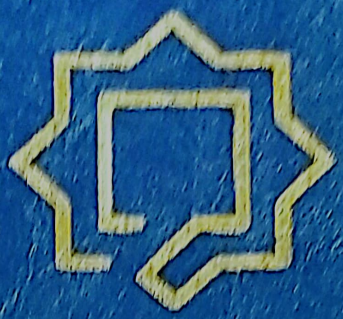

دانشگاه جامع علمی کاربردی

موسسه آموزش عالی آزاد انفورماتیک ایران

پایان نامه جهت دریافت درجه کارشناسی (B.S)

در رشته مهندسی فناوری امنیت اطلاعات

عنوان :

یادگیری ماشینی و هوش مصنوعی در امنیت اطلاعات

استاد راهنما : جناب مهندس بهمن افشار

نگارنده : مریم صادقی

پاییز و زمستان ۱۴۰۳

فهرست

فهرست شکل ها و جداول :

"چکیده"

در دنیای امروز، هوش مصنوعی (AI) و یادگیری ماشین (ML) به عنوان دو فناوری پیشرو، نقش مهمی در تحول و پیشرفت بسیاری از صنایع ایفا می‌کنند. این پایان‌نامه به بررسی نقش هوش مصنوعی و یادگیری ماشین در امنیت سایبری می‌پردازد. هدف اصلی این تحقیق، بررسی کاربردهای هوش مصنوعی و یادگیری ماشین در امنیت سایبری، شناسایی تهدیدات و فرصت‌های مرتبط با آن و ارائه راهکارهایی برای بهره‌برداری بهینه از این فناوری‌ها است.

روش تحقیق شامل بررسی منابع علمی و مقالات معتبر در زمینه هوش مصنوعی و امنیت سایبری، تحلیل داده‌ها و مطالعات موردی است. در بخش اول، مقدمه‌ای کوتاه بر هوش مصنوعی، تاریخچه مختصر آن، تفاوت‌های هوش مصنوعی با یادگیری ماشین و یادگیری عمیق، نگرانی‌ها و آینده هوش مصنوعی مورد بحث قرار می‌گیرد. در بخش دوم، نقش هوش مصنوعی و یادگیری ماشین در امنیت سایبری بررسی می‌شود. این بخش شامل بررسی اولیه هوش مصنوعی، تشخیص ناهنجاری، پیش‌پردازش داده‌ها، انتخاب الگوریتم، کلیت آموزش مدل، ارزیابی مدل، تجزیه و تحلیل و تشخیص بلادرنگ، رعایت حریم خصوصی و نتیجه‌گیری است. بخش سوم به کاربردهای هوش مصنوعی در امنیت سایبری می‌پردازد. این بخش شامل مشخصات یادگیری ماشین، انواع یادگیری ماشین، قابلیت‌های هوش مصنوعی مرتبط با امنیت سایبری، تکنیک‌های یادگیری ماشین، امکانات هوش مصنوعی برای بررسی داده‌ها، ملاحظات برای استفاده از هوش مصنوعی در امنیت سایبری، درایورها و مزایای هوش مصنوعی، مزایای هوش مصنوعی در امنیت سایبری، ویژگی‌ها و چالش‌های هوش مصنوعی برای امنیت سایبری، نگرانی‌های مربوط به حریم خصوصی و برنامه‌های کاربردی هوش مصنوعی برای امنیت سایبری است. بخش چهارم به افزایش تهدیدات امنیتی توسط هوش مصنوعی پیشرفته و راهکارهای مقابله با آن‌ها اختصاص دارد. این بخش شامل افزایش جرایم سایبری مبتنی بر هوش مصنوعی و نتایج آن، تکنیک‌های محافظت و برنامه‌های کاربردی در دنیایی با هوش مصنوعی، فناوری‌های امنیت برنامه (AppSec)، انواع جدیدی از آسیب‌پذیری و مشابه است. در نهایت، بخش پنجم به ملاحظات حقوقی و اخلاقی امنیت سایبری مبتنی بر هوش مصنوعی و چشم‌انداز آینده این حوزه می‌پردازد. این بخش شامل ملاحظات حقوقی و اخلاقی، حریم خصوصی و حفاظت از داده‌ها و موارد مهم دیگر است .

نتیجه‌گیری این تحقیق نشان می‌دهد که هوش مصنوعی و یادگیری ماشین نقش بسیارمهمی در بهبود امنیت سایبری و البته تهدید آن دارد، و نیاز ویژه به توجه به چالش‌ها و تهدیدات مرتبط با آن داریم .