



دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

به نام خدا

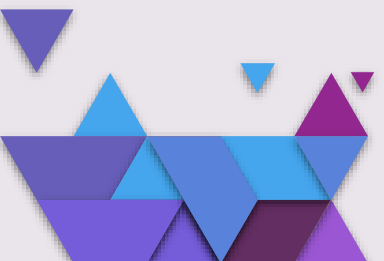
تشخیص نفوذ شبکه‌های کامپیوتری مبتنی بر یادگیری ماشین

گردآورنده: بهار کاویانی
استاد راهنما: دکتر رضا صفابخش

خردادماه بهار ۱۴۰۰



فهرست

- ۱ اهداف پژوهش
 - ۲ مقدمه و اهمیت پژوهش
 - ۳ رویکردهای مبتنی بر یادگیری ماشین
 - ۴ الگوریتم‌های تحت نظارت
 - ۵ الگوریتم‌های نظارت نشده
 - ۶ مقایسه و بررسی الگوریتم‌ها
 - ۷ جمع‌بندی و نتیجه‌گیری
 - ۸ پیشنهادات
 - ۹ منابع
- 

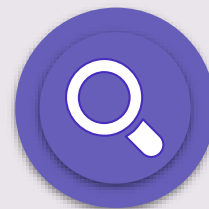
فهرست

- ۱ اهداف پژوهش
- ۲ مقدمه و اهمیت پژوهش
- ۳ رویکردهای مبتنی بر یادگیری ماشین
- ۴ الگوریتم‌های تحت نظارت
- ۵ الگوریتم‌های نظارت نشده
- ۶ مقایسه و بررسی الگوریتم‌ها
- ۷ جمع‌بندی و نتیجه‌گیری
- ۸ پیشنهادات
- ۹ منابع



اهداف پژوهش

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



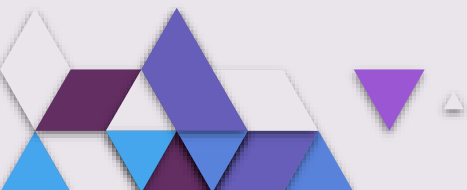
معرفی مقدماتی هر یک از
الگوریتم‌ها



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



ارائه‌ی الگوریتم‌های پیشنهادی با
توجه به منابع در دسترس



فهرست

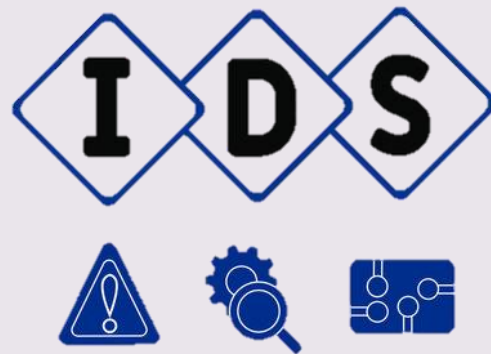
- ۱ اهداف پژوهش
- ۲ مقدمه و اهمیت پژوهش
- ۳ رویکردهای مبتنی بر یادگیری ماشین
- ۴ الگوریتم‌های تحت نظارت
- ۵ الگوریتم‌های نظارت نشده
- ۶ مقایسه و بررسی الگوریتم‌ها
- ۷ جمع‌بندی و نتیجه‌گیری
- ۸ پیشنهادات
- ۹ منابع



مقدمه

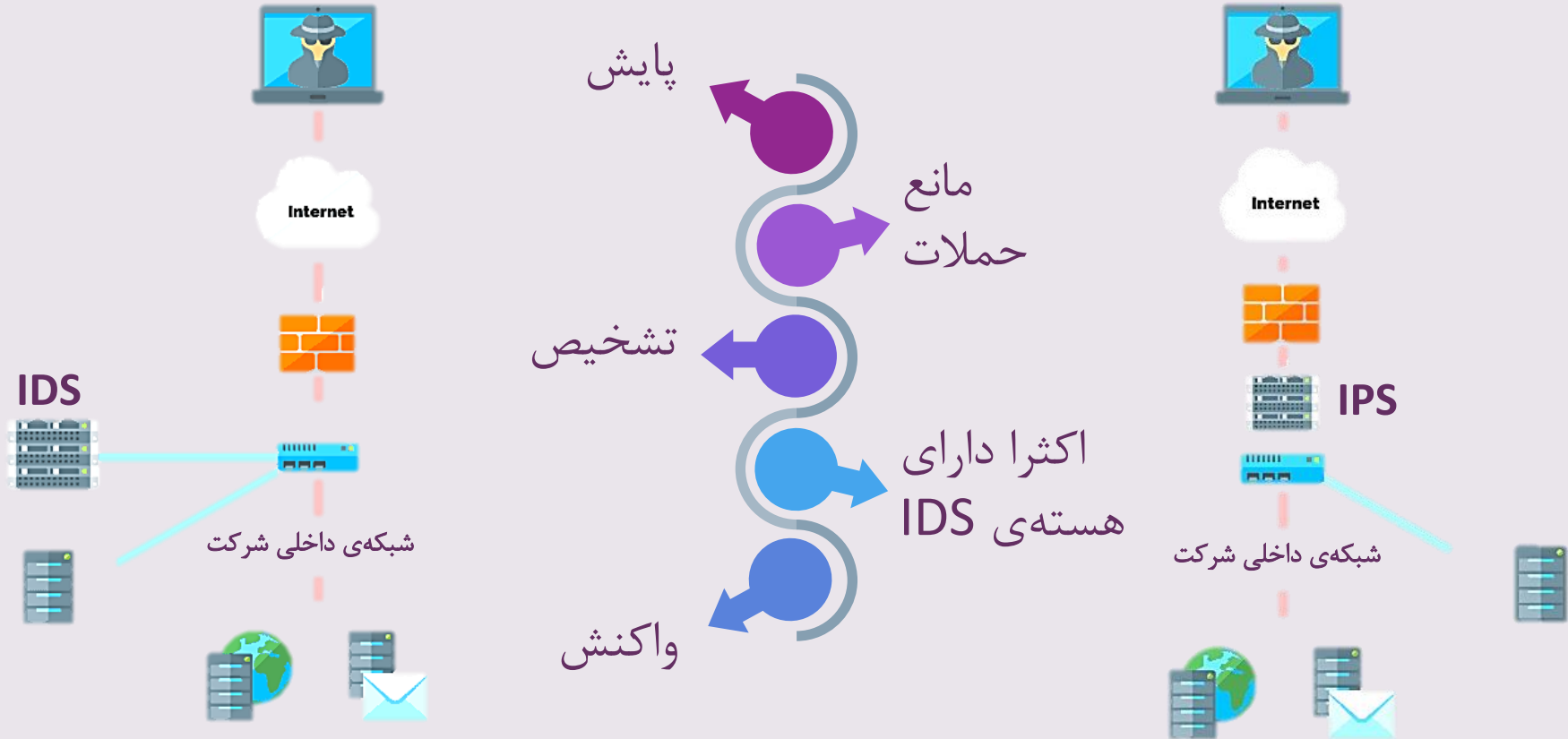
در دنیای امروز، اهمیت امنیت در استفاده از اینترنت و تجهیزات مربوط به آن بر کسی پوشیده نیست. راه‌های مختلفی برای مقابله با حملات امنیتی وجود دارد مانند:

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



سیستم جلوگیری از نفوذ

سیستم تشخیص نفوذ



فهرست

- ۱ اهداف پژوهش
- ۲ مقدمه و اهمیت پژوهش
- ۳ رویکردهای مبتنی بر یادگیری ماشین
- ۴ الگوریتم‌های تحت نظارت
- ۵ الگوریتم‌های نظارت نشده
- ۶ مقایسه و بررسی الگوریتم‌ها
- ۷ جمع‌بندی و نتیجه‌گیری
- ۸ پیشنهادات
- ۹ منابع



رویکردهای تشخیص نفوذ مبتنی بر یادگیری ماشین

تفاوت با راهکارهای دستی چیست؟



- ✓ دقت بهتر و سرعت تشخیص بیشتر
- ✓ 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 نظارت نشده
- ❖ کم عمق و عمیق
- ❖ طبقه‌بندی‌های تکی، ترکیبی و گروهی



فهرست

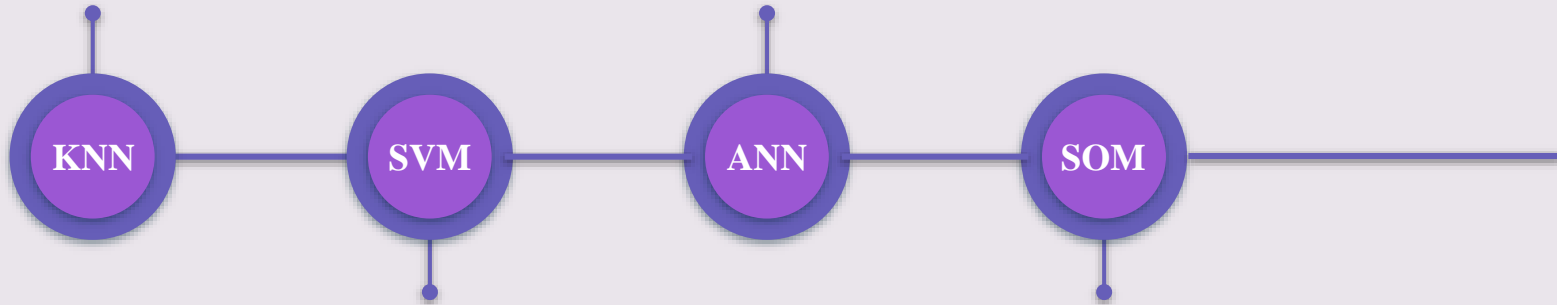
- ۱ اهداف پژوهش
- ۲ مقدمه و اهمیت پژوهش
- ۳ رویکردهای مبتنی بر یادگیری ماشین
- ۴ الگوریتم‌های تحت نظارت
- ۵ الگوریتم‌های نظارت‌نشده
- ۶ مقایسه و بررسی الگوریتم‌ها
- ۷ جمع‌بندی و نتیجه‌گیری
- ۸ پیشنهادات
- ۹ منابع



الگوریتم‌های تحت نظارت کم عمق

k-نزدیک‌ترین همسایه

شبکه‌های عصبی مصنوعی



ماشین بردار پشتیبان

نقشه‌های خود سازمان دهی شده

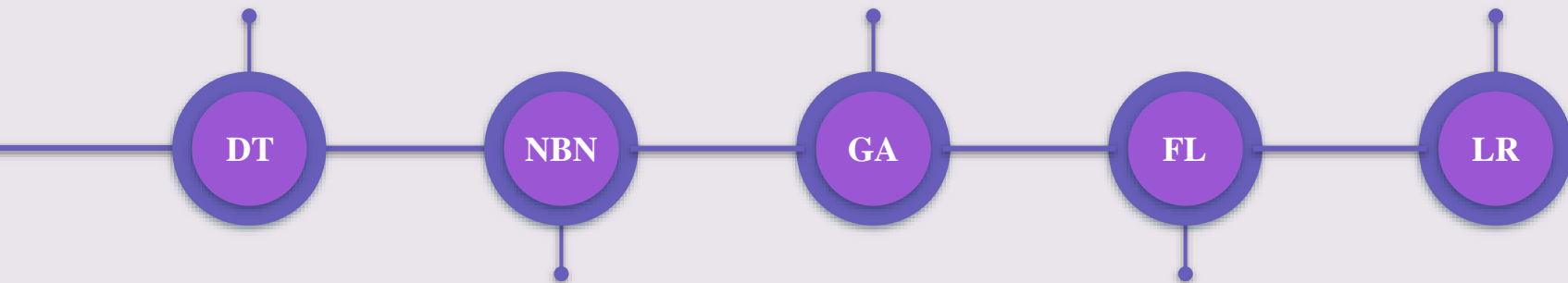


الگوریتم‌های تحت نظارت کم عمق (ادامه)

درخت تصمیم

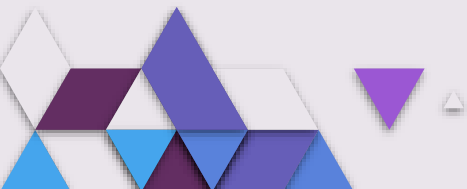
الگوریتم‌های ژنتیک

رگرسیون لجستیک

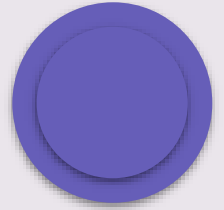


شبکه‌های خلیج ساده

منطق فازی



جمع‌بندی



توضیح و مقایسه‌ی هر بخش

کامنت

الگوریتم‌های تحت نظارت عمیق

DBN

شبکه کوتاه عمیق

DNN

شبکه عصبی عمیق

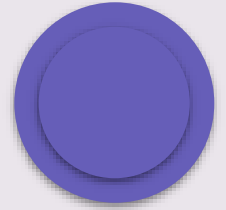
CNN

شبکه عصبی کانولوشن

RNN

شبکه عصبی راجعه

جمع‌بندی



توضیح و مقایسه‌ی مختصر هر بخش

فهرست

- ۱ اهداف پژوهش
- ۲ مقدمه و اهمیت پژوهش
- ۳ رویکردهای مبتنی بر یادگیری ماشین
- ۴ الگوریتم‌های تحت نظارت
- ۵ **الگوریتم‌های نظارت‌نشده**
- ۶ مقایسه و بررسی الگوریتم‌ها
- ۷ جمع‌بندی و نتیجه‌گیری
- ۸ پیشنهادات
- ۹ منابع



الگوریتم‌های نظارت نشده

شبکه‌های خصمانه تولیدی

عمیق

کم عمق

مدل k -معنی

ماشین بولتزمن محدود

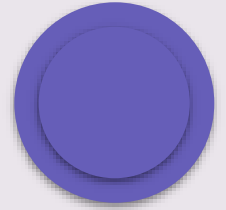
عمیق

عمیق

خود رمزگذار



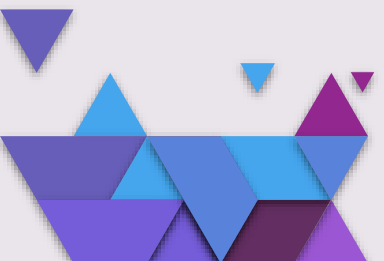
جمع‌بندی



توضیح و مقایسه‌ی مختصر هر بخش



فهرست

- ۱ اهداف پژوهش
 - ۲ مقدمه و اهمیت پژوهش
 - ۳ رویکردهای مبتنی بر یادگیری ماشین
 - ۴ الگوریتم‌های تحت نظارت
 - ۵ الگوریتم‌های نظارت نشده
 - ۶ **مقایسه و بررسی الگوریتم‌ها**
 - ۷ جمع‌بندی و نتیجه‌گیری
 - ۸ پیشنهادات
 - ۹ منابع
- 



پایان

بسیاس از توجه شما