیاز F1 (F1-score) و پرسیژن (Precision)که در قسمت زیر به‌تفصیل شرح داده شده‌اند.

دقت، از نسبت پیش‌بینی‌های صحیح به کل نمونه‌ها محاسبه می‌شود که به‌صورت زیر محاسبه می‌شود:

$$AC = \frac{\partial_p + \mu_n}{\partial_p + \partial_n + \mu_p + \mu_n)} \qquad (۱۶)$$

که در آن TP ، TN، FP و FN به ترتیب نشان‌دهنده نمونه‌های مثبت واقعی[2]، منفی واقعی[3]، مثبت کاذب[4] و منفی کاذب[5] هستند.

معیار F (F-measure) به‌عنوان میانگین همساز[6] معیارهای پرسیژن و ریکال (Recall) محاسبه می‌شود. معیار F باFS نشان داده می‌شود که به‌صورت زیر به دست می‌آید:

$$FS = \frac{T_p}{T_p + 0.5\,(F_p + T_p)} \qquad (۱۷)$$

که در آن (بر اساس فرمول معیارF)، TP نشان‌دهنده مثبت‌های واقعی، FP نشان‌دهنده مثبت‌های کاذب و FN نشان‌دهنده منفی‌های کاذب است.

پرسیژن (Precision) به‌عنوان نسبت مثبت‌های واقعی به مجموع مثبت‌های واقعی و مثبت‌های کاذب تعریف می‌شود. پرسیژن به‌صورت زیر فرموله می‌شود:

$$\varepsilon = \frac{T_p}{T_p + F_p} \qquad (۱۸)$$

که در آن $\mathcal{E}$ نشان‌دهنده پرسیژن است، T_p نشان‌دهنده مثبت‌های واقعی و F_p نشان‌دهنده مثبت‌های کاذب است.

5.2. تحلیل عملکرد

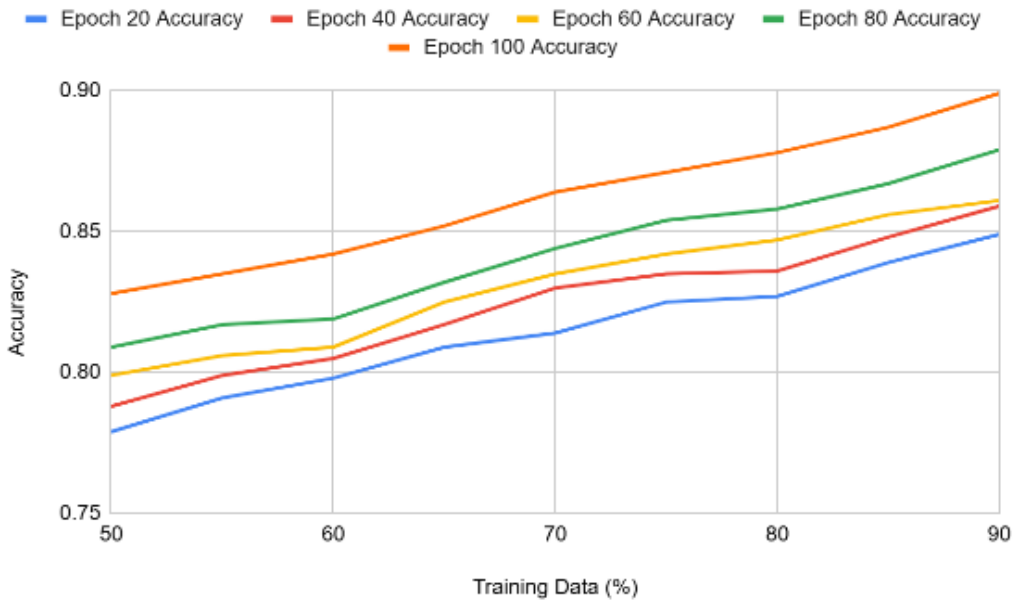
در این بخش، عملکرد مدل پیشنهادی Fuzzy-DKSA از طریق معیارهای دقت، معیار F (F-measure)و دقت پیش‌بینی (Precision)مورد ارزیابی قرار می‌گیرد. این ارزیابی با استفاده از مقادیر و درصدهای مختلف داده‌های آموزشی و نیز اعتبارسنجی متقاطع (K-fold) در تعداد تکرارهای آموزشی (Epochs) بین ۲۰ تا ۱۰۰ انجام شده است.

شکل ۴ به‌تفصیل نتایج به‌دست‌آمده از داده‌های آموزشی را نشان می‌دهد:

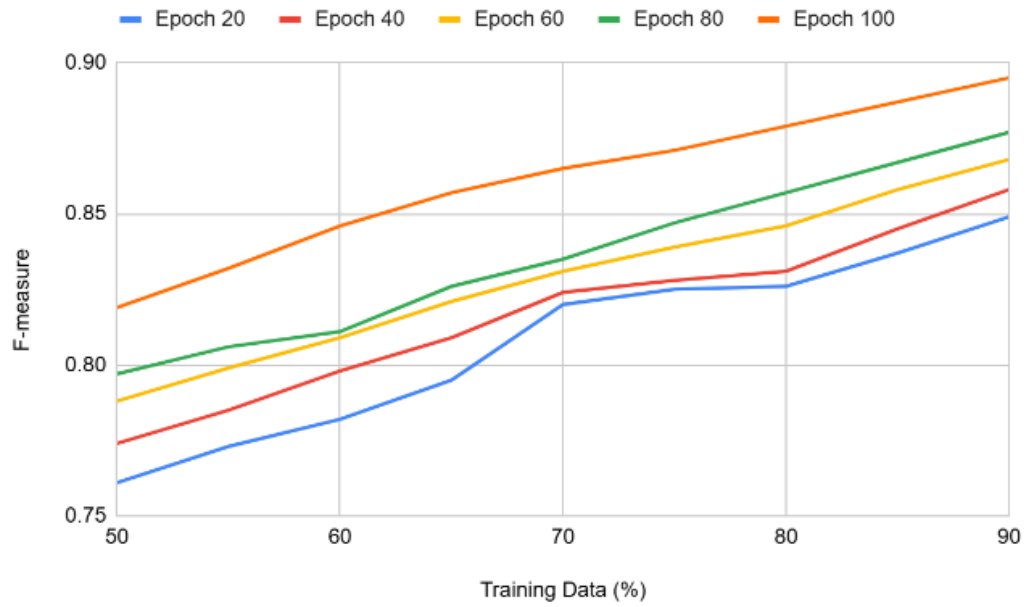
- در قسمت (الف)، ارزیابی دقت مدل Fuzzy-DKSA ارائه شده است. زمانی که ٪۹۰ از داده‌ها برای آموزش استفاده شده‌اند، دقت مدل در اپک‌های ۲۰، ۴۰، ۶۰، ۸۰ و ۱۰۰ به ترتیب برابر با ۰.۸۴۹، ۰.۸۵۹، ۰.۸۶۱، ۰.۸۷۹ و ۰.۹۰۱ بوده است.
- در قسمت (ب)، مقدار معیار اف (F-measure) مدل نمایش‌داده‌شده است. در حالت مشابه، مقدار این معیار به ترتیب برابر با ۰.۸۴۸، ۰.۸۵۸، ۰.۸۶۹، ۰.۸۷۶ و ۰.۸۹۵ ثبت شده است.
- در قسمت (پ)، دقت پیش‌بینی (Precision) مورد بررسی قرار گرفته است. در حالت استفاده از ٪۹۰ داده آموزشی، این مقدار به ترتیب برابر با ۰.۸۳۷، ۰.۸۴۸، ۰.۸۵۹، ۰.۸۷۰ و ۰.۸۹۲ در اپک‌های مختلف بوده است.

---

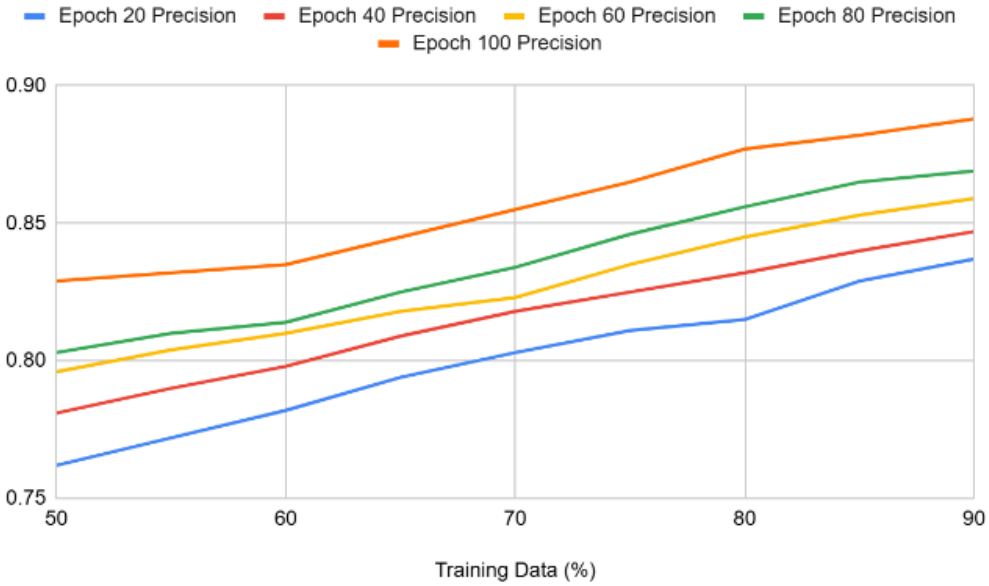
[1] Accuracy
[2] True Positive
[3] True Negative
[4] False Positive
[5] False Negative
[6] harmonic mean


Epoch 20 Accuracy
Epoch 40 Accuracy
Epoch 60 Accuracy
Epoch 80 Accuracy
Epoch 100 Accuracy
0.90
0.85
0.80
0.75
Accuracy
50
60
70
80
90
Training Data (%)

(الف)


Epoch 20
Epoch 40
Epoch 60
Epoch 80
Epoch 100
0.90
0.85
0.80
0.75
F-measure
50
60
70
80
90
Training Data (%)

(ب)

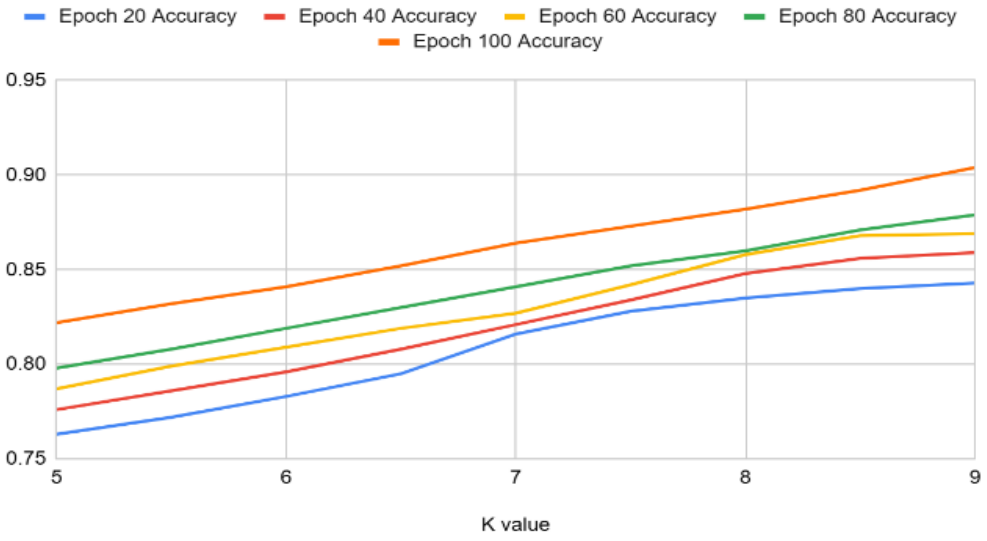


(ج)

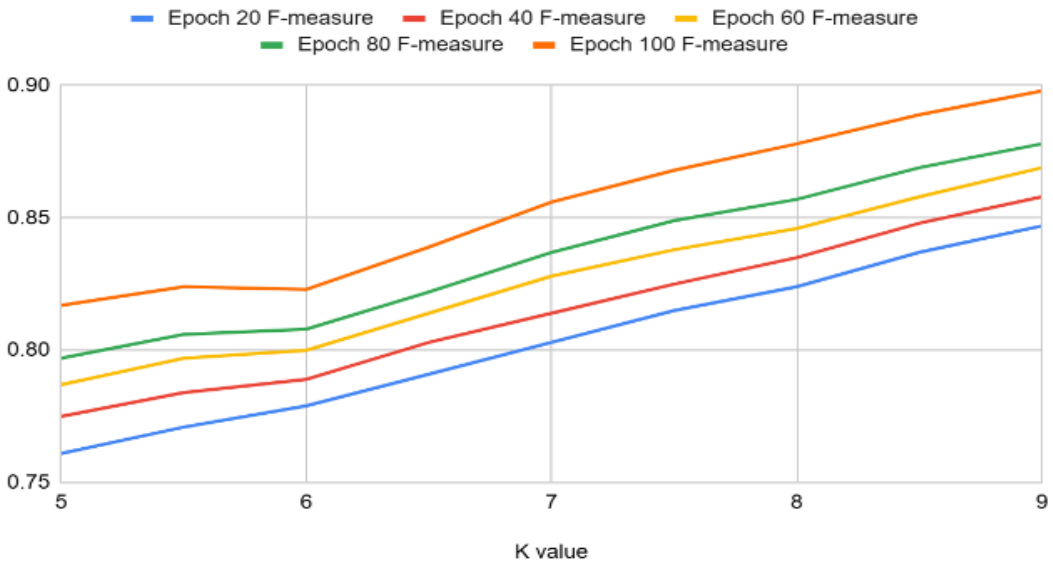
شکل ۴: ارزیابی عملکرد Fuzzy-DKSA بر اساس داده‌های آموزش: الف دقت، ب معیار F ، و ج پرسیژن.

ارزیابی بر اساس اعتبارسنجی K-fold نیز در شکل ۵ ارائه شده است. در این تحلیل، مقدار K برابر با ۹ در نظر گرفته شده و عملکرد مدل در اپک‌های ۲۰ تا ۱۰۰ مورد بررسی قرار گرفته است:

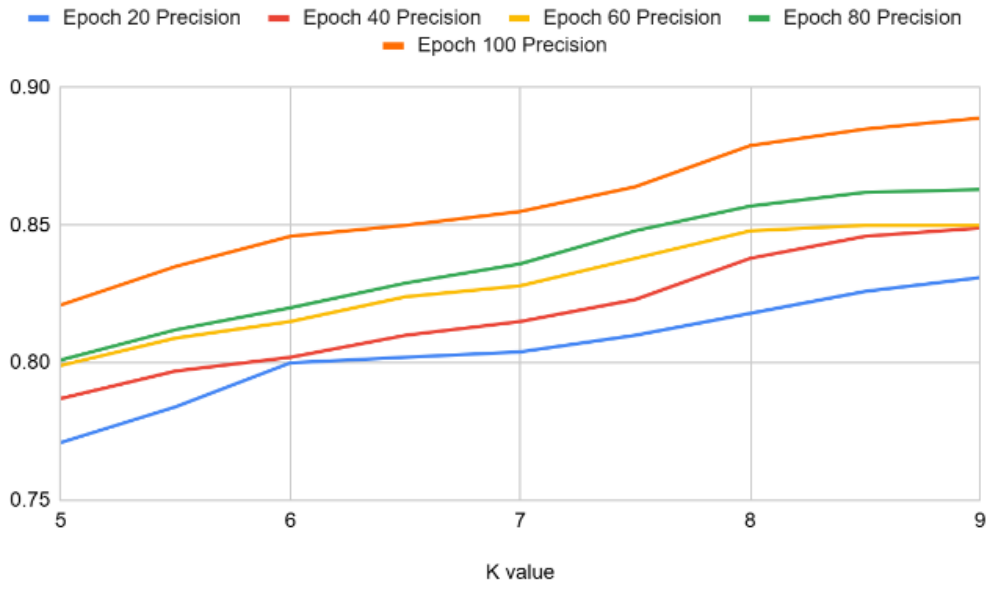
- در قسمت (الف)، دقت مدل به ترتیب برابر با ۰.۸۴۳، ۰.۸۶۰، ۰.۸۷۰، ۰.۸۸۰ و ۰.۹۰۷ ثبت شده است.
- قسمت (ب) نتایج معیار اف را نشان می‌دهد که به ترتیب برابر با ۰.۸۴۷، ۰.۸۵۷، ۰.۸۶۷، ۰.۸۷۱ و ۰.۸۹۶ بوده‌اند.
- در قسمت (ج)، مقادیر دقت پیش‌بینی به ترتیب برابر با ۰.۸۳۰، ۰.۸۵۰، ۰.۸۵۰، ۰.۸۶۲ و ۰.۸۹۱ گزارش شده‌اند.



(الف)



(ب)



(ج)

شکل ۵: تحلیل عملکرد مدل Fuzzy DKSA با اعتبارسنجی متقابل K fold: الف دقت (Accuracy)، ب معیار F1 (F measure)، ج دقت پیش‌بینی (Precision)

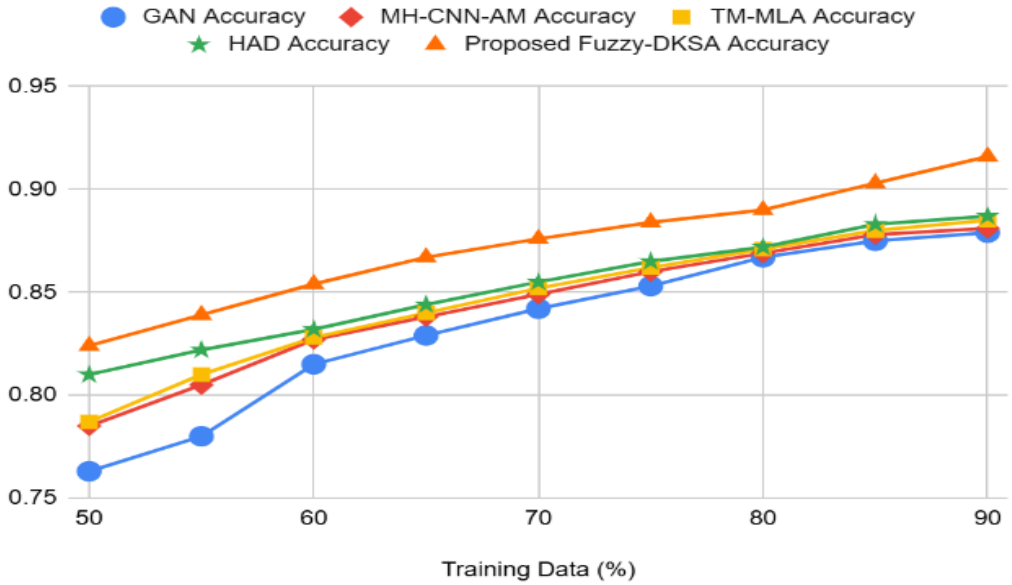
5.3. مقایسه با روش‌های موجود

در این بخش، عملکرد مدل Fuzzy-DKSA با روش‌های پیشین تشخیص حمله شامل مدل‌های GAN [17]، MH-CNN-AM [18]، TM-MLA [21] و HAD [22] مقایسه شده است. هدف از این مقایسه، ارزیابی اثربخشی مدل پیشنهادی در مقایسه با رویکردهای سنتی و مبتنی بر یادگیری ماشین است.

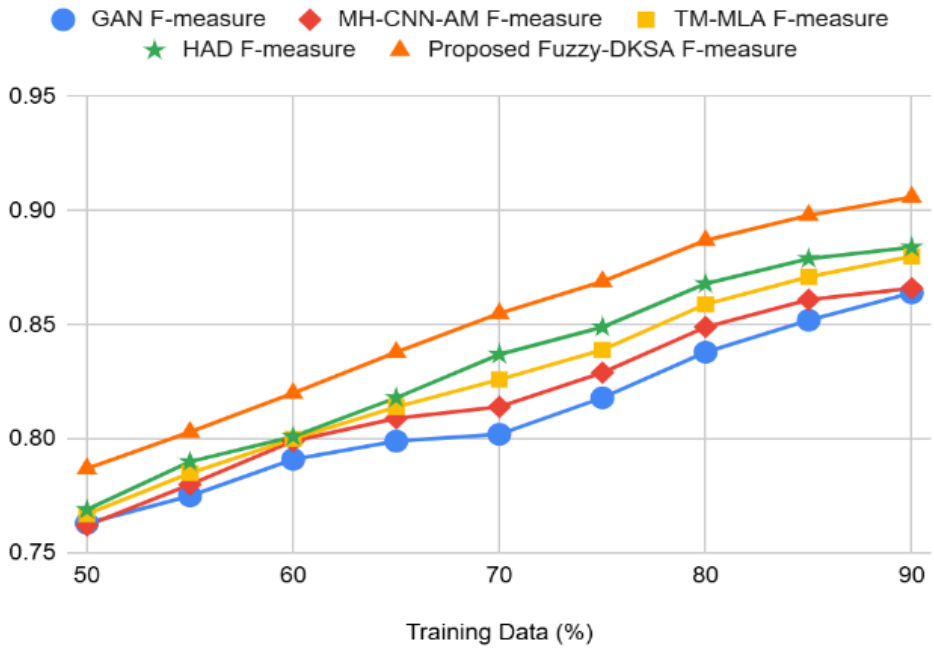
تحلیل مدل Fuzzy-DKSA بر اساس معیارهای دقت، F-measure و دقت پیش‌بینی صورت‌گرفته است:

• **شکل ۶ (الف)** نشان می‌دهد که مدل Fuzzy-DKSA در استفاده از ٪۹۰ داده آموزشی توانسته دقت ۰.۹۱۵ را به دست آورد؛ درحالی‌که مدل‌هایGAN ، MH-CNN-AM، TM-MLAو HAD به ترتیب دقت‌های ۰.۸۸۰، ۰.۸۷۹، ۰.۸۸۹ و ۰.۸۹۰ را کسب کرده‌اند. این امر نشان‌دهنده‌ی بهبود عملکرد به میزان ٪۳.۸۳، ٪۳.۹۳، ٪۲.۸۴ و ٪۲.۷۳ نسبت به مدل‌های یادشده است.

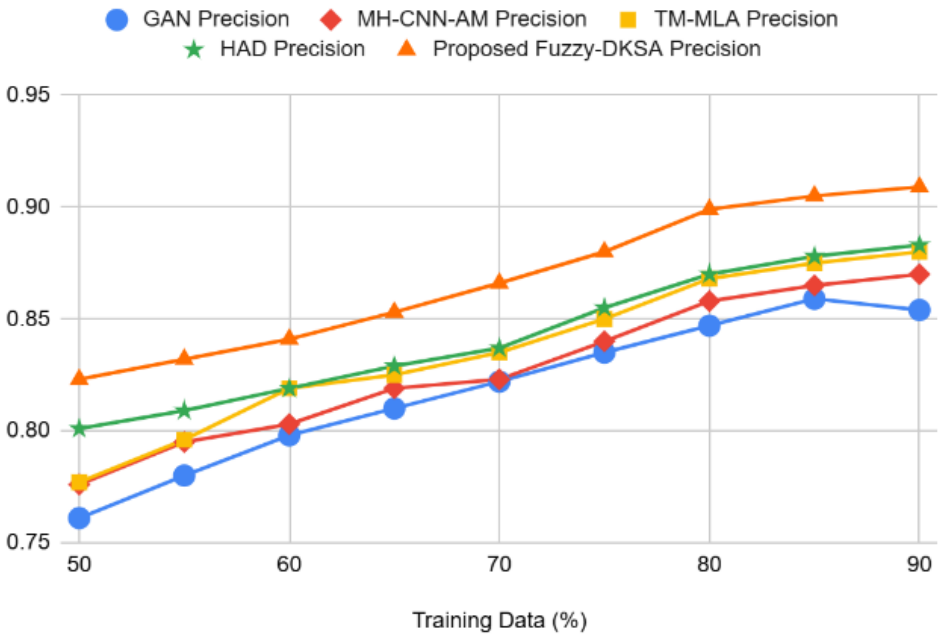
• در **شکل‌های ۶ (ب) و** (ج)، معیار F-measure نیز برای مدل Fuzzy-DKSA برابر با ۰.۹۱۵ گزارش شده، درحالی‌که این مقدار برای مدل‌های مرجع به ترتیب برابر با ۰.۸۸۰، ۰.۸۷۹، ۰.۸۸۹ و ۰.۸۹۰ بوده است. به‌این‌ترتیب، میزان بهبود عملکرد مدل پیشنهادی به ترتیب ٪۲.۲۴، ٪۴.۶۰، ٪۲.۸۶ و ٪۲.۵۱ گزارش شده است.



(الف)



(ب)



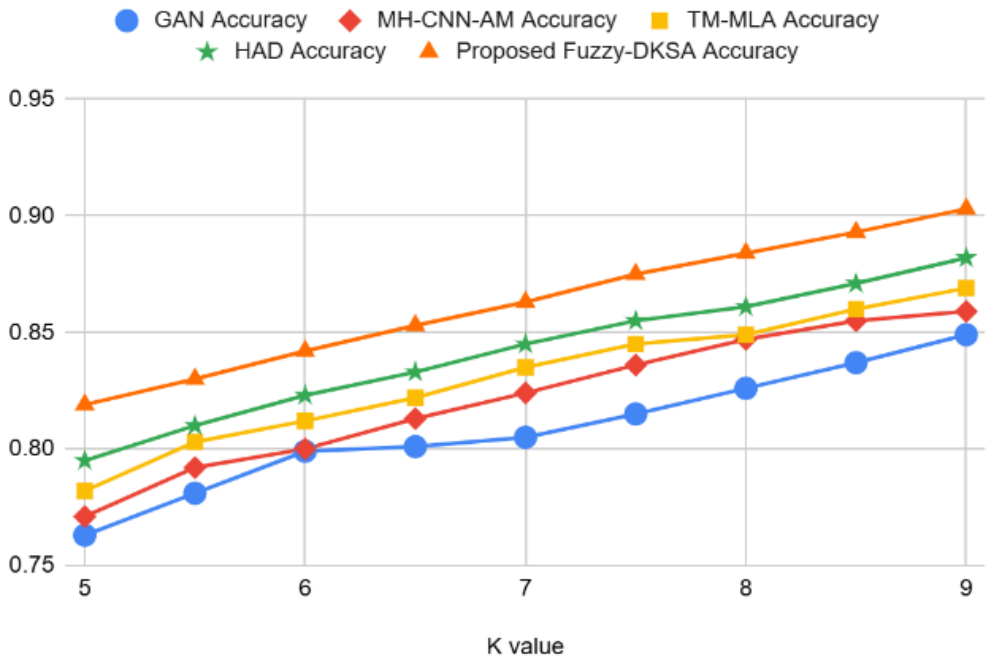
(ج)

شکل ۶: ارزیابی مقایسه‌ای مدل Fuzzy DKSA با داده‌های آموزش: الف دقت (Accuracy)، ب معیار F1 (F measure)، ج دقت پیش‌بینی (Precision)

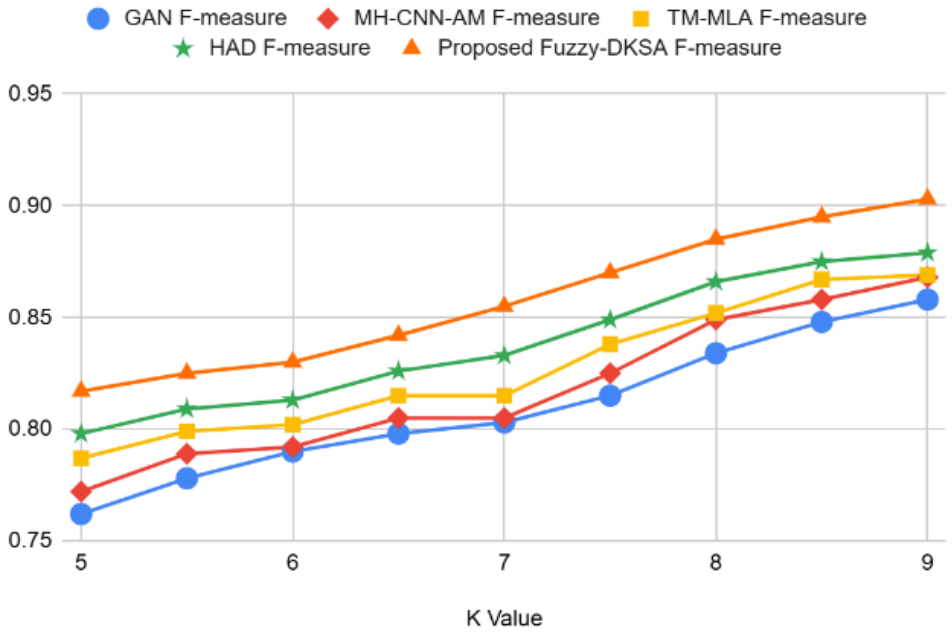
این نتایج نشان می‌دهند که مدل Fuzzy-DKSA در تمامی شاخص‌های ارزیابی عملکرد نسبت به روش‌های پیشین برتری دارد و قابلیت بالایی در تشخیص حملات در شبکه‌های اجتماعی اینترنت اشیا (Social IoT) دارد.

شکل ۷ (الف)، (ب) و (ج) عملکرد مدل Fuzzy-DKSA را در شرایط اعتبارسنجی با مقدار K برابر با ۹ نشان می‌دهد. این مدل توانسته دقت ۰.۹۰۹ را به دست آورد که بالاتر از مقادیر حاصل‌شده از مدل‌های مرجع شامل(0.849) GAN ، MH-CNN-AM (0.860)، TM-MLA (۰.۸۷۰ و HAD ۰.۸۸۱) است. این بهبود به ترتیب معادل ۶.۰۶٪، ۵.۴۴٪، ۴.۳۴٪ و ۳.۰۷٪ بوده است.

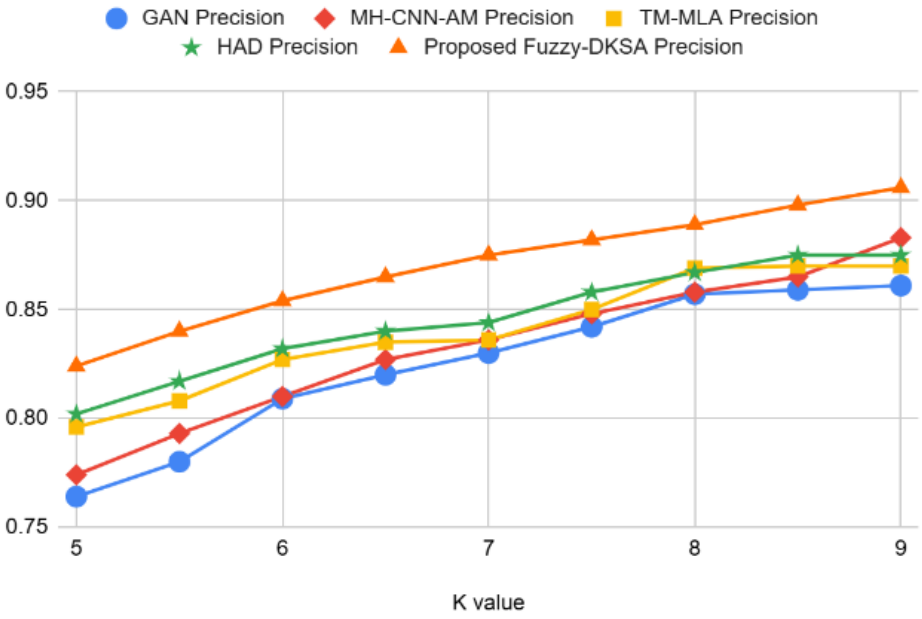
جدول ۳ نیز به‌صورت تفصیلی به مقایسه بین مدل Fuzzy-DKSA و روش‌های سنتی اشاره دارد. معیارهای ارزیابی مورد استفاده شامل دقت، F-measure و دقت پیش‌بینی هستند. نتایج نشان می‌دهد که مدل Fuzzy-DKSA با استفاده از ۹۰٪ داده آموزشی به ترتیب به‌دقت ۹۲٪، معیار F-measure برابر با ۹۱٪ و دقت پیش‌بینی ۹۱٪ دست‌یافته است که این عملکرد قابل‌توجه بیانگر اثربخشی بالای آن در زمینه تشخیص حملات در محیط‌های Social IoT است.


GAN Accuracy
MH-CNN-AM Accuracy
TM-MLA Accuracy
HAD Accuracy
Proposed Fuzzy-DKSA Accuracy
0.95
0.90
0.85
0.80
0.75
5
6
7
8
9
K value

(الف)


GAN F-measure
MH-CNN-AM F-measure
TM-MLA F-measure
HAD F-measure
Proposed Fuzzy-DKSA F-measure
0.95
0.90
0.85
0.80
0.75
5
6
7
8
9
K Value

(ب)



(ج)

شکل ۷: تحلیل مقایسه‌ای مدل Fuzzy DKSA بر اساس اعتبارسنجی K fold: الف دقت (Accuracy)، ب معیار F1 (F measure)، ج دقت پیش‌بینی (Precision)

جدول ۳: شاخص‌های عملکرد مدل پیشنهادی

مجموعه‌داده	معیارها / روش‌ها	GAN	MH-CNN-AM	TM-MLA	HAD	مدل پیشنهادی
داده‌های آموزشی	دقت	٪۸۸	٪۸۸	٪۸۹	٪۸۹	٪۹۲
	امتیازF1	٪۸۹	٪۸۶	٪۸۸	٪۸۸	٪۹۱
	دقت مثبت	٪۸۶	٪۸۸	٪۸۷	٪۸۷	٪۹۱
K-fold	دقت	٪۸۵	٪۸۶	٪۸۷	٪۸۸	٪۹۱
	امتیاز F1	٪۸۶	٪۸۷	٪۸۷	٪۸۸	٪۹۱
	دقت مثبت	٪۸۶	٪۸۸	٪۸۷	٪۸۷	٪۹۱

6. نتیجه‌گیری

در این مقاله، یک مدل نوین با عنوان رمزگشای خودکار پشته‌ای کرونکر عمیق فازی[۳۴] برای تشخیص زودهنگام حملات در محیط‌های اینترنت اشیای اجتماعی ارائه شده است. این سامانه از نرمال‌سازی Z-Score جهت مقیاس‌گذاری داده‌ها بهره برده و با استفاده از شبکه‌های عصبی عمیق تقویت‌شده با معیار شباهت گوور[۳۵]، ترکیب ویژگی‌ها را به‌صورت مؤثر انجام داده است. همچنین، با بهره‌گیری از منطق فازی، توانایی مواجهه با عدم قطعیت‌های موجود در الگوهای حمله فراهم شده است.

نتایج تجربی نشان داد که مدل پیشنهادی Fuzzy-DKSA عملکردی برتر نسبت به سایر روش‌های موجود دارد؛ به‌طوری که در ارزیابی‌ها به‌دقت ٪۹۲، معیار F1 برابر با ٪۹۱ و دقت پیش‌بینی ٪۹۱ دست‌یافته است. این نتایج نشان‌دهنده‌ی قابلیت بالای مدل در شناسایی حملات در محیط‌های پیچیده SIoT هستند.

در ادامه‌ی این مقاله، قصد داریم از معماری‌های پیشرفته‌تری در حوزه یادگیری عمیق نظیر مدل‌های مبتنی بر ترنسفورمر[۳۶] و شبکه‌های عصبی گراف[۳۷] استفاده کنیم تا توانایی شناسایی مدل را بیش‌ازپیش ارتقا دهیم. همچنین، پیاده‌سازی عملی مدل در محیط‌های متنوع SIoT به‌منظور ارزیابی مقیاس‌پذیری، کارایی محاسباتی و سازگاری با رفتار پویا در شبکه‌های واقعی مدنظر قرار خواهد گرفت. بهره‌گیری از سامانه‌های فازی تطبیقی و استراتژی‌های یادگیری پیوسته[۳۸] نیز به‌عنوان گام‌هایی در جهت

[34] Fuzzy-DKSA
[35] Gower Similarity
[36] Transformer-based
[37] Graph Neural Networks
[38] Continual Learning

افزایش انعطاف‌پذیری مدل در برابر تهدیدات نوظهور سایبری مدنظر قرار دارد.

6.1. محدودیت‌های تحقیق حاضر

باوجود دستاوردهای قابل‌توجه، مدل پیشنهادی با محدودیت‌هایی نیز همراه است:

- **پیچیدگی محاسباتی** :ادغام مؤلفه‌های مختلف نظیر DKN (شبکه کرونکر عمیق)، DSA (رمزگشای خودکار پشته‌ای) و منطق فازی، منجر به افزایش هزینه‌ی محاسباتی شده و ممکن است باعث طولانی‌تر شدن زمان آموزش و مصرف بالاتر حافظه شود.
- **وابستگی به تنظیمات پارامترها** :عملکرد مدل ممکن است نسبت به انتخاب پارامترهای فازی) مانند β، c و غیره (و ابرپارامترهای یادگیری عمیق حساس باشد. این موضوع نیازمند تنظیم دقیق پارامترها برای دستیابی به بهترین عملکرد است.
- **چالش در مقیاس‌پذیری** :در شبکه‌های IoT با تراکم بالای گره‌ها، عملکرد مؤلفه‌های DKN و منطق فازی ممکن است با محدودیت‌هایی در زمینه‌ی مقیاس‌پذیری مواجه شود.
- **احتمال بیش برازش**[39]: باوجود بهره‌گیری از DSA برای تطبیق‌پذیری دینامیک، در صورت تنوع ناکافی داده‌ها یا به‌کارگیری نامناسب روش‌های منظم‌سازی، احتمال بیش برازش در مدل وجود دارد.
- **پیاده‌سازی بلادرنگ** :اگرچه مدل باهدف تشخیص بلادرنگ حملات طراحی شده است، اما پیچیدگی ساختاری منطق فازی و لایه‌های عمیق یادگیری ممکن است در محیط‌هایی با محدودیت سخت‌گیرانه در تأخیر پاسخ، عملکرد بلادرنگ را تحت‌تأثیر قرار دهد.

مراجع

[1] R. Latif, ConTrust: A novel context-dependent trust management model in social Internet of Things, IEEE Access, 10 (2022) 46526-46537.

[2] J. Senthil Kumar, G. Sivasankar, S. Selva Nidhyananthan, An artificial intelligence approach for enhancing trust between social IoT devices in a network, in: Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications: Emerging Technologies for Connected and Smart Social Objects, Springer, 2019, pp. 183-196.

[3] T. Al-Shurbaji, M. Anbar, S. Manickam, I.H. Hasbullah, N. ALfriehate, B.A. Alabsi, A.R. Alzighaibi, H. Hashim, Deep Learning-Based Intrusion Detection System For Detecting IoT Botnet Attacks: A Review, IEEE Access, (2025).

[4] S.K. Jagatheesaperumal, Q.-V. Pham, R. Ruby, Z. Yang, C. Xu, Z. Zhang, Explainable AI over the Internet of Things (IoT): Overview, state-of-the-art and future directions, IEEE Open Journal of the Communications Society, 3 (2022) 2106-2136.

[5] S. Divya, R. Tanuja, S. Manjula, K. Venugopal, Securing Social Internet of Things: Intrusion Detection Models in Collaborative Edge Computing, in: International Conference on Frontiers in Computing and Systems, Springer, 2023, pp. 103-113.

[6] M. Rahouti, M. Ayyash, S.K. Jagatheesaperumal, D. Oliveira, Incremental learning implementations and vision for cyber risk detection in iot, IEEE Internet of Things Magazine, 4(3) (2021) 114-119.

[7] K. Sahana Devi, M. Bharathi, Hybrid intrusion detection with weighted signature generation, International Journal of Computer Applications in Engineering Sciences, 1(IV) (2011).

[8] S. Divya, R. Tanuja, S. Manjula, GAN-based autoencoder for anomaly detection in SIoT, in: Data Science & Exploration in Artificial Intelligence: Proceedings of the First International Conference On Data Science & Exploration in Artificial Intelligence (CODE-AI 2024) Bangalore, India, 3rd-4th July, 2024 (Volume 2), CRC Press, 2025, pp. 421.

[9] Y. Zhang, L. Zou, D. Pan, Cloud-Edge Collaboration Dynamics Information Dissemination Model for Social Internet of Things, IEEE Transactions on Network Science and Engineering, 10(4) (2023) 1905-1918.

[10] S. Divya, R. Tanuja, Enhancing SIoT Security Through Advanced Machine Learning Techniques for Intrusion Detection, in: International Conference on Communication and Intelligent Systems, Springer, 2023, pp. 105-116.

[11] M. Roopa, S. Pattar, R. Buyya, K.R. Venugopal, S. Iyengar, L. Patnaik, Social Internet of Things (SIoT): Foundations, thrust areas, systematic review and future directions, Computer Communications, 139 (2019) 32-57.

[12] M. Ahnaf Akif, I. Butun, A. Williams, I. Mahgoub, Hybrid Machine Learning Models for Intrusion Detection in IoT: Leveraging a Real-World IoT Dataset, arXiv e-prints, (2025) arXiv: 2502.12382.

[39] Overfitting

network community perception and social trust against Sybil attacks, International Journal of Network Management, 32(1) (2022) e2181.

[21] P. Hankare, S. Babar, P. Mahalle, Trust management approach for detection of malicious devices in siot, Tehnički glasnik, 15(1) (2021) 43-50.

[22] M.S. Mekala, G. Srivastava, J.H. Park, H.-Y. Jung, An effective communication and computation model based on a hybridgraph-deeplearning approach for SIoT, Digital Communications and Networks, 8(6) (2022) 900-910.

[23] M. Ramesh Babu, K.N. Veena, Optimal DBN ‐ based distributed attack detection model for Internet of Things, International Journal of Communication Systems, 33(17) (2020) e4595.

[24] A.A. Diro, N. Chilamkurti, Distributed attack detection scheme using deep learning approach for Internet of Things, Future Generation Computer Systems, 82 (2018) 761-768.

[25] Z. Yu, H. Deng, S. Tang, A Judging Scheme for Large-Scale Innovative Class Competitions Based on Z-Score Pro Computational Model and BP Neural Network Model, Entropy, 27(6) (2025) 591.

[26] H. Mohsen, E.-S.A. El-Dahshan, E.-S.M. El-Horbaty, A.-B.M. Salem, Classification using deep learning neural networks for brain tumors, Future Computing and Informatics Journal, 3(1) (2018) 68-71.

[27] S.-H. Cha, Comprehensive survey on distance/similarity measures between probability density functions, City, 1(2) (2007) 1.

[13] M.S. Ahsan, S. Islam, S. Shatabda, A systematic review of metaheuristics-based and machine learning-driven intrusion detection systems in IoT, Swarm and Evolutionary Computation, 96 (2025) 101984.

[14] F. Tamtam, A. Tourabi, Applying Xfuzzy for the Development of Fuzzy Logic-Based Anomaly Detection Systems in Network Security: Moroccan Agribusiness SME, International Journal of Safety & Security Engineering, 15(2) (2025).

[15] X. Zhou, Y. Wu, J. Lin, Y. Xu, S. Woo, A Stacked Machine Learning-Based Intrusion Detection System for Internal and External Networks in Smart Connected Vehicles, Symmetry, 17(6) (2025) 874.

[16] T. Hasan, A. Hossain, M.Q. Ansari, T.H. Syed, Enhanced Intrusion Detection in IIoT Networks: A Lightweight Approach with Autoencoder-Based Feature Learning, arXiv preprint arXiv:2501.15266, (2025).

[17] L. Nie, Y. Wu, X. Wang, L. Guo, G. Wang, X. Gao, S. Li, Intrusion detection for secure social internet of things based on collaborative edge computing: a generative adversarial network-based approach, IEEE Transactions on Computational Social Systems, 9(1) (2021) 134-145.

[18] R. Mohan Das, U. Arun Kumar, S. Gopinath, V. Gomathy, N. Natraj, N. Anushkannan, A. Balashanmugham, A novel deep learning-based approach for detecting attacks in social IoT, Soft Computing, (2023) 1-11.

[19] C. Marche, M. Nitti, Trust-related attacks and their detection: A trust management model for the social IoT, IEEE Transactions on Network and Service Management, 18(3) (2020) 3297-3308.

[20] G.H. de Oliveira, A. de Souza Batista, M. Nogueira, A.L. dos Santos, An access control for IoT based on