گزارش مقاله

”A Transformer-based network intrusion detection approach for cloud security”

امنیت شبکه : دکتر اصغریان
محمدمهدی فرح بخش

۲۴ خرداد ۱۴۰۳

به نام خداوند بخشنده مهربان

۱.۰ مقدمه

با گسترش اهمیت رایانش ابری بین ذی نفعان دنیای نرم افزار، لزوم تأمین امنیت آن بیش از پیش موضوعیت پیدا کرده است. با توجه به این که ابزار های وارسی و تشخیص ترافیک غیر عادی در شبکه به طور قطعی قادر به ایفای نقش در این زمینه نیستند، لزوم استفاده از الگوریتم های ماشین لرنینگ جهت یادگیری و پیشبینی انواع نفوذ مورد توجه قرار گرفته است.

مدل های ترنسفورمر (Transformer) در مسائلی که ترتیب داده اهمیت دارد گوی سبقت را از رقبای خود از جمله RNN و CNN ربوده است. در مقاله "A Transformer-based network intrusion detection" [۱] به صورت تجربی توانایی شبکه Transformer در تشخیص انواع نفوذ مورد آزمایش قرار گرفته است.

۲.۰ رایانش ابری

از مزایای استفاده از ابر که باعث همه گیری آن شده عبارت است از:

۱. demand On

۲. دسترسی آسان از شبکه

۳. استخر منابع محاسباتی که باعث می شود ارائه و آزاد سازی اونها با کمترین اعمال مدیریت انجام شود.

۱.۲.۰ امنیت ابر

عدم توانایی شناسایی قطعی آنها توسط ابزار های ؟؟، از دلایل در معرض خطر قرارگرفتن ابر در برابر نفوذ ها می باشد.از جمله حملاتی که امنیت ابر را تهدید می کند می توان به موارد زیر اشاره کرد:

۱. IP Spoofing

۲. Routeing Information Protocol

۳. Man in The Middle Attack

۴. Port Scanning

۵. Insider Attack

۶. Dos

۷. DDos

۳.۰ شبکه های عصبی عمیق

به تحقیق، عملکرد شبکه های عصبی عمیق محدود به داده های آموزشی هستند، از این رو محدودیت هایی در بکارگیری در تشخیص نوع نفوذ خواهند داشت.

ایده شبکه های Transformer بر مبنای پیش آموزش (pretrain) به صورت عمومی برروی دیتای بزرگ و سپس آموزش اختصاصی برای یادگیری یک تسک مشخص با حجم کمتر از نظر داده می باشد. این امر باعث می شود مدل در تشخیص داده هایی که با داده های آموزش تفاوت داشتند نیز تا حد زیادی بهتر عمل کنند.

۱.۳.۰ شبکه های بازگشتی

تشخیص نوع نفوذ با بررسی سریالی از پکت ها امکان پذیر است. شبکه های عصبی بازگشتی توانایی بررسی داده های sequential را دارا می باشند اما مشکلاتی نیز گریبان گیر آنهاست:

جدول ۱: Your caption here.

	RNN	LSTM
مزایا	قابلیت یادگیری از روی داده های سری زمانی	طولانی تر کردن مدت محوشدگی گرادیان
معایب	• نیاز به زمان زیاد برای یادگیری • عدم امکان موازی سازی • ضعف در همگرایی • محو شدگی گرادیان • عدم توانایی حفظ یادگیری در بازه های زمانی طولانی	همچنان مشکلات RNN رو داراست.

Bibliography

[1] Zhenyue Long et al. A transformer-based network intrusion detection approach for cloud security. *Journal of Cloud Computing:Advances, Systems and Applications*, 11, 2024.