TEEGES

Technovations of Electrical Engineering in Green Energy System

Research Article (2025) 4(2):35-66

Investigating Use of Kinds of Deep Learning Methods in Internet of Things Networks Security

Hadi Mahdavinia[1], *PhD Student*, Mohammadreza Soltanaghaei[1], *Assistant Professor*, Mahdi Esmaeili[2], *Assistant Professor*

[1] *Department of Computer Engineering, Isfahan (Khorasgan) Branch, Islamic Azad University, Khorasgan, Isfahan, Iran*
[2] *Department of Computer Engineering, Kashan Branch, Islamic Azad University, Kashan, Isfahan, Iran*

Abstract:

The development of smart devices in many aspects of our daily lives is accompanied by the increasing use of appropriate mechanisms to counter them against various attacks and applications in the Internet of Things environment. In this context, it is emerging as one of the most successful and suitable techniques for use in various aspects of IoT security. The aim of this is to systematically review and analyze research studies on research eyes conducted in different Internet of Things security scenarios. The reviewed researches are classified according to different perspectives in a coherent and structured classification to identify the gap in this research area. This research has been published on articles related to the keywords "concept learning", "security" and "Internet of Things" in the four main databases IEEEXplore, ScienceDirect, SpringerLink, and ACM Digital Library. In the end, 90 articles have been selected and reviewed. These studies are conducted according to three main research questions, i.e. the security aspects involved, the network architectures used, and the datasets used in IoT security. The final discussion explores the research gaps and acknowledges the outstanding flaws and vulnerabilities in the IoT security scenario.

Keywords: Deep learning methods, Network security, Internet of things, Internet of things security, Deep learning approaches.

Received: 10 Murch 2024
Revised: 23 April 2024
Accepted: 07 August 2024
Corresponding Author: Dr. Mohammadreza Soltanaghaei, soltan@khuisf.ac.ir
DOI: http://dx.doi.org/10.30486/TEEGES.2025.1104906

فناوری‌های نوین مهندسی برق در سیستم انرژی سبز

TEEGES

مقاله مروری

بررسی استفاده از انواع روش‌های یادگیری عمیق در امنیت شبکه‌های اینترنت اشیا

هادی مهدوی نیا[۱]، *دانشجوی دکتری*، محمدرضا سلطان آقائی[۱]، *استادیار* ، مهدی اسماعیلی[۲]، *استادیار*

۱- دانشکده فنی مهندسی، واحد اصفهان (خوراسگان)، دانشگاه آزاد اسلامی، خوراسگان، اصفهان، ایران

۲- دانشکده برق و کامپیوتر، واحد کاشان، دانشگاه آزاد اسلامی، کاشان، اصفهان، ایران

چکیده: گسترش مداوم دستگاه‌های هوشمند در بسیاری از جنبه‌های زندگی روزمره ما همراه با تقاضای روزافزون برای مکانیسم‌های مناسب برای اطمینان از مقاومت آنها در برابر انواع مختلف تهدیدات و حملات در محیط اینترنت اشیا است. در این زمینه، یادگیری عمیق به عنوان یکی از موفق‌ترین و مناسب‌ترین تکنیک‌ها برای استفاده در جنبه‌های مختلف امنیت اینترنت اشیا در حال ظهور است. هدف این پژوهش، بررسی و تحلیل سیستماتیک چشم‌انداز تحقیقاتی در مورد رویکردهای یادگیری عمیق اعمال شده در سناریوهای مختلف امنیت اینترنت اشیا است. تحقیقات بررسی شده، بر اساس دیدگاه‌های مختلف در یک طبقه‌بندی منسجم و ساختاریافته به منظور شناسایی شکاف در این حوزه تحقیقاتی محوری طبقه‌بندی می‌شوند. این تحقیق بر روی مقالات مرتبط با کلمات کلیدی "یادگیری عمیق"، "امنیت" و "اینترنت اشیا" در چهار پایگاه داده اصلی IEEEXplore، ScienceDirect، SpringerLink و کتابخانه دیجیتال ACM متمرکز شده است. در پایان، ۹۰ مقاله، انتخاب و بررسی شده است. این مطالعات با توجه به سه سؤال اصلی تحقیق، یعنی جنبه‌های امنیتی درگیر، معماری‌های شبکه یادگیری عمیق مورد استفاده و مجموعه داده‌های مورد استفاده در زمینه امنیت اینترنت اشیا انجام می‌شود. بحث نهایی، شکاف‌های تحقیقاتی را که باید بررسی شوند و اشکالات و آسیب‌پذیری‌های رویکردهای یادگیری عمیق در سناریوی امنیت اینترنت اشیا را برجسته می‌کند.

واژه‌های کلیدی: روش‌های یادگیری عمیق، امنیت شبکه، اینترنت اشیا، امنیت اینترنت اشیا، رویکردهای یادگیری عمیق.

تاریخ ارسال مقاله: ۱۴۰۲/۱۲/۲۰

تاریخ بازنگری مقاله: ۱۴۰۳/۰۲/۰۴

تاریخ پذیرش مقاله: ۱۴۰۳/۰۵/۱۷

نویسنده‌ی مسئول: دکتر محمدرضا سلطان آقائی، soltan@khuisf.ac.ir

DOI: http://dx.doi.org/10.30486/TEEGES.2025.1104906

۱- مقدمه

در حال حاضر، چشم انداز اینترنت اشیا[۱] و دستگاه‌های هوشمند آن در تمام جنبه‌های جامعه انسانی در حال گسترش است[۱]، مانند بیمارستان‌های هوشمند، خانه‌های هوشمند، وسایل نقلیه هوشمند، شبکه‌های توزیع شده هوشمند[۲]، صنایع تولید هوشمند، شبکه‌های هوشمند[۳] و محیط‌های یادگیری مجازی هوشمند[۴]. با این حال، گسترش روزافزون اینترنت اشیا با چندین مسئله امنیتی مرتبط با موضوع حجم وسیع جریان‌های داده‌ای دستگاه‌های هوشمند، همراه است. در نتیجه، بسیاری از برنامه‌های کاربردی اینترنت اشیا به امنیت و حفاظت نیاز دارند که خود شامل احراز هویت دقیق[۵,۶]، تکنیک‌های طبقه‌بندی[۷] و راه‌حل‌های کافی برای تضمین محرمانه بودن و یکپارچگی است. علاوه بر این، با توجه به استفاده گسترده از دستگاه‌های اینترنت اشیا، اقدامات مخرب می‌تواند پیامدهای عمیقی بر امنیت و قدرت کل اینترنت داشته باشد. حمله سایبری راه‌اندازی شده توسط بدافزار Mirai[۲] مخصوص اینترنت اشیا، نمونه‌ای بارز از پتانسیل مخرب چنین فعالیت‌ها و گواه ضرورت اتخاذ اقدامات متقابل مناسب است[۸].

از سوی دیگر، پژوهش در یادگیری عمیق[۳] در سال‌های اخیر، شتاب بیشتری به خود گرفته است زیرا از آن برای حل با دقت بالای مشکلات مختلف استفاده می‌شود که معمولاً از طریق تکنیک‌های یادگیری ماشین سنتی مانند طبقه‌بندی، پیش‌بینی، رگرسیون و مانند آن حل می‌شدند[۹]. در واقع، یادگیری عمیق شامل گروهی از تکنیک‌های معروف یادگیری ماشین مبتنی بر شبکه‌های عصبی مصنوعی است که به فرد امکان می‌دهد پردازش اطلاعات سیستم‌های عصبی بیولوژیکی ساخته شده از لایه‌های مختلف پرسپترون[۴] را شبیه‌سازی کند[۱۰]. شبکه‌های عصبی مصنوعی در قرن گذشته ابداع شده‌اند اما اخیراً به لطف پیشرفت قدرت محاسباتی رایانه‌ها که به معماری‌های یادگیری عمیق معروف است، به طور عملی و کارآمد در زمینه‌های کاربردی مختلف مانند بینایی کامپیوتر[۱۱]، تشخیص گفتار[۱۲] و انفورماتیک سلامت[۱۳] مورد استفاده قرار می‌گیرد.

به عنوان موضوع تحقیقاتی در حال ظهور، کاربرد یادگیری عمیق در امنیت اینترنت اشیا یک زمینه تحقیقاتی بسیار داغ است که در سال های اخیر در حال رشد بوده است. یک بررسی سیستماتیک خاص در مورد رویکردهای یادگیری عمیق برای امنیت اینترنت اشیا هنوز در ادبیات مربوطه وجود ندارد، زیرا تنها موردی که یادگیری عمیق را فقط در عنوان در بر می‌گیرد، یک بررسی سیستماتیک مناسب نیست چون هیچ مدرکی از پایگاه‌های داده استفاده شده، پرس و جوهای کاربردی و تعداد مقالات بازیابی شده در آن نیز ارائه نشده است و بر روی یادگیری عمیق متمرکز نیست، بلکه بر روی یادگیری ماشین نیز متمرکز است[۱۴]. بررسی‌های اخیر دیگر در ادبیات موجود است، اما عمدتاً بر روی تکنیک‌های کلی یادگیری ماشین تمرکز می‌کنند[۱۵,۱۶] یا به یک مشکل امنیتی خاص مانند تشخیص نفوذ می‌پردازند[۱۷] یا اصلاً به امنیت اینترنت اشیا نمی‌پردازند[۱۸].

در مقابل، در این مقاله به طور خاص تمرکز بر روی رویکردهای یادگیری عمیق است زیرا این اعتقاد وجود دارد که رویکردهای مختلف یادگیری عمیق می‌توانند سناریوهای مختلف اینترنت اشیا را در مقابل فناوری‌های مختل کننده، به طور قطعی ایمن کنند؛ در نتیجه باعث تقویت پذیرش کامل و گسترده فناوری اینترنت اشیا در آینده خواهد شد.

به طور خلاصه، اهداف اصلی این بررسی سیستماتیک به شرح زیر است:

- خلاصه‌ای از آخرین دستاوردهای محققان در واکنش به نیاز حیاتی به راه‌حل‌های یادگیری عمیق در امنیت اینترنت اشیا؛
- برجسته‌ترین کاربردهای یادگیری عمیق در زمینه امنیت اینترنت اشیا.
- معماری‌های مختلف شبکه‌های عصبی عمیق[۵] استفاده شده در سناریوهای امنیتی اینترنت اشیا.
- توصیف واضح مجموعه داده‌های مورد استفاده توسط رویکردهای یادگیری عمیق در چشم انداز امنیت اینترنت اشیا.
- اشاره به مسائل محاسباتی در استفاده از تکنیک‌های یادگیری عمیق برای امنیت اینترنت اشیا.
- ارزیابی روند انتشار زمانی یادگیری عمیق استفاده شده در مبحث امنیت اینترنت اشیا.
- بررسی شکاف‌های تحقیقاتی در این زمینه.

ساختار باقی مانده مقاله به این شرح است : در بخش ۲، برخی از بررسی‌های اخیر در مورد یادگیری عمیق در زمینه امنیت اینترنت اشیا خلاصه شده است؛ در بخش ۳ معماری اینترنت اشیا و طبقه‌بندی یادگیری عمیق توضیح داده شده است. در بخش ۴، روش تحقیق به کار رفته در این بررسی سیستماتیک، به تفصیل شرح داده شده است؛ سؤالات تحقیق، پایگاه‌های داده در نظر گرفته شده، معیارهای فیلتر و همچنین ارقام مقالات شامل و حذف شده، برجسته شده است. در بخش ۵، طبقه‌بندی مقالات با توجه به سؤالات پژوهشی در

نظر گرفته شده، ارائه شده است. در نهایت، در بخش۶ بحثی از تجزیه و تحلیل انجام شده با تمرکز بر شکاف‌های تحقیق فعلی ارائه می‌شود و بخش ۷، مقاله را با خلاصه‌ای از بررسی سیستماتیک انجام شده به پایان می‌رساند.

۲- کارهای مرتبط

در این بخش، نظرسنجی‌های موجود در مورد موضوع مورد مطالعه خلاصه می‌شود و تفاوت‌ها در مقایسه با نظرسنجی پیشنهادی برجسته می‌شود. نظرسنجی‌های مورد نظر و ویژگی‌های آن‌ها در جدول شماره ۱ خلاصه شده است.

مطالعه پرداخته شده در [۱۶]، به طور خلاصه به تکنیک‌های امنیت اینترنت اشیا با استفاده از رویکردهای یادگیری ماشین می‌پردازد. با این حال، موضوع یادگیری عمیق را به صورت مختصر و جزئی بررسی می‌کند و فاقد هرگونه اطلاعاتی در مورد پرس و جوهای انجام شده، روش فیلتر کردن و پایگاه‌های اطلاعاتی پژوهشی در نظر گرفته شده است. علاوه بر این، هیچ اطلاعاتی در مورد مجموعه داده‌های مورد استفاده توسط رویکردهای یادگیری ماشین که شرح داده شده‌اند و همچنین در مورد روند انتشار زمانی برای رویکردها ارائه نمی‌کند.

برمن و همکاران[۱۸] یک نظرسنجی در مورد یادگیری عمیق در زمینه کلی امنیت سایبری ارائه می‌دهد که به طور خاص بر روی یک سناریوی اینترنت اشیا تمرکز دارد. با توجه به اینکه در این تحقیق و پژوهش، پایگاه‌های اطلاعاتی پژوهشی و پرسش‌های پژوهشی مورد استفاده، نشان داده نشده‌اند و روند زمانی انتشار تکنیک‌های مدنظر وجود ندارد، مرور سیستماتیک مناسبی نیست.

لیانگ و همکاران[۱۹] روی سه جنبه ی استفاده از یادگیری ماشین در زمینه امنیت اینترنت اشیا یعنی استفاده از یادگیری ماشین به عنوان یک اقدام متقابل در برابر حملات سایبری، یادگیری ماشین به عنوان نقطه ضعف در معرض حملات و یادگیری ماشین مورد استفاده برای انجام حملات علیه محیط‌های اینترنت اشیا تمرکز دارد. بنابراین، تمرکز این تحقیق، به درستی بر یادگیری عمیق نیست، اما این مزیت را دارد که به تمام جنبه‌های مرتبط با امنیت تکنیک‌های یادگیری ماشین در زمینه اینترنت اشیا و همچنین مسائل و چالش‌های آینده اشاره می‌کند. مزیت دوم نیز توسط [۲۰] به اشتراک گذاشته شده است که بر روی سنجش جمعیت ایمن سیار با کمک تکنیک‌های یادگیری عمیق تمرکز دارد. این مقاله همچنین برای برجسته کردن جنبه‌های مختلف امنیتی (احراز هویت، حفاظت از حریم خصوصی و غیره) سناریوی سنجش جمعیت تلفن همراه مفید است که با این حال، در زمینه گسترده‌تر اینترنت اشیا محدود است. در [۲۱] نویسندگان یک نظرسنجی در مورد یادگیری عمیق به طور کلی ارائه می‌کنند که با پلتفرم‌ها، برنامه‌ها و همچنین جهت‌های تحقیقاتی آینده سر و کار دارد. این مقاله برای درک طبقه‌بندی کلی یادگیری عمیق مفید است اما به ویژگی‌های امنیت اینترنت اشیا نمی‌پردازد. همان جنبه مثبت (یک طبقه بندی عمیق یادگیری عمیق) توسط [۱۷،۲۲] نیز مشترک است. با این حال، آنها فقط بر روی حملات خاص، یعنی تشخیص نفوذ، تمرکز می‌کنند و به طور خاص به محیط اینترنت اشیا نمی‌پردازند. همچنین کار [۲۳] تنها به حمله انکار سرویس توزیع شده[۶] می‌پردازد و به طور خاص به یادگیری عمیق نمی‌پردازد. با این حال، این مزیت را دارد که به دقت به توضیح لایه‌های اینترنت اشیا و طبقه‌بندی مسائل امنیتی اینترنت اشیا اشاره می‌کند. این اطلاعات مفید را می‌توان با انگیزه‌های حملات اینترنت اشیا در نظر گرفته شده توسط مقاله [۲۴] تکمیل کرد، که با این حال، تنها یک بررسی غیرسیستماتیک در مورد حمله انکار سرویس توزیع شده در محیط‌های اینترنت اشیا و ابر[۷] است. علاوه بر این، در [۲۵] و [۲۶] به ترتیب تنها توضیحی از مکانیسم‌های یادگیری عمیق برای شناسایی بات‌نت[۸] در محیط‌های اینترنت اشیا و به طور کلی برای کشف بدافزار ارائه می‌دهد. در نهایت، Aly و همکاران[۲۹] یک بررسی سیستماتیک جزئی ارائه می‌دهد، زیرا پرس و جوها از سؤالات تحقیق در مورد چارچوب‌های امنیتی در یک محیط اینترنت اشیا تنها با اشاره‌ای جزئی به یادگیری عمیق، مشتق نشده اند، در حالی که بررسی اخیر Ullah و همکاران[۲۷]، منتشر شده در Computer Communications، به هوش مصنوعی و یادگیری ماشین به طور کلی در بافت شهرهای هوشمند می‌پردازد و فقط یادگیری تقویتی عمیق را مورد بحث قرار می‌دهد و هیچ اطلاعاتی در مورد مجموعه داده‌های استفاده شده ارائه نمی‌دهد. علاوه بر این، این یک بررسی سیستماتیک مناسب نیست. به نظر می‌رسد مطالعه اخیر امان‌الله و همکاران[۲۸] اهداف مشابهی با اهداف این مقاله داشته باشد، اما بر روی داده‌های بزرگ و یادگیری عمیق تمرکز دارد ولی از یک فرآیند بررسی سیستماتیک مانند این مقاله پیروی نمی‌کند.

جدول (۱): مقایسه نظرسنجی‌های اخیر در مورد رویکردهای یادگیری عمیق برای امنیت اینترنت اشیا

شماره مرجع	عنوان	محل انتشار	سال	مطالعه سیستماتیک	متمرکز بر روی IoT	متمرکز بر روی یادگیری عمیق	عدم درنظرگیری حملات	توصیف مجموعه داده‌ها	مسائل
[۱۸]	A Survey of Deep Learning Methods for Cyber Security	Information	۲۰۱۹	No	No	Yes	۱۴	Yes	No
[۱۶]	IoT Security Techniques Based on Machine Learning	IEEE Signal Processing Magazine	۲۰۱۸	No	Yes	Partly	۶	No	Yes
[۱۹]	Machine Learning for Security and the Internet of Things: The Good, the Bad, and the Ugly	IEEE Access	۲۰۱۹	No	Yes	Partly	۱۷	No	Yes
[۲۰]	Secure Mobile Crowdsensing Based on Deep Learning	China Communications	۲۰۱۸	No	Partly	Partly	۸	No	No
[۲۱]	A Survey of Deep Learning: Platforms, Applications and Emerging Research Trends	IEEE Access	۲۰۱۸	No	No	Yes	-	No	No
[۲۲]	Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study	Journal of Information Security and Applications	۲۰۲۰	No	No	Yes	۱	Yes	No
[۱۷]	Review of intrusion detection systems based on deep learning techniques: coherent taxonomy, challenges, motivations, recommendations, substantial analysis and future directions	Neural Computing and Applications	۲۰۱۹	Yes	No	Yes	۱	Yes	Yes
[۲۳]	A survey of DDoS attacking techniques and defence mechanisms in the IoT network	Telecommunication Systems	۲۰۲۰	No	Yes	Partly	۱	No	Yes
[۲۴]	Distributed denial of service attacks and its defenses in IoT: a survey	The Journal of Supercomputing	۲۰۱۹	No	Yes	Partly	۱	No	Yes
[۲۵]	Forensics and Deep Learning Mechanisms for Botnets in Internet of Things: A Survey of Challenges and Solutions	IEEE Access	۲۰۱۹	No	Yes	Yes	۱	Partly	Yes
[۲۶]	A Comprehensive Review on Malware Detection Approaches	IEEE Access	۲۰۲۰	No	Partly	Partly	۱	Yes	Yes
[۲۷]	Applications of Artificial Intelligence and Machine learning in smart cities	Computer Communications	۲۰۲۰	No	Yes	Partly	-	No	Yes
[۲۸]	Deep learning and big data technologies for IoT security	Computer Communications	۲۰۲۰	No	Yes	Partly	۵	Yes	Yes
[۲۹]	Enforcing security in Internet of Things frameworks: A Systematic Literature Review	Internet of Things	۲۰۱۹	Partly	Yes	Partly	Several	No	Yes

۳- پیش‌زمینه

در این بخش، پیش‌زمینه‌ای در مورد معماری‌های اینترنت اشیا و آسیب‌پذیری‌ها و رویکردهای یادگیری عمیق ارائه می‌شود.

۳-۱- معماری اینترنت اشیا

هدف این بخش برجسته کردن ویژگی‌های سیستم‌های عمومی اینترنت اشیا و معرفی مسائل امنیتی اصلی است که چنین سیستم‌هایی ممکن است تحت تأثیر قرار گیرند. نوآوری بزرگ اینترنت اشیا در جامعه، تبدیل یک شیء معمولی به یک شیء هوشمند با بهره‌برداری از فناوری‌های ارتباطی، پروتکل‌ها و برنامه‌های کاربردی اینترنت و همچنین الگووارههای[۹] محاسباتی لبه و فراگیر است[۳۰,۳۱]. اگرچه همه سیستم‌های اینترنت اشیا مستلزم اتصال تعداد زیادی از دستگاه‌های ناهمگن هستند که به نوبه خود از الگوهای ارتباطی مختلفی مانند ماشین به ماشین، انسان به انسان یا انسان به ماشین بهره می‌برند[۳۲]. تمام معماری‌های اینترنت اشیا را می‌توان مانند شکل ۱ نشان داد. طبق شکل، معماری‌های اینترنت اشیا را می‌توان با در نظر گرفتن سه لایه عملکردی اصلی، یعنی سطح ادراک یا فیزیکی، سطح شبکه یا ارتباط و سطح کاربرد، که می‌توان آنها را بیشتر تقسیم کرد، انتزاع کرد. در بخش‌های فرعی زیر، هر سطح به اختصار خلاصه می‌شود و لایه‌های فرعی خاصی که می‌تواند از آن تشکیل شود نیز برجسته می‌شود.

۳-۱-۱- لایه فیزیکی

این لایه هم فعالیت‌های ادراک و هم قابلیت‌های اتصال سطح پایین را که توسط دستگاه‌های هوشمند مشخص می‌شود، در بر می‌گیرد. فعالیت‌های ادراک شامل کارکردهای اصلی اشیا هوشمند است که خود شامل سنجش، جمع‌آوری و پردازش می‌شود. بنابراین، این لایه شامل حسگرهایی مانند سنسورهای دما، رطوبت، حرکت و شتاب و همچنین محرک‌هایی برای اجرای اقدامات مختلف بر روی اشیا دنیای واقعی است. با توجه به ماهیت ناهمگن حسگرها، مکانیزم plug-and-play معمولاً در این سطح برای اهداف پیکربندی اجرا می‌شود[۳۳]. حسگرهای اینترنت اشیا، دستگاه‌هایی با محدودیت منابع هستند زیرا ظرفیت باتری و قابلیت محاسبات محدودی دارند. بخش بزرگی از کلان داده‌ها و جریان‌های کلان داده [۳۴] که سیستم‌های فعلی فناوری اطلاعات را شامل می‌شود، دقیقاً از این لایه اینترنت اشیا می‌آید. با این حال، داده‌های تولید شده در این سطح خام هستند و درک دقیق آن‌ها گامی کلیدی در دستیابی به یک سیستم اینترنت اشیا آگاه از زمینه است[۳۵]. در واقع، درک مؤثر داده‌های بزرگ در مورد اینترنت اشیا می‌تواند به مزایای مختلفی منجر شود، اما این معمولاً وظیفه لایه برنامه است. جنبه‌های ارتباطی در این سطح باید با ماهیت محدود منابع و قدرت محدود دستگاه‌های هوشمند در محیط‌های ارتباطی پرتلفات و پر سر و صدا کنار بیاید[۸]. بنابراین ارتباطات لایه فیزیکی نیازمند مصرف انرژی کم برای انتقال داده‌های جمع‌آوری شده توسط حسگرها است. فناوری‌های اصلی که با چالش‌های فوق‌الذکر برای ارتباطات اینترنت اشیا در این لایه مواجه هستند، شامل بلوتوث، IEEE 802.15.4، Wi-Fi، پهنای باند فوق‌العاده، RFID و ارتباطات میدان نزدیک[۱۰] است.

۳-۱-۲- لایه شبکه

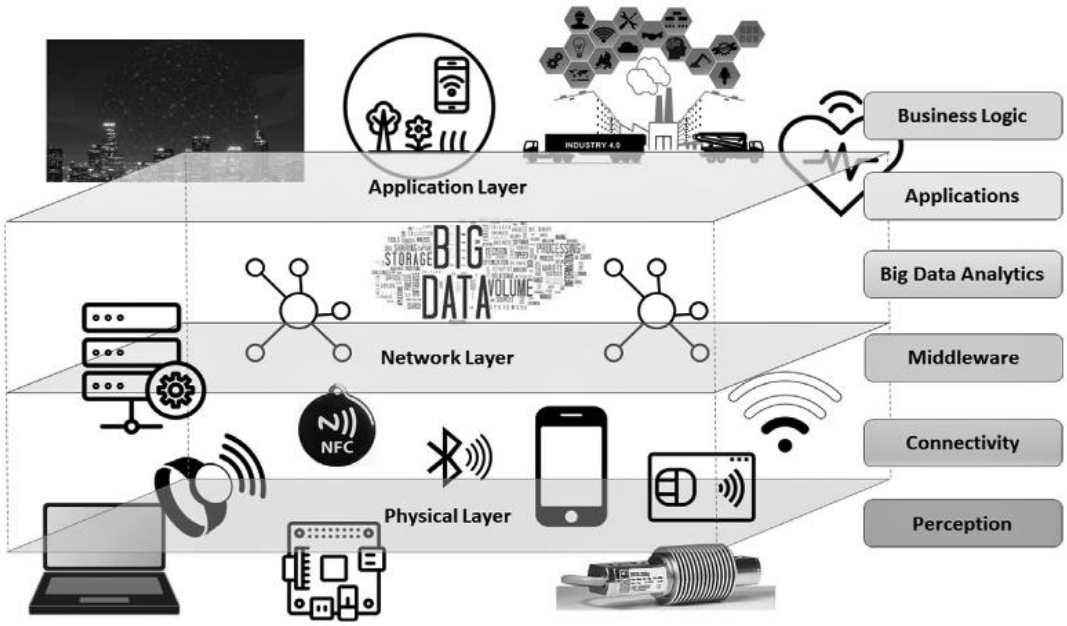
این لایه هم شامل قابلیت‌های ارتباطی و هم قابلیت‌های میان‌افزاری است. در مورد قابلیت ارتباط، ماهیت محدود دستگاه‌های اینترنت اشیا باید به دقت مورد توجه قرار گیرد. در این لایه، یکی از چالش‌های اصلی ارائه یک آدرس IP منحصر به فرد برای میلیاردها دستگاه هوشمند متصل به اینترنت است. این چالش را می‌توان به تدریج با بهره‌برداری از طرح آدرس‌دهی IPv6 بهبود داد. چالش دیگر، در مورد ارتباطات لایه شبکه، ابعاد بسته‌های در حال مبادله است و این امر با اتخاذ پروتکل‌های مناسب، قادر به ارائه قابلیت‌های فشرده‌سازی مناسب، مانند پروتکل LoWPAN6 حل می‌شود. چالش سوم بر عملکردهای مسیریابی تأثیر می‌گذارد، زیرا پروتکل‌های مسیریابی باید حافظه محدود حسگرها را در نظر بگیرند و از تحرک و انعطاف‌پذیری اشیا هوشمند پشتیبانی کنند. یکی از راه‌حل‌های ابداع شده مستلزم[۱۱](پروتکل مسیریابی برای شبکه‌های کم مصرف و کم اتلاف)، یک پروتکل مسیریابی برای شبکه‌های بی‌سیم با مصرف انرژی کم و عموماً مستعد از دست دادن بسته است. این یک پروتکل مبتنی بر بردار فاصله است و معمولاً روی کانال‌های IEEE 802.15.4 کار می‌کند و از ارتباطات چند به یک و یک به یک چند هاب پشتیبانی می‌کند[۳۶]. با در نظر گرفتن عملکردهای میان‌افزار، معمولاً به یک لایه نرم‌افزاری بین سطوح برنامه و شبکه اشاره می‌کنند که قادر به رسیدگی به مسائل ارتباطی و محاسباتی به روشی مشترک است. در یک محیط اینترنت اشیا، عملیات مفید مختلفی مانند انجام می‌شود[۳۷]:

- همکاری و قابلیت همکاری بین دستگاه‌های ناهمگن اینترنت اشیا، به طوری که اشیا هوشمند مختلف بتوانند به راحتی با یکدیگر ارتباط برقرار کنند[۳۸].
- مقیاس‌پذیری برای مدیریت بسیاری از اشیا هوشمند به طور همزمان.
- جستجوی دستگاه‌ها و محتویات.
- آگاهی از زمینه سایر اشیا اینترنت اشیا اطراف.
- امنیت ارتباطات اینترنت اشیا، به ویژه در جهت حفظ حریم خصوصی داده‌های جمع‌آوری شده و همچنین به احراز هویت خود دستگاه‌ها در یک سناریوی ماشین به ماشین.

۳-۱-۳- سطح کاربردی

بالاترین لایه معمولاً شامل تجزیه و تحلیل داده‌های بزرگ، برنامه‌های کاربردی مختلف نرم‌افزاری در دنیای واقعی و همچنین منطق هوش تجاری است. تجزیه و تحلیل داده‌های بزرگ، به تجزیه و تحلیل عمیق حجم عظیمی از داده‌های ارزشمند جمع‌آوری شده توسط اشیا در لایه فیزیکی اشاره دارد[۳۹]. داده‌های حجیم، سرعت تولید بالا و تنوع زیادی از ساختارها مشخص می‌شوند[۴۰]. برای به دست آوردن درک درست از این داده‌ها، روش‌های تحلیلی کلان داده باید در طراحی کلی اینترنت اشیا ادغام شوند، که در آن الگوریتم‌های یادگیری ماشین می‌توانند نقش حیاتی برای استخراج ارزش از داده‌های بزرگ فوق‌الذکر و تبدیل آن‌ها به اطلاعات مفید ایفا کنند. همچنین لایه برنامه شامل تمام قطعات خاص نرم‌افزار است که تعامل بین معماری کلی اینترنت اشیا و کاربران نهایی را شامل می‌شود، که این کاربران نهایی می‌تواند شهروندان ساده و یا مدیران شهرها یا کارخانه‌ها باشند.

قطعات نرم‌افزار بر اساس کاربرد خاصی که معماری اینترنت اشیا برای آن استفاده می‌شود، مشخص می‌شوند؛ به طور مثال این کاربردهای خاص شامل شهرهای هوشمند، سیستم‌های مراقبت بهداشتی هوشمند، حمل‌ونقل هوشمند، کشاورزی هوشمند، زنجیره‌های تأمین هوشمند و تولید در زمینه صنعت، شبکه‌های هوشمند، ساختمان‌های هوشمند، نظارت بر محیط هوشمند و مواردی از این دست می‌شوند. در نهایت، لایه کاربردی، قابلیت‌های هوش تجاری را نیز پوشش می‌دهد که با توجه به یک هدف تجاری خاص که معمولاً به بهبود جنبه‌های اجتماعی و اقتصادی مربوط می‌شود، به کاربران خاص ارائه می‌شود. این بخش معمولاً با تجزیه و تحلیل کلان داده‌های فوق‌الذکر به منظور شناسایی عوامل، پیش‌بینی نتایج یا پیشنهاد اقداماتی که می‌تواند نتیجه کسب و کار را بهبود بخشد یا برنامه‌های کسب و کار استراتژیک بهینه ایجاد کند، در هم تنیده می‌شود.



شکل (۱): معماری اینترنت اشیا

۳-۲- نقاط ضعف و حملات اینترنت اشیا

با توجه به توصیف یک معماری کلی اینترنت اشیا، همانطور که در بخش‌های فرعی قبلی ارائه شد، در اینجا برخی از خطرات و حملات امنیتی که محیط اینترنت اشیا مستعد آن است و همچنین برخی انگیزه‌های حمله احتمالی به صورت خلاصه بیان می‌شود. هدف حملات انکار سرویس[۱۲]، پر کردن یک سرور هدف با حجم عظیمی از درخواست‌ها برای جلوگیری از دریافت خدمات توسط دستگاه‌های اینترنت اشیا از آن است[۴۱]. یکی از خطرناک‌ترین انواع حملات انکار سرویس، حملات انکار سرویس توزیع‌شده است که زمانی اتفاق می‌افتد که مهاجمان به هزاران دستگاه اینترنت اشیا دسترسی پیدا می‌کنند و آنها را به زامبی‌های یک باتنت تبدیل می‌کنند. این امر تشخیص دستگاه‌های اینترنت اشیا قانونی از دستگاه های مخرب را برای سرور دشوار می کند، حتی اگر برخی از راه حل های مبتنی بر Honeypots ثابت کرده باشند که تا حدودی مشکل را کاهش می‌دهند، اما آنها اغلب به داده های شبیه سازی شده متکی هستند و سناریوهای توزیع شده را در نظر نمی گیرند. حملات پارازیت مستلزم ارسال سیگنال های خراب به منظور خنثی کردن انتقال رادیویی چیزهای هوشمند است. این می‌تواند عواقب بیشتری مانند کاهش پهنای باند و باتری‌ها و متعاقباً اختلال در واحدهای پردازش مرکزی و منابع حافظه خود اشیا اینترنت اشیا داشته باشد[۴۲,۴۳]. در واقع، مصرف انرژی یک جنبه بسیار مورد بهره برداری در تشخیص نفوذ همچنین برای برنامه های تلفن همراه به طور کلی است[۴۴,۴۵].

حملات جعل، شامل جعل هویت اشیا قانونی با سوء استفاده از هویت آن‌ها، به عنوان مثال، آدرس کنترل دسترسی رسانه[۱۳] یا تگ سامانه بازشناسی با امواج رادیویی[۱۴]، به منظور دسترسی به سناریوی کلی اینترنت اشیا و سپس انجام انواع دیگر اقدامات مخرب است[۴۶]. حملات شخصی میانی[۱۵] از پارازیت و جعل اقدامات مخرب به منظور استراق سمع، تغییر و نظارت مخفیانه بر ارتباطات خصوصی بین اشیا اینترنت اشیا استفاده می‌کنند[۴۷]. حملات نرم‌افزاری معرفی بدافزارها، به عنوان مثال، ویروس‌ها، کرم‌ها، تروجان و غیره را برای ایجاد فاجعه‌هایی مانند اختلال در حریم خصوصی، از دست دادن پول یا داده‌های حساس، کاهش توان، ازدحام شبکه و موارد مشابه در نظر می‌گیرند[۴۸]. برخی از راه‌حل‌های خودکار اخیر برای تسکین این حملات مستلزم کشف اشکال قطعی در تصویر میان‌افزار دستگاه‌های اینترنت اشیا یا تجزیه و تحلیل به‌روزرسانی‌های نرم‌افزاری برنامه‌های اینترنت اشیا است. با این حال، برخی محققان تاکید می‌کنند که حتی اگر نرخ منفی کاذب با توجه به رویکردهای جایگزین پایین باشد، آنها به طور کامل همه موارد اشکالات منفی کاذب را حذف نمی‌کنند. علاوه بر این، برخی دیگر از محققان، استدلال می‌کنند که روش‌شناسی آن‌ها نیازمند گسترش به تعداد بیشتری از معماری‌های اینترنت اشیا، سیستم‌های عامل و جریان‌های کاری به‌روزرسانی میان‌افزار است. آن‌ها همچنین ضرورت بررسی و تعریف سیاست‌های امنیتی جدید و جامع‌تر را برجسته می‌کنند[۴۹,۵۰]. نشت حریم خصوصی داده‌های شخصی کاربر ذخیره شده یا منتقل شده توسط اشیا هوشمند اینترنت اشیا، پوشیدنی‌ها، جمع‌آوری طیف وسیعی از اطلاعات شخصی، مانند ضربان قلب، موقعیت مکانی در سامانه موقعیت‌یابی جهانی[۱۶]، تماس‌های تلفنی دریافتی و ارسالی، پیام‌ها و موارد مشابه، معمولاً هدف مهاجمانی هستند که به این نوع اطلاعات علاقه‌مند هستند[۵۱].

۳-۳- رویکردهای یادگیری عمیق

یادگیری عمیق زیرمجموعه‌ای از تکنیک‌های یادگیری ماشین است که بر اساس شبکه‌های عصبی مصنوعی، بازتاب پردازش اطلاعات سیستم‌های عصبی بیولوژیکی واقعی و ساخته‌شده از لایه‌های مختلف پرسپترون است[۱۰]. شبکه‌های عصبی مصنوعی در قرن گذشته ابداع شده‌اند اما اخیراً به لطف پیشرفت‌ها در قدرت محاسباتی رایانه‌ها و تشویق به پذیرش معماری‌های یادگیری عمیق، ساخته‌شده از چندین لایه مرتبط، که هر یک به نوبه خود تشکیل شده‌اند، دوباره مورد توجه قرار گرفته‌اند. به طور دقیق‌تر، هر لایه، داده‌های ورودی و چکیده‌ها را دریافت می‌کند و آنها را در نوعی سلسله مراتب سازماندهی می‌کند که برای یادگیری ویژگی‌ها و همچنین طبقه‌بندی الگوهای مختلف مفید است. در مقایسه با تکنیک‌های یادگیری ماشین سنتی، الگوریتم‌های یادگیری عمیق، در زمینه‌هایی که دارای سطح بالایی از پیچیدگی هستند و توانایی دستیابی به عملکرد بسیار بالا، بسیار مناسب‌تر در نظر گرفته می‌شوند.

آموزش شبکه عصبی عمیق دارای یک ویژگی خاص است: می‌توان آن را به دو مرحله اصلی تقسیم کرد، یعنی انتشار به جلو و عقب. در حالت اول، فعال‌سازی گره‌های داخلی که نشان‌دهنده نورون‌ها یا پرسپترون‌ها هستند، طبق یک تابع فعال‌سازی مشخص، لایه‌ای به لایه، از ورودی شبکه تا خروجی آن انجام می‌شود[۵۲]. برعکس، دومی اجازه می‌دهد تا در صورت لزوم، عملکرد شبکه را با استفاده از وزن‌های به‌روز شده و مقادیر سوگیری[۱۷] به گره‌های واحد اختصاص دهیم. انواع مختلفی از شبکه‌های عصبی عمیق وجود دارد که هر یک از نظر

تعداد لایه‌ها، انواع عملیات انجام شده در لایه‌ها، اتصالات بین لایه‌ها و غیره ویژگی‌های اصلی خود را دارند. با این حال، اولین طبقه‌بندی تقریبی می‌تواند به شبکه‌های تحت نظارت عمیق مربوط به رویکردهای یادگیری بدون نظارت، ترکیبی و تقویتی باشد.

رویکردهای یادگیری عمیق تحت نظارت، پیش‌بینی‌ها یا طبقه‌بندی‌های خود را بر اساس یک نقشه‌برداری آموخته‌شده خاص بین یک نمونه و یک برچسب یا کلاس خاص که یک مدل متمایز ایجاد می‌کند، پایه‌گذاری می‌کنند[۵۳]. به عبارت دیگر، این روش‌ها قادر هستند پارامترهای ورودی (ویژگی‌ها) و خروجی مورد نیاز (کلاس) را به لطف دانش قبلی از برچسب یک نمونه خاص به هم مرتبط کنند. در ابتدا یک رویکرد نظارت شده فراهم می‌شود و سپس برای پیش‌بینی یا طبقه‌بندی یک نمونه ورودی بدون برچسب جدید استفاده می‌شود[۵۴]. این رویکردها معمولاً شامل شبکه‌های عصبی پیچشی[۱۸] و همچنین شبکه‌های عصبی تکراری[۱۹] می‌شوند. از سوی دیگر، رویکردهای یادگیری عمیق بدون نظارت می‌توانند نمایش‌های مهّم ورودی را بدون نیاز به داده‌های آموزشی از پیش برچسب‌گذاری‌شده بیاموزند و یک مدل به اصطلاح تولیدی ایجاد کنند[۵۵]. این رویکردها عموماً قصد دارند داده‌های بدون برچسب را تجزیه و تحلیل کنند تا روابط شباهت ناشناخته قبلی را در نمونه‌های آموزشی پیدا کنند و سپس با استفاده از شباهت‌های موجود در مجموعه آموزشی، نمونه‌های بدون برچسب جدید را در گروه‌های متمایز دسته‌بندی کنند. برخی از اعضای نماینده این رویکردها رمزگذار خودکار عمیق[۲۰]، ماشین‌های محدود بولتزمن[۲۱] و شبکه‌های باور عمیق[۲۲] هستند. رویکردهای یادگیری عمیق ترکیبی، ترکیبی از موارد فوق هستند که هر دو مدل متمایز و مولد را ترکیب می‌کنند. نمونه‌هایی از چنین رویکردهای یادگیری عمیق را می‌توان در شبکه‌های زایای دشمن‌گونه[۲۳] و مجموعه‌های شبکه‌های یادگیری عمیق[۲۴] مشاهده کرد.

در نهایت، یادگیری تقویتی عمیق، نهادهایی را فراهم می‌کند که طبق یک روش آزمون و خطا یاد می‌گیرند، که شامل این است که چگونه اقدامات آن‌ها می‌تواند بر زمینه اطراف تأثیر بگذارد. پاداش مشخصی پس از هر عمل تخمین زده می‌شود که کل سیستم یادگیری را بر این اساس به سمت یک حالت جدید حرکت می‌دهد. نهادها برای اقدامات خوب، پاداش و برای اعمال بد، مجازات دریافت خواند کرد[۵۶]. نمونه‌ای از این دسته، یادگیری عمیق Q[۲۵]است. در بخش‌های فرعی بعدی، انواع اصلی شبکه‌های عصبی عمیق را که در انجام بازبینی این پژوهش سیستماتیک انجام شده است، به صورت خلاصه بیان می‌شود.

۳-۳-۱- نظارت بر شبکه‌های عصبی عمیق[۲۶]

اولین نوع از شبکه‌های عصبی عمیق تحت نظارت، شبکه‌ی عصبی پیچشی است که در ابتدا برای کاهش تعداد پارامترها در تشخیص تصویر، جایگزین شبکه‌های عصبی مصنوعی سنتی شد. کاهش پارامترها، با استفاده از تعامل پراکنده، به اشتراک‌گذاری پارامتر و نمایش معادل[۹]، امکان قطع همزمان اتصالات بین لایه‌ها را فراهم می‌کند، بنابراین مقیاس‌پذیری را افزایش می‌دهد و همچنین پیچیدگی کلی زمان آموزش را بهبود می‌بخشد. اساساً یک شبکه‌ی عصبی پیچشی از دو نوع لایه ساخته شده است که معمولاً با هم تعویض می‌شوند، یعنی لایه‌های پیچش و لایه‌های ادغام. لایه پیچش مسئول پیچیده کردن پارامترهای داده با استفاده از چندین فیلتر هم اندازه هستند[۵۷]. لایه ادغام با استفاده از حداکثر ادغام (تقسیم به خوشه‌های غیرهمپوشانی و انتخاب حداکثر مقدار در هر خوشه) یا عملیات ادغام متوسط، که به عنوان نوعی نمونه‌برداری پایین[۲۷] عمل می‌کند، اندازه لایه‌های زیر را کاهش می‌دهد. کاهش پارامترها زمانی قابل مشاهده است که یک شبکه عصبی پیچشی به طور گسترده در مجموعه آموزشی اعمال می‌شود، بنابراین امکان یادگیری خودکار ویژگی‌ها از داده‌های خام با عملکرد بالا را فراهم می‌کند. با وجود این، نقطه ضعف شبکه‌ی عصبی پیچشی هزینه‌ی محاسباتی بالا است. بنابراین، پیاده‌سازی آن بر روی دستگاه‌های محدود به منابع، مانند دستگاه‌هایی که در محیط اینترنت اشیا وجود دارند، چالش‌برانگیز است و اغلب به کمک دستگاه‌های محاسباتی لبه‌ای نیاز دارد. نوع دیگری ازشبکه‌های عصبی عمیق نظارت شده، شبکه‌ی عصبی تکراری است که برای مدیریت داده‌های ورودی متوالی، به عنوان مثال: گفتار، متن، داده‌های حسگر و غیره معرفی شده است، بنابراین، در پیش‌بینی نمونه فعلی، ارتباط چند نمونه قبلی را نیز در نظر می‌گیرد. به طور خلاصه، خروجی یک شبکه‌ی عصبی تکراری به ورودی‌های حال و گذشته بستگی دارد. بنابراین، طرح سنتی پیش‌خور در این زمینه مناسب نیست، در حالی که روش انتشار به عقب کاملاً مطابقت دارد[۵۸]. ویژگی اصلی یک شبکه‌ی عصبی تکراری یک لایه، زمانی است که داده‌های ورودی متوالی را دریافت می‌کند و تغییرات چند وجهی آن را یاد می‌گیرد. این کار با استفاده از واحدهای پنهان یک سلول بازگشتی[۵۹] انجام می‌شود که وضعیت فعلی شبکه را با استفاده از تخمین وضعیت زیر به عنوان فعال‌سازی حالت قبلی توضیح می‌دهد. با این حال، نقطه ضعف اصلی یک شبکه‌ی عصبی تکراری به ناپدید شدن گرادیان[۲۸]و انفجار گرادیان[۲۹][۶۰] است که از به روزرسانی صحیح وزن‌های شبکه جلوگیری می‌کند. شبکه‌های عصبی تکراری را

می‌توان برای امنیت اینترنت اشیا، با تجزیه و تحلیل مقدار زیادی از داده‌های متوالی تولید شده توسط اشیا هوشمند اینترنت اشیا، یعنی با شناسایی تهدیدات مبتنی بر سری زمانی، استفاده کرد.

۳-۳-۲- شبکه‌های عصبی عمیق بدون نظارت

اولین نوع شبکه‌های عصبی عمیق بدون نظارت از یک رمزگذار خودکار[۳۰] ساخته شده است، که همانطور که از نام آن پیداست، هدف آن بازتولید ورودی در خروجی است. معمولاً، رمزگذار خودکار فقط یک لایه پنهان دارد که دو بخش اصلی خود را به هم می‌رساند: یک تابع رمزگذاری $h = f(x)$ و یک تابع رمزگشایی $r = g(h)$، که سعی می‌کند آن را تکرار کند[۶۱]. یکی از مزیت‌ها این است که یک رمزگذار خودکار می‌تواند به برخی از ویژگی‌های ورودی در فرآیند کپی اولویت بدهد. بنابراین، معمولاً در استخراج مجموعه کاهش یافته‌ای از ویژگی‌های مفید از داده‌های ورودی بسیار مؤثر است. یک نقطه ضعف ممکن است این واقعیت باشد که یک رمزگذار خودکار نمی‌تواند ورودی را به طور کامل بازسازی کند زیرا فقط تقریبی از آن را به سادگی با کپی کردن ورودی‌های مشابه با داده های آموزشی که قبلاً پردازش شده اند، بازتولید می‌کند. علاوه بر این، یک رمزگذار خودکار به زمان محاسباتی بالایی نیاز دارد و تنها در صورتی می‌تواند فرآیند یادگیری را پیچیده‌تر کند که مجموعه داده آموزشی در نظر گرفته شده هیچ ارتباط معناداری با مجموعه داده آزمایشی نداشته باشد. انواع دیگر شبکه‌های عصبی عمیق بدون نظارت، مدل‌های مولد عمیق مانند ماشین‌های محدود بولتزمن هستند که در آن هیچ پیوندی بین دو گره متعلق به یک لایه وجود ندارد[۶۲]. یک ماشین محدود بولتزمن از دو نوع لایه اصلی یعنی لایه‌های مرئی و پنهان ساخته شده است تا ویژگی‌های سلسله مراتبی را از داده‌های ورودی درک کند. اولی ورودی‌های شناخته شده را در بر می‌گیرد، در حالی که دومی متغیرهای پنهان را شامل می‌شود، به عنوان مثال، ویژگی‌هایی که در لایه قابل مشاهده اولیه ثبت می‌شوند، در لایه‌های متعدد دیگری پخش می‌شوند. مسائل اصلی با ماشین‌های محدود بولتزمن مربوط به پیگیری دقیق تکامل داده‌های آموزشی در طول زمان و همچنین توانایی محدود برای نمایش ویژگی‌ها است. با این حال، ماشین‌های محدود بولتزمن را می‌توان با انباشتن دو یا چند عدد از آن‌ها به منظور ایجاد نوع دیگری از شبکه‌های عصبی عمیق مولد، یعنی شبکه‌های باور عمیق، بهبود بخشید. ماشین‌های محدود بولتزمن انباشته شده، تمرینات حریصانه و بدون نظارت را به صورت لایه‌ای انجام می‌دهند تا استحکام و عملکرد کل روند تمرین را افزایش دهند. این هدف با آموزش هر لایه ماشین‌های محدود بولتزمن، یکی پس از دیگری، اجرای عملیات هر لایه در بالای لایه آموزش دیده قبلی و اعمال یک لایه SoftMax در طول مرحله تنظیم دقیق ویژگی‌ها با توجه به نمونه‌های برچسب‌گذاری شده به دست می‌آید[۶۳]. در واقع، پس از مرحله پیش‌آموزشی، یک شبکه باور عمیق به یک شبکه پیش‌خور تبدیل می‌شود که وزن‌ها را با هم‌گرایی متضاد تنظیم می‌کند[۵۹]. علاوه بر این، اگرچه همگرایی متضاد ممکن است زمان محاسباتی را کاهش دهد، این نوع شبکه‌های عصبی عمیق هنوز برای دستگاه‌های دارای محدودیت منابع چندان قابل استفاده نیستند.

۳-۳-۳- شبکه‌های عصبی عمیق ترکیبی

اولین نوع شبکه‌های عصبی عمیق که می‌تواند تحت این دسته ثبت شود، شبکه‌های زایای دشمن‌گونه است که همزمان با بهره‌برداری از یک فرآیند خصمانه، هر دو مدل تولیدی و افتراقی، آموزش می‌دهد. هدف اولی یادگیری توزیع داده‌های ورودی و همچنین ایجاد نمونه‌های داده است، در حالی که دومی سعی می‌کند با تمرکز بر این پیش‌بینی که یک نمونه از مجموعه داده‌های آموزشی می‌آید نه از نمونه‌های تولیدی که به تازگی ایجاد شده‌اند، صحت یک نمونه را ارزیابی کند. هدف اصلی مدل مولد، افزایش شانس فریب مدل افتراقی در طبقه‌بندی نمونه با تولید آن از نویز تصادفی است. از سوی دیگر، مدل تمایز، تغذیه شده توسط هر دو نمونه داده واقعی و نمونه‌های تولید شده از نویز تصادفی، وظیفه طبقه‌بندی صحیح نمونه‌های دریافت شده به عنوان ورودی از هر دو منبع را بر عهده دارد. هنگامی که عملکرد هر دو مدل اندازه‌گیری شد، به‌طور تکراری به‌روزرسانی می‌شوند تا خروجی مدل متمایز به مدل مولد کمک کند تا نمونه‌های تولید شده برای تکرار را بهبود بخشد[۶۴]. یک شبکه زایای دشمن‌گونه دارای مزایای زیادی است، که شامل موارد زیر است:

- قادر به یادگیری سناریوهای جدید مختلف است، بنابراین قادر به مقابله با حملات روز صفر[۳۱] و ارائه الگوریتم‌هایی با مجموعه‌ای از نمونه‌ها فراتر از حملات موجود است.
- برای آموزش از طریق یک رویکرد نیمه نظارتی، مناسب است.

- می‌تواند نمونه‌ها را بسیار سریعتر از یک شبکه باور عمیق کاملاً قابل مشاهده ایجاد کند. این امر به این دلیل اتفاق می‌افتد که یک شبکه زایای دشمن‌گونه یک نمونه را تنها از طریق یک گذر به مدل تبدیل می‌کند، در حالی که ماشین‌های محدود بولتزمن نیاز به تکرار یک زنجیره مارکوف برای چندین بار ناشناخته پیشینی دارند[۶۵].

از سوی دیگر، برخی از اشکالات یک شبکه زایای دشمن‌گونه این است که مرحله آموزش، خیلی پایدار نیست بلکه دشوار است و تولید داده‌های گسسته یک کار چالش برانگیز برای مدل تولیدی است[۶۴]. نوع دوم شبکه‌های عصبی عمیق هیبریدی یا ترکیبی را می‌توان در مجموعه‌های شبکه‌های یادگیری عمیق مشاهده کرد. این نوع، ادغام مشترک مدل‌های مولد، متمایز و ترکیبی یادگیری عمیق است تا به عملکرد بهتری نسبت به زمانی که به طور مستقل در نظر گرفته می‌شوند، دست یابد. مجموعه‌های شبکه‌های یادگیری عمیق، اغلب برای رویارویی با وظایفی با سطح پیچیدگی بالا، با توجه به عدم قطعیت‌های ذاتی و ویژگی‌هایی با ابعاد بالا، استفاده می‌شوند. این مجموعه ممکن است شامل هر دو طبقه‌بندی‌کننده یادگیری عمیق منفرد همگن و ناهمگن باشد که در کنار هم قرار گرفته‌اند؛ در نتیجه عملکرد و قابلیت‌های تعمیم ممکن است تقویت شوند[۶۶]. مجموعه‌های شبکه‌های یادگیری عمیق در بسیاری از برنامه‌ها از موفقیت خاصی برخوردار بوده‌اند؛ به عنوان مثال: در تشخیص فعالیت‌های مختلف انسانی، کاربرد مستقیم آن‌ها در یک سناریوی امنیتی اینترنت اشیا، پیاده‌سازی طبقه‌بندی کننده‌های نور. همچنین مجموعه‌های شبکه‌های یادگیری عمیق قابلیت اجرا در یک محیط توزیع شده را دارد.

۳-۳-٤- یادگیری تقویتی عمیق[۳۲]

یکی از نمونه‌های اصلی این دسته را می‌توان در شبکه‌های یادگیری عمیق-Q[۳۳] مشاهده کرد. این نوع، شبکه‌های عصبی(معمولاً شبکه‌های عصبی پیچشی) و الگوریتم یادگیری-Q را که به طور سنتی برای یادگیری تقویتی در سناریوهای یادگیری ماشینی قدیمی استفاده می‌شود، ادغام می‌کنند. شبکه عصبی را می‌توان به عنوان تقریبی از تابع-Q مشاهده کرد، که در آن وضعیت، به عنوان ورودی شبکه ارائه می‌شود و خروجی‌های شبکه مقادیر-Q مقدار تمام اقدامات ممکن را نشان می‌دهد[۶۷]. اقدام بعدی که باید انجام شود توسط حداکثر خروجی شبکه عصبی تعیین می‌شود که تابع تلفات آن معمولاً میانگین مربعات خطای Q-value پیش بینی شده و Q-value هدف است و کار کلی را به نوعی مشکل رگرسیونی تبدیل می‌کند که در آن هدف یا مقدار واقعی ناشناخته است زیرا این یک مشکل یادگیری تقویتی است. شبکه‌های یادگیری عمیق-Q، گرادیان خود را با استفاده از پس‌انتشار[۳۴] به روز می‌کند تا در نهایت همگرا شود. یکی از اشکالات یادگیری عمیق-Q، مسئله هدف غیر ثابت یا ناپایدار است. در واقع، در یادگیری عمیق-Q، هدف در هر تکرار، به طور مداوم در حال تغییر است، در حالی که در یادگیری عمیق سنتی، متغیر هدف تغییر نمی‌کند و از این رو آموزش، پایدار است. با این حال، یادگیری عمیق-Q همچنین می‌تواند از دو شبکه عصبی در یک ساختار بهره برداری کند: یکی برای به روزرسانی بلادرنگ و دیگری برای به روزرسانی پارامترهای همزمان در هر بازه زمانی؛ در نتیجه همگرایی الگوریتم را بهبود می‌بخشد.

٤- روش‌شناسی

روش اتخاذ شده در این مقاله، از دستورالعمل‌هایی پیروی می‌کند که باربارا کیچنهام در سال ۲۰۰۴ به آن اشاره کرد[۳۰] و شامل مراحل متوالی زیر است:

- تعریف تعداد معینی از سوالات تحقیق مرتبط.
- بازیابی برخی کلمات کلیدی از سوالات تحقیق برای ایجاد پرس و جوهای مناسب.
- تعریف پایگاه‌های داده‌ای که در آن جستجو باید انجام شود.
- تعریف برخی معیارهای فیلتر اولیه مانند فاصله زمانی جستجو، کیفیت نتایج جستجو شده و غیره.
- خلاصه عناوین و چکیده برای حذف مقالات بی‌ربط و تکراری.
- تعریف دقیق معیارهای واجد شرایط بودن و بکارگیری آن‌ها در طول مطالعه کامل مقالات باقی مانده.
- تجزیه و تحلیل مقالات باقی مانده بر اساس سوالات تحقیق که در ابتدا تعریف شده است.

٤-۱- سوالات

هدف این پژوهش بررسی وضعیت هنر یادگیری عمیق در امنیت اینترنت اشیا است. سوالات این مرور سیستماتیک به شرح زیر است:

- RQ1 : کدام مسائل امنیتی اینترنت اشیا در رویکردهای یادگیری عمیق با آن مواجه است؟
- RQ2 : کدام معماری شبکه عصبی عمیق در امنیت اینترنت اشیا استفاده می‌شود و دامنه کاربرد آن‌ها چیست؟
- RQ3 : کدام نوع از مجموعه داده‌ها در زمینه امنیت اینترنت اشیا با استفاده از رویکرد یادگیری عمیق استفاده می‌شود؟

اولین سوال با هدف بررسی این است که با اتخاذ رویکردهای یادگیری عمیق، چه نوع مسائل امنیتی اینترنت اشیا مطرح خواهد شد و موارد زیر را در نظر گرفته شده است:

۱. حفظ حریم خصوصی، مستلزم حفاظت و محرمانه بودن داده‌هایی است که توسط دستگاه‌های اینترنت اشیا جمع‌آوری و منتقل می‌شود.

۲. تشخیص ناهنجاری، که شامل شناسایی ترافیک غیرعادی در شبکه‌های اینترنت اشیا می‌شود.

۳. شناسایی بدافزار، با تمرکز بر شناسایی ترافیک مخرب خاص در شبکه‌های اینترنت اشیا که توسط ربات‌ها یا بدافزارهای خاص راه‌اندازی شده‌اند.

۴. آسیب پذیری‌های نرم‌افزار، با هدف شناسایی اشکالات و مشکلات نرم افزار اینترنت اشیا.

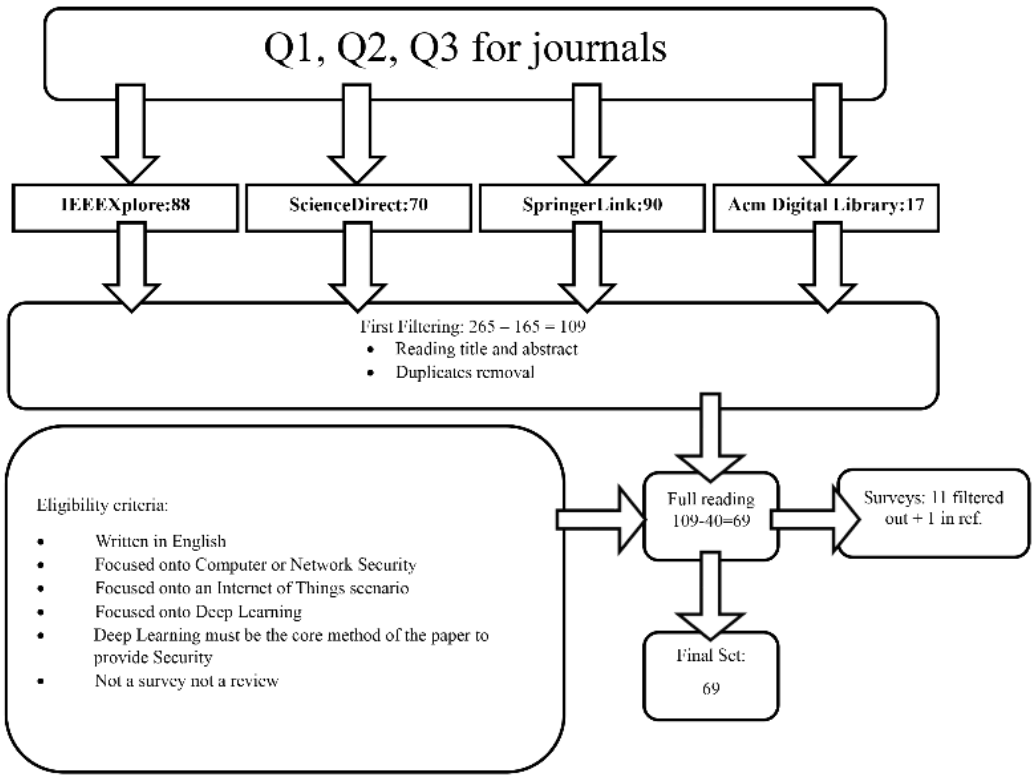
۵. حفاظت از مالکیت معنوی، به ویژه در مورد ساخت قطعات سخت افزاری و نرم افزاری اینترنت اشیا.

۶. احراز هویت و مجوز، در مورد کاربران یا ماشین‌هایی که به دستگاه‌ها یا شبکه‌های هوشمند اینترنت اشیا دسترسی دارند.

۷. شناسایی حملات خاص در محیط اینترنت اشیا، مانند حمله انکار سرویس توزیع شده، حمله جعل هویت، حمله حفره خاکستری و غیره.

۸. موارد دیگر، شامل همه مسائلی است که نمی‌توان آن‌ها را در دسته‌های قبلی برچسب‌گذاری کرد.

در مورد RQ2، به رویکردهای یادگیری عمیق ارائه شده در بخش ۳ اشاره می‌شود و همچنین یک طبقه‌بندی فرعی در مورد دامنه‌های کاربردی ایجاد شده است که در آن هر معماری یادگیری عمیق در نظر گرفته شده به کار گرفته شده است، در حالی که برای RQ3 دو دسته اصلی را در نظر گرفته شده است: مجموعه داده‌های ساخته شده از داده‌های واقعی و مجموعه داده‌های متشکل از نمونه‌های داده‌های مصنوعی یا شبیه‌سازی شده.



شکل (۲): فرآیند اتخاذ شده برای انتخاب مقاله

پرسش‌های پژوهشی فوق به پرسش‌های مناسب تبدیل شده‌اند، که سپس برای بازجویی از پایگاه‌های داده انتخاب شده شرح داده‌شده در زیربخش زیر استفاده می‌شوند. از پرس و جوهای زیر استفاده شده که در آن اعداد با سؤالات تحقیق یکسان است:

- Q1 (امنیت) و (اینترنت اشیا) و (یادگیری عمیق).
- Q2 (آموزش عمیق) و (معماری) و (اینترنت اشیا) و (امنیت).
- Q3 (آموزش عمیق) و (مجموعه داده) و (اینترنت اشیا) و (امنیت).

٤-٢- پایگاه‌های داده

جستجو جهت انتخاب مقالات از چهار پایگاه داده اصلی زیر متمرکز شده است:

- IEEEXplore، پایگاه داده مؤسسه مهندسین برق و الکترونیک (IEEE)، حاوی ادبیات فنی در مهندسی برق، الکترونیک، علوم کامپیوتر و سایر زمینه های مرتبط.
- ScienceDirect، دسترسی به مجلات و مقالات فنی و علمی منتشر شده توسط Elsevier.
- SpringerLink، که دسترسی به مقالات علمی منتشر شده توسط گروه تحریریه Springer Nature را فراهم می‌کند.
- کتابخانه دیجیتال ACM، مخزن منابع منتشر شده در زمینه محاسبات که توسط انجمن ماشین‌های محاسباتی نگهداری می‌شود.

٤-٣- فرآیند جستجو و معیارهای فیلتر

کل فرآیند جستجو و فیلتر در شکل ۲ نشان داده شده است. معیارهای گنجاندن (IC) و حذف (EC) در جدول ۲ خلاصه شده است. سؤالات شرح داده شده در بخش ۴.۱ برای پایگاه‌های داده فهرست شده در بخش ۴.۲ مقالاتی انتخاب شده‌اند که از سال ۲۰۱۳ تا ۲۰۲۰ منتشر شده بودند(IC2) . این محدوده به این دلیل انتخاب شد که قبل از سال ۲۰۱۳، رویکردهای یادگیری عمیق هنوز مورد توجه قرار نگرفته بودند. علاوه بر این، این تحقیق به مقالات منتشر شده یا در نشریات مجلات(IC1) محدود شده است، بنابراین کنفرانس‌ها و پیش چاپ‌ها را فیلتر می‌کند. این انتخاب مستلزم الزامات کیفی است که با توجه به اینکه پیش‌چاپ‌ها هنوز توسط همتایان بررسی نشده‌اند و آثار معتبر کنفرانس معمولاً در مجلات با جزئیات بیشتر و گسترده‌تر منتشر می‌شوند، برای بررسی سیستماتیک انجام شده است. اولین مرحله جستجو، در مجموع، ۲۶۵ مقاله تولید کرد که ۸۸ مقاله از IEEEXplore، ۷۰ مقاله از ScienceDirec، ۹۰ مقاله از SpringerLink و ۱۷ مقاله از کتابخانه دیجیتال ACM است. سپس، به مرحله خلاصه کردن چکیده‌ها و حذف مقالات تکراری و همچنین مقالاتی که (i)به اینترنت اشیا (EC2) نمی‌پردازند، (ii)یادگیری عمیق را به عنوان یک رویکرد اصلی (EC4) در نظر نمی‌گیرند و (iii) به امنیت رایانه یا شبکه (EC3) مرتبط نیستند، پرداخته می‌شود.

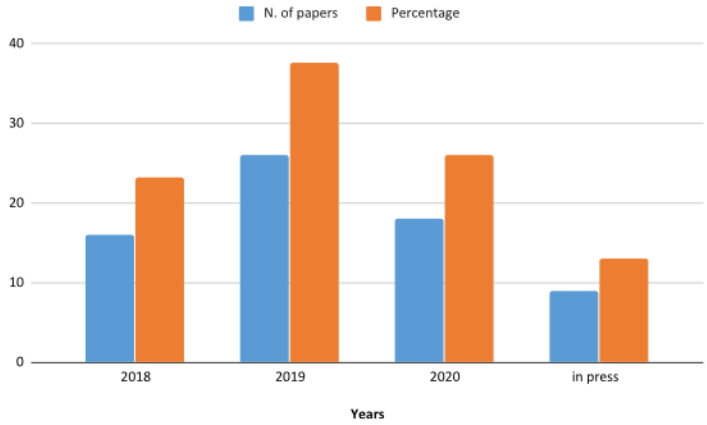
در مجموع ۱۰۹ مقاله پس از اسکن چکیده‌ها شناسایی شد. این مقالات به طور کامل برای مرحله نهایی فیلتر مطابق با معیارهای واجد شرایط بودن زیر، خوانده شده‌اند: به زبان انگلیسی (IC3) نوشته شده‌اند، بر روی امنیت رایانه یا شبکه (IC4) متمرکز شده اند، بر روی سناریوی اینترنت اشیا متمرکز شده‌اند(EC2) ، به طور خاص بر یادگیری عمیق (EC4) متمرکز بودند، یادگیری عمیق باید روش اصلی مقاله برای تأمین امنیت (IC4) باشد و مقالاتی که نظرسنجی هستند(EC1). مرحله نهایی فیلتر این امکان را می‌دهد که در مجموع ۹۰ مقاله برای تجزیه و تحلیل و استخراج و ۱۱ نظرسنجی جدید که قبلاً در بخش ۲ مورد بحث قرار گرفته اند، در نظر گرفته شوند.

در شکل ۳، توزیع زمانی مقالات باقی مانده ارائه شده است. در شکل ۴، توزیع مقالات در نظر گرفته شده در هر مکان، با توجه به مجلات IEEE، نشان داده می‌شوند. می‌توان به وضوح از این شکل استنباط کرد که مرتبط‌ترین مجلات IEEE، که در آنها مقالاتی در مورد امنیت اینترنت اشیا و یادگیری عمیق منتشر می‌شود، IEEE Internet of Things Journal و IEEE Access هستند. مقالات دیگر، کم و بیش به طور مساوی در چندین مجله دیگر توزیع می‌شوند، با برخی از نوسانات کوچک در مورد دو مجله بسیار محبوب، مانند مجله ارتباطات IEEE و IEEE Computer. توزیع مقالات در مجلات Elsevier و Springer نشان داده نشده است زیرا آن‌ها چندان مرتبط نیستند. در مورد اولی، مجلات اصلی، Future Generation Computer Systems (با ۴ مقاله از ۲۲ مقاله منتشر شده)، اینترنت اشیا و Journal of Parallel and Distributed Computing (هر دو با ۳ مقاله از ۲۲ مقاله منتشر شده) هستند. سایر مجلات فقط ۲ مقاله یا کمتر را شامل می‌شوند. از سوی دیگر، توزیع مقالات در مجلات Springer تقریباً کاملاً ثابت است؛ به طوری که اکثر مجلات تنها یک مقاله مرتبط با

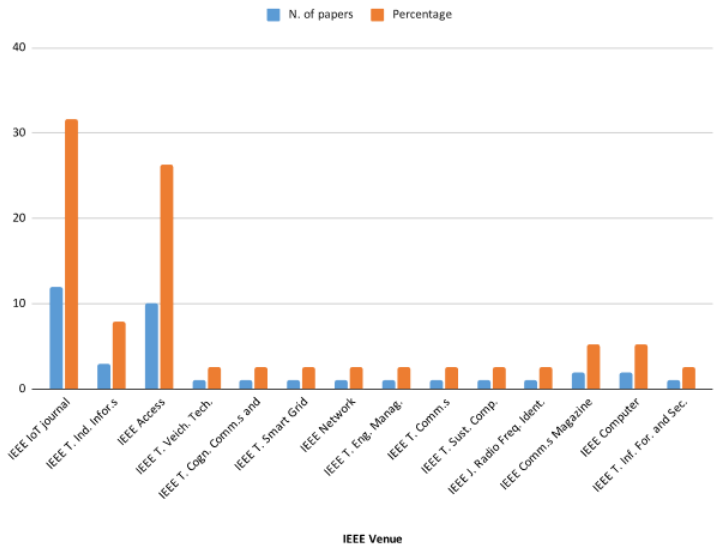
موضوع این بررسی سیستماتیک منتشر می‌کنند. تنها دو سایتی که دو مقاله مرتبط را منتشر کردند، مجله ابرکامپیوتر و مجله بین‌المللی شبکه‌های اطلاعات بی‌سیم هستند.

جدول (۲): معیارهای ورود و خروج به کار گرفته شده در فرآیند تحقیق

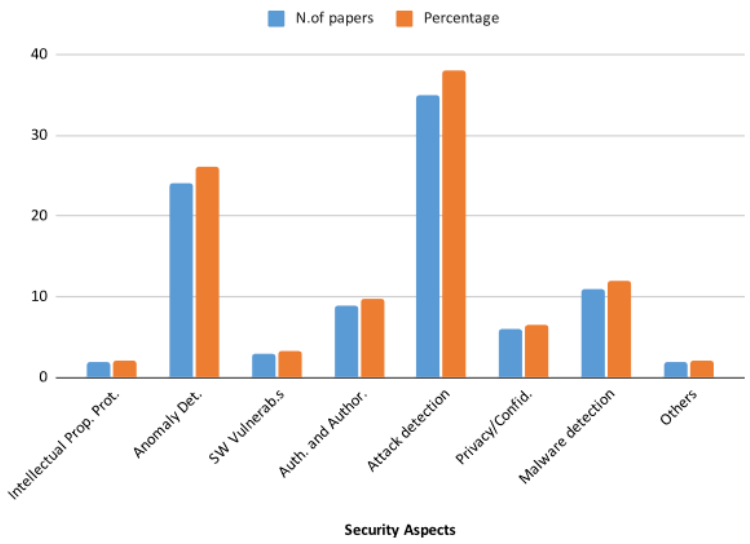
شرح مخفف‌های معیارها	
معیارهای ورودی	
مطالعات منتشر شده یا چاپ شده در مجلات	IC1
مطالعات منتشر شده در محدود سال‌های ۲۰۱۳ تا ۲۰۲۰	IC2
مطالعات نوشته شده به زبان انگلیسی	IC3
مطالعاتی که باید از یادگیری عمیق برای امنیت شبکه اینترنت اشیا استفاده کند	IC4
معیارهای خروجی	
این یک مطالعه مروری معمولی یا مروری سیستماتیک است	EC1
این مطالعه نیاز به اینترنت اشیا ندارد	EC2
این مطالعه بر روی امنیت رایانه و شبکه تمرکز ندارد	EC3
این مطالعه به طور خاص بر روی یادگیری عمیق تمرکز ندارد	EC4



شکل (۳): توزیع سالانه مقالات تحلیل شده



شکل(۴): توزیع مقالات در مجلات IEEE



شکل (۵): توزیع مقالات با توجه به جنبه‌های امنیتی

۵- نتایج

در این بخش، با توجه به طبقه‌بندی که از سؤالات تحقیق شرح داده شده در بخش ۴ الهام گرفته است، نتایج بررسی ادبیات سیستماتیک انجام شده، مورد بحث قرار می‌گیرد.

۵-۱- RQ1 با چه مسائل امنیتی اینترنت اشیا در رویکردهای یادگیری عمیق مواجه هستیم؟

اولین سوال تحقیق به توصیف جنبه‌های امنیتی با رویکردهای یادگیری عمیق در نظر گرفته شده مربوط می‌شود. این موارد را می‌توان بر اساس مسائل ذکر شده در بخش ۴.۱ طبقه بندی کرد (حفظ حریم خصوصی، تشخیص ناهنجاری، شناسایی بدافزار، آسیب پذیری‌های نرم افزار، حفاظت از مالکیت معنوی، احراز هویت و مجوز، تشخیص حمله و موارد دیگر). شکل ۵ تعداد مطلق مقالات (به رنگ آبی) و همچنین درصد وزن (به رنگ نارنجی) هر جنبه امنیتی، خلاصه می‌کند. می‌توان مشاهده کرد که اکثر مقالات (۳۸.۰۴٪) با تشخیص حمله خاص سروکار دارند، در حالی که تشخیص ناهنجاری در رتبه دوم (۲۶.۰۹٪) قرار دارد. با این حال، هر یک از این دسته‌ها شامل ۱۹ مقاله است که توسط دیگری نیز به اشتراک گذاشته شده است (به ترتیب از ۳۴ و ۲۴ مقاله). بنابراین، ممکن است تا حدی به عنوان یک ابر دسته واحد نیز در نظر گرفته شوند. مشکلات احراز هویت و شناسایی بدافزار برای جایگاه سوم رقابت می‌کنند زیرا به ترتیب ۹.۷۸٪ و ۱۱.۹۶٪ هستند. چهارمین جنبه بررسی شده مستلزم حفظ حریم خصوصی و محرمانه بودن داده‌های جمع آوری شده توسط دستگاه‌های اینترنت اشیا (۶.۵۲٪) است، در حالی که تحقیقات در مورد آسیب‌پذیری‌های نرم‌افزار کمی بالاتر از (۳.۲۶٪) جنبه‌های کمتر بررسی شده، یعنی حفاظت از مالکیت معنوی و استفاده از عمیق است. در بخش‌های فرعی بعدی، هر مقاله در نظر گرفته شده را با توجه به جنبه امنیتی خاصی که به آن می‌پردازد و با توجه به لایه درگیر معماری اینترنت اشیا که در بخش ۳ توضیح داده شده است، به اختصار بررسی می‌شوند.

۵-۱-۱- حفظ حریم خصوصی

در مورد لایه فیزیکی، در مقاله [۶۸]، نویسندگان با استفاده از ترکیبی از شبکه‌های یادگیری عمیق Q- و شبکه‌های عصبی پیچشی، به مسائل مربوط به حریم خصوصی در سنجش جمعیت می‌پردازند تا شرکت کنندگان را تشویق کنند تا داده‌های جمع‌آوری شده توسط اینترنت اشیا خود را، با اطمینان از درجه خاصی از محرمانه بودن در داده‌های خصوصی مشترک، به اشتراک بگذارند؛ در حالی که هی و همکاران [۶۹] با مشکل حفظ حریم خصوصی در سناریوی محاسباتی لبه تلفن همراه با استفاده از یک الگوریتم پیشنهادی جدید، که تکنیک‌های یادگیری وضعیت پس از تصمیم را در یک شبکه‌های یادگیری عمیق Q- معمولی ادغام می‌کند، مواجه می‌شوند. از سوی دیگر، با توجه به لایه برنامه، در مقاله [۷۰]، مشکل حفظ درجه خاصی از حریم خصوصی در ارتباطات مخفی اینترنت اشیا با استفاده از پنهان‌نگاری[۳۵] و تبدیل داده‌های اینترنت اشیا به تصاویر حل می‌شود. این با استفاده از یک طرح پنهان‌نگاری جدید، S-CycleGAN، با

بهره‌برداری از فرآیندهای تعبیه دو چرخه به دست می‌آید. برعکس، یان و همکاران[۷۱] از حریم خصوصی متفاوت برای محافظت از مجموعه داده‌های آموزشی یادگیری عمیق که از سرورهای لبه می‌آیند با ارائه خدمات پیشرفته به دستگاه‌های اینترنت اشیا نزدیک استفاده می‌کنند. این با یک شبکه عصبی پیچشی استاندارد به دست می‌آید که در آن هرس وزنی فقط در لایه‌های بالا انجام می‌شود. در نهایت، در [۷۲]، تمرکز دوباره بر روی ارتباطات داده آگاه از حریم خصوصی است، اما در این مورد مربوط به چارچوب‌های ترکیبی لبه به ابر است که در آن بخشی از شبکه عصبی پیچشی در لبه و بخشی در ابر، قرار دارد در حالی که در مقاله [۷۳]، نویسندگان بر روی یک روش پنهان‌نگاری صوتی سبک وزن تمرکز می‌کنند که می‌تواند برای دستگاه‌های هوشمند اعمال شود و از سه الگوریتم شبکه عصبی متفاوت و سبک، یعنی یک رمزگذار و رمزگشا مبتنی بر شبکه‌های زایای دشمن‌گونه و یک شبکه عصبی پیچشی متمایز، استفاده می‌کند.

۵-۱-۲- تشخیص ناهنجاری

اکثر مقالاتی که به مسائل تشخیص ناهنجاری می‌پردازند، به تشخیص ترافیک غیرعادی شبکه مربوط می‌شوند. تنها پنج مورد به جنبه‌های مختلف ناهنجاری مانند ناهنجاری‌های انرژی(۳ مورد)، ناهنجاری‌های زمینه‌ای(۱ مورد) و ناهنجاری‌های نامشخص(۱ مورد) می‌پردازند. در این بخش فرعی، فقط مقالاتی توصیف می‌شوند که می‌توانند در دسته تشخیص ناهنجاری عمومی قرار بگیرند و مقالات مربوط به حملات خاص به بخش ۵.۱.۷ موکول می‌شوند. هیچ مقاله ای مربوط به تشخیص ناهنجاری در لایه فیزیکی وجود ندارد. فقط یک مقاله را می‌توان در لایه شبکه قاب کرد که مقاله [۷۴]، مقابله با مسائل تشخیص نفوذ برای سناریوی لبه‌ای از اشیا در شبکه‌های تعریف شده نرم‌افزار برای اینترنت اشیا را بررسی می‌کند. سه مقاله را می‌توان به عنوان بخشی از لایه کاربرد قاب کرد: نویسندگان در [۷۵] با استفاده از یک الگوریتم طبقه‌بندی لولای نوآورانه بر اساس نزول گرادیان دسته‌ای کوچک با سرعت و حرکت تطبیقی یادگیری، ناهنجاری شبکه اینترنت صنعتی اشیا[۳۶] را تشخیص می‌دهد؛ نویسندگان در [۷۶]، با تشخیص نفوذ سنتی برای دستگاه‌های لبه در یک سناریوی صنعتی اینترنت اشیا مقابله می‌کنند؛ در مقاله [۷۷]، مشکل تشخیص ناهنجاری برای پیش‌بینی ناهنجاری‌های زمینه‌ای جمعی در لایه کاربرد با استفاده از ترکیبی نوآورانه از یادگیری عمیق نیمه‌نظارت‌شده، مدل‌سازی سری‌های زمانی و تجزیه و تحلیل گراف را مورد بررسی قرار می‌دهد.

۵-۱-۳- شناسایی بدافزار و بات نت

کار در [۷۸] بر شناسایی بدافزار و ترافیک شبکه خوش‌خیم[۳۷] از طریق هر دو رویکرد باینری و چند طبقه‌بندی متمرکز است. این تنها سهمی است که با بدافزارها در سطح شبکه مورد توجه قرار می‌گیرد و از جمله مواردی است که در این بررسی سیستماتیک مد نظر قرار گرفته شده است. علاوه بر این، این تنها شبکه‌ای است که از شبکه‌های کپسولی اخیراً معرفی‌شده بهره‌برداری می‌کند و امکان ادغام طبقه‌بندی و استخراج/انتخاب ویژگی‌ها را فراهم می‌کند. در رابطه با سطح برنامه، مقاله [۷۹] سعی می‌کند تا با استفاده از توالی‌های کد دستور[۳۸] قطعات بدافزار را شناسایی کند، مشابه آنچه در [۸۰] انجام شد، که در آن شکار تهدید بدافزار با تجزیه و تحلیل OpCode ARM 32 بیتی انجام می‌شود. نمونه‌های بدافزار مبتنی بر برعکس، مطالعه شده در [۸۱] با بهره‌برداری از بایت کدهای خام فایل‌های Android class.dex و دو مدل جدید یادگیری عمیق، یعنی DexCNN و DexCRNN، که مدل دوم شبکه‌های عصبی پیچشی و تکراری را ترکیب می‌کند، همین هدف را دارد. در [۸۲]، نویسندگان سعی می‌کنند با استفاده از یک رویکرد بدون نظارت، تهدیدات و حملات ناشی از نرم‌افزارهای مخرب را شناسایی کنند که می‌توانند سیستم کنترل صنعتی را با استفاده از دستگاه‌های اینترنت اشیا مبتنی بر ابر، دستکاری کنند. مقاله [۸۳]، ابزاری خودکار و توزیع‌شده برای شناسایی قطعات بدافزار اندروید در دستگاه‌های اینترنت اشیا را ارائه می‌کند؛ این ابزار از دنباله‌های خام فراخوانی متد API یک برنامه اندروید برای استخراج الگوهای مخرب یا خوش‌خیم سوء استفاده می‌کند که MalDozer نامیده شده است. کار مشابهی در [۸۴] با استفاده از مجموعه داده‌های مختلف و معماری‌های یادگیری عمیق یعنی ترکیبی از یک شبکه عصبی قوی و یک شبکه عصبی پیچشی، انجام شده است. در نهایت، مقاله [۸۵]، به شناسایی بدافزار اندروید از منظر حملات برچسب‌زنی و استفاده از رویکردی نوآورانه، مبتنی بر شبکه‌های عصبی پیچشی نیمه نظارت شده می‌پردازد. در مقاله [۸۶]، نویسندگان سعی می‌کنند بدافزارهای مؤثر بر سیستم‌های مراقبت سلامت الکترونیک را که از دستگاه‌های هوشمند اینترنت اشیا و ترکیبی از شبکه‌های یادگیری عمیق-Q و شبکه‌های عصبی پیچشی بهره‌برداری می‌کنند، شناسایی کنند در حالی که در [۸۷] کار مشابهی با تبدیل کدهای باینری به تصاویر انجام می‌شود.

۵-۱-٤- تشخیص آسیب‌پذیری نرم‌افزار

مقالات مربوط به شناسایی خاص آسیب‌پذیری‌های نرم‌افزار فقط لایه برنامه را شامل می‌شود. در [۸۸]، مشکل تشخیص خودکار آسیب‌پذیری‌های کد باینری به عنوان یک کار طبقه‌بندی باینری، با استفاده از توابع باینری به عنوان ویژگی‌ها حل می‌شود. در [۸۹]، نویسندگان با استفاده از یک معماری یادگیری معنایی دو سطحی جدید، با ترکیبی از شبکه‌های توجه گراف و شبکه‌های عصبی متراکم، باگ‌ها و آسیب‌پذیری‌ها را در کدهای مونتاژ معماری متقابل مقیاس بزرگ جستجو می‌کنند. در [۹۰]، محلی‌سازی خودکار آسیب‌پذیری‌های نرم‌افزار اینترنت اشیا با استفاده از مسیرهای انتشار لکه‌ای که از طریق تجزیه و تحلیل لکه‌های استاتیک به دست می‌آیند، پرداخته می‌شود.

۵-۱-۵- حفاظت از مالکیت معنوی

در خصوص دفاع از مالکیت معنوی، دو مقاله را می‌توان از جمله مواردی که بررسی شده، در نظر گرفت. مقاله [۹۱]، مورد اول است که با تأیید مالکیت و حق چاپ مدارهای الکترونیکی اینترنت اشیا با کمک واترمارک‌های مجازی مناسب، که به صورت تطبیقی در موقعیت‌های مناسب قرار گرفته‌اند، مشکل را در لایه فیزیکی حل می‌کند. راه حل پیشنهادی کاملاً نوآورانه است، با توجه به اینکه از یک تکنیک یادگیری تقویتی عمیق برای ایجاد موقعیت‌های واترمارک شده به صورت تطبیقی و تشخیص درستی واترمارک مالکیت معنوی مناسب استفاده می‌کند. علاوه بر این، از نظر سرعت تشخیص واترمارک و کاهش سربار به نتایج بسیار خوبی دست می‌یابد. مورد دوم مقاله [۹۲] است که به مشکل در لایه برنامه می‌پردازد؛ سعی می‌کند نرم‌افزارهای غیرقانونی و همچنین سرقت ادبی کد منبع را با کمک تکنیک‌های توکن‌سازی و وزن‌دهی نشان دهد. راه حل پیشنهادی همچنین قادر به شناسایی بدافزار از طریق تجسم تصویر رنگی است، بنابراین در دسته‌بندی مربوطه نیز در نظر گرفته می‌شود، حتی اگر تنها یک بار در این بخش توضیح داده شود.

۵-۱-٦- احراز هویت و مجوز

مقاله‌های مربوط به احراز هویت یا مجوز، ۹ مقاله هستند که یک مقاله با دسته شناسایی بدافزار مشترک است. اکثر مطالعات در نظر گرفته شده بر روی لایه فیزیکی اینترنت اشیا متمرکز شده اند. در حقیقت، در مورد لایه فیزیکی، در [۹۳]، نویسندگان سعی می‌کنند با بهره‌گیری از ویژگی‌های اثر انگشت فرکانس رادیویی[۴۹]استخراج شده از طریق ارقام ردیابی صورت فلکی دیفرانسیل برای کانال‌های ZigBee واقعی، شناسایی اثر انگشت فرکانس رادیویی را انجام دهند. این امر با یک رویکرد جدید که شبکه‌های عصبی پیچشی را با شکل ردیابی صورت فلکی دیفرانسیل ترکیب می‌کند، به دست می‌آید که منجر به دقت شناسایی بالا و پیچیدگی کم می‌شود. همین کار در [۹۴]، با بهره‌برداری از نقص‌های خاص سخت‌افزار تحمیل‌شده بر نمونه‌های I/Q کانال‌های Wi-Fi، با یک شبکه پیچشی نسبتاً استاندارد، انجام می‌شود. در [۹۵]، احراز هویت چند کاربر را برای شناسایی حملات جعل در شبکه‌های بی‌سیم با بهره‌برداری از اطلاعات وضعیت کانال فراهم می‌کند. برعکس، در [۹۶] از واترمارکینگ ویژگی فیزیکی برای انجام احراز هویت سیگنال پویا در محیط‌های عظیم اینترنت اشیا، با استفاده از الگوریتم حافظه طولانی کوتاه مدت[۴۰] و تقویت عمیق استفاده می‌شود که به نویسندگان اجازه می‌دهد تا تقریباً ۱۰۰٪ قابلیت اطمینان را به دست آورند. نویسندگان [۹۷] مشکل احراز هویت بلادرنگ را از طریق توابع غیرقابل کلون فیزیکی برای شناسایی منحصر به فرد تراشه‌های دستگاه‌های اینترنت اشیا با استفاده از ویژگی‌های سیلیکونی آن‌ها، که تکرار آن تقریباً غیرممکن است، بررسی می‌کنند. مقاله [۹۸] بر روی شناسایی فرستنده فرکانس رادیویی، با استفاده از ویژگی‌های شکل موج مدولاسیون تقسیم فرکانس عمودبرهم[۴۱] با توجه به سطح کاربرد متمرکز است. مقاله [۹۹] وظیفه احراز هویت را با استفاده از ویژگی‌های صوتی تنفس انسان برای دستگاه‌های اینترنت اشیا با منابع محدود می‌کند در حالی که نویسندگان مقاله [۸۶] هم به احراز هویت و هم تشخیص بدافزار در سیستم‌های مراقبت بهداشتی مبتنی بر اینترنت اشیا می‌پردازند. در نهایت، مقاله [۱۰۰] با احراز هویت لایه برنامه با استفاده از تشخیص چهره مبتنی بر ویژگی‌های بصری در محیط‌های هوشمند اینترنت اشیا سروکار دارد.

۵-۱-۷- تشخیص حمله خاص

کارهایی که با تشخیص حمله خاص سروکار دارند و می‌توانند در لایه فیزیکی قاب شوند، پنج مقاله است. مقاله [۱۰۱] به حملات فیزیکی-سایبری مختلف با توجه خاص به کشف رفتارهای مصرف انرژی طبیعی و غیرعادی می‌پردازد. به طور مشابه، لی و همکاران

[۱۰۲] با نظارت بر ناهنجاری‌ها در خواندن داده‌های مصرف انرژی از طریق معماری یادگیری عمیق دوگانه، حملات فیزیکی-سایبری را شناسایی می‌کنند. همچنین مقاله [۱۰۳] در یک زمینه مخرب بات‌نت، با حملات فیزیکی-سایبری مختلف مقابله می‌کند. از سوی دیگر، کار در [۱۰۴] تشخیص رفتارهای غیرعادی را در سطح فیزیکی با اندازه‌گیری استفاده از CPU، استفاده از دیسک و غیره ارائه می‌کند. در نهایت، در [۱۰۵] نویسندگان موفق به مبارزه با حملات جعل هویت در سناریوهای بی‌سیم باز، با استفاده از یک روش جدید شدند؛ روش استخراج و انتخاب با ویژگی عمیق که یک رمزگذار خودکار پشته‌ای را با حداکثر دو لایه پنهان و یک شبکه عصبی مصنوعی نهایی برای طبقه‌بندی نهایی در مجموعه‌ای از ویژگی‌ها ادغام می‌کند. در لایه شبکه، مطالعات متعددی در میان مواردی که انتخاب شده‌اند وجود دارد. گوو و همکاران تشخیص ناهنجاری‌ها در برابر حملات انکار سرویس توزیع شده و حفره‌های خاکستری را با استفاده از یک پروتکل مسیریابی جدید برای شبکه‌های تعریف‌شده نرم‌افزاری که از یادگیری تقویتی عمیق بهره‌برداری می‌کند و آگاهی از کیفیت خدمت[۴۲] را فراهم می‌کند[۱۰۶]. نتایج ارائه شده در [۱۰۷]، به مشکل تشخیص ناهنجاری در مورد حملات انکار سرویس توزیع شده نیز می‌پردازد، اما از دستگاه‌های زامبی می‌آید. نویسندگان از ترکیبی جدید از شبکه‌های عصبی پیچشی و رمزگذارهای خودکار برای استخراج ویژگی‌های جریان مناسب استفاده می‌کنند که نزدیک به ۱۰۰ درصد دقت را به دست می‌آورند. همچنین در [۱۰۸] و [۱۰۹] جنبه امنیتی اصلی، تشخیص حملات انکار سرویس توزیع شده، با تمرکز ویژه بر روی شبکه‌های صنعتی اینترنت اشیا و شبکه‌های تعریف‌شده نرم‌افزاری برای اینترنت اشیا است. در [۱۰۸]، نویسندگان یک رمزگذار خودکار عمیق و یک شبکه عصبی رو به جلو عمیق را ادغام می‌کنند در حالی که در [۱۰۹]، از یک شبکه باور عمیق ساده که در یک شبکه اختصاری تعریف شده نرم افزاری ادغام می‌شود، استفاده می‌شود.

به طور مشابه، Ujjan و همکاران با ادغام Snort IDS با یک مدل رمزگذار خودکار انباشته شده در صفحه کنترل، بر روی حملات انکار سرویس توزیع شده، همیشه در زمینه شبکه‌های تعریف شده نرم‌افزاری برای اینترنت اشیا تمرکز می‌کند[۱۱۰]. برعکس، نویسندگان در [۱۱۱]، نفوذهای شبکه را در ارتباطات بی‌سیم اینترنت اشیا، با بهره‌برداری از یک رمزگذار خودکار عمیق همراه با الگوریتم ماشین بردارپشتیبان، به کمک یک روش کلونی زنبورهای مصنوعی برای یافتن پارامترهای بهینه آن، تحلیل می‌کنند. پژوهش [۱۱۲]، به چهار حمله نفوذی می‌پردازد که در لایه شبکه با استفاده از یک شبکه باور عمیق خودسازگار، همراه با یک الگوریتم ژنتیک برای بهینه‌سازی تعداد لایه‌ها و نورون‌ها انجام می‌شود. همچنین مشارکت در [۱۱۳] و [۱۱۴] به طور کلی با تشخیص نفوذ مواجه است، در حالی که پژوهش [۱۱۵] با موضوع تشخیص نفوذ برای یک سناریوی لبه اشیا مقابله می‌کند. لی و همکاران برای یک زمینه صنعتی اینترنت اشیا یک روش همجوشی شبکه عصبی چند پیچشی[۴۳] پیشنهاد می‌دهند[۱۱۶]؛ در حالی که در [۱۱۷] سناریوی در نظر گرفته شده یک شهر هوشمند است. همچنین مقالات [۱۲۰-۱۱۸] با حملات نفوذ در سطح شبکه مقابله می‌کنند که پژوهش [۱۲۰] با توجه خاص به سناریوی بی‌سیم است. دیرو و همکاران سعی می‌کنند حملات متعدد را در سناریوی مه به اشیا با بهره‌برداری از تکنیک‌های محاسباتی توزیع شده، مشابه آنچه در [۱۲۱] انجام شده است، شناسایی کنند[۱۲۲]. پژوهش [۱۲۳] نیز با مشکل تشخیص حمله در لایه شبکه به صورت توزیع شده مقابله می‌کند. مطالعه در [۱۲۴] به حملات ناهنجاری مختلف در لایه شبکه همیشه به صورت توزیع شده، یعنی در زمینه محاسبات لبه، پرداخته است. مطالعات در [۱۲۵] و [۱۲۶]، هر دو در سطح شبکه، به ترتیب به تشخیص حملات غیرعادی در سیستم‌های صنعتی اینترنت اشیا و شناسایی حمله انکار سرویس می‌پردازند. در [۱۲۷] با حملات رمزگیری[۴۴]، حمله انکار سرویس توزیع شده و بات نت، در لایه‌های شبکه و برنامه، از طریق همکاری نزدیک بین یک شبکه عصبی پیچشی توزیع شده و یک شبکه حافظه طولانی کوتاه مدت زمانی مبتنی بر ابر، مقابله می‌کند. مقالات [۱۲۸,۱۲۹] به حملات بات نت می‌پردازند؛ در [۱۲۸]، با استفاده از یک رویکرد انگشت نگاری مبتنی بر اینترنت اشیا پویا و در حال تکامل به موضوع حملات بات نت می‌پردازد و [۱۲۹] با تمرکز بر ایجاد یک مجموعه داده ربات اینترنت اشیا مناسب به عنوان یک خط پایه برای شناسایی بات‌نت در شبکه‌های خاص اینترنت اشیا، با استفاده از شبکه‌های عصبی تکراری و حافظه طولانی کوتاه مدت به این نوع از حملات می‌پردازد. در نهایت، در [۱۳۰] حملات سایبری مختلف، از جمله حملات روز صفر، از طریق یک تکنیک باینری و چند طبقه‌بندی شناسایی می‌شوند که شش مدل مختلف یادگیری عمیق، یعنی شبکه‌های عصبی تکراری، حافظه طولانی کوتاه مدت، حافظه طولانی کوتاه مدت دوطرفه[۴۵]، واحدهای بازگشتی دروازه‌ای[۴۶]، شبکه‌های عصبی پیچشی و CNN-LSTM را مقایسه می‌کند و به دقتی تقریباً ۱۰۰٪ دست می‌یابد.

از سوی دیگر، تحقیقاتی که فقط می‌توانند در دسته لایه برنامه قرار بگیرند چهار دسته هستند: (۱) شناسایی‌URLهای عادی و غیرعادی تمرکز برای تشخیص حمله وب[۴۷] در دستگاه‌های لبه، با استفاده از چندین ResNets اصلاح شده با دو شاخه موازی همزمان است[۱۳۱].

(۲) فراگ و همکاران با مشکل تشخیص نفوذ در زمینه تبادل انرژی برای شبکه‌های هوشمند روبرو هستند[۱۳۲]. (۳) وانگ و همکاران سعی کرده‌اند نمونه‌های متخاصم را در برابر پنج حمله شناخته شده در سطح برنامه به روشی فراگیر شناسایی کنند[۱۳۳] و (۴) در [۱۳۴]، با تجزیه و تحلیل بار بسته‌ها برای سناریوی اینترنت همه‌جا[۴۸]، به مشکل تشخیص ناهنجاری می‌پردازد.

۵-۱-۸- کاربردهای دیگر

تنها مقاله‌ای که به استفاده از یادگیری عمیق متفاوت از اقدامات متقابل ذکر شده در بالا می‌پردازد، دو مقاله است و ابزاری برای حمله به محیط‌های اینترنت اشیا ارائه می‌کند. به طور خاص، تحقیقات لی و همکاران، از یادگیری تقویتی عمیق برای حملات مسمومیت داده‌ها[۴۹] برای تداخل با سیستم‌های سنجش جمعیت مبتنی بر اینترنت اشیا استفاده می‌کند[۱۳۵] در حالی که مطالعه در [۱۳۶] از یادگیری عمیق برای حمله به سیستم‌های سلامت الکترونیک مبتنی بر اینترنت اشیا، به‌ویژه هدف قرار دادن الکتروانسفالوگرام‌ها[۵۰] و سایر داده‌های مغزی یک فرد خاص استفاده می‌کند. این با یک پیکربندی یادگیری عمیق خاص به دست می‌آید که شامل یک شبکه عصبی پیچشی مکرر مشترک با دو شاخه موازی است که با این حال، از نظر دقت به نتایج بسیار بالایی نمی‌رسد.

۵-۲- RQ2 کدام معماری شبکه عصبی عمیق در امنیت اینترنت اشیا استفاده می‌شود و حوزه‌های کاربردی آن‌ها چیست؟

در این بخش، طبقه‌بندی مقالات بررسی شده در این بخش، بر اساس معماری‌های یادگیری عمیق شرح داده شده در بخش ۳ انجام شده است؛ به ویژه، با طبقه‌بندی مقالات بر اساس دسته‌بندی کلان شبکه‌های یادگیری عمیق مناسب (مثلاً تحت نظارت، هر دو طبقه‌بندی درشت‌دانه را در نظر گرفته شده، بدون نظارت و غیره) و یک طبقه بندی ریزدانه، بر اساس معماری‌های خاص شبکه‌های یادگیری عمیق به کار رفته در مقاله بررسی شده. شکل ۶، توزیع مقالات بررسی شده را بر اساس مقوله‌های کلان فوق‌الذکر، یعنی یادگیری با نظارت، بدون نظارت، ترکیبی و تقویت عمیق نشان می‌دهد. همچنین دو دسته کلان دیگر زیر در نظر گرفته می‌شود: "دیگران" و "نامشخص". "دیگران" به مقالاتی اشاره دارد که در آن‌ها شبکه‌های یادگیری عمیق مورد استفاده نمی‌تواند به طور کامل در دسته‌بندی‌هایی که در نظر گرفته شده است قاب‌بندی شود، در حالی که "نامشخص" شامل آن دسته از مقالاتی است که معماری یادگیری عمیق خاص در آن‌ها اصلاً مشخص نشده است. همانطور که می‌توان از شکل استنباط کرد، تقریباً نیمی (۴۹.۴۳٪) از مقالات بررسی شده از معماری شبکه‌های یادگیری عمیق نظارت شده استفاده می‌کنند که شاید ساده‌ترین آنها برای به کارگیری و تنظیم باشد. با این حال، درصد مربوطه (۲۲.۹۹٪) نیز از معماری‌های شبکه‌های یادگیری عمیق بدون نظارت استفاده می‌کند. استفاده از شبکه‌های هیبریدی یادگیری عمیق بسیار محدود است (فقط ۳.۴۵٪) و بیشتر از یادگیری تقویتی عمیق (۵.۷۵٪) استفاده می‌شود.

در نهایت، بخش مربوطه (۱۰.۳۴٪) معماری‌هایی را اتخاذ می‌کنند که نمی‌توانند در هیچ یک از مقوله‌های ذکر شده قرار گیرند و در ۸.۰۵٪ از مقالات بررسی شده، معماری شبکه‌های یادگیری عمیق استفاده شده به وضوح ذکر نشده است. شکل ۷، طبقه‌بندی را با توجه به رویکرد یادگیری عمیق مورد استفاده با جزئیات بیشتر ارائه می‌دهد و شبکه یادگیری عمیق خاصی که در مقاله بررسی شده و مورد بهره‌برداری قرار گرفته است را مشخص می‌کند. به وضوح مشخص می‌شود که بیشتر مقالات (۳۲.۱۸٪) به روش‌هایی (آموزش، آزمایش یا هر دو فاز) از یک شبکه عصبی پیچشی بهره می‌برند. چندین مطالعه از شبکه‌های عصبی بازگشتی (۱۷.۲۴٪) و رمزگذارهای خودکار عمیق (۱۳.۷۹٪) استفاده می‌کنند، در حالی که چهارمین دسته یادگیری عمیق"دیگران" (۱۰.۳۴٪) است. علاوه بر این، ۸.۰۵٪ از مقالات تجزیه و تحلیل شده از شبکه‌های باور عمیق یا معماری‌های یادگیری عمیق نامشخص استفاده می‌کنند. تعداد کمی از مقالات (۵.۷۵٪) از شبکه‌های یادگیری عمیق-Q استفاده می‌کنند، در حالی که آخرین موقعیت‌ها، با درصدهای بسیار ناچیز، به ترتیب نزولی توسط شبکه‌های زایای دشمن‌گونه (۲.۳۰٪)، ماشین‌های محدود شده بولتزمن حفظ می‌شوند (۱.۱۵٪) و مجموعه‌های شبکه‌های یادگیری عمیق (۱.۱۵٪).

در نهایت، در جداول ۳ و ۴، دو ماتریس برای تلاقی معماری‌های شبکه‌های یادگیری عمیق که تجزیه و تحلیل شده‌اند و حوزه‌های کاربردی اینترنت اشیا، که در آنها استفاده شده‌اند، وجود دارد. دامنه‌هایی که در نظر گرفته شده‌اند، هشت حوزه زیر هستند:

- هر کاربرد صنعتی عمومی که توسط دستگاه‌های اینترنت اشیا توانمند شده است
- مصرف انرژی و توان برای دستگاه های اینترنت اشیا

- محیط موبایل اینترنت اشیا
- جمعیت‌سنجی[۵۱] از طریق اشیا هوشمند اینترنت اشیا
- شهرهای هوشمند و محیط‌های شهری هوشمند
- سیستم‌های مراقبت بهداشتی دیجیتال با کمک دستگاه‌های اینترنت اشیا
- محاسبات لبه و مه
- شبکه نرم‌افزار محور[۵۲] در محیط اینترنت اشیا

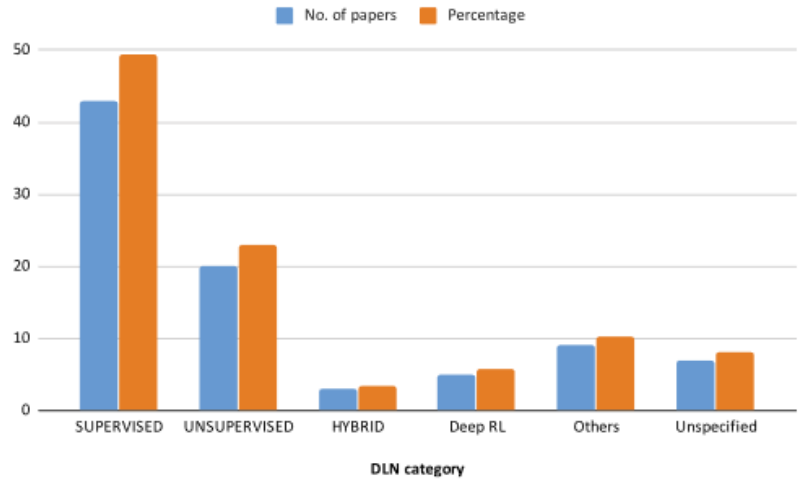
علاوه بر این، در این مقاله؛ دو دسته دامنه برنامه دیگر در نظر گرفته شده‌اند؛ به عنوان مثال، "عمومی" برای دامنه‌های برنامه نامشخص و "سایر"، برای دامنه‌های برنامه که فقط یک بار ظاهر می‌شوند. با نگاهی به جدول ۳، اکثر مقالاتی که بررسی شده‌اند را می‌توان در دسته‌بندی «عمومی» (۴۰ مقاله) قرار داد. دومین دسته اصلی، محاسبات لبه / مه (۱۱ مقاله)، سپس دسته صنعتی (۸ مقاله)، تقریباً با همان تعداد مقاله به عنوان رده بهداشتی (۷ مقاله) است. سه حوزه کاربردی شامل ۵ مقاله، یعنی محیط موبایل، شهرهای هوشمند و شبکه‌های نرم‌افزار محور در اینترنت اشیا هستند، در حالی که دسته انرژی و دسته سنجش ازدحام به ترتیب با ۴ و ۳ مقاله، فهرست را به پایان می‌رسانند. مقوله "دیگران" نیز شامل مقالات بسیار کمی مثل یادگیری عمیق نظارت شده بیشترین استفاده شده در حوزه انرژی، شهر هوشمند، سلامت و حوزه برنامه‌های کاربردی محاسبات لبه است در حالی که یادگیری عمیق بدون نظارت بیشترین استفاده را در حوزه های صنعتی و صنعتی دارد. دامنه‌های برنامه SDN-DRL در سناریوهایی که با سنجش ازدحام سروکار دارند کمتر ترجیح داده می شود، در حالی که محیط‌های تلفن همراه در دسته ماکرو یادگیری عمیق استفاده شده شیوع واضحی ندارند. با نگاهی به جدول ۴، شبکه‌های عصبی پیچشی، پر استفاده‌ترین معماری‌های شبکه‌های یادگیری عمیق در دسته‌های «عمومی»، سلامت و «سایر» هستند، در حالی که شبکه‌های عصبی تکراری بیشتر در حوزه‌های عمومی و حداقل در حوزه سلامت و لبه به کار می‌روند. بیشترین استفاده از معماری شبکه‌های یادگیری عمیق در سنجش جمعی، شبکه‌های یادگیری عمیق-Q است، در حالی که برای سناریوهای محاسبات لبه، شبکه‌های عصبی پیچشی، شبکه‌های عصبی تکراری و شبکه‌های باور عمیق به طور مساوی استفاده می‌شوند. به طور مشابه، هیچ اکثریت واضحی برای سناریوهای موبایل، انرژی و شبکه‌های نرم‌افزار محور وجود ندارد.

۵-۳- RQ3 کدام نوع مجموعه داده در امنیت اینترنت اشیا با استفاده از رویکرد یادگیری عمیق استفاده می‌شود؟

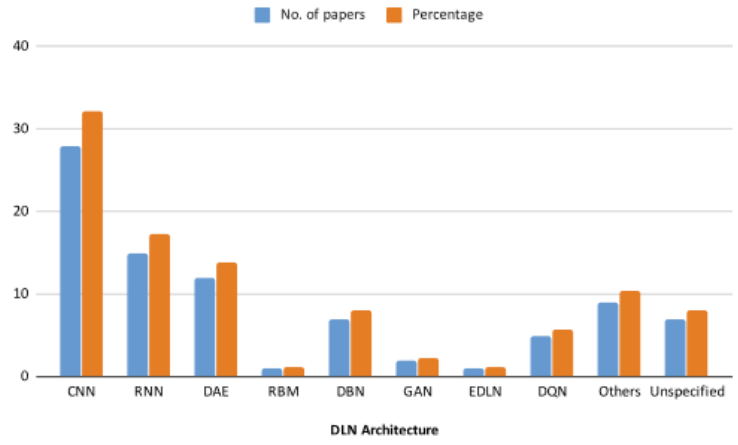
در این بخش، طبقه‌بندی مقالات بررسی‌شده، بر اساس مجموعه داده‌های خاص به کار گرفته شده ارائه می‌شوند تا بتوان برخی از مجموعه‌های داده معیار برای کاربرد یادگیری عمیق در زمینه امنیت اینترنت اشیا را پیدا کرد. در ابتدا، یک طبقه‌بندی دوگانه از مجموعه‌های داده ایجاد شد، یعنی (i) بر اساس ماهیت داده‌های مورد استفاده، یعنی داده‌های واقعی یا داده‌های مصنوعی و (ii) با توجه به امکان دسترسی به داده‌ها، یعنی مجموعه داده‌های عمومی یا خصوصی. قسمت سمت چپ شکل ۸ طبقه‌بندی را بر اساس ماهیت ذاتی داده‌ها نشان می‌دهد. اکثر (۸۵.۷۱٪) مقالات بررسی شده از داده‌های واقعی بهره‌برداری می‌کنند و تنها بخش کوچکی (۱۴.۲۹٪) از داده‌های شبیه‌سازی شده استفاده می‌کنند. از طرف دیگر، قسمت سمت راست شکل ۸، طبقه‌بندی را بر اساس خط مشی دسترسی به داده‌ها نشان می‌دهد. اکثر (۶۴.۴۷٪) مقالات در نظر گرفته شده، از مجموعه داده‌های در دسترس عموم استفاده می‌کنند، در حالی که ۳۵.۵۲٪ از آن‌ها، داده‌های جمع‌آوری شده شخصی را که به طور عمومی منتشر نشده‌اند، تجزیه و تحلیل می‌کنند. جدول ۵، وقوع ۱۷ مجموعه داده پرکاربرد را در مقالات بررسی شده نشان می‌دهد. مجموعه داده‌های در نظر گرفته شده آنهایی هستند که حداقل دو مورد در مقالات در نظر گرفته شده دارند. ۲۷ مجموعه داده باقی مانده، اگرچه در جدول فهرست نشده‌اند، تنها یک بار در تمام مقالات بررسی شده ظاهر می‌شوند. بیشترین استفاده از مجموعه داده NSL-KDD است که نسخه بهبود یافته KDD CUP 99 است و توسط سه مقاله استفاده شده است. دومین مجموعه داده پر استفاده UNSW-NB-2015 است که توسط ابزار IXIA PerfectStorm در آزمایشگاه Cyber Rangeمرکز استرالیا برای امنیت سایبری ایجاد شده است. مجموعه داده‌های ذکر شده عمدتاً مجموعه داده‌های ترافیک شبکه هستند، بنابراین برای مقابله با تشخیص ترافیک غیرعادی مناسب هستند. برعکس، با نگاهی به مجموعه داده‌های بدافزار، آمار آن‌ها از MalGENOME، DREBIN، (CONTAGIO تا Leopard Mobile)، Virusshare، NVD و Malimg بیشتر توزیع شده است. در نهایت، آمار خلاصه‌ای در مورد همه مجموعه داده‌های مورد استفاده از نظر تعداد نمونه‌های آموزش و مجموعه تست و همچنین تعداد ویژگی‌ها محاسبه شده است. مجموعه داده‌ها می‌توانند توسط نویسندگان مقالات بررسی شده از قبل پردازش شوند، بنابراین در این مقاله، هم

مجموعه داده اصلی و هم مجموعه داده واقعی استفاده شده، در نظر گرفته شده است. برای هر دوی آن‌ها، میانگین تعداد کل نمونه‌ها، نمونه‌های آموزشی، نمونه‌های تست و ویژگی‌ها محاسبه شد.

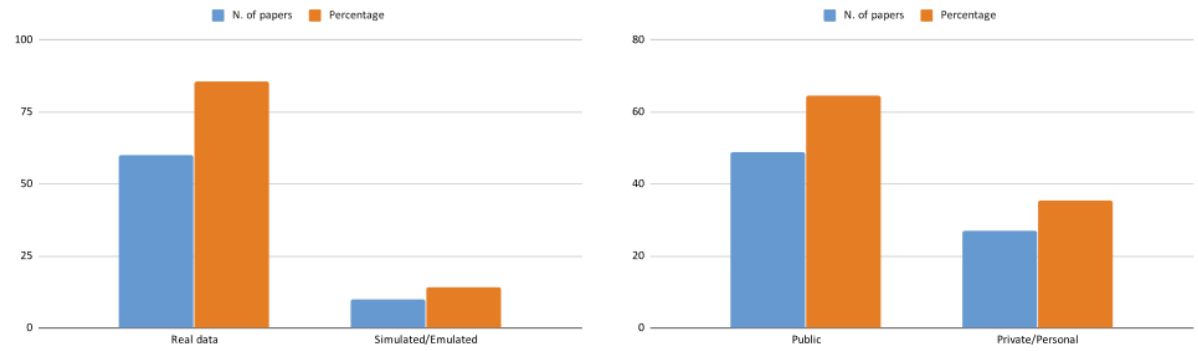
نتایج در جدول ۶ نشان داده شده است، که در آن میانگین‌ها تنها با در نظر گرفتن مقالاتی که اطلاعات مربوطه از آن‌ها قابل بازیابی بود، محاسبه شده است. در سیزده مقاله امکان بازیابی هیچ اطلاعاتی در مورد ویژگی‌ها و یا تعداد نمونه‌های موجود در مجموعه داده‌های مورد استفاده وجود نداشت. با نگاهی به جدول، می‌توان استنباط کرد که به طور متوسط مجموعه داده‌های واقعی استفاده شده دارای ۱.۵ میلیون نمونه هستند، مرتبه بزرگی برای تکنیک‌های یادگیری عمیق مناسب است و تعداد نمونه‌های آزمون، به طور متوسط، نصف تعداد نمونه‌های موجود در مجموعه آموزشی است. در نهایت، تعداد ویژگی‌های به کار گرفته شده معمولاً به طور متوسط بسیار زیاد است (بیش از ۵۰۰)، یعنی می‌توان عنوان کرد که تقریباً پنج برابر تعداد ویژگی‌های مجموعه داده‌های اصلی است. این ممکن است نشان دهنده کار قابل توجهی در استخراج ویژگی‌های جدید از مجموعه داده اصلی از طریق تکنیک‌های پیش‌پردازش مناسب باشد.



شکل (۶): تعداد مقالات و درصد نسبی، بر اساس دسته‌های کلان شبکه‌های یادگیری عمیق



شکل (۷): تعداد مقالات و درصد نسبی، بر اساس معماری خاص شبکه‌های یادگیری عمیق



شکل (۸): توزیع مقالات بررسی شده بر اساس ماهیت مجموعه داده‌ها (سمت چپ) و خط مشی دسترسی مجموعه داده‌ها (سمت راست)

جدول (۳): ماتریس ترکیب کننده دامنه برنامه و دسته کلی شبکه‌های یادگیری عمیق

Domain/DLN category	Supervised	Unsupervised	Hybrid	DRL	Others	Unspecified
Generic	۲۳	۹	۳	۰	۳	۲
Industrial	۱	۳	۰	۱	۱	۲
Energy	۲	۱	۰	۰	۱	۰
Mobile	۱	۱	۰	۱	۱	۱
Crowdsensing	۱	۰	۰	۲	۰	۰
Smart city	۲	۱	۰	۰	۱	۱
Health	۵	۱	۰	۱	۰	۰
Edge/Fog	۴	۳	۰	۰	۱	۳
SDN	۱	۳	۰	۱	۰	۰
Others	۳	۰	۰	۰	۰	۱

جدول (۴): ماتریس ترکیب کننده دامنه برنامه و معماری خاص شبکه‌های یادگیری عمیق

Domain/DLN Type	CNN	RNN	DAE	RBM	DBN	GAN	EDLN	DQN	Others	Unspec.
Generic	۱۵	۸	۷	۰	۲	۲	۱	۰	۳	۲
Industrial	۱	۰	۲	۰	۱	۰	۰	۱	۱	۲
Energy	۱	۱	۱	۰	۰	۰	۰	۰	۱	۰
Mobile	۱	۰	۰	۰	۱	۰	۰	۱	۱	۱
Crowdsensing	۱	۰	۰	۰	۰	۰	۰	۲	۰	۰
Smart city	۱	۱	۰	۱	۰	۰	۰	۰	۱	۱
Health	۳	۲	۰	۰	۱	۰	۰	۱	۰	۰
Edge/Fog	۲	۲	۱	۰	۲	۰	۰	۰	۱	۳
SDN	۱	۰	۱	۱	۱	۰	۰	۱	۰	۰
Others	۲	۱	۰	۰	۰	۰	۰	۰	۰	۱

جدول (۵): وقوع مجموعه داده‌ها در مقالات بررسی شده.

Dataset	KDD CUP 99	CICIDS 2017	MNIST	NSL-KDD	Bot-IoT	N_BaIoT
N. of papers	۳	۳	۲	۸	۳	۲
Dataset	ISCX2012	CIFAR-10	AWID	UNSW-NB-2015	DREBIN	CONTAGIO
N. of papers	۲	۲	۲	۴	۳	۳
Dataset	MalGENOME	NVD	Leopard mobile	Malimg	Virusshare	-
N. of papers	۳	۲	۲	۲	۲	-

٦- بحث

در این بخش، یافته‌های اصلی و مسائل باز در مورد کاربرد موفقیت‌آمیز تکنیک‌های یادگیری عمیق در زمینه امنیت اینترنت اشیا مورد بحث قرار می‌گیرد. به طور کلی، از تجزیه و تحلیل انجام شده، مشخص شد: (i) اکثر مقالات بررسی شده با شناسایی حملات خاص یا رفتارهای ترافیک شبکه غیرعادی سروکار دارند، در حالی که تمرکز بر آسیب‌پذیری‌های نرم‌افزار و بدافزارها هنوز حاشیه‌ای است؛ (ii) استفاده از تکنیک‌های یادگیری عمیق تحت نظارت، به‌ویژه شبکه‌های عصبی پیچشی، هنوز غالب است، حتی اگر دیگر معماری‌های شبکه‌های یادگیری عمیق جدیدتر نیز شروع به بکارگیری کنند؛ (iii) دامنه کاربرد اغلب بیش از حد معمول است و برای تطبیق بهتر، معماری شبکه‌های یادگیری عمیق با سناریوی استقرار خاص، باید بیشتر مشخص شود؛ (IV) بسیاری از مجموعه داده‌هایی که به کار گرفته شده‌اند هنوز عمومی نیستند؛ (V) روند انتشار در مورد موضوع انتخاب شده در سال‌های اخیر به شدت افزایش یافته است. بنابراین، با رفع مشکلاتی که در ادامه توضیح داده می‌شود، فضای زیادی برای افزایش استفاده از یادگیری عمیق در امنیت اینترنت اشیا در سال‌های آینده وجود دارد. چندین موضوع باز از مقالات بررسی شده پدید آمده است که می توان آن‌ها را در دسته‌های زیر خلاصه کرد:

۱. کمبود اطلاعات فنی مفید
۲. زمان واقعی و مبادله بین عملکرد به دست آمده و پیچیدگی راه حل یادگیری عمیق پیشنهادی
۳. عدم آزمایش بیشتر
۴. کیفیت پایین عملکرد
۵. عدم توجه به آسیب‌پذیری راه‌حل پیشنهادی در برابر حملات خاص
۶. استفاده از مجموعه داده‌های نامناسب
۷. عدم بررسی قابل تفسیر بودن نتایج به دست آمده

با توجه به نکته اول، ذکر این نکته ضروری است که درصد ناچیز مقالات بررسی شده به هیچ وجه شبکه عصبی عمیقی را که استفاده می‌کنند مشخص نمی‌کنند و باعث می‌شود که انتشار در پرداختن به سایر مطالعات تحقیقاتی کمتر مفید باشد. گاهی اوقات، اطلاعات گمشده بیشتر مربوط به ماهیت و ابعاد مجموعه داده استفاده شده و تعداد زیادی از مقالات بدون دامنه کاربردی مشخص است. در برخی موارد نادر، حتی نتایج عددی واقعی نیز وجود ندارد.

نکته دوم برای پیاده‌سازی واقعی راه‌حل‌های یادگیری عمیق بررسی شده، در دنیای واقعی بسیار مهم است. در واقع، برای ادغام واقعی یادگیری عمیق در تمام سناریوهای محاسبات فراگیر و لبه اینترنت اشیا، باید به ارزیابی صحیح پیچیدگی محاسباتی و مصرف انرژی تکنیک‌های پیشنهادی پرداخته شود. ارزیابی پاسخگویی بلادرنگ و زمان اجرای واقعی، سنگ بنای دیگری در استقرار واقعی تکنیک‌هایی بررسی شده در شبکه‌های اصلی و شبکه‌های اینترنت اشیا لبه است. با توجه به بهینه‌سازی سریع پارامترهای آموزشی و برچسب‌گذاری صحیح نمونه‌های قابل استفاده در یادگیری عمیق و به ویژه در زمینه لبه، شناسایی راه‌هایی برای کاهش زمان آموزش و توزیع آموزش را الزامی می‌کند. مدل‌های شبکه عصبی ساده‌تر را می‌توان در یک زمان معقول آموزش داد اما مدل‌های پیشرفته‌تر مانند شبکه‌های عصبی نموداری و شبکه‌های مولد متخاصم برای آموزش کارآمد، دارای چالش هستند. معماری‌های پیچیده، زمان‌های آموزشی بالایی را در هر دوره نشان می‌دهند و اغلب فقط برای زمان مورد نیاز برای همگرایی استفاده نمی‌شوند، به‌ویژه با توجه به بهینه‌سازی فراپارامتر. زمان‌های چرخش باید بهبود یابد تا توسعه این مدل‌ها آسان‌تر شود. آموزش توزیع شده می‌تواند مرحله آموزش یا تمرین را به شدت کاهش دهد. الگوریتم‌های جدید حلقه کاهش که در کتابخانه‌های ارتباطی با کارایی بالا برای آموزش داده‌های توزیع‌شده پیاده‌سازی شده‌اند، توسط چندین کار استفاده می‌شوند. الگوریتم‌ها برای پهنای باند شبکه، بهینه‌سازی شده‌اند و هر فرآیند $(n-1)/n^2$ بار پیام‌های گرادیان را ارسال و دریافت می‌کند که در آن n تعداد فرآیندها است. سپس می‌تواند به طور مؤثر برای n بزرگ مقیاس شود، زیرا اندازه کل پیام ارسال شده در هر فرآیند زمانی که $n \to \infty$ ثابت می‌شود.

یک مانع مکرر برای آموزش داده‌های توزیع شده این است که معیار دقت برای اندازه‌های دسته بزرگ بدتر می‌شود. در برخی از مقالات، تاکید شده است که تخمین گرادیان در هر فاز با دسته‌های بزرگتر دقیق‌تر است و بنابراین بهینه‌سازی پایدارتر، تصادفی‌تر می‌شود و بنابراین احتمال پایان آموزش و یا بهینه‌سازی بیشتر است و در یک حداقل محلی به دام افتاده است. استراتژی‌هایی برای کاهش این موضوع وجود دارد، مانند مقیاس‌بندی نرخ تطبیقی(LARS). از روش‌های دیگر برای بهینه‌سازی توزیع‌شده فراپارامتری کارآمد، می‌توان از برآوردگر Parzen با ساختار درختی[۱۳۷] نام برد که یک رویکرد بهینه‌سازی مبتنی بر مدل متوالی[۵۳] است. به‌طور متوالی مدل‌هایی

را برای تقریب عملکرد فراپارامترها بر اساس اندازه‌گیری‌های قبلی می‌سازد و سپس پارامترهای فوق‌العاده جدیدی را برای آزمایش مکرر انتخاب می‌کند و استراتژی‌های هرس کارآمدی را به‌کار می‌برد که جایگشت‌های پارامتری امیدوارکننده نیستند.

نکته سوم شامل مقایسه گاه به گاه با دیگر معماری‌های شبکه‌های یادگیری عمیق یا حتی با تکنیک‌های یادگیری ماشینی ساده تر است؛ در واقع، عملکرد یک راه‌حل پیشنهادی اغلب با سایر تکنیک‌های ساده‌تر و سریع‌تر مقایسه نمی‌شود و نوع خاصی از طبقه‌بندی، به عنوان مثال، یک باینری، با دیگر دسته‌بندی‌های مفید و دقیق‌تر همراه نیست. علاوه بر این، اغلب هیچ پیش‌پردازشی انجام نمی‌شود، بنابراین به طور متوسط بیش از ۵۰۰ ویژگی در مجموعه داده‌های مورد استفاده ایجاد می‌شود. انتخاب یا استخراج ویژگی، با توجه به آنچه که در مورد مبادله عملکرد-پیچیدگی گفته شد، می‌تواند یک موضوع تحقیقاتی مفید برای بهبود برخی از راه‌حل‌های بررسی شده باشد.

نکته چهارم تمرکز بر روی عملکرد است که گاهی اوقات برای یک مدل یادگیری عمیق، خوب نیست زیرا از نظر دقت، فراتر از ۹۹٪ نمی‌رود. برخی از راه‌حل‌ها حتی به ۹۰٪ دقت نمی‌رسند و با تکنیک‌های ساده یادگیری ماشین شکست می‌خورند. نکته پنجم نشان می‌دهد که برخی از راه‌حل‌ها در برابر برخی از حملات از قبل شناخته‌شده، مانند نمونه‌گیری متخاصم، مسمومیت داده‌ها و موارد مشابه آسیب‌پذیر هستند و هیچ اقدام متقابل مناسبی در مقالات بررسی شده بیان نشده است. جنبه دیگر این نکته ممکن است شامل عدم شناسایی حملات به اصطلاح روز صفر، رفتارهای مخرب ناشناخته و همچنین تغییر پویا نگرش در جنبه امنیتی نظارت شده خاص باشد.

نکته ششم بر استفاده بسیار گسترده از هیچ مجموعه داده واقعی مبتنی بر اینترنت اشیا تأکید می‌کند. جدایی از برخی موارد، اکثر مجموعه داده‌های مورد استفاده کاملاً قدیمی هستند و بر اساس انواع دیگر ترافیک شبکه هستند. بنابراین، یافتن یک مجموعه داده با معیار مناسب برای یادگیری عمیق در امنیت اینترنت اشیا، هنوز دشوار است. علاوه بر این، گاهی اوقات مجموعه داده‌های مورد استفاده در دسترس عموم نیستند و برای استفاده مناسب در یادگیری عمیق بسیار کوچک هستند.

در نهایت، آخرین نکته مربوط به تفسیرپذیری نتایج به دست آمده توسط راه‌حل‌های بررسی شده، است. گاهی اوقات راه‌حل‌های ارائه شده، قابل اطمینان نیستند و به درستی با دامنه برنامه خاصی که در مقاله نامگذاری شده است، مرتبط نیستند. علاوه بر این، تفسیر صریح آن‌ها به هیچ وجه ساده نیست.

۷- نتیجه‌گیری

در این مقاله، یک بررسی سیستماتیک عمیق در مورد کاربرد تکنیک‌های یادگیری عمیق برای امنیت سیستم‌های مبتنی بر اینترنت اشیا انجام شده است. در ابتدا پیشینه امنیت اینترنت اشیا و همچنین طبقه‌بندی دقیق تکنیک‌های یادگیری عمیق شرح داده شده است. سپس، روش تحقیقی اتخاذ شده، به تفصیل شرح داده شد؛ از تعریف پرسش‌ها شروع می‌شود، سوالات دیگر از سؤالات تحقیق مشتق می‌شود و سپس مراحل مختلف الک و پالایش، تا رسیدن به مجموعه نهایی ۶۹ مقاله تحلیل شده، ادامه پیدا می‌کند. در نهایت، نتایج بررسی سیستماتیک، با توجه به سه طبقه‌بندی اصلی منعکس کننده سؤالات تحقیق، توصیف می‌شوند. سه طبقه‌بندی ذکر شده عبارتند از: جنبه‌های امنیتی بررسی شده، معماری‌های شبکه‌های یادگیری عمیق استفاده شده و حوزه‌های کاربردی آن‌ها و همچنین مجموعه داده‌های به کار گرفته شده. نتیجه نهایی این است که در آینده نزدیک به تلاش‌های تحقیقاتی بیشتری نیاز است تا استفاده از یادگیری عمیق به یک رویکرد دائمی و بالغ در زمینه امنیت اینترنت اشیا تبدیل شود.

مراجع

[1] H. Tahaei, F. Afifi, A. Asemi, F. Zaki, and N. B. Anuar, "The rise of traffic classification in IoT networks: A survey," *Journal of Network and Computer Applications*, vol. 154, p. 102538, 2020. doi: 10.1016/j.jnca.2020.102538.

[2] R. Pecori, "A PKI-free key agreement protocol for P2P VoIP applications," in *2012 IEEE International Conference on Communications (ICC)*, 2012, pp. 6748–6752. doi: 10.1109/ICC.2012.6364948.

[3] R. Bonetto, I. Sychev, O. Zhdanenko, A. Abdelkader, and F. H. P. Fitzek, "Smart Grids for Smarter Cities," in *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*, 2020, pp. 1–2. doi: 10.1109/CCNC46108.2020.9045309.

[4] R. Pecori, "Augmenting Quality of Experience in Distance Learning Using Fog Computing," *IEEE Internet Comput*, vol. 23, no. 5, pp. 49–58, 2019. doi: 10.1109/MIC.2019.2936754.

[5] M. Calabretta, R. Pecori, and L. Veltri, *A Token-based Protocol for Securing MQTT Communications*. 2018. doi: 10.23919/SOFTCOM.2018.8555834.

[6] M. Calabretta, R. Pecori, M. Vecchio, and L. Veltri, "MQTT-Auth: a Token-based Solution to Endow MQTT with Authentication and Authorization Capabilities," *Journal of Communications Software and Systems*, vol. 14, Dec. 2018. doi: 10.24138/jcomss.v14i4.604.

[7] A. Tayebi, L. Veltri, R. Pecori, and A. Vannucci, *IoT Attack Detection with Deep Learning Analysis*. 2020. doi: 10.1109/IJCNN48605.2020.9207171.

[8] G. Perrone, M. Vecchio, R. Pecori, and R. Giaffreda, *The Day After Mirai: A Survey on MQTT Security Solutions After the Largest Cyber-attack Carried Out through an Army of IoT Devices*, 2017. doi: 10.5220/0006287302460253.

[9] I. goodfellow, Y. bengio, A. courville, "Machine Learning basics", *Deep Learning*, MIT Press, 2016, pp. 95–151. doi: 10.1007/s10710-017-9314-z.

[10] L. Deng and D. Yu, "Deep learning: methods and applications," *Foundations and trends® in signal processing*, vol. 7, no. 3–4, pp. 197–387, 2014. doi: 10.1561/2000000039.

[11] A. S. Lundervold and A. Lundervold, "An overview of deep learning in medical imaging focusing on MRI," *Z Med Phys*, vol. 29, no. 2, pp. 102–127, 2019. doi: 10.1016/j.zemedi.2018.11.002.

[12] H. M. Fayek, M. Lech, and L. Cavedon, "Evaluating deep learning architectures for speech emotion recognition," *Neural Networks*, vol. 92, pp. 60–68, 2017. doi: 10.1016/j.neunet.2017.02.013.

[13] G. H.-J. Kwak and P. Hui, "DeepHealth: Review and challenges of artificial intelligence in health informatics," *arXiv preprint arXiv:1909.00384*, 2019. doi:10.48550/arXiv.1909.00384.

[14] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020, doi: 10.1109/COMST.2020.2988293.

[15] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1686–1721, 2020. doi: 10.1109/COMST.2020.2986444.

[16] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?," *IEEE Signal Process Mag*, vol. 35, no. 5, pp. 41–49, 2018. doi: 10.1109/MSP.2018.2825478.

[17] A. M. Aleesa, B. B. Zaidan, A. A. Zaidan, and N. M. Sahar, "Review of intrusion detection systems based on deep learning techniques: coherent taxonomy, challenges, motivations, recommendations, substantial analysis and future directions," *Neural Comput Appl*, vol. 32, pp. 9827–9858, 2020. doi: 10.1007/s00521-019-04557-3.

[18] D. S. Berman, A. L. Buczak, J. S. Chavis, and C. L. Corbett, "A survey of deep learning methods for cyber security," *Information*, vol. 10, no. 4, p. 122, 2019. doi: 10.3390/info10040122.

[19] F. Liang, W. G. Hatcher, W. Liao, W. Gao, and W. Yu, "Machine learning for security and the internet of things: the good, the bad, and the ugly," *Ieee Access*, vol. 7, pp. 158126–158147, 2019. doi: 10.1109/ACCESS.2019.2948912.

[20] L. Xiao, D. Jiang, D. Xu, W. Su, N. An, and D. Wang, "Secure mobile crowdsensing based on deep learning," *China Communications*, vol. 15, no. 10, pp. 1–11, 2018, doi: 10.1109/CC.2018.8485464.

[21] W. G. Hatcher and W. Yu, "A survey of deep learning: Platforms, applications and emerging research trends," *IEEE access*, vol. 6, pp. 24411–24432, 2018. doi: 10.1109/ACCESS.2018.2830661.

[22] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *Journal of Information Security and Applications*, vol. 50, p. 102419, 2020. doi: 10.1016/j.jisa.2019.102419.

[23] R. Vishwakarma and A. K. Jain, "A survey of DDoS attacking techniques and defence mechanisms in the IoT network," *Telecommun Syst*, vol. 73, no. 1, pp. 3–25, 2020. doi: 10.1007/s11235-019-00599-z.

[24] M. M. Salim, S. Rathore, and J. H. Park, "Distributed denial of service attacks and its defenses in IoT: a survey," *J Supercomput*, vol. 76, pp. 5320–5363, 2020. doi: 10.1007/s11227-019-02945-z.

[25] N. Koroniotis, N. Moustafa, and E. Sitnikova, "Forensics and deep learning mechanisms for botnets in internet of things: A survey of challenges and solutions," *IEEE Access*, vol. 7, pp. 61764–61785, 2019. doi: 10.1109/ACCESS.2019.2916717.

[26] Ö. A. Aslan and R. Samet, "A comprehensive review on malware detection approaches," *IEEE access*, vol. 8, pp. 6249–6271, 2020. doi: 10.1109/ACCESS.2019.2963724.

[27] Z. Ullah, F. Al-Turjman, L. Mostarda, and R. Gagliardi, "Applications of artificial intelligence and machine learning in smart cities," *Computer Communications*, vol. 154, pp. 313–323, 2020. doi: 10.1016/j.comcom.2020.02.069.
[28] M. A. Amanullah, R. A. A. Habeeb, F. H. Nasaruddin, A. Gani, E. Ahmed, A. S. M. Nainar, N. M. Akim and M. Imran, "Deep learning and big data technologies for IoT security," *Computer Communications*, vol. 151, pp. 495–517, 2020. doi: 10.1016/j.comcom.2020.01.016.
[29] M. Aly, F. Khomh, M. Haoues, A. Quintero, and S. Yacout, "Enforcing security in Internet of Things frameworks: A systematic literature review," *Internet of Things*, vol. 6, p. 100050, 2019. doi: 10.1016/j.iot.2019.100050.
[30] B. Kitchenham, "Procedures for performing systematic reviews," *Keele University*, vol. 33, no. 2004, pp. 1–26, 2004.
[31] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE communications surveys & tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015. doi: 10.1109/COMST.2015.2444095.
[32] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, 2017. doi: 10.1016/j.jnca.2017.04.002.
[33] Z. Yang, Y. Yue, Y. Yang, Y. Peng, X. Wang, and W. Liu, "Study and application on the architecture and key technologies for IOT," in *2011 international conference on multimedia technology*, IEEE, 2011, pp. 747–751. doi: 10.1109/ICMT.2011.6002149.
[34] R. Pecori, P. Ducange, and F. Marcelloni, "Incremental learning of fuzzy decision trees for streaming data classification," in *11th Conference of the European Society for Fuzzy Logic and Technology (EUSFLAT 2019)*, Atlantis Press, 2019, pp. 748–755. doi: 0.2991/eusflat-19.2019.102.
[35] P. Sethi and S. R. Sarangi, "Internet of things: architectures, protocols, and applications," *Journal of electrical and computer engineering*, vol. 2017, no. 1, p. 9324035, 2017. doi: 10.1155/2017/9324035.
[36] P. Thubert, C. Bormann, L. Toutain, and R. Cragie, "IPv6 over low-power wireless personal area network (6LoWPAN) routing header," 2017.
[37] T. Winter *et al.*, "RPL: IPv6 routing protocol for low-power and lossy networks," 2012.
[38] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for internet of things: a survey," *IEEE Internet of Things Journal*, vol. 3, no. 1, pp. 70–95, 2015. doi: 10.1109/JIOT.2015.2498900.
[39] E. Ahmed, I. Yaqoob, I. A. T. Hashem, I. Khan, A. I. A. Ahmed, M. Imran, A. V. Vasilakos, "The role of big data analytics in Internet of Things," *Computer Networks*, vol. 129, pp. 459–471, 2017. doi: 10.1016/j.comnet.2017.06.013.
[40] P. Ducange, R. Pecori, and P. Mezzina, "A glimpse on big data analytics in the framework of marketing strategies," *Soft Computing*, vol. 22, no. 1, pp. 325–342, 2018. doi: 10.1007/s00500-017-2536-4.
[41] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in *2015 IEEE symposium on computers and communication (ISCC)*, IEEE, 2015, pp. 180–187. doi: 10.1109/ISCC.2015.7405513.
[42] M. Anirudh, S. A. Thileeban, and D. J. Nallathambi, "Use of honeypots for mitigating DoS attacks targeted on IoT networks," in *2017 International conference on computer, communication and signal processing (ICCCSP)*, IEEE, 2017, pp. 1–4. doi: 10.1109/ICCCSP.2017.7944057.
[43] G. Han, L. Xiao, and H. V Poor, "Two-dimensional anti-jamming communication based on deep reinforcement learning," in *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2017, pp. 2087–2091. doi: 10.1109/ICASSP.2017.7952524.
[44] A. Merlo, M. Migliardi, and P. Fontanelli, "Measuring and estimating power consumption in Android to support energy-based intrusion detection," *Journal of Computer Security*, vol. 23, pp. 611–637, 2015, doi: 10.3233/JCS-150530.
[45] M. Migliardi and A. Merlo, "Improving energy efficiency in distributed intrusion detection systems," *Journal of High Speed Networks*, vol. 19, pp. 251–264, 2013, doi: 10.3233/JHS-130476.
[46] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "PHY-layer spoofing detection with reinforcement learning in wireless networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 10037–10047, 2016. doi: 10.1109/TVT.2016.2524258.

[47] R. Pecori and L. Veltri, "A key agreement protocol for P2P VoIP applications," in *SoftCOM 2009 - 17th International Conference on Software, Telecommunications & Computer Networks*, 2009, pp. 276–280.

[48] L. Xiao, Y. Li, X. Huang, and X. Du, "Cloud-Based Malware Detection Game for Mobile Devices with Offloading," *IEEE Transactions on Mobile Computing*, vol. 16, no. 10, pp. 2742–2750, 2017, doi: 10.1109/TMC.2017.2687918.

[49] P. Srivastava, H. Peng, J. Li, H. Okhravi, H. Shrobe, and M. Payer, "Firmfuzz: Automated iot firmware introspection and analysis," in *Proceedings of the 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things*, 2019, pp. 15–21. doi: 10.1145/3338507.3358616.

[50] N. Dejon, D. Caputo, L. Verderame, A. Armando, and A. Merlo, "Automated security analysis of IoT software updates," in *IFIP International Conference on Information Security Theory and Practice*, Springer, 2019, pp. 223–239. doi: 10.1007/978-3-030-41702-4_14.

[51] Z. Yan, P. Zhang, and A. V Vasilakos, "A survey on trust management for Internet of Things," *Journal of network and computer applications*, vol. 42, pp. 120–134, 2014. doi: 10.1016/j.jnca.2014.01.014.

[52] M. W. Gardner and S. R. Dorling, "Artificial neural networks (the multilayer perceptron)—a review of applications in the atmospheric sciences," *Atmospheric Environment*, vol. 32, no. 14–15, pp. 2627–2636, 1998. doi: 10.1016/S1352-2310(97)00447-0.

[53] M. I. Jordan and T. M. Mitchell, "Machine learning: Trends, perspectives, and prospects," *Science (1979)*, vol. 349, no. 6245, pp. 255–260, 2015. doi: 10.1126/science.aaa8415.

[54] T. Hastie, R. Tibshirani, J. H. Friedman, and J. H. Friedman, *The elements of statistical learning: data mining, inference, and prediction*, vol. 2. Springer, 2009. doi: 10.1007/978-0-387-21606-5.

[55] G. E. Hinton and R. R. Salakhutdinov, "Reducing the dimensionality of data with neural networks," *Science (1979)*, vol. 313, no. 5786, pp. 504–507, 2006. doi: 10.1126/science.1127647.

[56] F. Hussain, A. Anpalagan, A. S. Khwaja, and M. Naeem, "Resource allocation and congestion control in clustered M2M communication using Q-learning," *Transactions on Emerging Telecommunications Technologies*, vol. 28, no. 4, p. e3039, 2017. doi:10.1002/ett.3039.

[57] X.-W. Chen and X. Lin, "Big data deep learning: challenges and perspectives," *IEEE access*, vol. 2, pp. 514–525, 2014. doi: 10.1109/ACCESS.2014.2325029.

[58] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015. doi: 10.1038/nature14539.

[59] H. F. Nweke, Y. W. Teh, M. A. Al-Garadi, and U. R. Alo, "Deep learning algorithms for human activity recognition using mobile and wearable sensor networks: State of the art and research challenges," *Expert Systems with Applications*, vol. 105, pp. 233–261, 2018. doi: 10.1016/j.eswa.2018.03.056.

[60] R. Pascanu, T. Mikolov, and Y. Bengio, "On the difficulty of training recurrent neural networks," in *International conference on machine learning*, Pmlr, 2013, pp. 1310–1318.

[61] M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, "Deep learning for IoT big data and streaming analytics: A survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2923–2960, 2018. doi: 10.1109/COMST.2018.2844341.

[62] G. E. Hinton, "A Practical Guide to Training Restricted Boltzmann Machines," in *Neural Networks: Tricks of the Trade: Second Edition*, G. Montavon, G. B. Orr, and K.-R. Müller, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 599–619. doi: 10.1007/978-3-642-35289-8_32.

[63] Q. Zhang, L. T. Yang, Z. Chen, and P. Li, "A survey on deep learning for big data," *Information Fusion*, vol. 42, pp. 146–157, 2018, doi: https://doi.org/10.1016/j.inffus.2017.10.006.

[64] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, SH. Ozair, A. Courville, Y. Bengio, "Generative adversarial nets," *Advances in Neural Information Processing Systems*, vol. 27, 2014. doi: 10.48550/arXiv.1406.2661.

[65] T. Salimans, I. Goodfellow, W. Zaremba, V. Cheung, A. Radford, and X. Chen, "Improved techniques for training gans," *Advances in Neural Information Processing Systems*, vol. 29, 2016. doi: 10.48550/arXiv.1606.03498.

[66] L. I. Kuncheva, *Combining pattern classifiers: methods and algorithms*. John Wiley & Sons, 2014. doi:10.1002/0471660264.

[67] V. Mnih, K. Kavukcuoglu, D. Silver, A. A. Rusu, J. Veness, M. G. Bellemare, A. Graves, M. Riedmiller, A. K. Fidjeland, G. Ostrovski, S. Petersen, C. Beattie, A. Sadik, I. Antonoglou, H. King, D. Kumaran, D. Wierstra, S.Legg and D. Hassabis, "Human-level control through deep reinforcement learning," *Nature*, vol. 518, no. 7540, pp. 529–533, 2015. doi: 10.1038/nature14236.

[68] Y. Liu, H. Wang, M. Peng, J. Guan, J. Xu, and Y. Wang, "DeePGA: A privacy-preserving data aggregation game in crowdsensing via deep reinforcement learning," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4113–4127, 2019. doi: 10.1109/JIOT.2019.2957400.

[69] X. He, R. Jin, and H. Dai, "Deep PDS-learning for privacy-aware offloading in MEC-enabled IoT," *IEEE Internet Things Journal*, vol. 6, no. 3, pp. 4547–4555, 2018. doi: 10.1109/JIOT.2018.2878718.

[70] R. Meng, Q. Cui, Z. Zhou, Z. Fu, and X. Sun, "A steganography algorithm based on CycleGAN for covert communication in the Internet of Things," *IEEE Access*, vol. 7, pp. 90574–90584, 2019. doi: 10.1109/ACCESS.2019.2920956.

[71] Y. Yan, Q. Pei, and H. Li, "Privacy-preserving compressive model for enhanced deep-learning-based service provision system in edge computing," *IEEE Access*, vol. 7, pp. 92921–92937, 2019. doi: 10.1109/ACCESS.2019.2927163.

[72] S. A. Osia, A. S. Shamsabadi, A. Taheri, H. R. Rabiee, and H. Haddadi, "Private and scalable personal data analytics using hybrid edge-to-cloud deep learning," *Computer (Long Beach Calif)*, vol. 51, no. 5, pp. 42–49, 2018. doi: 10.1109/MC.2018.2381113.

[73] S. Jiang, D. Ye, J. Huang, Y. Shang, and Z. Zheng, "SmartSteganogaphy: Light-weight generative audio steganography model for smart embedding application," *Journal of Network and Computer Applications*, vol. 165, p. 102689, 2020. doi: 10.1016/j.jnca.2020.102689.

[74] A. Dawoud, S. Shahristani, and C. Raun, "Deep learning and software-defined networks: Towards secure IoT architecture," *Internet of Things*, vol. 3, pp. 82–89, 2018. doi: 10.1016/j.iot.2018.09.003.

[75] X. Yan, Y. Xu, X. Xing, B. Cui, Z. Guo, and T. Guo, "Trustworthy network anomaly detection based on an adaptive learning rate and momentum in IIoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6182–6192, 2020. doi: 10.1109/TII.2020.2975227.

[76] H. Yao, P. Gao, P. Zhang, J. Wang, C. Jiang, and L. Lu, "Hybrid intrusion detection system for edge-based IIoT relying on machine-learning-aided detection," *IEEE Network*, vol. 33, no. 5, pp. 75–81, 2019. doi: 10.1109/MNET.001.1800479.

[77] S. Dou, K. Yang, and H. V. Poor, "Pc²a: predicting collective contextual anomalies via LSTM with deep generative model," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 9645–9655, 2019. doi: 10.1109/JIOT.2019.2930202.

[78] H. Yao, P. Gao, J. Wang, P. Zhang, C. Jiang, and Z. Han, "Capsule network assisted IoT traffic classification mechanism for smart cities," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7515–7525, 2019. doi: 10.1109/JIOT.2019.2901348.

[79] A. Azmoodeh, A. Dehghantanha, and K.-K. R. Choo, "Robust malware detection for internet of (battlefield) things devices using deep eigenspace learning," *IEEE transactions on sustainable computing*, vol. 4, no. 1, pp. 88–95, 2018. doi: 10.1109/TSUSC.2018.2809665.

[80] H. HaddadPajouh, A. Dehghantanha, R. Khayami, and K.-K. R. Choo, "A deep recurrent neural network based approach for internet of things malware threat hunting," *Future Generation Computer Systems*, vol. 85, pp. 88–96, 2018. doi: 10.1016/j.future.2018.03.007.

[81] Z. Ren, H. Wu, Q. Ning, I. Hussain, and B. Chen, "End-to-end malware detection for android IoT devices using deep learning," *Ad Hoc Networks*, vol. 101, p. 102098, 2020. doi: 10.1016/j.adhoc.2020.102098.

[82] S. Huda, S. Miah, J. Yearwood, S. Alyahya, H. Al-Dossari, and R. Doss, "A malicious threat detection model for cloud assisted internet of things (CoT) based industrial control system (ICS) networks using deep belief network," *Journal of Parallel and Distributed Computing*, vol. 120, pp. 23–31, 2018. doi: 10.1016/j.jpdc.2018.04.005.

[83] E. B. Karbab, M. Debbabi, A. Derhab, and D. Mouheb, "MalDozer: Automatic framework for android malware detection using deep learning," *Digital Investigation*, vol. 24, pp. S48–S59, 2018, doi: 10.1016/j.diin.2018.01.007.

[84] R. Taheri, R. Javidan, and Z. Pooranian, "Adversarial android malware detection for mobile multimedia applications in IoT environments," *Multimedia Tools and Applications*, vol. 80, pp. 16713–16729, 2021. doi: 10.1007/s11042-020-08804-x.

[85] R. Taheri, R. Javidan, M. Shojafar, Z. Pooranian, A. Miri, and M. Conti, "On defending against label flipping attacks on malware detection systems," *Neural Computing and Applications*, vol. 32, pp. 14781–14800, 2020. doi: 10.1007/s00521-020-04831-9.

[86] P. Mohamed Shakeel, S. Baskar, V. R. Sarma Dhulipala, S. Mishra, and M. M. Jaber, "Retracted article: maintaining security and privacy in health care system using learning based deep-Q-networks," *Journal of Medical Systems*, vol. 42, no. 10, p. 186, 2018. doi: 10.1007/s10916-018-1045-z.

[87] H. Naeem, "Detection of malicious activities in internet of things environment based on binary visualization and machine intelligence," *Wireless Personal Communications*, vol. 108, no. 4, pp. 2609–2629, 2019. doi: 10.1007/s11277-019-06540-6.

[88] S. Liu, M. Dibaei, Y. Tai, C. Chen, J. Zhang, and Y. Xiang, "Cyber vulnerability intelligence for internet of things binary," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2154–2163, 2019. doi: 10.1109/TII.2019.2942800.

[89] H. Wu, H. Shu, F. Kang, and X. Xiong, "BiN: A two-level learning-based bug search for cross-architecture binary," *IEEE Access*, vol. 7, pp. 169548–169564, 2019. doi: 10.1109/ACCESS.2019.2953173.

[90] W. Niu, X. Zhang, X. Du, L. Zhao, R. Cao, and M. Guizani, "A deep learning based static taint analysis approach for IoT software vulnerability location," *Measurement*, vol. 152, p. 107139, 2020. doi.org/10.1016/j.measurement.2019.107139. doi: 10.1016/j.measurement.2019.107139.

[91] W. Liang, W. Huang, J. Long, K. Zhang, K.-C. Li, and D. Zhang, "Deep reinforcement learning for resource protection and real-time detection in IoT environment," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6392–6401, 2020. doi: 10.1109/JIOT.2020.2974281.

[92] F. Ullah, H. Naeem, S. Jabbar, Sh. Khalid, M. A. Latif, F. Al-turjman, L. Mostarda , "Cyber security threats detection in internet of things using deep learning approach," *IEEE access*, vol. 7, pp. 124379–124389, 2019. doi: 10.1109/ACCESS.2019.2937347.

[93] L. Peng, J. Zhang, M. Liu, and A. Hu, "Deep learning based RF fingerprint identification using differential constellation trace figure," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 1, pp. 1091–1095, 2019. doi: 10.1109/TVT.2019.2950670.

[94] K. Sankhe, M. Belgiovine, F. Zhou, L. Angioloni, F. Restuccia, S. D'Oro, T. Melodia, S. Ioannidis, K. Chowdhury, "No radio left behind: Radio fingerprinting through deep learning of physical-layer hardware impairments," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 1, pp. 165–178, 2019. doi: 10.1109/TCCN.2019.2949308.

[95] R.-F. Liao *et al.*, "Security enhancement for mobile edge computing through physical layer authentication," *IEEE Access*, vol. 7, pp. 116390–116401, 2019. doi: 10.1109/ACCESS.2019.2934122.

[96] A. Ferdowsi and W. Saad, "Deep learning for signal authentication and security in massive internet-of-things systems," *IEEE Transactions on Communications*, vol. 67, no. 2, pp. 1371–1387, 2018. doi: 10.1109/TCOMM.2018.2878025.

[97] B. Chatterjee, D. Das, S. Maity, and S. Sen, "RF-PUF: Enhancing IoT security through authentication of wireless nodes using in-situ machine learning," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 388–398, 2018. doi: 10.1109/JIOT.2018.2849324.

[98] K. Youssef, L. Bouchard, K. Haigh, J. Silovsky, B. Thapa, and C. Vander Valk, "Machine learning approach to RF transmitter identification," *IEEE Journal of Radio Frequency Identification*, vol. 2, no. 4, pp. 197–205, 2018. doi: 10.1109/JRFID.2018.2880457.

[99] J. Chauhan, S. Seneviratne, Y. Hu, A. Misra, A. Seneviratne, and Y. Lee, "Breathing-based authentication on resource-constrained IoT devices using recurrent neural networks," *Computer (Long Beach Calif)*, vol. 51, no. 5, pp. 60–67, 2018. doi: 10.1109/MC.2018.2381119.

[100] S. H. Oh, G.-W. Kim, and K.-S. Lim, "Compact deep learned feature-based face recognition for Visual Internet of Things," *The Journal of Supercomputing*, vol. 74, no. 12, pp. 6729–6741, 2018. doi: 10.1007/s11227-017-2198-0.

[101] Y. Zhang *et al.*, "Cyber physical security analytics for transactive energy systems," *IEEE Transactions on Smart Grid*, vol. 11, no. 2, pp. 931–941, 2019. doi: 10.1109/TSG.2019.2928168.

[102] F. Li, Y. Shi, A. Shinde, J. Ye, and W. Song, "Enhanced cyber-physical security in internet of things through energy auditing," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5224–5231, 2019. doi: 10.1109/JIOT.2019.2899492.

[103] W. Jung, H. Zhao, M. Sun, and G. Zhou, "IoT botnet detection via power consumption modeling," *Smart Health*, vol. 15, p. 100103, 2020. doi: 10.1016/j.smhl.2019.100103.

[104] F. Li, A. Shinde, Y. Shi, J. Ye, X.-Y. Li, and W. Song, "System statistics learning-based IoT security: Feasibility and suitability," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6396–6403, 2019. doi: 10.1109/JIOT.2019.2897063.

[105] M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo, and K. Kim, "Deep abstraction and weighted feature selection for Wi-Fi impersonation detection," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 3, pp. 621–636, 2017. doi: 10.1109/TIFS.2017.2762828.

[106] X. Guo, H. Lin, Z. Li, and M. Peng, "Deep-reinforcement-learning-based QoS-aware secure routing for SDN-IoT," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6242–6251, 2019. doi: 10.1109/JIOT.2019.2960033.

[107] R.-H. Hwang, M.-C. Peng, C.-W. Huang, P.-C. Lin, and V.-L. Nguyen, "An unsupervised deep learning model for early network traffic anomaly detection," *IEEE Access*, vol. 8, pp. 30387–30399, 2020. doi: 10.1109/ACCESS.2020.2973023.

[108] M. AL-Hawawreh, N. Moustafa, and E. Sitnikova, "Identification of malicious activities in industrial internet of things based on deep learning models," *Journal of information security and applications*, vol. 41, pp. 1–11, 2018. doi: 10.1016/j.jisa.2018.05.002.

[109] P. K. Sharma, S. Singh, and J. H. Park, "OpCloudSec: Open cloud software defined wireless network security for the Internet of Things," *Computer Communications*, vol. 122, pp. 1–8, 2018. doi: 10.1016/j.comcom.2018.03.008.

[110] R. M. A. Ujjan, Z. Pervez, K. Dahal, A. K. Bashir, R. Mumtaz, and J. González, "Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN," *Future Generation Computer Systems*, vol. 111, pp. 763–779, 2020. doi: 10.1016/j.future.2019.10.015.

[111] Q. Tian, J. Li, and H. Liu, "A method for guaranteeing wireless communication based on a combination of deep and shallow learning," *IEEE Access*, vol. 7, pp. 38688–38695, 2019. doi: 10.1109/ACCESS.2019.2905754.

[112] Y. Zhang, P. Li, and X. Wang, "Intrusion detection for IoT based on improved genetic algorithm and deep belief network," *IEEE Access*, vol. 7, pp. 31711–31722, 2019. doi: 10.1109/ACCESS.2019.2903723.

[113] A. Telikani and A. H. Gandomi, "Cost-sensitive stacked auto-encoders for intrusion detection in the Internet of Things," *Internet of Things*, vol. 14, p. 100122, 2021. doi: 10.1016/j.iot.2019.100122.

[114] N. Balakrishnan, A. Rajendran, D. Pelusi, and V. Ponnusamy, "Deep Belief Network enhanced intrusion detection system to prevent security breach in the Internet of Things," *Internet of things*, vol. 14, p. 100112, 2021. doi: 10.1016/j.iot.2019.100112.

[115] A. S. Almogren, "Intrusion detection in Edge-of-Things computing," *Journal of Parallel and Distributed Computing*, vol. 137, pp. 259–265, 2020. doi: 10.1016/j.jpdc.2019.12.008.

[116] Y. Li *et al.*, "Robust detection for network intrusion of industrial IoT based on multi-CNN fusion," *Measurement*, vol. 154, p. 107450, 2020. doi: 10.1016/j.measurement.2019.107450.

[117] D. Li, L. Deng, M. Lee, and H. Wang, "IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning," *International Journal of Information Management*, vol. 49, pp. 533–545, 2019. doi: 10.1016/j.ijinfomgt.2019.04.006.

[118] J. Li and B. Sun, "A network attack detection method using SDA and deep neural network based on internet of things," *International Journal of Wireless Information Networks*, vol. 27, no. 2, pp. 209–214, 2020. doi: 10.1007/s10776-019-00462-7.

[119] S. Manimurugan, S. Al-Mutairi, M. M. Aborokbah, N. Chilamkurti, S. Ganesan, and R. Patan, "Effective attack detection in internet of medical things smart environment using a deep belief neural network," *IEEE Access*, vol. 8, pp. 77396–77404, 2020. doi: 10.1109/ACCESS.2020.2986013.

[120] X. Wang and X. Zhang, "Wireless network attack defense algorithm using deep neural network in internet of things environment," *International Journal of Wireless Information Networks*, vol. 26, pp. 143–151, 2019. doi: 10.1007/s10776-019-00430-1.

[121] A. Abeshu and N. Chilamkurti, "Deep learning: The frontier for distributed attack detection in fog-to-things computing," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 169–175, 2018. doi: 10.1109/MCOM.2018.1700332.

[122] A. Diro and N. Chilamkurti, "Leveraging LSTM networks for attack detection in fog-to-things communications," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 124–130, 2018. doi: 10.1109/MCOM.2018.1701270

[123] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things," *Future Generation Computer Systems*, vol. 82, pp. 761–768, 2018. doi:10.1016/j.future.2017.08.043.

[124] R. Kozik, M. Choraś, M. Ficco, and F. Palmieri, "A scalable distributed machine learning approach for attack detection in edge computing environments," *Journal of Parallel and Distributed Computing*, vol. 119, pp. 18–26, 2018. doi: 10.1016/j.jpdc.2018.03.006.
[125] V. M. Krundyshev, "Identifying cyberthreats in modern industrial systems by means of deep-learning networks," *Automatic Control and Computer Sciences*, vol. 53, no. 8, pp. 1006–1011, 2019. doi: 10.3103/S014641161908011X.
[126] C. U. Om Kumar and P. R. K. Sathia Bhama, "Detecting and confronting flash attacks from IoT botnets," *The Journal of Supercomputing*, vol. 75, pp. 8312–8338, 2019. doi: 10.1007/s11227-019-03005-2.
[127] G. D. L. T. Parra, P. Rad, K.-K. R. Choo, and N. Beebe, "Detecting Internet of Things attacks using distributed deep learning," *Journal of Network and Computer Applications*, vol. 163, p. 102662, 2020. doi: 10.1016/j.jnca.2020.102662.
[128] M. S. Pour *et al.*, "On data-driven curation, learning, and analysis for inferring evolving internet-of-Things (IoT) botnets in the wild," *Computers & Security*, vol. 91, p. 101707, 2020. doi: 10.1016/j.cose.2019.101707
[129] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset," *Future Generation Computer Systems*, vol. 100, pp. 779–796, 2019. doi: 10.48550/arXiv.1811.00701.
[130] A. Samy, H. Yu, and H. Zhang, "Fog-based attack detection framework for internet of things using deep learning," *Ieee Access*, vol. 8, pp. 74571–74585, 2020. doi: 10.1109/ACCESS.2020.2988854.
[131] Z. Tian, C. Luo, J. Qiu, X. Du, and M. Guizani, "A distributed deep learning system for web attack detection on edge devices," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1963–1971, 2019. doi: 10.1109/TII.2019.2938778.
[132] M. A. Ferrag and L. Maglaras, "DeepCoin: A novel deep learning and blockchain-based energy exchange framework for smart grids," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1285–1297, 2019. doi: 10.1109/TEM.2019.2922936.
[133] S. Wang and Z. Qiao, "Robust pervasive detection for adversarial samples of artificial intelligence in IoT environments," *IEEE Access*, vol. 7, pp. 88693–88704, 2019. doi: 10.1109/ACCESS.2019.2919695.
[134] S. Kim, W. Jo, and T. Shon, "APAD: Autoencoder-based payload anomaly detection for industrial IoE," *Applied Soft Computing*, vol. 88, p. 106017, 2020. doi: 10.1016/j.asoc.2019.106017.
[135] M. Li, Y. Sun, H. Lu, S. Maharjan, and Z. Tian, "Deep reinforcement learning for partially observable data poisoning attack in crowdsensing systems," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6266–6278, 2019. doi: 10.1109/JIOT.2019.2962914.
[136] Y. Xiao, Y. Jia, X. Cheng, J. Yu, Z. Liang, and Z. Tian, "I can see your brain: Investigating home-use electroencephalography system security," *IEEE Internet Things J*, vol. 6, no. 4, pp. 6681–6691, 2019. doi: 10.1109/JIOT.2019.2910115.
[137] J. Bergstra, D. Yamins, and D. Cox, "Making a science of model search: Hyperparameter optimization in hundreds of dimensions for vision architectures," in *International conference on machine learning*, PMLR, 2013, pp. 115–123.

زیرنویس

[1] Internet of Things (IoT)
[2] IoT-specific Mirai malware
[3] Deep Learning (DL)
[4] Multilayer perceptron
[5] Deep Neural Network (DNN)
[6] Distributed Denial-Of-Service (DDoS)
[7] Cloud
[8] Botnets
[9] Paradigm
[10] Near-Field Communication (NFC)
[11] Routing Protocol for Low-Power and Lossy Networks (RPL)
[12] Denial of Service attack (DoS)

[13] Media Access Control (MAC)
[14] Radio Frequency Identification (RFID)
[15] Man-In-The-Middle attack (MITM)
[16] Global Positioning System (GPS)
[17] Bias
[18] Convolutional Neural Networks (CNN)
[19] Recurrent Neural Networks (RNN)
[20] Auto Deep Encoder (ADE)
[21] Restricted Boltzmann Machine (RBM)
[22] Deep Belief Network (DBN)
[23] Generative Adversarial Network (GAN)
[24] Ensemble Deep Learning Network (EDLN)
[25] Q-learning (QL)
[26] Deep Neural Networks (DNN)
[27] Undersampling
[28] vanishing gradient
[29] exploding gradient
[30] AutoEncoder (AE)
[31] Zero-day vulnerability exploit
[32] Deep Reinforcement Learning (DRL)
[33] Deep Q-Network (DQN)
[34] Backpropagation
[35] Steganography
[36] Industrial Internet of Things (IIoT)
[37] Benign Network Traffic
[38] Operation Code (Opcode)
[39] Radio Frequency Fingerprint (RFF)
[40] Long Short-Term Memory (LSTM)
[41] Orthogonal Frequency-Division Multiplexing (OFDM)
[42] Quality Of Service (QoS)
[43] Multi-CNN Fusion
[44] Phishing attacks
[45] Bidirectional Long Short-Term Memory (BiLSTM)
[46] Gated Recurrent Units (GRU)
[47] Web Attack
[48] Internet of Everything (IoE)
[49] Data Poisoning Attacks
[50] Electroencephalography (EEG)
[51] Crowdsensing
[52] Software-Defined Networking (SDN)
[53] Sequential Model-Based Optimization (SMBO)