به نام خدا

دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

تشخیص نفوذ شبکه‌های کامپیوتری مبتنی بر یادگیری‌ماشین

گردآورنده: بهار کاویانی
استاد راهنما: دکتر رضا صفابخش

خردادماه بهار ۱۴۰۰

فهرست

اهداف پژوهش

بررسی الگوریتم‌های جمع‌آوری شده در حوزه‌ی تشخیص نفوذ مبتنی بر یادگیری ماشین

معرفی مقدماتی هر یک از الگوریتم‌ها

مقایسه و دسته‌بندی نتایج به دست‌آمده از تحقیقات انجام شده در این زمینه

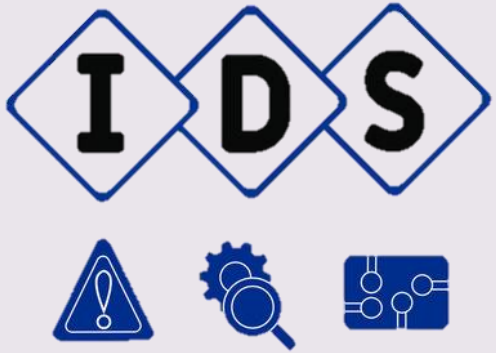
ارائه‌ی الگوریتم‌های پیشنهادی با توجه به منابع در دسترس

فهرست

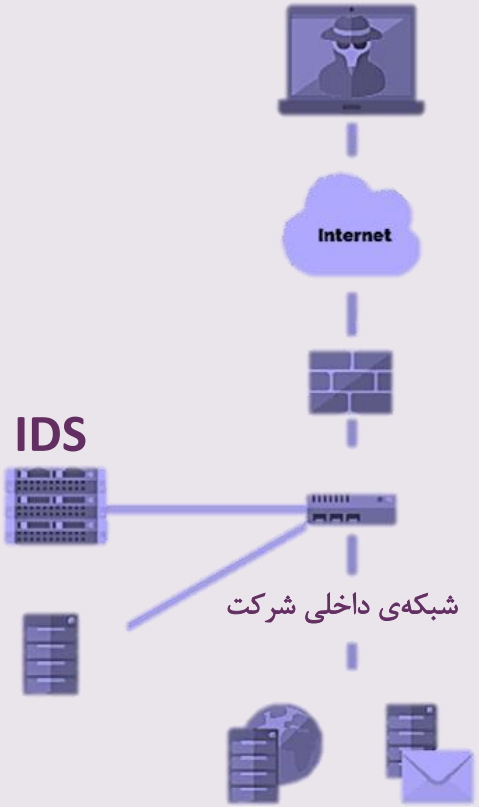
مقدمه

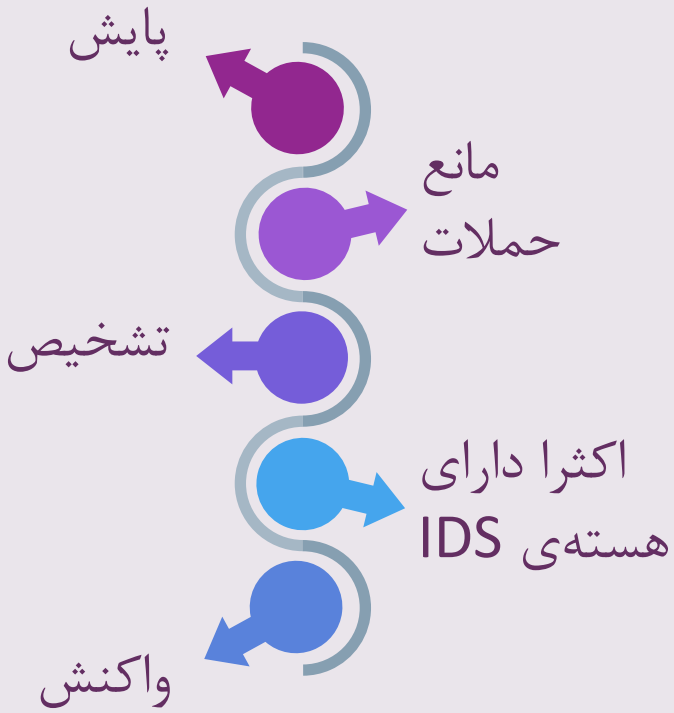
در دنیای امروز، اهمیت امنیت در استفاده از اینترنت و تجهیزات مربوط به آن بر کسی پوشیده نیست.
راه‌های مختلفی برای مقابله با حملات امنیتی وجود دارد مانند:

- استفاده از دیواره‌های آتش
- جلوگیری از نفوذ (IPS)
- تشخیص نفوذ (IDS)
- و غیره

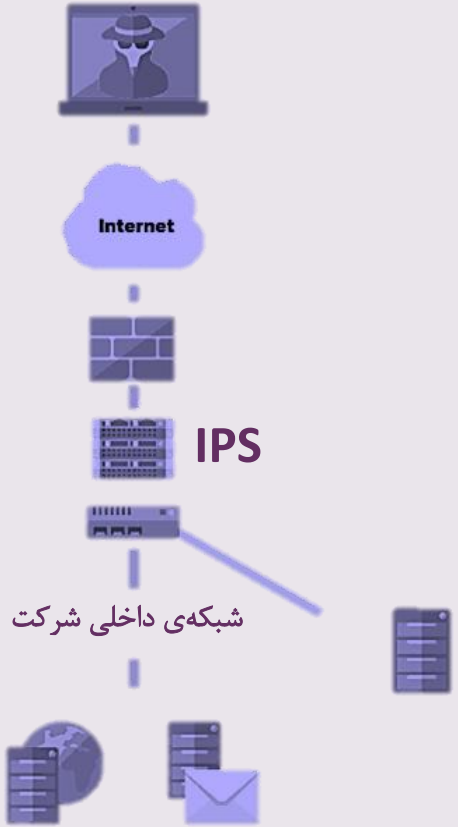


سیستم تشخیص نفوذ

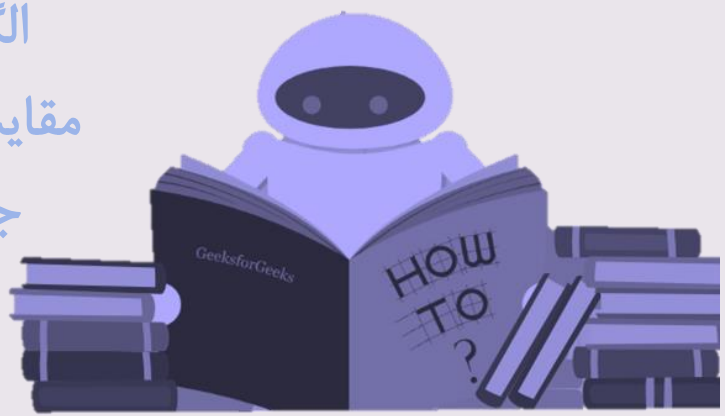




سیستم جلوگیری از نفوذ



فهرست



رویکردهای تشخیص نفوذ مبتنی بر یادگیری ماشین

تفاوت با راهکارهای دستی چیست؟

- ✓ دقت بهتر و سرعت تشخیص بیش‌تری
- ✓ عدم نیاز به تجربه و دانش کارشناسان و متخصصین
- ✓ جمع‌آوری الگوهای حملات
- ✓ پیش‌بینی حملات از روی الگوهای به دست آمده
- ✓ وجود هشدارهای غیر ضروری زیاد در صورت داشتن حساسیت بالا

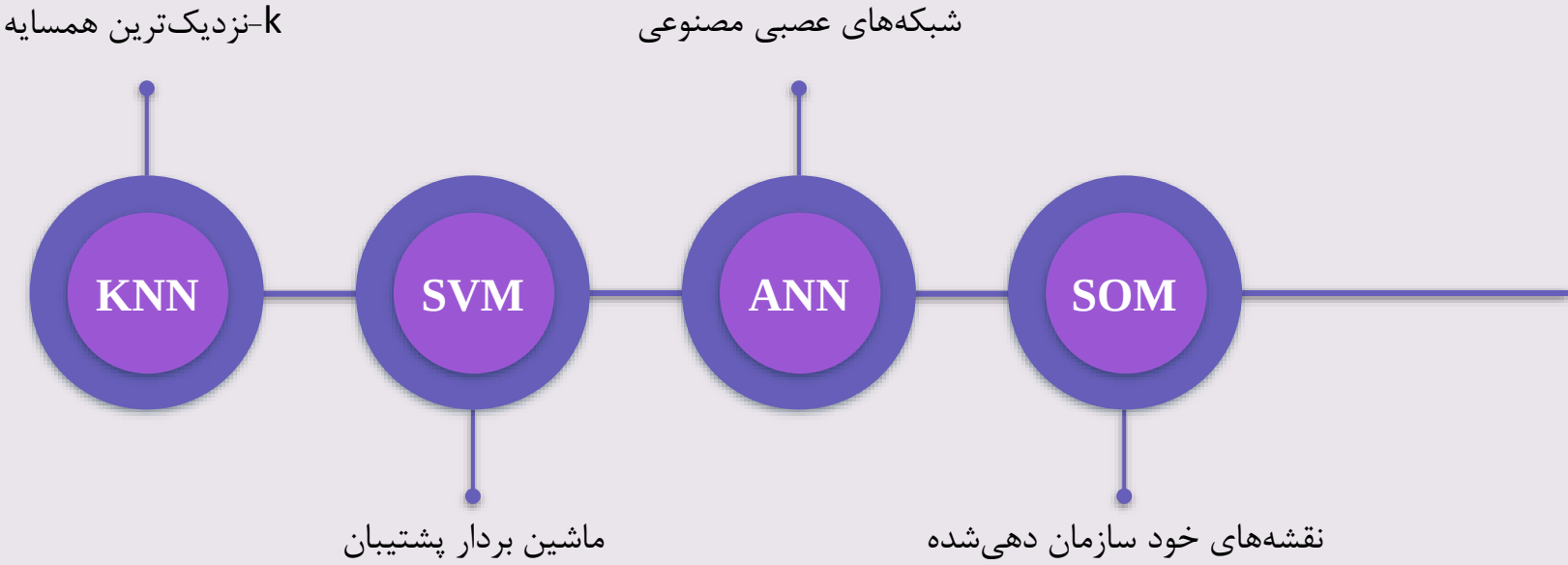
دسته‌بندی الگوریتم‌ها

انواع دسته‌بندی؟

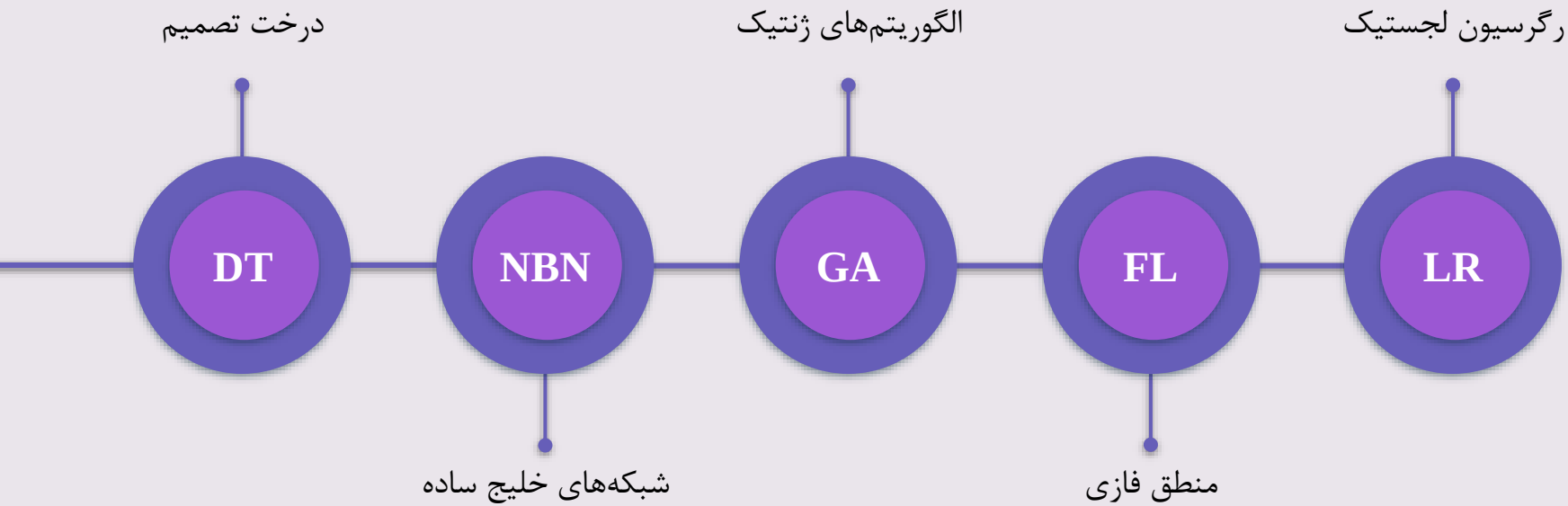
- تشخیص رفتار غیر عادی و تشخیص مبتنی بر امضا
- تحت نظارت و نظارت‌نشده
- کم‌عمق و عمیق
- طبقه‌بندی‌های تکی، ترکیبی و گروهی

فهرست

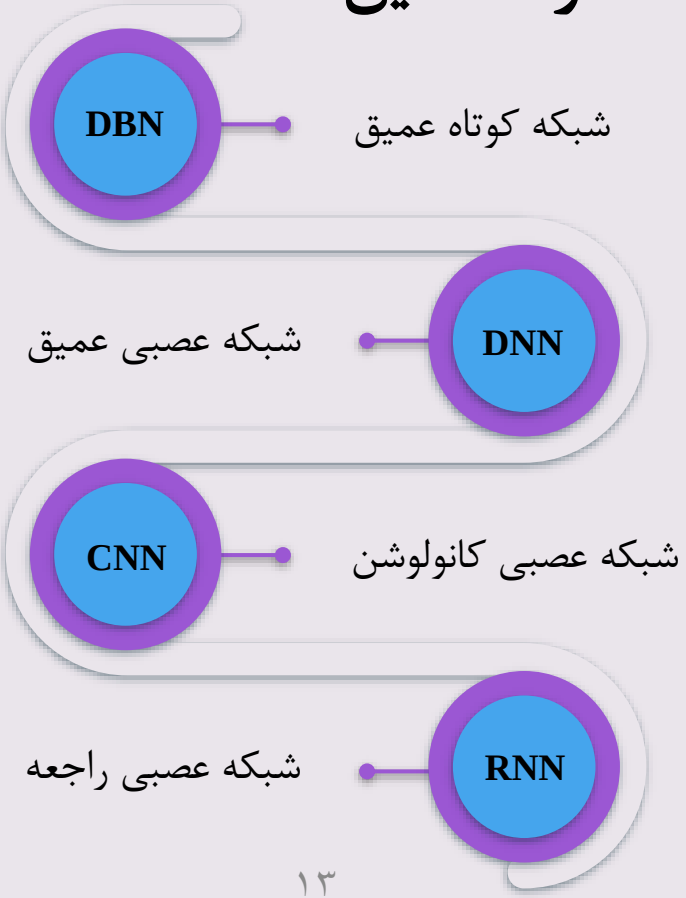
الگوریتم‌های تحت نظارت کم عمق



الگوریتم‌های تحت نظارت کم عمق (ادامه)



الگوریتم‌های تحت نظارت عمیق



فهرست

الگوریتم‌های نظارت‌نشده

مدل k-میانگین

شبکه‌های خصمانه تولیدی

خود رمزگذار

ماشین بولتزمن محدود

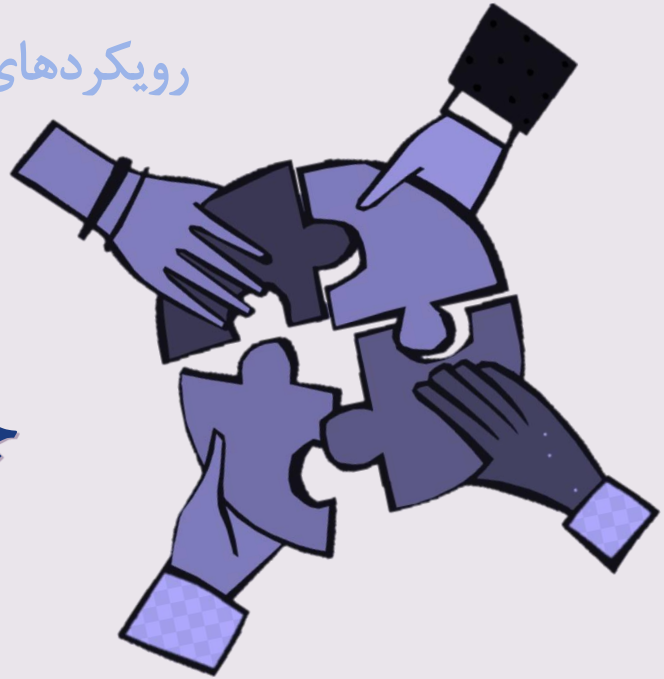
فهرست

مقایسه‌ی الگوریتم‌ها

انواع داده‌های پردازشی

- بسته (Packet)
- جریان (Flow)
- نشست (Session)
- وقایع ثبت شده (Log)

فهرست



نتیجه‌گیری و جمع‌بندی مباحث

حال می‌توانیم به کمک مطالعاتی که داشتیم، در شرایط مختلف مناسب‌ترین الگوریتم را انتخاب کنیم. این انتخاب با توجه به نکات زیر می‌تواند باشد:

- ✓ عملکرد الگوریتم‌ها و مزایا و معایب هر یک از آن‌ها
- ✓ توجه به انواع داده‌هایی که با آن‌ها سر و کار داریم
- ✓ توانایی بهبود بخشیدن به الگوریتم موردنظر
- ✓ توجه به هزینه، پیچیدگی و منابع مورد نیاز هر الگوریتم
- ✓ استفاده‌ی ترکیبی از الگوریتم‌ها (Hybrid)

فهرست

پیشنهادات

مطالعه‌ی دقیق‌تر منابع و آشنایی بیش‌تر با الگوریتم‌ها در زمینه‌ی افزایش کارآیی و بهبود مشکلات آن‌ها

جست و جو و بررسی بیش‌تر الگوریتم‌های ترکیب‌شده و ایجاد بهبود به وسیله‌ی ادغام

بررسی دیگر ویژگی‌های الگوریتم‌ها و ارائه‌ی دسته‌بندی‌های مختلف

فهرست

منابع

[1]C.-F. Tsai, Y.-F. Hsu, C.-Y. Lin, and W.-Y. Lin, “Intrusion detection by machine learning: A review,” Expert Syst. Appl., vol. 36, no. 10, pp. 11994–12000, Dec. 2009, doi: 10.1016/j.eswa.2009.05.029.

[2]J. A. Anderson, An Introduction to Neural Networks. MIT Press, 1995.

[3]H. Liu and B. Lang, “Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey,” Appl. Sci., vol. 9, no. 20, Art. no. 20, Jan. 2019, doi: 10.3390/app9204396.

[4]H. H. Pajouh, G. Dastghaibyfard, and S. Hashemi, “Two-tier network anomaly detection model: a machine learning approach,” J. Intell. Inf. Syst., vol. 48, no. 1, pp. 61–74, Feb. 2017, doi: 10.1007/s10844-015-0388-x.

[5]F. Kuang, S. Zhang, Z. Jin, and W. Xu, “A novel SVM by combining kernel principal component analysis and improved chaotic particle swarm optimization for intrusion detection,” Soft Comput., vol. 19, no. 5, pp. 1187–1199, May 2015, doi: 10.1007/s00500-014-1332-7.

پایان

باسپاس از توجه شما