Tabriz Journal of Electrical Engineering (TJEE), vol. 53, no. 2, Summer 2023 Serial no. 104
DOI: 10.22034/tjee.2023.16066

Improving Detection of Intrusion to Internet of Things Network Using Deep Learning and Chaotic Krill Optimization Algorithm

Mona Zendehdell[1], Javad Hamidzadeh[2*]

[1]Faculty of Computer Engineering and Information Technology, Sadjad University, Iran, Mashhad, mon.zendehdel877@sadjad.ac.ir
[2*] Associate Professor, Faculty of Computer Engineering and Information Technology, Sadjad University, Iran, Mashhad, j_hamidzadeh@sadjad.ac.ir

Abstract
The Internet of Things is a new technology that communicates with the surrounding objects through the Internet and is used for the purpose of remote measurement and control. Today, the rapid development of Internet of Things (IoT) technology in the world has also caused the frequent occurrence of network attacks. In the field of Internet of Things (IoT) network security, it is very important to accurately identify the types of attacks on these networks that are launched by zombie hosts under the control of the attacker. To reduce these threats, new methods are needed to identify the attacks that have compromised IoT devices in the shortest possible time and prevent the losses caused by the attacks. In this article, a new neural network is proposed to improve the detection of intrusion into the Internet of Things network based on the ALEXNET convolutional neural network and chaotic krill optimization algorithm (MONANET). In the MONANET network, in order to improve the accuracy in detecting intrusion into the IoT network and not need to manually adjust the parameters, the hyperparameters of the neural network are dynamically selected using the chaotic krill algorithm. The value of the loss function of the validation set obtained from the first training of the neural network model using the Danmini doorbell dataset is considered as the CKH fitness value. The comprehensive performance of the proposed network and GRU, ANN, SVM, LSTM, FNN, R-CNN, and APSO-CNN algorithms have been compared in five evaluation indices and 12 times independent experiments. The obtained results show the improvement of intrusion detection to the Internet of Things network. The proposed algorithm has been able to accurately detect%99.89 attacks on the Internet of Things network. The experimental results show the superiority of the proposed method over other knowledge boundary methods in terms of improving classification accuracy.

Keywords
MONANET network, Convolutional neural network, Alexnet network, IoT Network Security, Chaotic Krill Herd (CKHA), Attack Detection.

1- Short Introduction
Today, the expansion of the Internet of Things devices has caused network attacks. Therefore, timely identification of these attacks is very important. In this article, a combined method of deep learning and chaotic krill algorithm is proposed to detect intrusion into the Internet of Things network. Neural networks has hyperparameters that take time to adjust manually. Therefore, using the chaotic krill herd algorithm, it optimized the neural network's meta-parameters and then, with these hyperparameters, adjusted the neural network and detected the attacks on the Internet of Things network well.

2- Proposed Work and Methodology
In this work, a new neural network has been introduced for the timely detection of attacks on the Internet of Things network based on the Alexnet neural network and the Chaotic Krill Herd optimization algorithm.
The innovations of this work can be summarized in the following two aspects:

- Using the Chaotic Krill Herd optimization algorithm, the hyperparameters of the neural network model are determined for a specific dataset.
- Using the method of this work for each problem, a special neural network is created that guarantees the accuracy and stability of the system for that problem.

3- Conclusion
In this article, a new MONANET algorithm is proposed, which has been able to detect different attacks launched on IoT networks with 99.89% accuracy. Compared to the other 7 methods, APSO-CNN, FNN, R-CNN, SVM, LSTM, ANN, and GRU has been evaluated in detecting attacks on the IoT network. The evaluation results show that the proposed algorithm has not only achieved high accuracy in detecting network attacks, but the stability of the proposed algorithm has improved compared to other algorithms.

4- References
[4] Y.Meidan, M.Bohadana, Y.Mathov, Y.Mirsky, A.Shabtai, D.Breitenbacher, Y.Elovici. "N-BaIoT: network-based detection of iot botnet attacks using deep autoencoders." IEEE Pervasive Computing 17, no.3, PP.12-22, 2018.
[6] M.Mudassir, D.Unal, M.Hammoudeh, F.Azzedin. "Detection of Botnet Attacks against Industrial IoT Systems by Multilayer Deep Learning Approaches." Wireless Communications and Mobile Computing, 2022.
[16] X.Kan, Y.Fan, Z.Fang, L.Cao, Neal N. Xiong, D.Yang, X.Li, "A novel IoT network intrusion detection approach based on adaptive particle swarm optimization convolutional neural network." Information Sciences 568, PP.147-162, 2021.

بهبود تشخیص نفوذ به شبکه اینترنت اشیاء با استفاده از یادگیری عمیق و الگوریتم بهینه‌سازی میگوی آشوبی

[۱] منا زنده‌دل، [۲*] جواد حمیدزاده
[۱] دانشجوی ارشد مهندسی کامپیوتر گرایش هوش مصنوعی و رباتیک، دانشگاه سجاد، مشهد، ایران
[۲*] دانشیار، دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه سجاد، مشهد، ایران

چکیده

اینترنت اشیاء، یک فناوری جدید است که این فناوری از طریق اینترنت با اشیاء پیرامون خود ارتباط برقرار می‌کند و باهدف سنجش و کنترل از راه دور استفاده می‌گردد. امروزه توسعه سریع فناوری اینترنت اشیاء در جهان باعث بروز مکرر حملات شبکه‌ای نیز شده است. در زمینه امنیت شبکه اینترنت اشیاء (IoT)، شناسایی دقیق انواع حملات به این شبکه‌ها که توسط میزبان‌های زامبی تحت کنترل مهاجم راه‌اندازی می‌شوند، اهمیت زیادی دارد. برای کاهش این تهدیدات، به روش‌های جدیدی نیاز است تا حملاتی که دستگاه‌های IoT را به خطر انداخته است، در کم‌ترین زمان ممکن شناسایی و از زیان‌های ناشی از حملات جلوگیری کنند. در این مقاله، یک شبکه عصبی جدید جهت بهبود تشخیص نفوذ به شبکه اینترنت اشیاء بر اساس شبکه عصبی کانولوشنال ALEXNET و الگوریتم بهینه‌سازی میگوی آشوبی به نام (MONANET) پیشنهاد شده است. در شبکه MONANET به‌منظور بهبود دقت در تشخیص نفوذ به شبکه IOT و عدم نیاز به تنظیم دستی پارامترها، فراپارامترهای شبکه عصبی با استفاده از الگوریتم میگوی آشوبی به‌صورت پویا انتخاب می‌شوند. مقدار تابع تلفات مجموعه اعتبارسنجی که از اولین آموزش مدل شبکه عصبی با استفاده از مجموعه‌داده Danmini doorbell به دست می‌آید، به‌عنوان مقدار تناسب CKH در نظر گرفته می‌شود. عملکرد جامع شبکه پیشنهادی و الگوریتم‌های R-CNN،FNN،LSTM، SVM، ANN،GRU و APSO-CNN در پنج شاخص ارزیابی و در ۱۲ اجرای مستقل مقایسه شده‌اند. نتایج به‌دست‌آمده نشان‌دهنده بهبود تشخیص نفوذ به شبکه اینترنت اشیاء است. الگوریتم پیشنهادی توانسته است با دقت ۹۹.۸۹٪ حملات به شبکه اینترنت اشیاء را تشخیص دهد. نتایج تجربی برتری روش پیشنهادی را نسبت به سایر روش‌های مرز دانش ازنظر بهبود دقت طبقه‌بندی نشان می‌دهد.

کلیدواژگان

شبکه MONANET، شبکه عصبی کانولوشن، شبکه ALEXNET، الگوریتم میگوی آشوبی (CKHA)، امنیت شبکه اینترنت اشیاء، تشخیص نفوذ

نام نویسنده مسئول: دکتر جواد حمیدزاده
ایمیل نویسنده مسئول: j_hamidzadeh@sadjad.ac.ir

تاریخ ارسال مقاله: ۱۴۰۱/۰۹/۱۰
تاریخ (های) اصلاح مقاله: ۱۴۰۱/۱۱/۰۴
تاریخ پذیرش مقاله: ۱۴۰۲/۰۱/۰۵

Tabriz Journal of Electrical Engineering (TJEE), vol. 53, no. 2, Summer 2023 Serial no. 104
DOI: 10.22034/tjee.2023.16066

۱- مقدمه

اینترنت اشیاء(IOT) ، یک مفهوم جدید در دنیای فناوری و ارتباطات است. عبارت اینترنت اشیاء به اتصال اشیاء موجود در محیط پیرامون به شبکه اینترنت گفته می‌شود. اینترنت اشیاء ارائه‌دهنده سهولت و کیفیت زندگی مصرف‌کنندگان با فناوری‌های مختلف است. اینترنت اشیاء شامل دستگاه‌های پیچیده‌ای است که بدون دخالت انسان حجم زیادی از داده را به اشتراک می گذارند، ازآنجاکه تعداد این دستگاه‌ها هرروزه در حال افزایش است؛ حجم ترافیک حملات DDOS مبتنی بر اینترنت اشیاء در راستای افزایش این دستگاه‌ها افزایش‌یافته است [۱]. با افزایش استفاده از دستگاه‌ها، کاربران بیشتری مستعد حملات سایبری شده‌اند؛ بنابراین تهدیدات موجود علیه این دستگاه‌ها باید تجزیه‌وتحلیل شوند تا مکانیسم‌های محافظتی در برابر آن‌ها ایجاد شود. ازآنجاکه اینترنت اشیاء برای کارکرد به اینترنت متکی است باید امنیت را مهم‌ترین چالش آن در نظر گرفت [۲]. در عصر فنّاوری اطلاعات، امنیت سایبری در اینترنت اشیاء از اهمیت بالایی برخوردار است دستگاه‌های متصل به شبکه‌های IoT در معرض حملات سایبری هستند و امنیت آن‌ها ازجمله نگرانی‌های اصلی است که بر قابلیت استفاده از آن‌ها تأثیر می‌گذارد، روش‌های موجود برای تأمین امنیت، ازنظر تجزیه‌وتحلیل داده‌ها در زمان واقعی و جلوگیری از حملات سایبری به برنامه‌های IoT، نیاز به بهبود دارند [۳]. تشخیص آنی امنیت شبکه را ارتقا می‌دهد، چون هشدار و قطع اتصال دستگاه‌های IoT آسیب‌دیده از شبکه را سرعت می‌بخشد، درنتیجه از انتشار بات نت جلوگیری می‌کند و از ترافیک حملات خروجی بیشتر جلوگیری می‌کند [۴]. تاکنون مطالعات بسیار زیادی در این زمینه برای شناسایی دقیق و فوری حملات به شبکه اینترنت اشیاء انجام‌گرفته است. این پژوهش‌ها بااینکه توانسته‌اند تا حد مطلوبی دقت در تشخیص نفوذ را بهبود دهند، بااین‌حال هنوز دارای چالش‌هایی هستند.

ازآنجاکه تنظیم دستی پارامترهای شبکه عصبی زمان‌بر و پیچیده است و عدم شناسایی به هنگام حملات باعث زیان‌های جبران‌ناپذیر به شبکه می‌شود؛ بنابراین تحقیقات فعلی با چالش‌های زیر روبرو هستند:

فرا پارامترهای شبکه‌های عصبی در مطالعات انجام‌شده نیاز به بهبود دارند، دقت در تشخیص بات نت‌ها نیاز به بهبود دارد، پیش‌بینی بات نت‌های نوظهور و دیده نشده. هدف از این پژوهش را می‌توان به شرح ذیل بیان کرد:

- شناسایی حملات در شبکه اینترنت اشیاء و افزایش امنیت در شبکه
- کاهش زیان حملات به شبکه با شناسایی به‌موقع حملات
- بهینه‌سازی و تنظیم فراپارامترهای مدل شبکه Alexnet با استفاده از الگوریتم CKH به‌منظور بهبود دقت در تشخیص نفوذ به شبکه‌های Iot
- عدم نیاز به تنظیم پارامترها به‌صورت دستی

مشارکت‌های اصلی این مقاله را می‌توان در دو جنبه به شرح زیر خلاصه کرد:

از یک نقشه آشوبی به‌منظور تسریع در سرعت همگرایی جهانی، الگوریتم بهینه‌سازی میگو استفاده شده است. نقشه آشوب برای تنظیم سه حرکت اصلی میگو در فرایند بهینه‌سازی در نظر گرفته شده است؛ در الگوریتم میگو آشوبی پارامترهای ساختار ALEXNET به‌عنوان عناصر موقعیت الگوریتم میگوآشوبی در نظر گرفته می‌شوند و مقدار تابع (cross entropy) مجموعه اعتبارسنجی تحت اولین دوره آموزش ALEXNET به‌عنوان تابع برازش الگوریتم میگو آشوبی در نظر گرفته می‌شود.

الگوریتم پیشنهادی توانسته است با دقت مطلوبی حملات مختلفی که در دستگاه‌های IOT راه‌اندازی می‌شوند را تشخیص دهد. نتایج تجربی برتری روش پیشنهادی را نسبت به سایر روش‌های مرز دانش ازنظر دقت طبقه‌بندی نشان می‌دهد.

ساختار ادامه مقاله به شرح ذیل است: در بخش دوم کارهای مرتبط موردبررسی قرار گرفته است. در بخش سوم مفاهیم و تعاریف روش‌ها و الگوریتم‌های مورداستفاده در این مقاله بررسی شده است. بخش چهارم روش پیشنهادی را تشریح می‌کند. در بخش پنجم آزمایش‌ها، مقایسه و نتایج موردبحث قرار گرفته است. درنهایت، در بخش ششم نتیجه‌گیری و کارهای آینده را برجسته می‌کند.

۲- کار مرتبط

اینترنت اشیاء در حال حاضر یکی از جدیدترین موضوعات تحقیقاتی است. دستگاه‌هایی که از این فناوری بهره‌مند هستند، اطلاعاتی را ارسال و دستوراتی را دریافت می‌کنند که به همین دلیل احتمال نفوذ هکرها در حین ارسال و دریافت اطلاعات وجود دارد. چالش‌های امنیتی زیادی در زمینه اینترنت اشیاء وجود دارد که رفع این چالش‌ها از اهمیت بسیار بالایی برخوردار است تا کاربران اطمینان داشته باشند که دستگاه‌های مجهز به اینترنت اشیاء از هرگونه آسیب‌پذیری ایمن هستند [۲]. ازآنجایی‌که تعداد دستگاه‌های اینترنت اشیاء مستقرشده در دنیا به‌طور چشمگیری افزایش می‌یابد و حجم ترافیک حملات DDoS مبتنی بر اینترنت اشیاء بیشتر می‌شود، نیاز مبرم به تشخیص به‌موقع چنین حملاتی برای کاهش خطرات مرتبط با آن‌ها وجود دارد [۵].

در سال ۲۰۱۸ میدان و همکاران، یک روش جدید تشخیص ناهنجاری مبتنی بر شبکه اینترنت اشیاء به نام N-BAIOT پیشنهاد دادند؛ که عکس‌های فوری رفتاری شبکه را استخراج می‌کند و از رمزگذارهای خودکار عمیق برای شناسایی استفاده می‌کنند. هنگامی‌که رمزگذار خودکار نتواند یک عکس فوری را بازسازی کند، این نشانه قوی است که رفتار مشاهده‌شده غیرعادی است [۴]. در سال ۲۰۲۲ مدسر و همکاران، از سه نوع مختلف از مدل‌های مبتنی بر یادگیری عمیق LSTM، GRU و ANN برای طبقه‌بندی حملات بات نت در شبکه‌های IOT استفاده کرده‌اند. هر سه مدل دارای عملکرد بالایی نسبت به سایر روش‌های مقایسه شده هستند [۶]. در سال ۲۰۱۸ خان و صلاح، در پژوهشی طبقه‌بندی IOT و عناصر معماری آن را شرح داده و یک پلتفرم عمومی IOTپیشنهاد کردند و حملات موجود و مشکلات امنیتی اصلی هر لایه در دستگاه‌های IoT را موردبحث قرار داده‌اند [۷]. در سال ۲۰۱۹ فی و همکاران، تکنیک‌های حفاظت از حریم خصوصی را ارائه دادند [۸]. در سال ۲۰۲۰ پررا و همکاران، بر روی تکنیک‌های تشخیص نفوذ مبتنی بر روش‌های یادگیری ماشین (ML) تمرکز کرده‌اند [۹]. در سال ۲۰۲۰ پودل و همکاران، بررسی‌های جامعی در مورد استراتژی‌های تجزیه‌وتحلیل IDS در معماری IOT به همراه تکنیک‌های ML و DL برای تشخیص حملات در شبکه‌های IOT و مسائل امنیتی و چالش‌های آن انجام دادند [۱۰]. در سال ۲۰۲۲ جویباری و همکاران، یک روش جدید با استفاده از پرسپترون چندلایه برای شناسایی حملاتDDoS و یادگیری عمیق معرفی کردند [۱۱].

در سال ۲۰۲۰ پارا و همکاران، یک چارچوب یادگیری عمیق توزیع‌شده مبتنی بر ابر برای شناسایی و کاهش حملات فیشینگ و بات نت پیشنهاد داده‌اند. این مدل شامل دو مکانیسم امنیتی کلیدی DCNN و LSTM است که به‌صورت مشترک کار می‌کنند [۱۲]. در سال ۲۰۲۰ شورمن و همکاران، یک روش جدید برای شناسایی بات نت با استفاده از ماشین بردار پشتیبان و الگوریتم بهینه‌سازی گرگ خاکستری ارائه داده‌اند. در این روش پارامترهای ماشین بردار پشتیبان نظیر ضریب جریمه و خطای تخطی از طریق الگوریتم بهینه‌سازی گرگ خاکستری بهینه می‌شوند [۱۳]. در سال ۲۰۲۰ حسینی و حسنی زاده، یک

روش ترکیبی جدید برای تشخیص حمله با استفاده از ترکیب الگوریتم‌های تکاملی، ماشین بردار پشتیبان و شبکه عصبی مصنوعی ارائه داده‌اند. در مرحله انتخاب ویژگی، از روش GA-SVM و در مرحله شناسایی حمله، از یک شبکه عصبی مصنوعی برای شناسایی حملات استفاده می‌شود. برای بهبود عملکرد آن، ترکیبی از جستجوی جاذبه و بهینه‌سازی ازدحام ذرات برای آموزش طبقه‌بندی استفاده شده است [۱۴]. در سال ۱۳۹۷ قومنجانی و حمیدزاده، یک دسته‌بند تک کلاسه جدید برای داده‌های نویزی به نام KH-SVDD معرفی کرده‌اند؛ موقعیت مرکز آبرکُره در فضای ویژگی‌های داده‌ها با استفاده از الگوریتم SVDD و الگوریتم میگوی آشوبی محاسبه شده است [۱۵]. در سال ۲۰۲۱ کن و همکاران، یک رویکرد جدید تشخیص نفوذ به شبکه اینترنت اشیاء بر اساس APSO-CNN پیشنهاد دادند. روش پیشنهادی با موفقیت برای تشخیص حملات multi-type راه‌اندازی شده و توسط میزبان‌های آلوده به ویروس‌های زامبی مورداستفاده قرار گرفته است. نتایج شبیه‌سازی، نشان‌دهنده برتری روش پیشنهادی نسبت به سایر روش‌های پیشین بوده است [۱۶].

باانگیزه بحث بالا، این مقاله روشی را برای بهینه‌سازی فراپارامترهای ساختار شبکه ALEXNET بر اساس الگوریتم CKH ارائه می‌کند که با موفقیت برای تشخیص حملات شبکه multi-type اعمال شده است.

۳- مفاهیم اولیه

۳-۱- ALEXNET

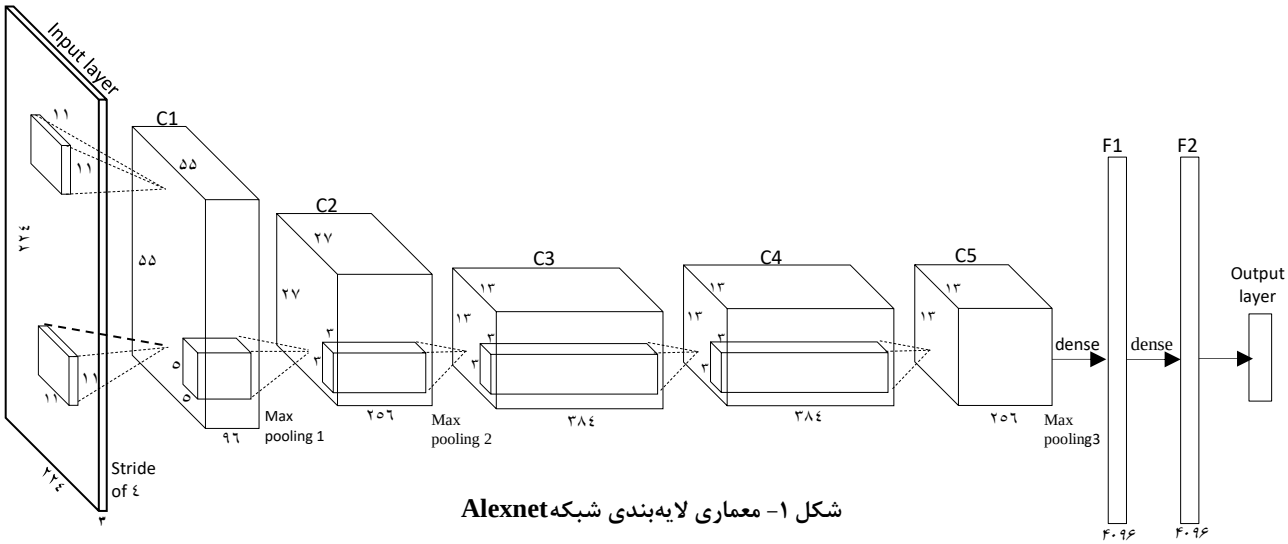
شبکه عصبی الکس نت، یک شبکه عصبی کانولوشنی عمیق است که به‌منظور شناسایی و طبقه‌بندی تصاویر رنگی با اندازه ۳×۲۲۴×۲۲۴ ارائه شده است. این شبکه عصبی دارای ۱۱ لایه است که از ۵ لایه کانولوشن و ۳ لایه اتصال کامل و ۳ لایه ادغام تشکیل شده است؛ لایه‌بندی شبکه عصبی الکس نت در شکل ۱ نمایش‌داده‌شده است.

تابع تلفات متقاطع آنتروپی H(p, q) برای اندازه‌گیری فاصله بین توزیع احتمال واقعی p(x) و توزیع احتمال محاسبه شده q(x) استفاده می‌شود که به‌صورت زیر نشان‌داده‌شده است [۱۶]:

$$\mathbf{H(p.q)} = -\sum_{\mathbf{x}} \mathbf{p(x)\log q(x)} \qquad (۱)$$

۳-۲- الگوریتم میگو آشوبی

عملکرد الگوریتم گروه میگوها مشابه سایر الگوریتم‌های فرا ابتکاری است که از نوع الگوریتم‌های بیولوژیکی هستند. عملکرد گروه میگوها بر اساس رفتار توده‌وار



شکل ۱- معماری لایه‌بندی شبکه Alexnet

میگوها در پاسخ به فرایند بیولوژیکی و زیست‌محیطی خاص است. آن‌ها بر اساس مکانیزم‌های اصلی رفتار میگوها را مدل‌سازی و درنهایت بهینه‌سازی ریاضی را بر اساس این روش استخراج می‌کنند.

هدف از الگوریتم گروه میگوها این است که بتوانیم یک مسئله بهینه‌سازی سراسری را حل کنیم و هدف این الگوریتم افزایش تراکم میگوها و دستیابی غذا خواهد بود که درنتیجه تشکیل یک توده از میگوها در محل غذا خواهیم داشت. موقعیت هر میگو که وابسته به زمان است توسط ۳ حرکت اصلی تعیین می‌شود که عبارت‌اند از: حرکت ناشی از سایر میگوهای موجود در جمعیت ((N، جستجوی غذا ((F، انتشار تصادفی ((D.

$$\frac{\boldsymbol{dx_i}}{\boldsymbol{dt}} = \boldsymbol{N_i} + \boldsymbol{F_i} + \boldsymbol{D_i} \qquad (۲)$$

اگر مقدار برازندگی هر یک از پارامترهای مؤثر ارائه شده بهتر از مقدار برازندگی میگو باشد اثر آن به‌صورت دافعه است؛ بنابراین در الگوریتم اصلی KH، موقعیت فعلی میگو در بازه زمانی t تا Δt با استفاده از رابطه ۳ به دست می‌آورد.

$$\boldsymbol{X_i(t+\Delta t) = X_i(t) + \Delta t\frac{dX_i}{dt}} \qquad (۳)$$

آشوب پدیده‌ای است که در سیستم‌های غیرخطی تعریف‌پذیر رخ می‌دهد؛ به دلیل تعریف‌پذیری سیستم چون رفتار غیرتصادفی دارد خروجی آن تصادفی مانند است. در میگو وزن‌های اینرسی w_n و w_f در مرحله جستجوی اولیه ابتدا روی ۰.۹ تنظیم می‌شود و سپس به ۰.۱ کاهش می‌یابد ولی نیازی نیست که به‌صورت خطی کاهش پیدا کند بلکه وزن‌های تصادفی ممکن است همگرایی الگوریتم بهینه‌سازی را سرعت بخشند؛ بعد از نرمال‌سازی محدوده یک نقشه آشوبی بین ۰ تا ۱ است. به همین دلیل برای تعیین وزن‌های اینرسی از یک نقشه آشوبی که حالت تصادفی مانند دارند استفاده می‌شود. در این پژوهش از نقشه آشوبی singer map استفاده شده است.

$$\mathbf{X_{k+1} = \mu(7.86X_k - 23.31X_k^2 + 28.75X_k^3 - 13.3028X_k^4)} \qquad (۴)$$

۴- روش پیشنهادی

Tabriz Journal of Electrical Engineering (TJEE), vol. 53, no. 2, Summer 2023 Serial no. 104
DOI: 10.22034/tjee.2023.16066

در این پژوهش از شبکه عصبی Alexnet استفاده می‌شود که این شبکه عصبی دارای فراپارامترهایی است که تنظیم دستی این فراپارامترها زمان‌بر است؛ بنابراین برای تنظیم این فراپارامترها از الگوریتم بهینه‌سازی استفاده می‌شود. در گام اول از الگوریتم ACKH برای پیدا کردن فراپارامترهای بهینه شبکه عصبی Alexnet استفاده می‌شود. در گام بعدی از مدل Alexnet تنظیم‌شده توسط ACKH برای تشخیص نوع حمله به شبکه IOT استفاده می‌شود. معماری شبکه عصبی MONANET در شکل ۳ نمایش‌داده‌شده است. در مدلAlexnet ، ۲۳ فراپارامتر داریم که این فراپارامترها، عناصر موقعیت میگو در الگوریتم CKH را تشکیل می‌دهند. در ابتدا، عناصر موقعیت میگوها به‌صورت تصادفی مقداردهی اولیه می‌شوند. محدوده تنظیم عناصر موقعیت هر میگو در جدول ۱ نشان‌داده‌شده است.

جدول ۱- محدوده مقدار پارامترهای موقعیت

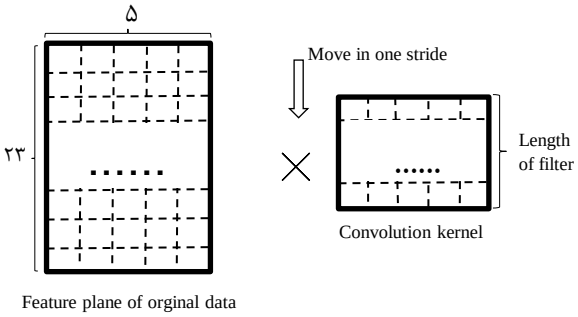
Position	Hyperparameter	Particle value range
x1	C1_n_filter	32-100(type int)
x2	C1_filter_len	[3,5,7](type int)
x3	C1_act	{tanh, relu, LeakyReLU, elu}
x4	C2_n_filter	100-260(type int)
x5	C2_filter_len	[1,3](type int)
x6	C2_act	{tanh, relu, LeakyReLU, elu}
x7	C3_n_filter	200-390(type int)
x8	C3_filter_len	[1,3](type int)
x9	C3_act	{tanh, relu, LeakyReLU, elu}
x10	C4_n_filter	200-390(type int)
x11	C4_filter_len	[1,3](type int)
x12	C4_act	{tanh, relu, LeakyReLU, elu}
x13	C5_n_filter	100-260(type int)
x14	C5_filter_len	[1,3](type int)
x15	C5_act	{tanh, relu, LeakyReLU, elu}
x16	D1_neuron	2048-4096(type int)
x17	D1_act	{tanh, relu, LeakyReLU, elu}
x18	D1_D2_dropout	0.2-0.8(type float)
x19	D2_neuron	500-2048(type int)
x20	D2_act	{tanh, relu, LeakyReLU, elu}
x21	D2_Out_dropout	0.2-0.8(type float)
x22	batch_size	32-200(type int)
x23	learning rate	0.0001-0.0009(type float)

در جدول ۱: C1_n_filter تعداد هسته کانولوشن در لایه C1 است، C1_filter_len طول فیلتر در لایه C1 است، C1_act نوع تابع فعال‌سازی در لایه C2 است، C2_n_filter تعداد هسته کانولوشن در لایه C2 است، C2_filter_len طول فیلتر در لایه C2 است، C2_act نوع تابع فعال‌سازی در لایه C1 است، C3_n_filter تعداد هسته کانولوشن در لایهC3 است، C3_filter_len طول فیلتر در لایه C3 است، C3_act نوع تابع فعال‌سازی در لایه C3 است، C4_n_filter تعداد هسته کانولوشن در لایهC4 است، C4_filter_len طول فیلتر در لایه C4 است، C4_act نوع تابع فعال‌سازی در لایه C4 است، C5_n_filter تعداد هسته کانولوشن در لایهC5 است، C5_filter_len طول فیلتر در لایه C5 است، C5_act نوع تابع فعال‌سازی در لایه C5 است، D1_neuron تعداد نرون‌های لایه D1 است، D1_act نوع تابع فعال‌سازی در لایه D1 است، D1_D2_dropout اندازه لایه حذف تصادفی بین لایه‌های D1 و D2 است، D2_neuron تعداد نرون‌های لایه D1 است، D2_act نوع تابع فعال‌سازی در لایه D2 است، D2_Out_dropout اندازه لایه حذف تصادفی بین لایه D2 و لایه خروجی است، batch_size اندازه نمونه آموزشی است و Lrate نرخ آموزش مدل است.

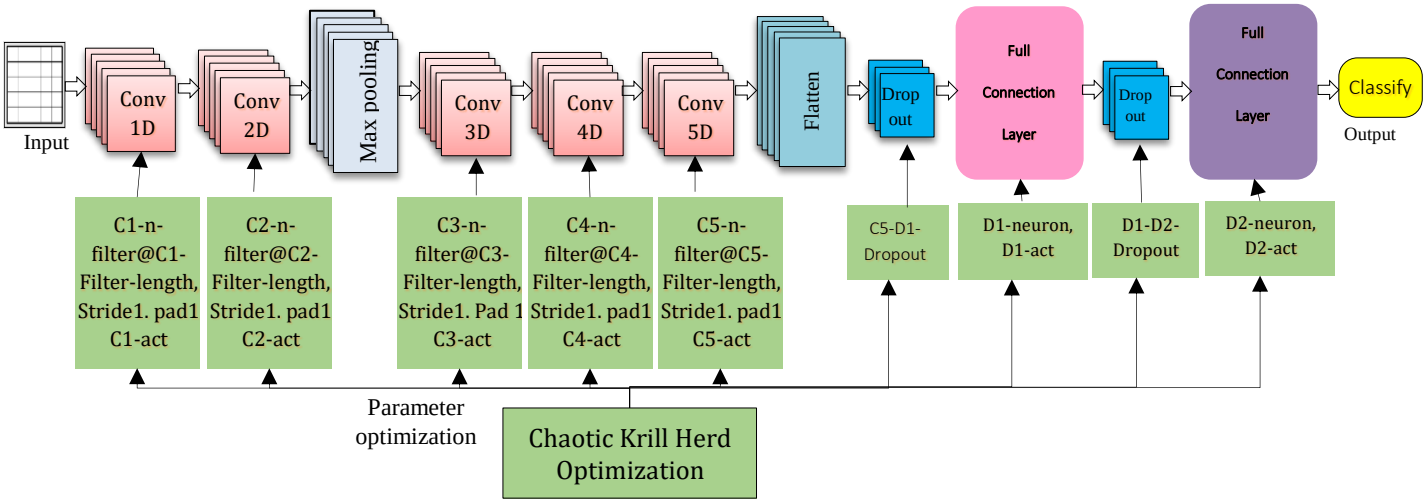
روش کار به این صورت است که از تابع تلفات متقاطع مدل Alexnet در اجرای اول به‌عنوان تابع برازش در الگوریتم CKH استفاده می‌شود که باید این مقدار کمینه شود. برای محاسبه تابع تلفات متقاطع مدل Alexnet از مجموعه‌داده Danmini doorbellاستفاده شده است؛ سپس برای هر میگو مقدار تابع برازش محاسبه می‌شود. درنهایت پس از اتمام اجرای الگوریتم میگوی آشوبی، فراپارامترهای بهینه مدل Alexnet توسط الگوریتم میگوی آشوبی به دست می‌آید. برای ایجاد جمعیت اولیه از یک روش حریصانه برای جایگزینی فراپارامترها به‌جای عناصر الگوریتم CKH استفاده شده است. در این روش ابتدا اعداد تصادفی بین (۱ تا ۱-) به هر عنصر در بردار موقعیت الگوریتم CKH اختصاص‌داده‌شده است. با استفاده از رابطه H_i فراپارامترهای بهینه مدل Alexnet ما مشخص می‌شود.

$$\boldsymbol{H_i} = \lfloor (\mathbf{Min_i} + ((\boldsymbol{X_i} + \mathbf{1})/\mathbf{2}) * (\mathbf{Max_i} - \mathbf{Min_i})) \rfloor \qquad (۵)$$

که در رابطه بالا، H_i، مقدار فراپارامتر i ام در مدل Alexnet Min_i، حد پایین فراپارامتر iام Max_i، حد بالای فراپارامتر iام و علامت ⌊ ⌋، گرد کردن به سمت پایین می‌باشد. فرآیند پیچیدگی یک‌بعدی در شکل۲ نشان داده شده است. در روش پیشنهادی از چهار نوع توابع فعال‌سازی غیرخطی tanh, relu, LeakyReLU, elu استفاده شده است؛



شکل ۲- فرآیند پیچیدگی یک بعدی [۱۶].



شکل ۳- معماری شبکه عصبی **MONANET**

Tabriz Journal of Electrical Engineering (TJEE), vol. 53, no. 2, Summer 2023 Serial no. 104
DOI: 10.22034/tjee.2023.16066

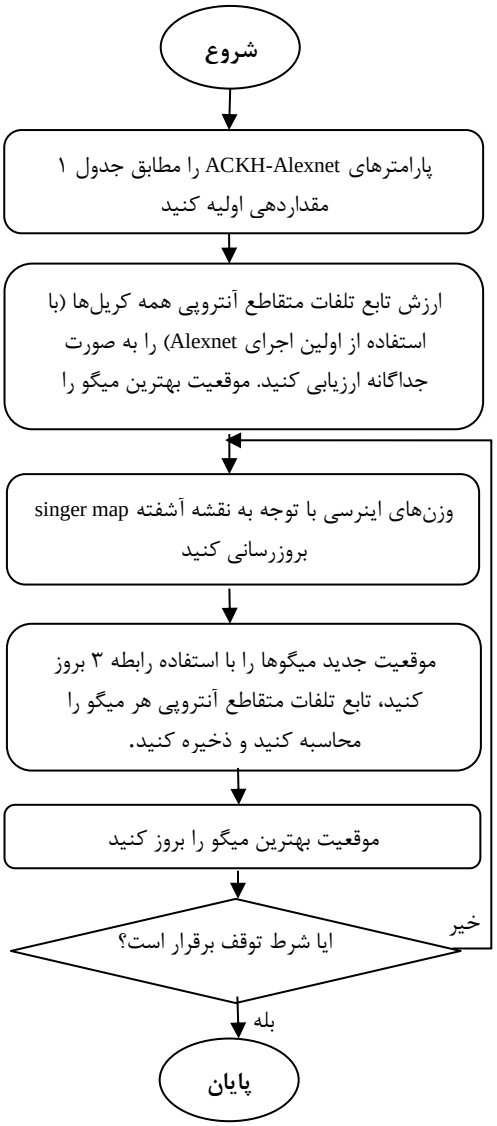
الگوریتم ۱ روند جستجوی پارامترهای ساختار بهینه Alexnet فوق را شرح می‌دهد. عناصر موقعیت هر میگو مربوط به فراپارامترهای ساختار شبکه Alexnet است و بهترین فراپارامترهای ساختار شبکه را می‌توان از طریق الگوریتم بهینه‌سازی ACKH پیدا کرد. به‌طورکلی، از تابع تلفات متقاطع آنتروپی در اولین اجرای مدل Alexnet به‌عنوان تابع تناسب الگوریتم CKH استفاده می‌شود. الگوریتم CKH تلاش می‌کند این مقدار را کاهش دهد. هر چه اندازه تابع برازش کمتر باشد، عملکرد مدل بهتر خواهد بود. به‌عنوان یک تابع درست‌نمایی لگاریتمی، تابع Loss-Function متقابل آنتروپی اغلب در طبقه‌بندی باینری و وظایف طبقه‌بندی چندگانه استفاده می‌شود [۱۶]. علاوه بر این، در مدل Alexnet، برچسب‌های واقعی به‌صورت بردارهای باینری کدگذاری می‌شوند و احتمال پیش‌بینی هر دسته از طریق لایه خروجی که دارای تابع فعال‌سازی softmax است به دست می‌آید.

در این روش، به دلیل قدرت بالای مدل Alexnet در آموزش، نیازی نیست تابع تلفات متقاطع آنتروپی را که با استفاده از الگوریتم بهینه‌سازی در اولین چرخه آموزشی به دست می‌آید را خیلی کاهش دهیم؛ بنابراین، نیاز به تعداد جمعیت، تعداد تکرار و تعداد اجراهای زیادی در الگوریتم بهینه‌سازی CKH نخواهیم داشت که این باعث افزایش سرعت تعیین فراپارامترها توسط الگوریتم CKH و افزایش سرعت آموزش مدل Alexnet می‌شود. نمودار جریان الگوریتم ACKH در شکل ۴ نشان‌داده‌شده است.

Algorithm 1 *The algorithm for searching for the optimal hyperparameters*

1. ***Initialize***:
   Set the position parameter x_i^t *according to Table 1;*
   2. *Calculate fitness value. Evaluate the cross_entropy loss_ function value of all krils individually (using the first Alexnet run);*
   3. *Save the position of the best krill*
4. ***while****: as long as the stop condition is met;*
   5. *Update the inertia weights using chaotic maps according to singermap in Equation 4;*
   6. *Update the new position of the krill using Equation 3;*
   7. *Update and save the cross entropy loss function value of each krill;*
   8. *Update the position of the best krill*
9. ***end while***
10. ***Output***: *The optimal hyperparameters.*

همان‌طور که در نمودار جریان شکل ۴ مشاهده می‌شود:
مرحله اول، مقداردهی اولیه عنا صر موقعیت در الگوریتم ACKH مطابق جدول ۱ اســـت. در مرحله دوم، ارزش تابع تلفات متقاطع آنتروپی همه میگوها (با اســـتفاده از اولین اجرای Alexnet) را به‌صـــورت جداگانه ارزیابی می‌کنیم و موقعیت بهترین میگو ذخیره می‌شود. در مرحله سوم وزن اینرسی طبق نقشه آشـــوبی singer map به‌صـــورت تطبیقی به‌روز می‌شـــود. در مرحله چهارم، پارامترهای موقعیت در ACKH بر اساس فرمول (۳) به‌روز می‌شوند و موقعیت جدید میگوها بعد از به‌روزرســـانی ذخیره می‌شـــوند. در مرحله پنجم، موقعیت بهترین میگو به‌روزرســـانی می‌شـــود و در مرحله آخر اگر شـــرط توقف برآورده نشد، برای ادامه تکرار به مرحله سوم خواهیم رفت. در غیر این صورت، تکرار را متوقف کرده و موقعیت بهترین میگو به‌عنوان فراپارامترهای بهینه مدل شـــبکه عصـــبی Alexnet انتخاب می‌شـــوند. شـــرط توقف ما در الگوریتم ACKH به این صورت ا ست تا زمانی ا ست که در اجرای runها اگر بهترین برازش نسبت به مرحله قبل بهتر نشود یا ثابت بماند خاتمه پیدا کند و خارج شود.
آزمایش بهینه‌ساز بر روی مجموعه‌داده Danmini doorbell انجام گردیده است؛ از بهینه‌ساز Adam استفاده شده است Adam تکانه اول و دوم را با هم ترکیب می‌کند به همین دلیل سرعت همگرایی بالایی دارد؛ بنابراین Adam برای بهینه‌سازی فرایند آموزش مدل برای دقت تشخیص بهتر استفاده شده است و تکانه مرتبه اول روی ۰.۹ تنظیم‌شده است و نرخ یادگیری به‌صورت پویا کاهش پیدا می‌کند تا اثر آموزش را بهبود دهد. درنتیجه بر اساس تجزیه‌وتحلیل فوق بهینه‌ساز روش Adam را انتخاب می‌کند که وزن اتصال و ارزش بایاس نورون‌ها را با مقدار تابع تلفات cross-entropy با نرخ آموزش مشخص تنظیم می‌کند.



شکل ۴- نمودار جریان الگوریتم ACKH

۵- نتایج و آزمایش‌ها

آزمایش‌ها و پیاده‌سازی انجام‌شده در سیستم‌عامل Windows 10 به زبان برنامه‌نویسی Python به‌وسیله سیستم کامپیوتر رومیزی با ۳۲ گیگابایت RAM و پردازنده ۸ هسته‌ای در محیط آزمایشگاهی دانشگاه صورت‌گرفته است. الگوریتم پیشنهادی در داکیومنت اجراشدنی گوگل کولب به دلیل ارائه خدمات پردازش ابری و GPU رایگان اجرا گردیده است.

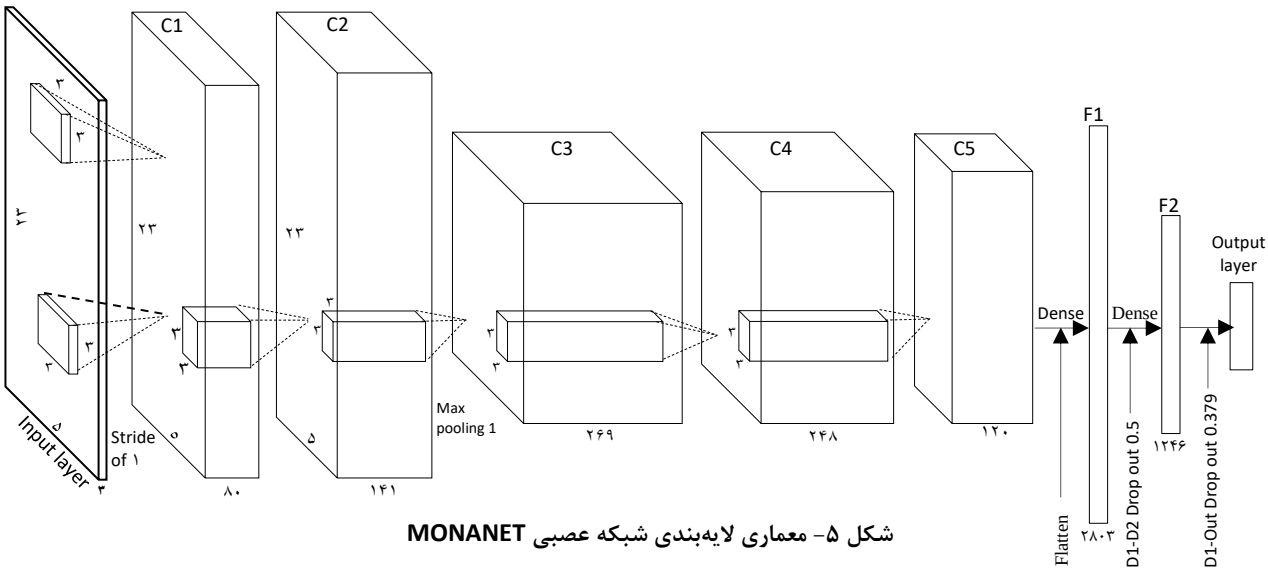
۵-۱- مجموعه‌داده

برای طبقه‌بندی چند کلاسه از مجموعه‌داده Danmini Doorbell استفاده می‌شود. مجموعه‌داده اصلی شامل ۹ نوع مجموعه‌داده است که ۸ مجموعه آن مربوط به ترافیک شبکه حملات مختلف و ۱ مجموعه آن مربوط به ترافیک شبکه نرمال است. از هر مجموعه‌داده ۱۰۰۰۰ رکورد به‌صورت تصادفی انتخاب می‌شود تا یک مجموعه‌داده با ۹۰۰۰۰ رکورد و ۱۱۵ بعد به دست آید. پس‌ازآنکه

فراپارامترهای مدل Alexnet توسط الگوریتم CKH تنظیم گردید، مدل توسط داده‌های آموزشی مجموعه‌داده آموزش می‌بیند و توسط داده‌های آزمایشی آن آزمایش می‌شود. برای استفاده از این مجموعه‌داده در شبکه عصبی Alexnet نیاز به پیش‌پردازش مجموعه‌داده است.

۵-۱-۱- پیش‌پردازش

داده‌های ترافیکی یک عکس فوری از رفتار میزبان‌ها و پروتکل‌های ارتباط‌دهنده بسته‌های داده می‌گیرند که عکس‌های فوری در ۵ پنجره زمانی (100ms, 500ms, 1.5s, 10s, 1min) است و هر پنجره زمانی ۲۳ ویژگی آماری را خلاصه می‌کند باتوجه‌به $x^{n\times p}$، ۱۱۵ بعد مشخصه داریم. N تعداد نمونه‌ها و p تعداد ویژگی‌ها می‌باشند. با توجه به اینکه ویژگی‌های مختلف دارای مقادیر متفاوتی می‌باشند به همین دلیل نیاز است که این ویژگی‌ها قبل از پردازش نرمال گردند زیرا برخی داده‌های غیرعادی بزرگ یا کوچک می‌توانند آموزش مدل را گمراه کنند و همچنین نتایج ممکن است به دلیل توزیع پراکنده ویژگی‌ها تحت تأثیر قرار گیرند؛ بنابراین ویژگی‌ها با تبدیل به توزیع نرمال استاندارد با میانگین ۰ و واریانس واحد استاندارد می‌شوند.



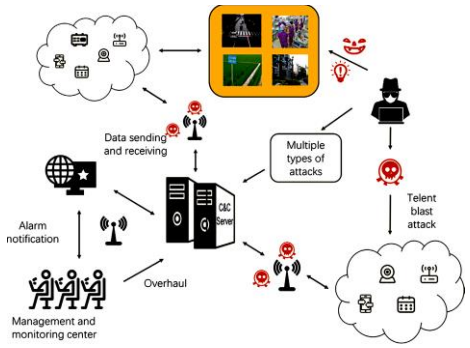
شکل ۵- معماری لایه‌بندی شبکه عصبی MONANET

۵-۱-۲- حملات استفاده شده در مجموعه‌داده

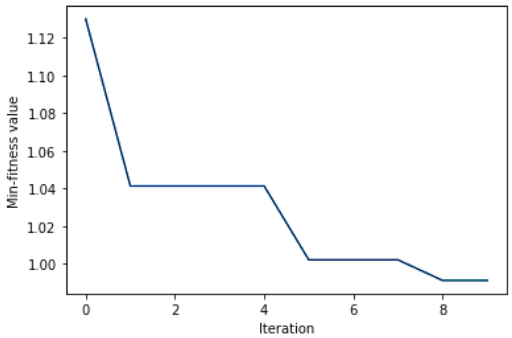
انواع حملات شبکه بر روی مجموعه‌داده‌های عمومی اینترنت اشیاء ایجاد شده طبقه‌بندی شده است [۸]. این مجموعه‌داده شامل ۹ دستگاه اینترنت اشیاء که به ۲ ویروس بدنام Mirai و BASHLITE آلوده شده است. حملات شبکه اجرا شده روی مجموعه‌داده عبارت‌اند از: COMBO،ACK ، SYN، Scan، Junk، UDPplain.، UDP،TCP. شکل ۶ نشان‌دهنده فرایند حمله ویروس زامبی است.

۵-۲- الگوریتم پیشنهادی در مقایسه با سایر روش‌ها

روش پیشنهادی این پژوهش با روش‌های ارائه شده در مطالعات مدسر و همکاران ۲۰۲۲، کن و همکاران ۲۰۲۱؛ میدن و همکاران ۲۰۱۸ مقایسه شده است [۱۶, ۴,۶]. در مطالعه مدسر و همکاران ۲۰۲۲ با استفاده از مدل‌های یادگیری عمیق مانند شبکه عصبی مصنوعی (ANN)، حافظه کوتاه‌مدت (LSTM) و واحد بازگشتی دروازه‌ای (GRU) برای طبقه‌بندی حملات بات نت در شبکه‌های IoT پیشنهاد می‌شود. نتایج نشان‌دهنده برتری روش پیشنهادی ما در مقایسه با روش‌های ارائه شده در مطالعه مدسر و همکاران است. در مطالعه میدن و همکاران ۲۰۱۸، از رمزگذارهای خودکار عمیق برای شناسایی استفاده می‌کنند. هنگامی که رمزگذار خودکار نتواند یک عکس فوری را بازسازی کند، این نشانه قوی است که رفتار مشاهده شده غیرعادی است. در این روش ممکن است رفتارهای ترافیکی غیرقابل‌پیش‌بینی (و درعین‌حال خوش‌خیم) را به‌اشتباه به‌عنوان غیرعادی شناسایی کند. مطالعه کن و همکاران ۲۰۲۱، در راستای بهبود مطالعه میدن و همکاران ۲۰۱۸، با ارائه روشی جدید با استفاده از شبکه عصبی کانولوشنال و الگوریتم بهینه‌سازی ازدحام ذرات تطبیقی به نام (APSO-CNN) به نتایج بهتری دست‌یافته است که توانسته تشخیص نفوذ به شبکه‌های اینترنت اشیاء را تا ۹۵.۵% بهبود دهد. روش پیشنهادی ما در مقایسه با روش‌های ارائه شده در این دو مطالعه توانسته دقت تشخیص نفوذ را به ۹۹.۸۹% بهبود دهد؛ نتایج نشان‌دهنده برتری روش پیشنهادی ما در مقایسه با این ۳ مطالعه است.



شکل ۶- فرایند حمله ویروس زامبی [۱۶].



Tabriz Journal of Electrical Engineering (TJEE), vol. 53, no. 2, Summer 2023 Serial no. 104
DOI: 10.22034/tjee.2023.16066

شکل ۷- نتایج تکرارهای الگوریتم CKH

۳-۵- آزمایش‌ها و تفسیر نتایج

در این پژوهش پارامترهای الگوریتم CKH به‌صورت زیر مقداردهی شده است: طبق مطالعه [۱۶]، ما در پژوهش خود مقادیر V_f، N^{max} و D^{max} را به ترتیب مقادیر ۰.۰۱، ۰.۰۲، ۰.۰۰۵ تنظیم کردیم.

Number of runs و Number of krills و Max iteration به ترتیب ۵ و ۴ و ۵ هستند که Number of krills تعداد جمعیت ما در الگوریتم ACKH است. باتوجه‌به اینکه هرکدام از این میگوها ۲۳ بعد دارد که هر بعد آن‌یکی از فراپارامترها است. Max iteration حداکثر تعداد تکرارها است که در هر تکرار با بهترین میگو مرحله قبل مقایسه می‌شود و در صورت بهتر بودن ذخیره می‌شود. Number of runs تعداد RUN ها است، در هر اجرا دوباره جمعیت جدید تولید می‌شود و مراحل را تکرار می‌کند. این کار تا زمانی ادامه می‌یابد که شرط توقف برقرار شود. حداقل و حداکثر وزن‌های اینرسی (w_n وv_f) به ترتیب ۰.۱ و ۰.۹ می‌باشد. تغییر حداقل مقدار تناسب با تعداد تکرارها در شبکه عصبی MONANET در شکل ۷ نشان داده شده است. با توجه به عناصر موقعیت بهترین میگو یافت شده و با استفاده از رابطه ۵، فراپارامترهای بهینه مدل Alexnet ما مشخص می‌شود. این فراپارامترها در جدول ۲ نشان داده شده است.

جدول ۲- مقدار فراپارامترهای مدل Alexnet

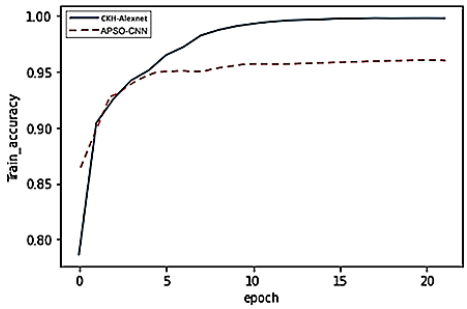
Position	Hyperparameter	Optimization value
x1	C1_n_filter	*80*
x2	C1_filter_len	*3*
x3	C1_act	*relu*
x4	C2_n_filter	*141*
x5	C2_filter_len	*3*
x6	C2_act	*LeakyReLU*
x7	C3_n_filter	*269*
x8	C3_filter_len	*3*
x9	C3_act	*LeakyReLU*
x10	C4_n_filter	*248*
x11	C4_filter_len	*3*
x12	C4_act	*relu*
x13	C5_n_filter	*120*
x14	C5_filter_len	*3*
x15	C5_act	*LeakyReLU*
x16	D1_neuron	*2803*
x17	D1_act	*elu*
x18	D1_D2_dropout	*0.500*
x19	D2_neuron	*1246*
x20	D2_act	*relu*
x21	D2_Out_dropout	*0.379*
x22	batch_size	*198*
x23	learning rate	*0.000459*

بعد از مشخص‌شدن فراپارامترهای بهینه شبکه عصبی Alexnet را تنظیم می‌کنیم. در شکل ۵ می‌توان شبکه عصبی تنظیم‌شده با فراپارامترهای بهینه را مشاهده کرد. در روند آموزش مدل Alexnet با مجموعه‌داده ترافیک شبکه، شرط توقف برای تسریع روند آموزش تنظیم‌شده است به این صورت که اگر دقت مجموعه اعتبارسنجی در یک دوره آموزشی بهبود نیابد، آموزش متوقف می‌شود و بهترین مدل شبکه ذخیره می‌شود. در شکل‌های ۸ تا ۱۱ می‌توانیم مشاهده کنیم شبکه MONANET پیشنهادی در مقایسه با الگوریتم APSO-CNN عملکرد بهتری دارد.

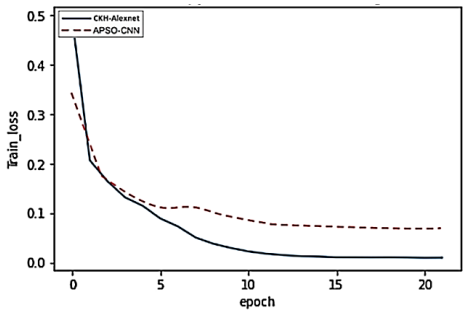
در این پژوهش cross-entropy روی داده‌های آموزشی در روش پیشنهادی را با روش APSO_CNN مقایسه شده است. در شکل ۸ مشاهده می شود، روش پیشنهادی ما به درصد خطای خیلی پایین‌تری نسبت به APSO_CNN (در مجموعه‌داده‌های آموزشی) رسیده است که نشان‌دهنده این است که روش پیشنهادی این پژوهش در تشخیص نفوذ به شبکه در مجموعه‌داده‌های آموزشی دارای خطای کمتری است. ازآنجایی‌که ممکن است مدل فقط داده‌های آموزشی را یاد گرفته باشد درنتیجه، باید نتایج را علاوه بر داده‌های آموزشی؛ بر روی داده‌های اعتبارسنجی نیز بررسی گردد. ممکن است نتایج خوبی در داده‌های آموزشی به دست آید؛ ولی در داده‌های اعتبارسنجی این‌گونه نباشد. باتوجه‌به شکل ۱۰ نتایج بر روی داده‌های اعتبارسنجی بررسی شده است و کاملاً مشخص است که خطا بسیار کاهش‌یافته است و این نشانگر آن است که روش پیشنهادی ما بهتر از روش APSO_CNN است.

دقت یکی از متریک‌های پرکاربرد است. به‌طورکلی، دقت به این معناست که مدل تا چه اندازه خروجی را درست پیش‌بینی می‌کند. همان‌طور که مشاهده می‌شود باتوجه‌به شکل ۹ میزان دقت در مجموعه‌داده‌های آموزشی در شبکه MONANET به بالاترین حد رسیده است؛ در شکل ۱۱ دقت بر روی داده‌های آزمایشی بررسی گردیده است. همان‌طور که در شکل کاملاً مشخص است میزان دقت در داده‌های اعتبارسنجی روش پیشنهادی بسیار بالاتر از الگوریتم APSO-CNN است. در روش APSO_CNN دقت نزدیک به ۹۶ درصد است درصورتی‌که روش این پژوهش در مجموعه‌داده آزمایشی به‌دقت ۹۹.۸ درصد رسیده است و این نشانگر آن است که مدل به‌خوبی آموزش‌دیده است و با دقت خیلی بالا می‌تواند ترافیک حمله به شبکه را از ترافیک نرمال تشخیص دهد.

همان‌طور که در شکل ۸ و ۹ مشاهده می‌شود؛ مقدار تابع تلفات متقاطع شبکه عصبی MONANET به‌مراتب کمتر از الگوریتم APSO-CNN در هر چرخه آموزش است و درعین‌حال از دقت بالاتری برخوردار است که نشان‌دهنده آن است که اثر آموزشی شبکه عصبی MONANET بهتر است و کارایی آن در آموزش مدل ثابت می‌شود. شکل‌های ۱۰ و ۱۱ تغییر مقدار تابع تلفات متقاطع و دقت را در مجموعه اعتبارسنجی را نمایش می‌دهند که کاملاً به‌وضوح دیده می‌شود که شبکه MONANET پیشنهادی قادر به دست آوردن مقدار تابع تلفات کم‌تر و دقت بالاتر در هر چرخه آزمایش است؛ بنابراین برای الگوریتم پیشنهادی، اینکه آیا دقت در یک تکرار بهبود می‌یابد یا نه به‌عنوان شرط توقف آموزش در نظر گرفته شده است که این شرط توقف باعث جلوگیری از آموزش بیش‌ازحد مدل می‌شود و پس از توقف آموزش، مدل شبکه با دقت بالاتر از چرخه قبلی ذخیره می‌شود.

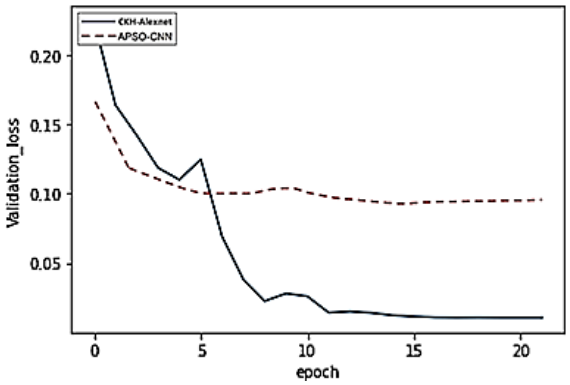


شکل ۸- مقایسه تابع تلفات متقاطع آنتروپی در مجموعه آموزش شبکه عصبی MONANET با الگوریتم APSO-CNN

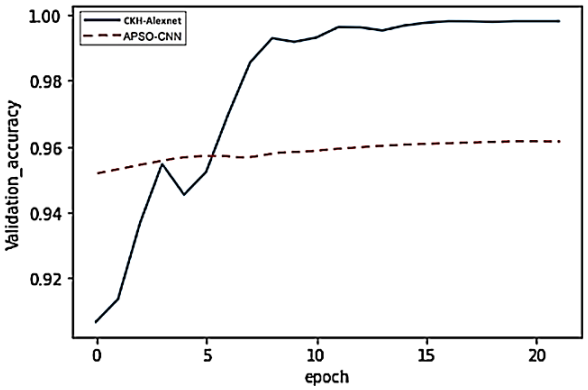


شکل ۹- مقایسه دقت در مجموعه آموزشی شبکه عصبی MONANET با

الگوریتم PSO-CNN



شکل ۱۰- مقایسه تابع تلفات متقاطع آنتروپی در مجموعه اعتبارسنجی شبکه عصبی MONANET با الگوریتم PSO-CNN



شکل ۱۱- مقایسه دقت در مجموعه اعتبارسنجی شبکه MONANET با الگوریتم PSO-CNN

۴-۵- نتایج و تجزیه‌وتحلیل عملکرد

به‌منظور ارزیابی اثربخشی روش‌های طبقه‌بندی مختلف در شناسایی انواع حملات شبکه‌ای که توسط میزبان‌های زامبی راه‌اندازی می‌شوند، شبکه MONANET ارائه شده در این مقاله با ۷ الگوریتم SVM, FNN, R-CNN, LSTM, ANN, GRU, APSO-CNN مقایسه شده است. سپس عملکرد جامع پنج الگوریتم در ۵ شاخص ارزیابی زیر ارزیابی می‌شود.

۱- صحت طبقه‌بندی

مهم‌ترین معیار برای ارزیابی عملکرد مدل است.

$$\mathbf{accuracy} = \mathbf{n_{true}}/\mathbf{n_{total}} \qquad (۶)$$

که در آن n_{true}تعداد نمونه‌های طبقه‌بندی‌شده درست را نشان می‌دهد، n_{total} نشان‌دهنده کل نمونه‌ها است.

۲- متوسط دقت

دقت تشخیص هر طبقه را در طبقه‌بندی‌های چند کلاسه نشان می‌دهد.

$$\boldsymbol{ave-precision} = (\mathbf{1}/\boldsymbol{class}) \times [\sum_{i=1}^{class} \boldsymbol{n_i^{true}}/(\boldsymbol{n_i^{true}} + \boldsymbol{n_i^{false}})] \qquad (۷)$$

که در آن n_i^{true} نشان‌دهنده تعداد نمونه‌های درست تقسیم‌شده دسته i است، n_i^{false}تعداد نمونه‌های خطای تقسیم‌شده دسته i را نشان می‌دهد. $class$ نشان‌دهنده انواع حملات شبکه.

۳- ضریب کاپا

ضریب کاپا برای ارزیابی اینکه نتایج پیش‌بینی مدل ما با نتایج طبقه‌بندی واقعی مطابقت دارد استفاده می‌شود که محدوده آن در کاربرد عملی بین [0,1] است. همان‌طور که در تصویر ۱۲ مشاهده می‌شود ضریب کاپا الگوریتم پیشنهادی نزدیک به ۱ است که نشان‌دهنده سازگاری بالای مدل پیشنهادی ما است.

$$\mathbf{Kappa} = (\mathbf{accuracy} - \boldsymbol{p_e})/(\mathbf{1} - \boldsymbol{p_e}) \qquad (۸)$$

$$\mathbf{p_e} = (\sum_{i=1}^{class} \mathbf{n_i^{label\_true}} \times \mathbf{n_i^{predict\_true}})/(\mathbf{n_{total}} \times \mathbf{n_{total}}) \qquad (۹)$$

$n_i^{label\_true}$ نشان‌دهنده تعداد نمونه‌هایی است که واقعاً به دسته i-ام تعلق دارند، $n_i^{predict_true}$نشان‌دهنده تعداد نمونه‌های پیش‌بینی‌شده متعلق به دسته i است.

۴- ضرر همینگ

برای اندازه‌گیری فاصله بین برچسب پیش‌بینی‌شده و برچسب واقعی با مقدار ۰ و ۱ استفاده می‌شود.

$$Hamming - loss = (1/n_{total}) \times \left[\frac{\sum_{i=1}^{n_{total}} count\left(y_i^{true} \oplus y_i^{predict}\right)}{class}\right] \qquad (۱۰)$$

که در آن n_{total} نشان‌دهنده کل نمونه‌ها می‌باشد، count(۰) نشان‌دهنده تعداد ۱ است، y_i^{true} نشان‌دهنده برچسب واقعی نمونه i-ام، $y_i^{predict}$ نشان‌دهنده برچسب پیش‌بینی‌شده i-امین نمونه، کلاس است. $class$ تعداد دسته‌های نمونه را نشان می‌دهد.

۵- ضریب شباهت ژاکارد

ضریب شباهت ژاکارد نشان‌دهنده کیفیت مدل است.

$$j = (1/n_{total}) \times (\sum_{i=1}^{n_{total}} |y_i^{true} \cap y_i^{predict}|/|y_i^{true} \cup y_i^{predict}|) \qquad (۱۱)$$

باتوجه‌به شکل ۱۲ ما ۸ الگوریتم مختلف SVM, FNN, R-CNN, APSO-CNN, MONANET, LSTM, ANN, GRU را با ۵ معیار ارزیابی Hamming-loss, jacard, kappa, accuracy, ave-precision ارزیابی شده است.

باتوجه‌به تصویر ۱۲ روش پیشنهادی ما در تمام این ۵ معیار ارزیابی نسبت به روش‌های مقایسه شده از نتایج بهتری برخوردار است. البته باید ذکر کرد که haming-loss از نوع خطا است و هرچه کوچک‌تر باشد نتیجه بهتر است، برای این‌که بتوانیم در یک نمودار این معیار را نمایش دهیم از 1- haming-loss استفاده کردیم تا بتوانیم نتیجه را مقایسه کنیم.

باتوجه‌به شکل ۱۳، درمجموع تشخیص حمله multi-type بر اساس شبکه عصبی MONANET به‌طور قابل‌توجهی از الگوریتم‌های دیگر بهتر است. نتایج به‌دست‌آمده نشان‌دهنده آن است که شبکه MONANET می‌تواند به‌طور مؤثری حملات مختلف شبکه را شناسایی کند و ثابت می‌شود هنگامی‌که یک حمله شناسایی می‌شود می‌توان دستگاه‌های آلوده اینترنت اشیاء را از شبکه جدا کرد که این امر سبب کاهش زیان واردشده از حملات می‌شود.

برای مقایسه پایداری الگوریتم پیشنهادی نسبت به الگوریتم‌های دیگر، الگوریتم پیشنهادی ۱۲ بار به‌صورت مستقل با تغییر مجموعه نمونه آموزشی اعتبارسنجی اجراشده است و دقت تشخیص نفوذ برای مجموعه‌داده اعتبارسنجی در هر بار اجرا در جدول ۳ گزارش شده است. در شکل ۱۳ حداکثر مقدار، حداقل مقدار، مقدار میانه و مقدار میانگین دقت اعتبارسنجی برای هر ۵ الگوریتم به‌صورت

Tabriz Journal of Electrical Engineering (TJEE), vol. 53, no. 2, Summer 2023 Serial no. 104
DOI: 10.22034/tjee.2023.16066

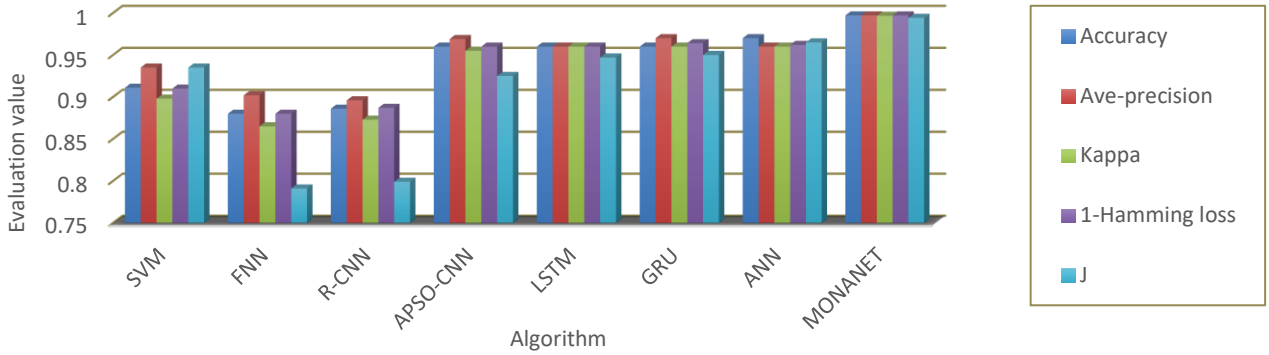
نمودار رسم شده است. فاصله بین حداکثر و حداقل دقت به‌دست‌آمده در ۱۲ اجرای مستقل برای الگوریتم پیشنهادی بسیار کمتر از ۷ الگوریتم دیگر است، این نشان می‌دهد که نتایج به‌دست‌آمده از الگوریتم پیشنهادی بسیار قابل‌اعتمادتر از دیگر الگوریتم‌ها است؛ بنابراین می‌توان نتیجه گرفت که الگوریتم پیشنهادی بسیار پایدارتر از دیگر الگوریتم‌ها است و در تشخیص حملات شبکه بسیار بالاتر و پایدارتر است. علاوه‌برآن دقت به‌دست‌آمده در این روش بسیار بالاتر از ۷ روش دیگر است. دقت روش پیشنهادی بین ۹۹.۰ و ۹۹.۸ درصد بوده است درصورتی‌که دقت در روش APSO_CNN بین ۹۱ و ۹۵.۵ درصد است.

جدول ۳- گزارش دقت مجموعه‌داده اعتبارسنجی در ۱۲ اجرای مستقل.

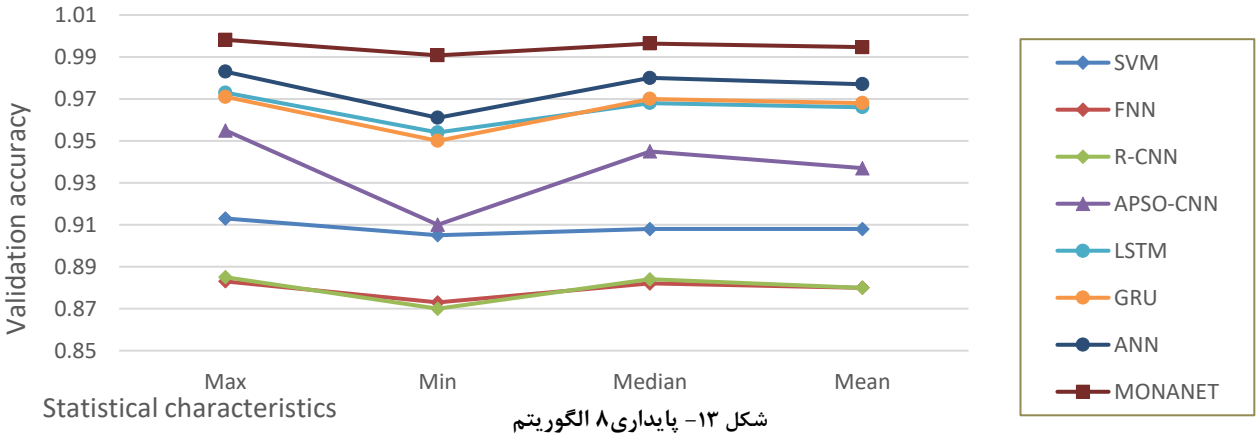
۹۹,۰	۹۹,۸	۹۹,۱	۹۹,۶	۹۹,۴	۹۹,۳	۹۹,۸	۹۹,۶	۹۹,۱	۹۹,۶	۹۹,۲	۹۹,۷

۶- نتیجه‌گیری و کار آینده

در این مقاله یک شبکه عصبی جدید MONANET پیشنهاد شده است که با دقت بالا توانسته است حملات مختلفی که به شبکه‌های Iot راه‌اندازی شده‌اند را تشخیص دهد. در این الگوریتم به‌جای تنظیم دستی فراپارامترهای ساختار شبکه Alexnet که بسیار زمان‌بر است از الگوریتم بهینه‌سازی میگوی آشوبی (ACKH) استفاده شده است. فراپارامترهای مدل Alexnet به‌عنوان عناصر موقعیت میگو در الگوریتم CKH در نظر گرفته شده است و مقدار تابع تلفات آنتروپی در اولین دوره آموزشی Alexnet به‌عنوان تابع تناسب در الگوریتم CKH استفاده شده است. الگوریتم CKH فراپارامترهای بهینه ساختار Alexnet را به‌نحوی‌که تابع تلفات آنتروپی کمینه شود تعیین می‌کند. درنهایت شبکه عصبی پیشنهادی با فراپارامترهای به‌دست‌آمده از CKH تنظیم‌شده و در مقایسه با الگوریتم APSO-CNN در تشخیص حملات به شبکه IOT ارزیابی شده است. نتایج ارزیابی‌ها نشان‌دهنده آن است که شبکه عصبی پیشنهادی نه‌تنها به‌دقت بالایی در تشخیص حملات به شبکه IOT رسیده است؛ بلکه پایداری شبکه پیشنهادی در مقایسه با سایر الگوریتم‌ها بهبودیافته است. بر اساس بحث فوق، جهت تحقیقات آینده پیشنهاد می‌گردد استفاده از روش‌های دیگر برای بهبود الگوریتم ACKH در راستای کاهش پیچیدگی زمانی برای تنظیم فراپارامترهای شبکه عصبی و بهبود زمان آموزش مدل تحقیق شود.



شکل ۱۲- عملکرد شاخص ارزیابی در ۸ الگوریتم



شکل ۱۳- پایداری۸ الگوریتم

مراجع

[1] A.Thakkar, R.Lohiya, "A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges." Archives of Computational Methods in Engineering 28, no.4, PP.3211-3243, 2021.

[2] Y.Shah, S.Shamik, "A survey on Classification of Cyber-attacks on IoT and IIoT devices." In 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), PP.0406-0413, IEEE, 2020.

[3] M.V.Kamal, P.Dileep, M.Gayatri, "A Novel Approach for Providing Security for IoT Applications Using Machine Learning and Deep Learning Techniques." In Intelligent Systems and Sustainable Computing, PP.155-164, Springer, Singapore, 2022.

[4] Y.Meidan, M.Bohadana, Y.Mathov, Y.Mirsky, A.Shabtai, D.Breitenbacher, Y.Elovici. "N-baiot—network-based detection of iot botnet attacks using deep autoencoders." IEEE Pervasive Computing 17, no.3, PP.12-22, 2018.

[5] Shah, Zawar, I.Ullah, H.Li, A.Levula, K.Khurshid, "Blockchain Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things (IoT): A Survey." Sensors 22, no. 3, P.1094, 2022.

[6] M.Mudassir, D.Unal, M.Hammoudeh, F.Azzedin. "Detection of Botnet Attacks against Industrial IoT Systems by Multilayer Deep Learning Approaches." Wireless Communications and Mobile Computing, 2022.

[7] M.A.Khan, K.Salah, "IoT security: Review, blockchain solutions, and open challenges." Future generation computer systems 82, PP.395-411, 2018.

[8] F.Zhu, W.Wu, Y.Zhang, and X.Chen, "Privacy-preserving authentication for general directed graphs in industrial IoT." Information sciences 502, PP.218-228, 2019.

[9]C.Perera, M.Barhamgi, A.K.Bandara, M.Ajmal, B.Price, B.Nuseibeh, "Designing privacy-aware internet of things applications." Information Sciences 512, PP.238-257, 2020.

[10] B.P.Poudel, A.Mustafa, A.Bidram, H.Modares, "Detection and mitigation of cyber-threats in the DC microgrid distributed control system." International Journal of Electrical Power & Energy Systems 120, P.105968, 2020.

[11] M.Vasou Jouybari, E.Ataie, M.Bastam, “An MLP-based Deep Learning Approach for Detecting DDoS Attacks”, Tabriz Journal of Electrical Engineering (TJEE), vol.52, no.3, PP.195-204, 2022.

[12] G.D.L.T.Parra, P.Rad, K.K.R.Choo, N.Beebe, "Detecting Internet of Things attacks using distributed deep learning." Journal of Network and Computer Applications 163, P.102662, 2020.

[13] A.Al Shorman, H.Faris, I.Aljarah, "Unsupervised intelligent system based on one class support vector machine and Grey Wolf optimization for IoT botnet detection." Journal of Ambient Intelligence and Humanized Computing 11, no. 7, PP.2809-2825, 2020.

[14] S.Hosseini, B.M.Hasani Zade. "New hybrid method for attack detection using combination of evolutionary algorithms, SVM, and ANN." Computer Networks 173, P.107168, 2020

[۱۵] محمدهادی قومنجانی، جواد حمیدزاده، "دسته‌بند تک کلاسه مبتنی بر بردارهای پشتیبان برای داده‌های نویزی با استفاده از الگوریتم گروه میگوی آشوبی و تراکم محلی"، مجله مهندسی برق دانشگاه تبریز، جلد ۴۸، شماره ۳، صفحات ۱۳۲۵-۱۳۱۵، ۱۳۹۷.

[16] X.Kan, Y.Fan, Z.Fang, L.Cao, Neal N. Xiong, D.Yang, X.Li, "A novel IoT network intrusion detection approach based on adaptive particle swarm optimization convolutional neural network." Information Sciences 568, PP.147-162, 2021.

[17]http://archive.ics.uci.edu/ml/datasets/detection_of_IoT_botnet_attacks_N_BaIoT.