(عنوان مقاله: تشخیص نفوذ امنیت سایبری
(Cybersecurity Intrusion Detection

نام و نام خانوادگی نویسنده اول (علی پناهی)
وابستگی سازمانی نویسنده (دانشجوی کارشناسی ارشد دانشگاه جامع امام حسین (ع))

نام و نام خانوادگی نویسنده دوم (محمدرضا حسنی آهنگر)
وابستگی سازمانی نویسنده (استاد تمام دانشگاه جامع امام حسین (ع))
نام و نام خانوادگی نویسنده سوم (رامین دلیر)
وابستگی سازمانی نویسنده (دانشجوی دکترای دانشگاه زنجان)

چکیده
این مقاله به بررسی داده‌های امنیت سایبری با تمرکز بر تشخیص نفوذ در شبکه‌های کامپیوتری می‌پردازد. داده‌های مورد استفاده شامل اطلاعاتی از قبیل اندازه بسته‌های شبکه، نوع پروتکل، تعداد تلاش‌های ورود به سیستم، مدت زمان جلسه، الگوریتم رمزنگاری، امتیاز اعتبار آدرس شبکه[1]، تعداد ورودهای ناموفق، نوع مرورگر و دسترسی در زمان‌های غیرمعمول است. هدف این مقاله تحلیل این داده‌ها به منظور شناسایی الگوهای حمله و بهبود سیستم‌های تشخیص نفوذ[2] است. با استفاده از تکنیک‌های یادگیری ماشین، سعی می‌شود تا مدل‌هایی توسعه داده شوند که قادر به تشخیص حملات با دقت بالا باشند. نتایج این تحقیق می‌تواند به بهبود امنیت شبکه‌ها و کاهش خطرات ناشی از حملات سایبری کمک کند. یافته‌های این تحقیق می‌تواند به سازمان‌ها در پیاده‌سازی سیستم‌های تشخیص نفوذ بلادرنگ و کاهش ریسک‌های ناشی از حملات پیشرفته کمک کند، همچنین به عنوان پایه‌ای برای پژوهش‌های آینده در حوزه امنیت سایبری و هوش مصنوعی قابل استناد می‌باشد.

واژگان کلیدی: تشخیص نفوذ، امنیت سایبری، IDS، Security، Network Security

[1] IP Reputation Score
[2] Intrusion Detection Systems (IDS)

مقدمه

امنیت سایبری یکی از چالش‌های مهم دنیای دیجیتال امروزی است. با افزایش تهدیدات سایبری و حملات نفوذ، سیستم‌های تشخیص نفوذ[3] نقش مهمی در شناسایی و مقابله با این تهدیدات ایفا می‌کنند. هدف اصلی سیستم‌های تشخیص نفوذ، شناسایی فعالیت‌های غیرعادی در شبکه و تفکیک رفتارهای قانونی از حملات احتمالی است. با توجه به پیچیدگی و پویایی حملات سایبری، استفاده از تحلیل داده و یادگیری ماشین به‌عنوان راهکاری مؤثر در تشخیص نفوذ مورد توجه قرار گرفته است.

در این پژوهش، یک مجموعه داده شامل اطلاعات مربوط به فعالیت‌های شبکه مورد بررسی قرار گرفته است. این داده‌ها شامل ویژگی‌هایی مانند تعداد تلاش‌های ورود، نوع رمزنگاری، و امتیاز اعتبار آدرس شبکه[4] است که می‌توانند در تشخیص فعالیت‌های مشکوک نقش مهمی ایفا کنند. هدف اصلی این مطالعه، تحلیل این ویژگی‌ها و تعیین میزان تأثیر آن‌ها در شناسایی حملات است. همچنین، این مقاله به بررسی روش‌های یادگیری ماشین برای بهبود دقت تشخیص نفوذ می‌پردازد. نتایج این تحقیق می‌توانند به سازمان‌ها کمک کنند تا سیستم‌های امنیتی کارآمدتری را برای حفاظت از اطلاعات و شبکه‌های خود توسعه دهند.

هدف

هدف از تدوین این مقاله ارزیابی و مقایسه دقت مدل‌های یادگیری ماشین برای کمک به تشخیص تهدیدات سایبری و حملات نفوذ است. همچنین، تلاش شده است تا نقاط قوت و ضعف هر کدام از مدل مشخص شود تا بتوان از آن‌ها در سامانه‌های تشخیص نفوذ استفاده کرد.

مجموعه دادگان

در این مقاله به منظور بررسی و تحلیل داده‌های امنیت سایبری از مجموعه دادگان[5] موجود در وب‌سایت Kaggle استفاده شده است. این مجموعه دادگان که به منظور شناسایی نفوذهای سایبری براساس ترافیک شبکه و رفتار کاربر طراحی شده است، شامل ۹۵۳۷ نمونه و ۱۰ ویژگی بوده و متغیر هدف نشان‌دهنده وقوع حمله می‌باشد. به صورت کلی مجموعه دادگان به بخش‌های زیر تقسیم می‌گردد:

۱) ویژگی‌های مبتنی بر شبکه

این ویژگی ها اطلاعات سطح شبکه مانند اندازه بسته‌ها، نوع پروتکل‌ها و روش‌های رمزنگاری را توصیف می‌کنند.

- Network Packet Size: اندازه بسته به بایت، بین ۶۴ تا ۱۵۰۰ است. معمولا بسته های کمتر از ۶۴ بایت پیام های کنترلی را نشان دهند. مهاجمان[6] ممکن است از بسته‌های غیرعادی کوچک یا بزرگ برای شناسایی شبکه یا بهره‌برداری از آن استفاده کنند.
- Protocol Type: پروتکل مورد استفاده شامل TCP، UDP و ICMP.
- Encryption Used : پروتکل رمزگذاری

۲) ویژگی‌های مبتنی بر رفتار کاربر

این ویژگی‌ها نشان‌دهنده فعالیت‌های کاربر مانند تلاش برای ورود به سیستم و مدت زمان جلسه را می‌باشند.

[3] IDS
[4] IP Reputation Score
[5] Dataset
[6] Attackers

- Login Attempts: تعداد تلاش های مکرر برای ورود به سیستم می‌باشد. کاربران معمولی یک الی سه تلاش برای ورود به سیستم دارند، در حالی که یک حمله ممکن است صدها یا هزاران بار داشته باشد.
- Session Duration: طول جلسه بر حسب ثانیه می‌باشد. یک جلسه بسیار طولانی ممکن است نشان دهنده دسترسی غیرمجاز یا تداوم دسترسی برای یک مهاجم باشد. مهاجمان ممکن است سعی کنند برای حفظ دسترسی در ارتباط بمانند.
- Fail Logins: تعداد تلاش‌هایی که منجر به ورود ناموفق شده است.
- Unusual Time Access: یک پرچم باینری[7] (۰ یا ۱) که نشان می‌دهد آیا دسترسی در زمان غیرعادی اتفاق افتاده است یا خیر. مهاجمان اغلب خارج از ساعات کاری عادی عمل می‌کنند تا از شناسایی در امان باشند.
- IP Reputation Score: امتیازی از ۰ تا ۱ که مقادیر بالاتر نشان دهنده فعالیت مشکوک برای یک آدرس شبکه خاص می‌باشد. آدرس‌های شبکه مرتبط با باتنت‌ها، هرزنامه‌ها یا حمله کنندگان امتیاز بالاتری دارند.
- Browser Type: نوع مرورگر کاربر را نشان می‌دهد. در صورت شناخته بودن می‌تواند نشانگر وجود اسکریپت‌ها یا ربات‌های خودکار باشد.

۳) متغیر هدف

متغیر هدف شامل یکی از مقادیر صفر یا یک می‌باشد. مقدار صفر به معنای فعالیت عادی و مقدار یک به معنای حمله شناسایی شده می‌باشد.

روش تحقیق

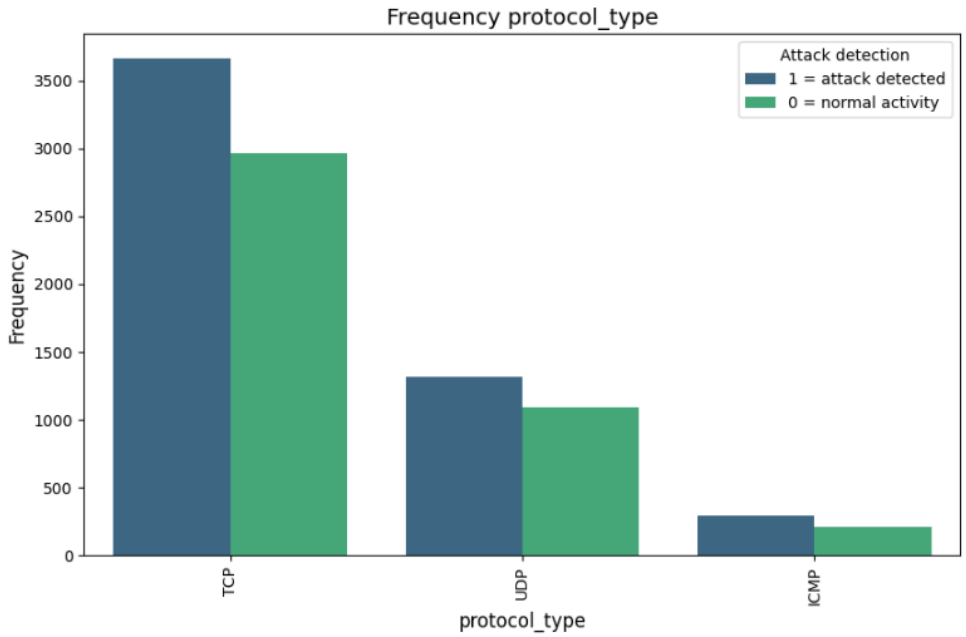
در این مقاله، با استفاده از تکنیک‌های یادگیری ماشین و دادگان مجموعه معرفی شده، مدلی برای تشخیص حملات سایبری توسعه داده می‌شود. فرآیند تحقیق شامل مراحل زیر است:

- جمع‌آوری و آماده‌سازی داده‌ها شامل حذف داده‌های پرت، پردازش مقادیر گمشده، نرمال‌سازی مقادیر عددی و تبدیل ویژگی‌های متنی به قالب عددی
- تحلیل داده‌ها شامل بررسی توزیع ویژگی‌های مختلف و همبستگی آنها با متغیر هدف
- انتخاب مدل و آموزش شامل الگوریتم‌های رگرسیون لجستیک[8]، درخت تصمیم[9]، جنگل تصادفی[10]، SVM، XGBoost و KNN می‌باشد.
- ارزیابی دقت مدل‌ها با استفاده از روش‌های F1-Score، Recall و...
- بهینه‌سازی و تنظیم هایپرپارامترها[11]
- تفسیر نتایج و تحلیل ویژگی‌های مهم در پیش‌بینی حمله

[7] Binary flag
[8] Logistic Regression
[9] Decision Tree Regressor
[10] Random Forest
[11] Hyperparameters

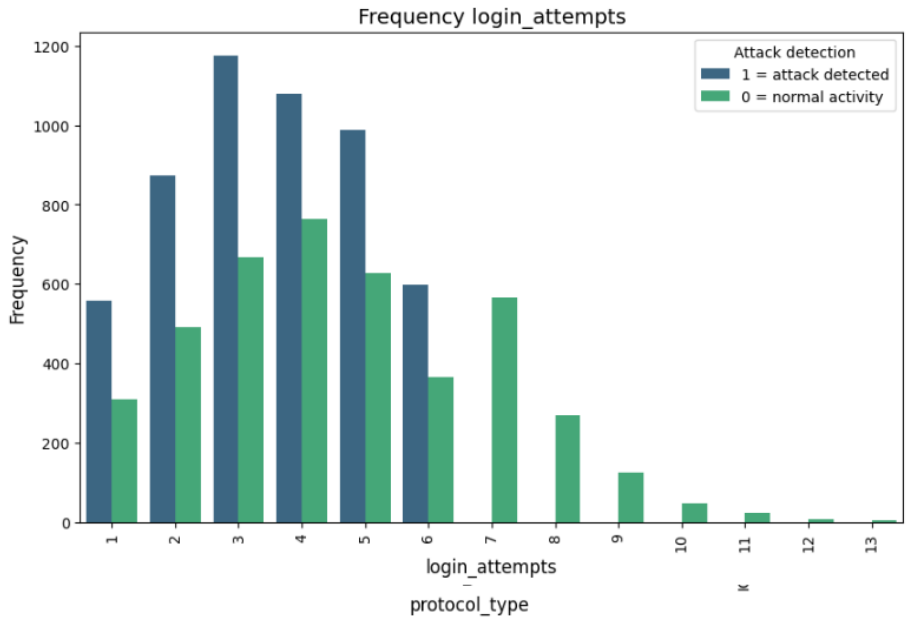
تحلیل داده‌ها

در ابتدا داده‌های غیرعددی همانند پروتکل رمزنگاری و نوع مرورگر کدگذاری می‌شوند. شکل زیر فراوانی حملات براساس پروتکل‌های مختلف را نشان می‌دهد. همانطور که در شکل زیر مشخص است، بیشترین حملات مربوط به پروتکل TCP می‌باشد.



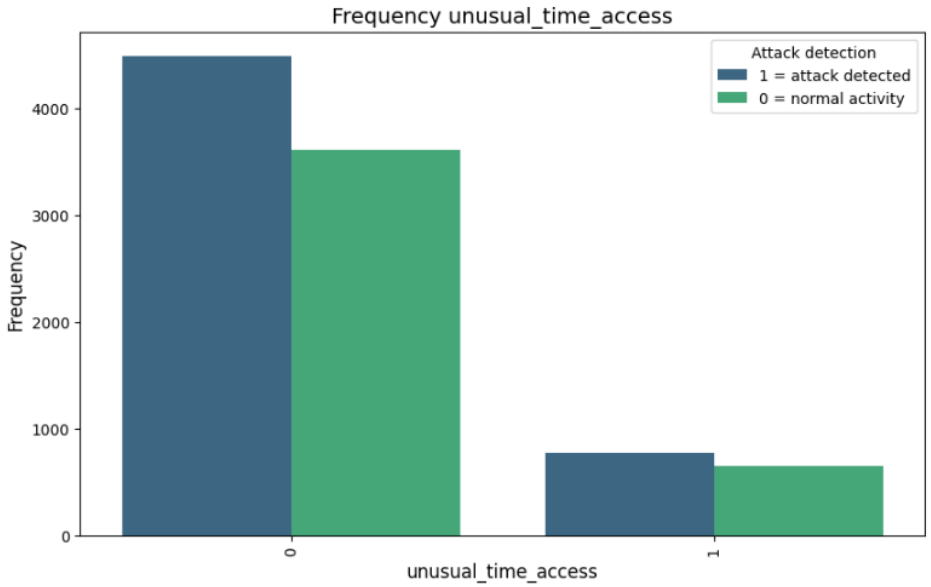
شکل ۱ – فراوانی حملات به نسبت پروتکل

همچنین در نمودار بعدی فراوانی حملات به نسبت تعداد تلاش ناموفق برای ورود نمایش داده شده است.



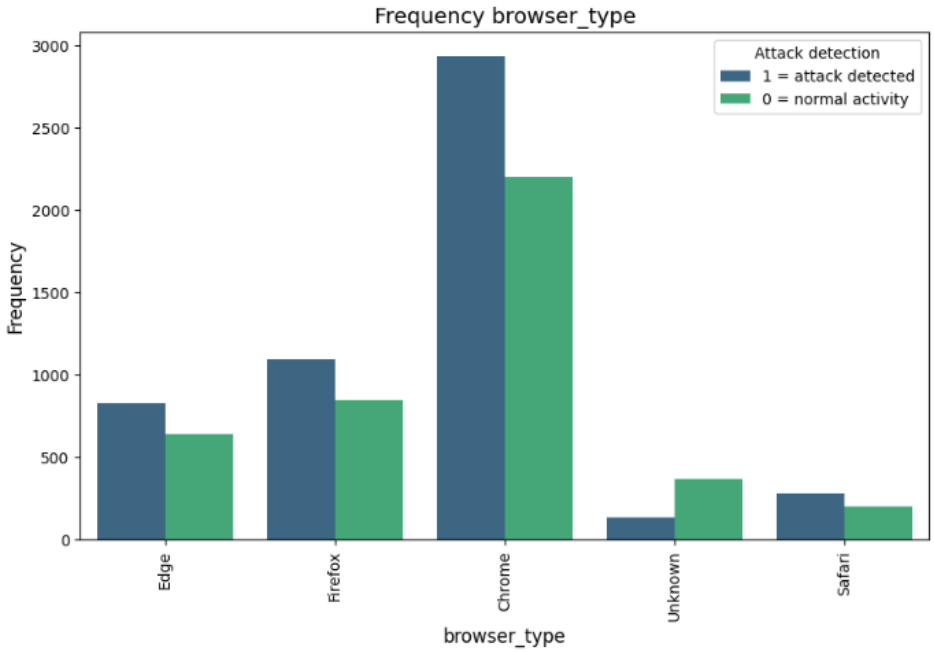
شکل ۲ – فراوانی حملات به نسبت تعداد تلاش‌های ناموفق برای ورود

نمودار بعدی فراوانی حملات به نسبت زمان نامتعارف برای دستیابی نمایش داده شده است.



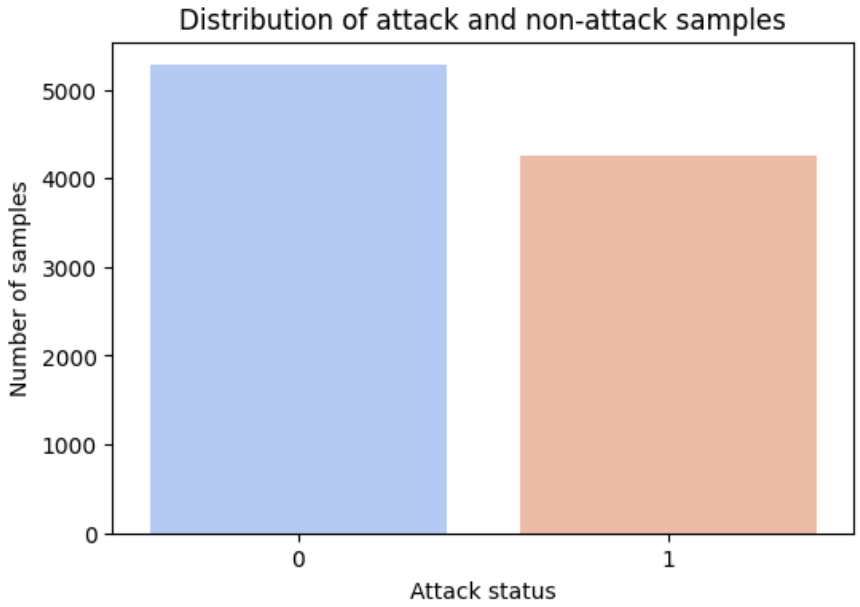
شکل ۳ - فراوانی حملات به نسبت تعداد تلاش‌های ناموفق برای ورود

نمودارهای فوق گواه تاثیر ویژگی‌های مذکور در تشخیص حمله می‌باشد. اما برخی از ویژگی‌ها همانند نوع مرورگر که در شکل زیر فراوانی آن آمده است، تاثیر کمی در تشخیص حمله دارند.



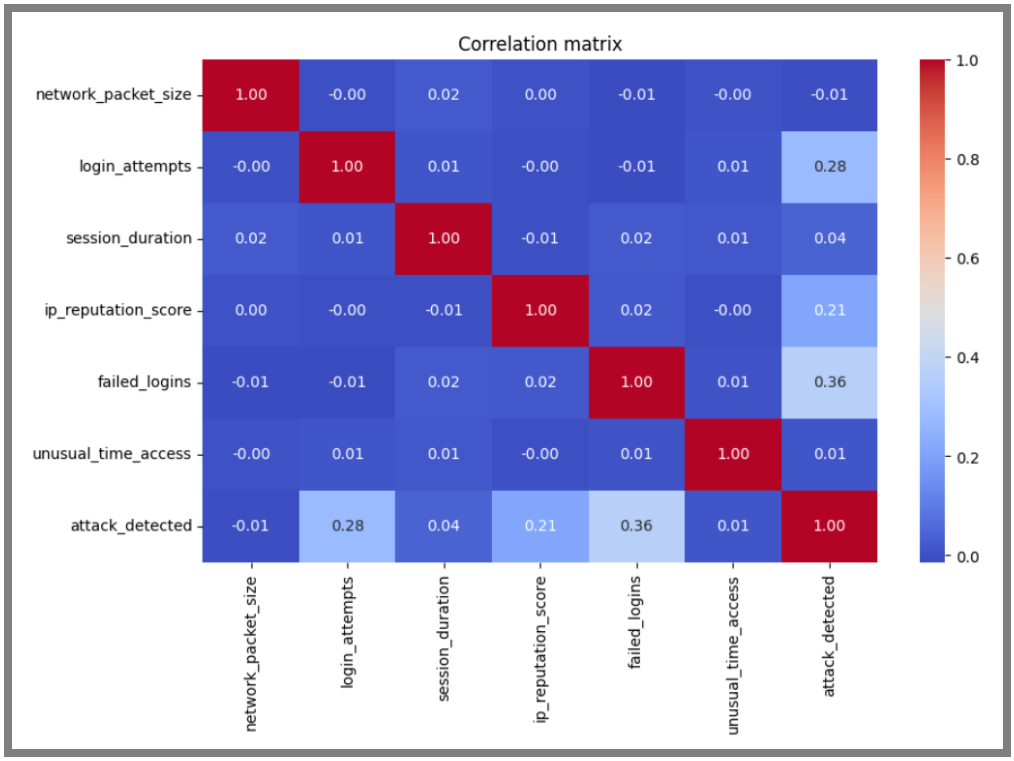
شکل ۴ - فراوانی حملات به نسبت نوع مرورگر

نمودار توزیع حملات سایبری در نمودار زیر ترسیم شده است. همانطور که مشخص می‌باشد، یک تعادل نسبی در مجموعه دادگان بین نمونه‌های سالم و نمونه‌های حمله وجود دارد.



شکل ۵ – تعداد نمونه‌های سالم و حمله

نمودار ذیل میزان همبستگی بین ویژگی‌های مختلف مجموعه دادگان تشخیص حملات سایبری را نمایش می‌دهد.



شکل ۶ – تعداد نمونه‌های سالم و حمله

چند نکته را می‌توان از این نمودار تحلیل نمود:

۱) ارتباط با متغیر هدف (attack_detected)

- failed_logins با مقدار ۰.۳۶ بیشترین همبستگی را با وقوع حمله دارد. این نشان می‌دهد که افزایش تعداد ورودهای ناموفق احتمال وقوع حمله را افزایش می‌دهد.
- login_attempts با مقدار ۰.۲۸ نیز دارای ارتباط متوسط با حملات است، که نشان‌دهنده‌ی تأثیر تلاش‌های ورود مشکوک بر تشخیص حمله است.
- ip_reputation_score همبستگی ۰.۲۱ دارد، که نشان می‌دهد اعتبار آدرس‌های شبکه نیز می‌تواند در پیش‌بینی حملات نقش داشته باشد.

۲) ارتباط بین متغیرهای مستقل

- اکثر ویژگی‌ها همبستگی نزدیکی با یکدیگر ندارند، که نشان‌دهنده‌ی استقلال نسبی آن‌ها است و می‌تواند به افزایش دقت مدل کمک کند.
- مقدار همبستگی بین network_packet_size و سایر ویژگی‌ها نزدیک به صفر است، که نشان می‌دهد این ویژگی ارتباط خاصی با سایر ویژگی‌ها ندارد.
- نتیجه‌گیری:
- ویژگی‌های تعداد تلاش‌های ورود ناموفق، تعداد تلاش‌های ورودها، و امتیاز اعتبار آدرس شبکه بیشترین تأثیر را در پیش‌بینی حملات دارند. از این رو، این ویژگی‌ها می‌توانند نقش کلیدی در بهبود مدل‌های یادگیری ماشین برای تشخیص تهدیدات سایبری داشته باشند.

پیش‌پردازش

برای بهبود عملکرد مدل‌ها، مراحل زیر بر روی مجموعه دادگان انجام‌شده است:

مدیریت داده‌های گمشده شامل بررسی و جایگزینی مقادیر ناموجود

تبدیل ویژگی‌های متنی به عددی شامل ویژگی‌های نوع مرورگر، الگوریتم رمزنگاری و...

استانداردسازی و نرمال‌سازی شامل مقیاس ویژگی‌ها به منظور بهبود عملکرد مدل‌ها.

تقسیم‌بندی داده‌ها

٪۸۰ داده‌ها) برای آموزش و ٪۲۰ برای تست استفاده شدند.

مدل‌های مورد استفاده

مدل‌های زیر به منظور آموزش مجموعه دادگان مورد استفاده قرار گرفتند:

- رگرسیون لجستیک[۱۲]
- SVM
- درخت تصمیم[۱۳]
- KNN
- XGBoost
- جنگل تصادفی[۱۴]

با توجه به اینکه برچسب دادگان کلاس‌بندی شده می‌باشد، مول‌های مذکور از نوع طبقه‌بند[۱۵] انتخاب شده‌اند.

معیارهای ارزیابی

برای مقایسه عملکرد مدل‌ها، از معیارهای زیر استفاده‌شده است.

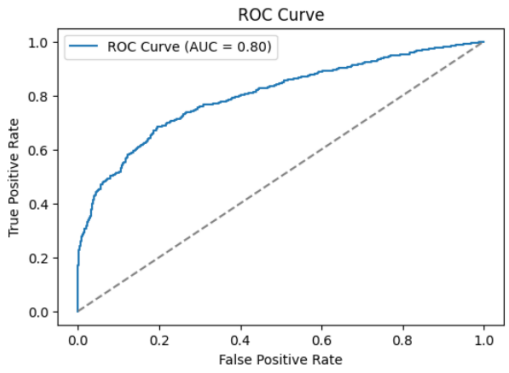
[12] Logistic regression
[13] Decision Tree
[14] Random Forest
[15] Classifier

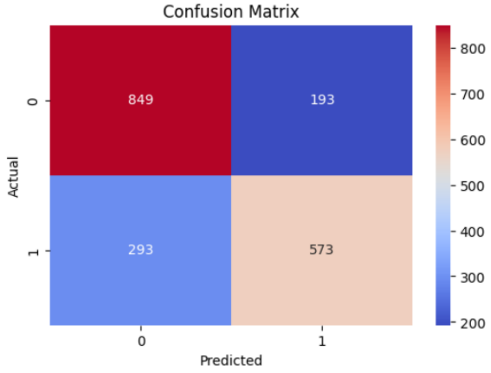
- دقت[16]: میزان پیش‌بینی‌های صحیح مدل
- صحت[17]: نسبت موارد مثبت درست پیش‌بینی‌شده به‌کل موارد مثبت پیش‌بینی‌شده
- فراخوانی[18]: نسبت موارد مثبت درست پیش‌بینی‌شده به‌کل موارد مثبت واقعی
- F1-Score: میانگین هارمونیک صحت و فراخوانی برای سنجش تعادل مدل
- مساحت زیر منحنی[19]: میزان توانایی مدل در تفکیک دو کلاس مثبت و منفی

نتایج

الف) رگرسیون لجستیک

- دقت[20] آن نسبت به مدل‌هایی مثل XGBoost و Random Forest پایین‌تر است.
- مقدار AUC برابر ۰.۸۰ نشان می‌دهد که این مدل قدرت تفکیک کمتری نسبت به مدل‌های پیشرفته‌تر دارد.
- بر اساس ماتریس درهم‌ریختگی، خطای طبقه‌بندی نمونه‌های مثبت در این مدل نسبتاً زیاد است.
- از آنجایی که این مدل نسبت به مدل‌های پیچیده‌تر مانند XGBoost ساده‌تر است، برای مجموعه داده‌های پیچیده یا دارای الگوهای غیرخطی، عملکرد بهینه‌ای ندارد.

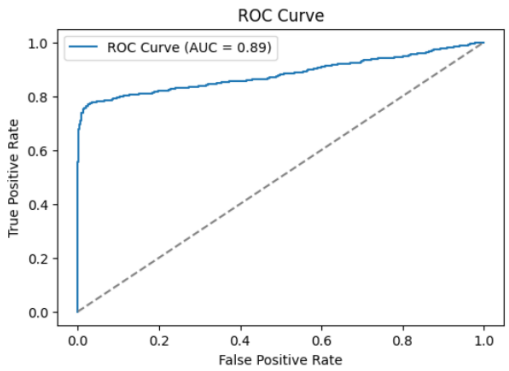


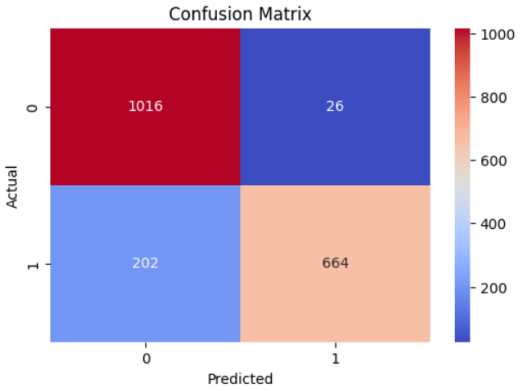


ب) SVM

- دقت این مدل ۰.۸۸ می‌باشد.
- مقدار AUC برابر ۰.۸۸ می‌باشد.
- بر اساس ماتریس درهم‌ریختگی، این مدل تعداد بسیار کمی نمونه‌ی مثبت را به اشتباه منفی تشخیص داده است، اما نسبت به مدل‌های دیگر دارای عملکرد متعادلی است.

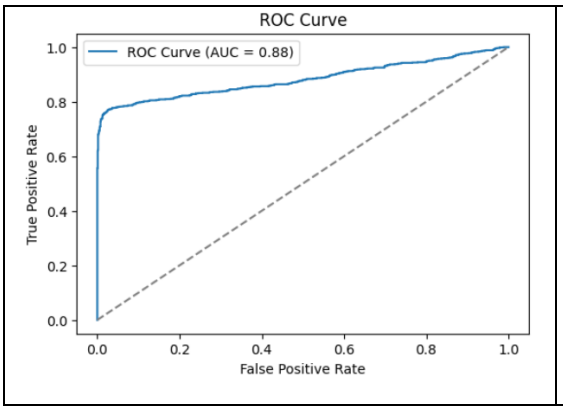
[16] Accuracy
[17] Precision
[18] Recall
[19] AUC-ROC
[20] Accuracy

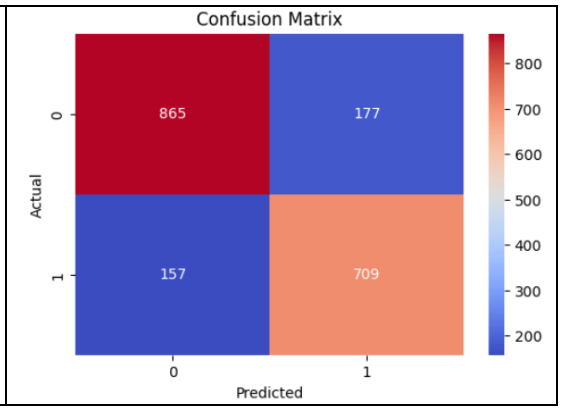




ج) درخت تصمیم

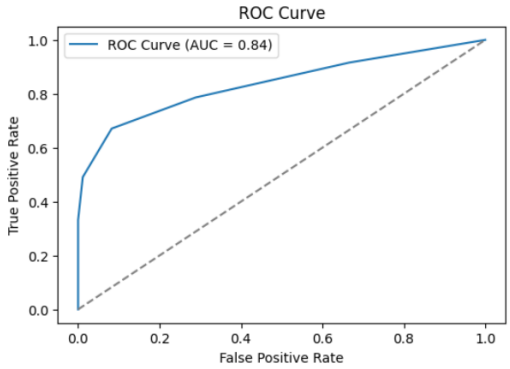
- دقت این مدل ۰.۸۲ می‌باشد.
- مقدار AUC برابر ۰.۸۸ می‌باشد.
- درخت تصمیم نسبت به SVM و KNN عملکرد خوبی دارد و خطای کمتری نسبت به KNN دارد، اما ممکن است در برابر داده‌های جدید کمتر تعمیم‌پذیر باشد.

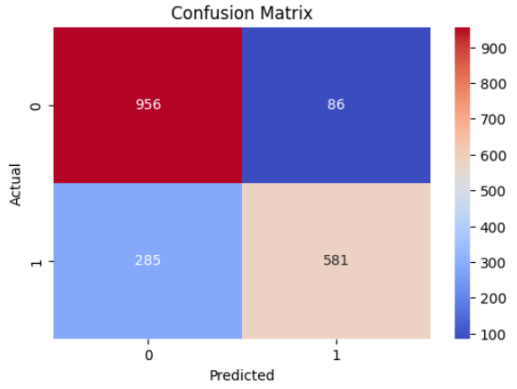




د) KNN

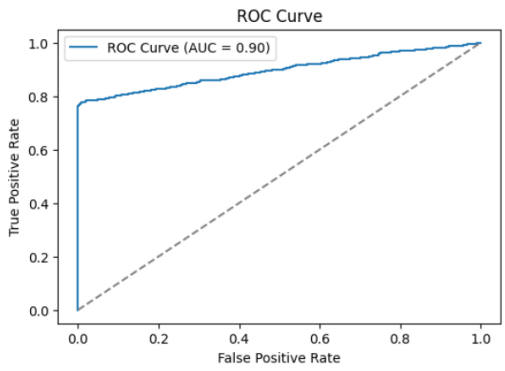
- دقت این مدل ۰.۸۰ می‌باشد.
- مقدار AUC برابر ۰.۸۳ می‌باشد.
- این مدل نسبت به مدل‌های پیچیده‌تر عملکرد ضعیف‌تری داشته است و خطای بیشتری در تشخیص نمونه‌های مثبت دارد.

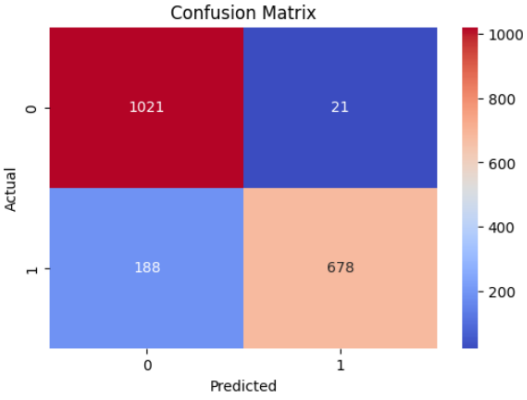




و) XGBoost

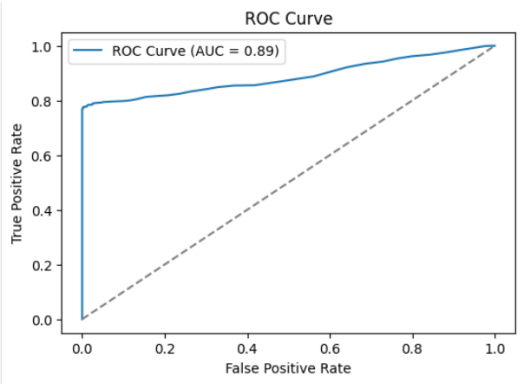
- دقت این مدل ۰.۹۰ می‌باشد.
- مقدار AUC برابر ۰.۸۹ می‌باشد.
- بهترین عملکرد را در بین مدل‌ها داشته است. این مدل قدرت تعمیم‌پذیری بالاتری نسبت به دیگر مدل‌ها دارد و نرخ تشخیص اشتباه بسیار پایینی را نشان می‌دهد.

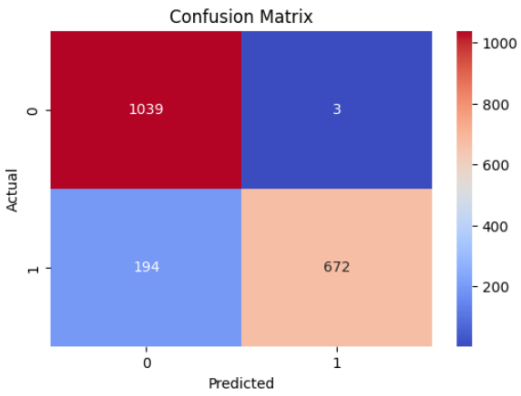




ه) جنگل تصادفی

- دقت این مدل ۰.۸۹ می‌باشد.
- مقدار AUC برابر ۰.۸۸ می‌باشد.
- بهترین عملکرد را در بین مدل‌ها داشته است. این مدل قدرت تعمیم‌پذیری بالاتری نسبت به دیگر مدل‌ها دارد و نرخ تشخیص اشتباه بسیار پایینی را نشان می‌دهد.





مقایسه تمامی مدل‌ها به صورت تجمیعی در جدول ذیل آمده است.

ROC AUC	F1 Score	Recall	Precision	Accuracy	مدل / معیار
0.8003	0.7022	0.6617	0.7480	0.7453	**رگرسیون لجستیک**
0.8863	0.8535	0.7667	0.9623	0.8805	**SVM**
0.8820	0.8094	0.8187	0.8002	0.8249	**درخت تصمیم**
0.8372	0.7580	0.6709	0.8755	0.8056	**KNN**
0.8963	0.8665	0.7829	0.9700	0.9005	**XGBoost**
0.8863	0.8722	0.7760	0.9956	0.8968	**جنگل تصادفی**

جمع‌بندی

- مدل XGBoost با بیشترین مقدار ۰.۹۰ دقت بهترین عملکرد را در میان مدل‌های بررسی شده داشته است.
- مدل جنگل تصادفی (Random Forest) نیز عملکرد قابل‌قبولی داشته و می‌تواند به‌عنوان جایگزین مناسب برای XGBoost در نظر گرفته شود.
- مدل‌های ساده‌تر مانند KNN و SVM عملکرد مناسبی دارند اما به اندازه مدل‌های پیچیده‌تر قدرتمند نیستند.
- مدل SVM نسبت به KNN و درخت تصمیم عملکرد بهتری داشته اما همچنان بهینه‌ترین مدل برای استفاده نیست.
- برای دادگان این مساله مدل‌های XGBoost و Random Forest پیشنهاد می‌شوند، زیرا تعادل خوبی بین دقت و نرخ تشخیص اشتباه دارند و در برابر داده‌های جدید نیز عملکرد بهتری دارند.

با توجه به بررسی‌های به عمل آمده در وب سایت Kaggle بالاترین دقت مربوط به مدل جنگل تصادفی با مقدار ۰.۸۹ می‌باشد، که مدل ارائه شده پیشنهادی یعنی XGBoost دقت را به ۰.۹۰ افزایش داده است.

منابع

مجموعه دادگان مورداستفاده در این مقاله مربوط به تشخیص نفوذ امنیت سایبری از طریق لینک زیر

قابل‌دسترسی است:

https://www.kaggle.com/datasets/dnkumars/cybersecurity-intrusion-detection-dataset

Cynet (۲۰۲۴)، نقش یادگیری ماشین در افزایش امنیت شبکه: کاربردها، چالش‌ها و آینده. Cynet

سیویلیکا (۲۰۲۴)، کاربرد یادگیری ماشین جهت تشخیص نفوذ در امنیت سایبری. سیویلیکا.

کاربرد یادگیری ماشین جهت تشخیص نفوذ در امنیت سایبری، ۱۴۰۳، سیویلیکا

Sommer, Robin and Vern Paxson. (2010). Analyzing the Generalizability of Intrusion Detection Systems. Proceedings of the 2010 ACM Conference on Computer and Communications Security. 2010. 413-424.

Moustafa, Nour, and Jun Yan. (2016). The Intrusion Detection System in Big Data: A Survey of Machine Learning Models and Their Challenges. Journal of Information Security and Applications. Vol. 27. 2016. 35-47.