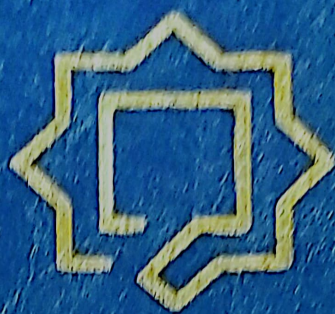




دانشگاه جامع علمی کاربردی

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

۱.....		چکیده
۲.....		بیش گفتار
۳.....	مقدمه ای کوتاه بر هوش مصنوعی	بخش ۱
۵.....	تاریخچه مختصری از هوش مصنوعی	
۵.....	اصطلاحات مهم مربوط به هوش مصنوعی :.....	
۶.....	الف - یادگیری ماشین.....	
۶.....	ب- یادگیری تحت نظارت	
۶.....	پ- یادگیری بدون نظارت	
۶.....	ت - یادگیری تقویتی	
۸.....	نگرانی ها در مورد هوش مصنوعی.....	
۸.....	آینده هوش مصنوعی.....	
۱۰.....	نقش هوش مصنوعی و یادگیری ماشین در امنیت سایبری.....	بخش ۲
۱۱.....	بررسی اولیه در مورد هوش مصنوعی.....	
۱۲.....	تشخیص ناهنجاری:	
۱۲.....	شناسایی و طبقه بندی بدافزار	
۱۲.....	سیستم های تشخیص نفوذ مبتنی بر هوش مصنوعی	
۱۲.....	تجزیه و تحلیل هوش تهدید	
۱۳.....	الگوریتم هایی برای حفاظت از داده ها	
۱۳.....	پیش پردازش داده ها.....	
۱۵.....	انتخاب الگوریتم.....	
۱۵.....	الگوریتم های رایج در امنیت سایبری	

کاربردهای کلیدی CNN در امنیت سایبری	۱۶
۱- سیستم‌های تشخیص نفوذ (IDS)	۱۶
۲- تشخیص بدافزار	۱۶
۳- فیشینگ و تشخیص هرزنامه	۱۶
۴- اصطلاح جالب پزشکی قانونی دیجیتال	۱۶
۵- هوش تهدید	۱۷
۶- الگوریتم Naive Bayes	۱۷
کلیت آموزش مدل	۱۷
مراحل کلیدی مربوط به آموزش مدل برای امنیت سایبری	۱۷
جمع‌آوری و پیش‌پردازش داده‌ها	۱۷
استخراج و مهندسی ویژگی	۱۸
انتخاب مدل	۱۸
آموزش مدل	۱۸
ارزیابی مدل	۱۸
تقسیم داده‌ها	۱۸
آموزش مدل	۱۹
تجزیه و تحلیل و تشخیص بلادرنگ	۲۰
یادگیری عمیق برای داده‌های پیچیده	۲۱
مقیاس‌پذیری و پردازش موازی	۲۱
رعایت حریم خصوصی	۲۱
نتیجه‌گیری	۲۲

- ۲۳..... کاربرد هوش مصنوعی در امنیت سایبری
- ۲۳..... مشخصات یادگیری ماشین
- ۲۴..... انواع یادگیری ماشین
- ۲۵..... قابلیت های هوش مصنوعی مرتبط با امنیت سایبری
- ۲۵..... تکنیک های یادگیری ماشین یا ML
- ۲۵..... ۱- طبقه بندی اطلاعات
- ۲۵..... ۲- تشخیص ناهنجاری
- ۲۶..... ۳- تحلیل رفتاری
- ۲۶..... ۴- تشخیص الگو ها
- ۲۷..... امکانات هوش مصنوعی برای بررسی داده ها
- ۲۷..... ۱- خوشه بندی
- ۲۷..... ۲- بازیابی اطلاعات
- ۲۷..... ۳- رتبه بندی
- ۲۷..... ۴- تولید محتوا
- ۲۸..... ملاحظات برای استفاده از هوش مصنوعی در امنیت سایبری
- ۲۸..... درایورها و مزایای هوش مصنوعی
- ۲۹..... مزایای هوش مصنوعی در امنیت سایبری
- ۲۹..... ۱- سرعت و اتوماسیون
- ۲۹..... ۲- مقیاس و پیچیدگی
- ۲۹..... ۳- سازگاری و تغییرپذیری
- ۳۰..... ۴- سازگاری
- ۳۰..... ۵- کشف حملات/تهدیدهای جدید
- ۳۱..... ویژگی ها و چالش های هوش مصنوعی برای امنیت سایبری
- ۳۱..... ۱- پاسخ سریع در زمان وقوع
- ۳۱..... ۲- تولید و ایجاد محیط های پویا
- ۳۲..... ۳- مقابله با حملات ماهیت خصمانه

۳۲.....	۴- کمترین هزینه خطا.....
۳۲.....	۵- کاهش چالش های داده در امنیت سایبری.....
۳۳.....	۶- تفسیر پذیری و توضیح پذیری.....
۳۳.....	۷- نگرانی های مربوط به حریم خصوصی.....
۳۴.....	اهمیت هوش مصنوعی برای امنیت سایبری.....
۳۵.....	پیشگیری و تشخیص تهدید.....
۳۷.....	نقطه پایانی و امنیت ابری.....
۳۸.....	امنیت شبکه.....
۴۰.....	تجزیه و تحلیل رفتار کاربر و نهاد (UEBA).....
۴۲.....	تجزیه و تحلیل امنیتی.....
۴۳.....	هوش تهدید.....
۴۵.....	مدیریت آسیب پذیری.....
۴۷.....	مدیریت ریسک امنیتی.....
۴۸.....	چگونه از هوش مصنوعی استفاده کنیم؟.....
۴۹.....	داستان توسعه موفق برنامه یادگیری ماشین (ML).....
۵۳.....	کلیدهای موفقیت در هوش مصنوعی برای امنیت سایبری.....
۵۷.....	آینده هوش مصنوعی برای امنیت سایبری.....
۵۷.....	کاربردهای LLM در امنیت سایبری.....
۶۰.....	خطرات، تهدیدها و چالش های پیش رو.....
۶۱.....	الزامات، مقررات و استانداردسازی هوش مصنوعی.....
۶۴.....	افزایش تهدیدات امنیتی توسط هوش مصنوعی پیشرفته.....
۶۶.....	اهمیت امنیت سایبری.....
۶۸.....	تکامل فناوری های هوش مصنوعی.....
۷۰.....	چگونه هوش مصنوعی جهان را تغییر می دهد.....
۷۲.....	هوش مصنوعی : یک شمشیر دو لبه.....
۷۲.....	تاثیر مثبت هوش مصنوعی بر امنیت سایبری.....
۷۴.....	جنبه تاریک هوش مصنوعی در امنیت سایبری.....
۷۴.....	تهدیدها و فرصت ها.....
۷۵.....	مزایای راه حل های امنیتی مبتنی بر هوش مصنوعی.....

۷۶.....	تشخیص تهدیدهای مبتنی بر هوش مصنوعی
۷۶.....	چالش ها و خطرات مرتبط با هوش مصنوعی در امنیت
۷۸.....	حملات سایبری مبتنی بر هوش مصنوعی
۷۸.....	۱- فازسازی خودکار و تولید Exploit
۷۸.....	۲- انطباق با اقدامات امنیتی در زمان واقعی
۷۹.....	۳- بدافزار و باج افزار هوشمند
۷۹.....	۴- تهدیدهای پایدار پیشرفته (APTs) و بازیگران دولت-ملت
۸۰.....	حملات دولت ملت با استفاده از هوش مصنوعی

بخش ۵

۸۱.....	افزایش تهدیدات امنیتی توسط هوش مصنوعی پیشرفته
۸۱.....	۱- تشخیص خودکار آسیب پذیری
۸۱.....	۲- حملات فیشینگ ایجاد شده توسط هوش مصنوعی
۸۲.....	۳- فناوری Deepfake و کمپین های اطلاعات نادرست
۸۲.....	افزایش جرایم سایبری مبتنی بر هوش مصنوعی و نتایج آن
۸۳.....	الف- تأثیر بر مشاغل و افراد
۸۳.....	ب- هزینه بازیابی بالا
۸۳.....	پ- پیامدهای قانونی و نظارتی
۸۴.....	ت- نگرانی های مربوط به حریم خصوصی شخصی
۸۴.....	تکنیک های محافظت و برنامه های کاربردی
۸۵.....	فناوری های امنیت برنامه (AppSec)
۸۶.....	انواع جدیدی از آسیب پذیری
۸۷.....	تقویت احراز هویت و کنترل دسترسی
۸۷.....	رمزگذاری و حفاظت از داده ها
۸۸.....	راه حل های امنیتی مبتنی بر هوش مصنوعی: هوش مصنوعی برای محافظت
۸۸.....	۱- تشخیص و تجزیه و تحلیل تهدید مبتنی بر هوش مصنوعی
۸۹.....	۲- واکنش و اصلاح حادثه مبتنی بر هوش مصنوعی
۸۹.....	۳- تجزیه و تحلیل رفتار کاربر و نهاد با هوش مصنوعی (UEBA)
۹۰.....	اهمیت AppSec فعال در عصر هوش مصنوعی

بخش ۶

۹۲.....	برای تغییرات آینده امنیت سایبری مبتنی بر هوش مصنوعی آماده شویم
۹۲.....	روندهای نوظهور در امنیت سایبری مبتنی بر هوش مصنوعی

۹۳.....	ملاحظات حقوقی و اخلاقی امنیت سایبری مبتنی بر هوش مصنوعی.....
۹۳.....	حریم خصوصی و حفاظت از داده ها.....
۹۴.....	شفافیت و توضیح پذیری.....
۹۴.....	آیا هوش مصنوعی اسرار ما را حفظ خواهد کرد؟.....
۹۵.....	تکلیف مسئولیت و مسئولیت قانونی.....
۹۵.....	ملاحظات اخلاقی.....
۹۶.....	نتیجه گیری چشم انداز آینده امنیت سایبری مبتنی بر هوش مصنوعی.....

فهرست شکل ها و جداول :

۵	شکل ۱ تاریخچه تصویری توسعه هوش مصنوعی.....
۷	شکل ۱ حوزه های کاربردی هوش مصنوعی.....
۱۵	شکل ۳ الگوریتم های یادگیری ماشین.....
۲۸	شکل ۴ مزایای هوش مصنوعی در امنیت سایبری.....
۳۵	شکل ۵ : سطح بلوغ برنامه های کاربردی امنیت سایبری هوش مصنوعی.....
۵۳.....	شکل ۶ - کلید موفقیت در کاربرد هوش مصنوعی در امنیت سایبری و مراحل پروژه.....

"حکیده"

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 می کنند. این پایان نامه به بررسی نقش هوش مصنوعی و یادگیری ماشین در امنیت سایبری می پردازد. هدف اصلی این تحقیق، بررسی کاربردهای هوش مصنوعی و یادگیری ماشین در امنیت سایبری، شناسایی تهدیدات و فرصت های مرتبط با آن و ارائه راهکارهایی برای بهره برداری بهینه از این فناوری ها است.

روش تحقیق شامل بررسی منابع علمی و مقالات معتبر در زمینه هوش مصنوعی و امنیت سایبری، تحلیل داده ها و مطالعات موردی است. در بخش اول، مقدمه ای کوتاه بر هوش مصنوعی، تاریخچه مختصر آن، تفاوت های هوش مصنوعی با یادگیری ماشین و یادگیری عمیق، نگرانی ها و آینده هوش مصنوعی مورد بحث قرار می گیرد. در بخش دوم، نقش هوش مصنوعی و یادگیری ماشین در امنیت سایبری بررسی می شود. این بخش شامل بررسی اولیه هوش مصنوعی، تشخیص ناهنجاری، پیش پردازش داده ها، انتخاب الگوریتم، کلیت آموزش مدل، ارزیابی مدل، تجزیه و تحلیل و تشخیص بلاذنگ، رعایت حریم خصوصی و نتیجه گیری است. بخش سوم به کاربردهای هوش مصنوعی در امنیت سایبری می پردازد. این بخش شامل مشخصات یادگیری ماشین، انواع یادگیری ماشین، قابلیت های هوش مصنوعی مرتبط با امنیت سایبری، تکنیک های یادگیری ماشین، امکانات هوش مصنوعی برای بررسی داده ها، ملاحظات برای استفاده از هوش مصنوعی در امنیت سایبری، درایورها و مزایای هوش مصنوعی، مزایای هوش مصنوعی در امنیت سایبری، ویژگی ها و چالش های هوش مصنوعی برای امنیت سایبری، نگرانی های مربوط به حریم خصوصی و برنامه های کاربردی هوش مصنوعی برای امنیت سایبری است. بخش چهارم به افزایش تهدیدات امنیتی توسط هوش مصنوعی پیشرفته و راهکارهای مقابله با آن ها اختصاص دارد. این بخش شامل افزایش جرایم سایبری مبتنی بر هوش مصنوعی و نتایج آن، تکنیک های محافظت و برنامه های کاربردی در دنیایی با هوش مصنوعی، فناوری های امنیت برنامه (AppSec)، انواع جدیدی از آسیب پذیری و مشابه است. در نهایت، بخش پنجم به ملاحظات حقوقی و اخلاقی امنیت سایبری مبتنی بر هوش مصنوعی و چشم انداز آینده این حوزه می پردازد. این بخش شامل ملاحظات حقوقی و اخلاقی، حریم خصوصی و حفاظت از داده ها و موارد مهم دیگر است.

نتیجه گیری این تحقیق نشان می دهد که هوش مصنوعی و یادگیری ماشین نقش بنیادین مهمی در بهبود امنیت سایبری و البته تهدید آن دارد، و نیاز ویژه به توجه به چالش ها و تهدیدات مرتبط با آن داریم.