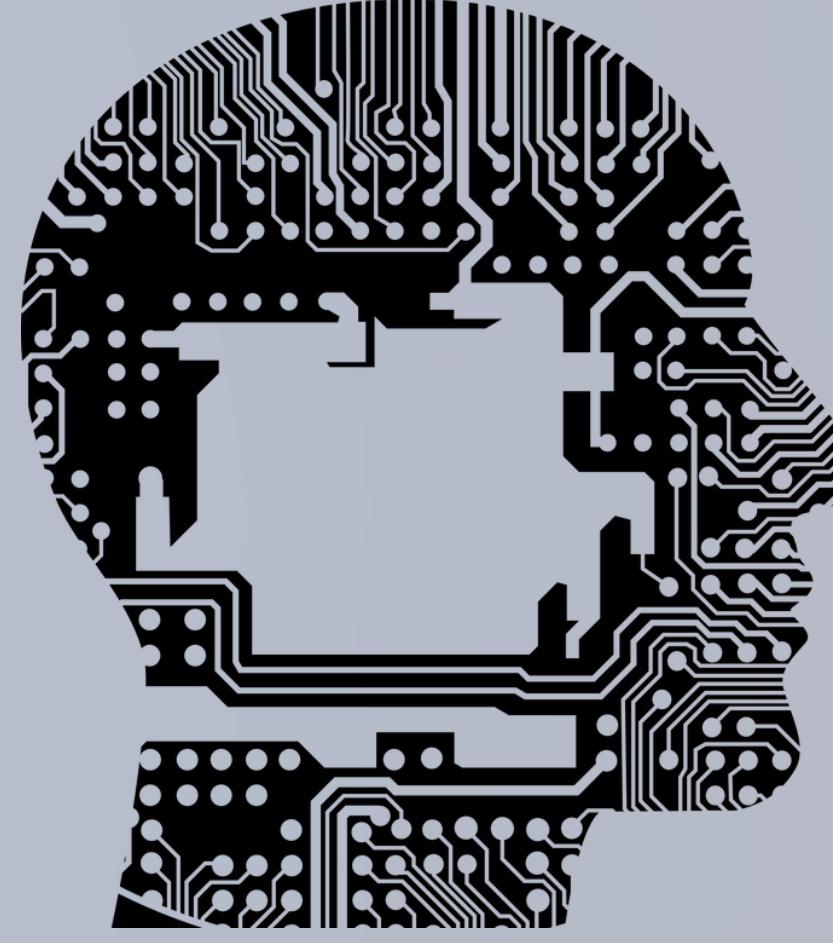


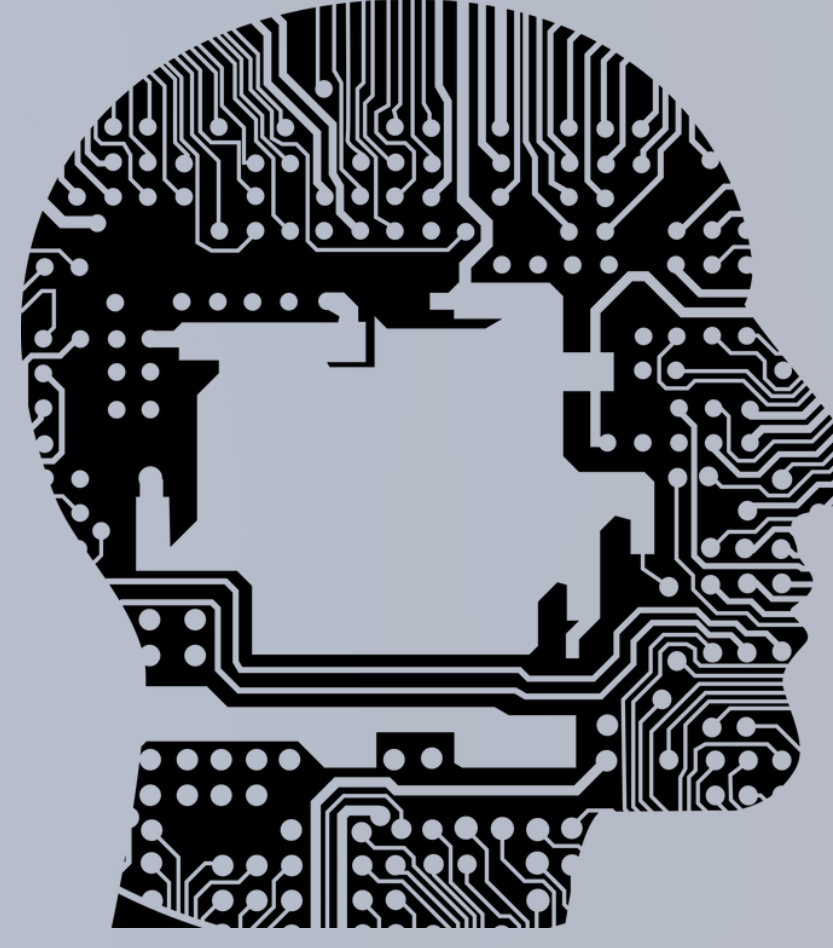


استخدام الذكاء الاصطناعي في كشف الجرائم السيبرانية

جامعة ميدأوشن

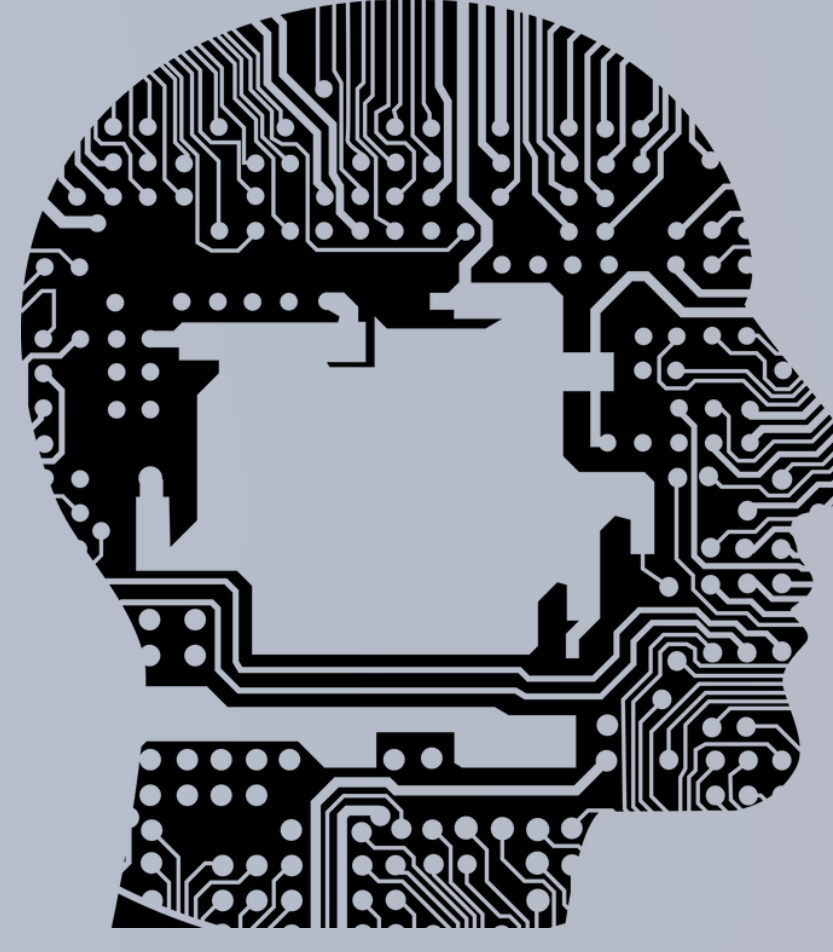
عمل الطالب / غازي غانم نصار الجهني

الرقم الجامعي / 251000251



المقدمة

يشهد العالم، والمملكة العربية السعودية على وجه الخصوص، نموًا مطردًا في استخدام التقنيات الرقمية، مما جعل الفضاء الإلكتروني جزءًا لا يتجزأ من حياتنا اليومية. ومع هذا التوسع الرقمي، تزايدت التهديدات السيبرانية وتزوّعت أساليب الهجمات الإلكترونية، مما استدعى الحاجة إلى حلول مبتكرة وفعالة لمكافحة هذه الجرائم. هنا يأتي دور الذكاء الاصطناعي (AI) كأداة قوية في مواجهة التحديات الأمنية وحماية الأفراد والمؤسسات من مخاطر الجرائم الإلكترونية.



الاهداء

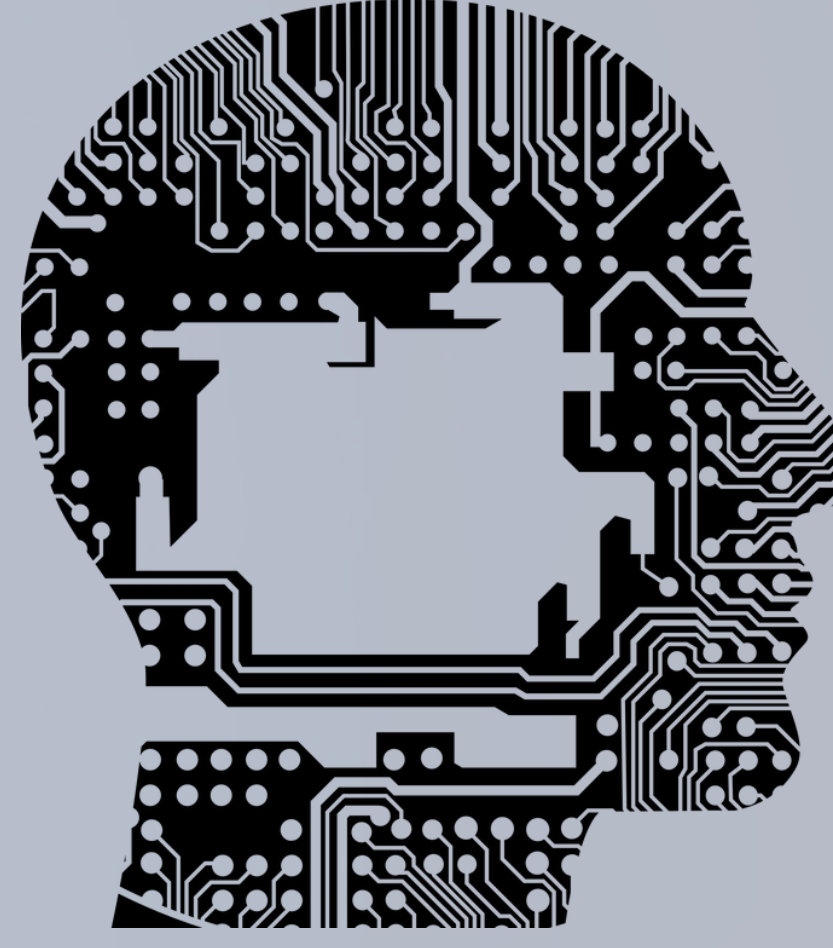
إلى أبي العطوف.... قدوتي، ومثلي الأعلى في الحياة؛
فهو من علّمني كيف أعيش بكرامة وشموخ.
إلى أمي الحنونة..... لا أجد كلمات يمكن أن تمنحها
حقها، فهي ملحمة الحب وفرحة العمر، ومثال التفاني
والعطاء.

إلى إخوتي.... سندي وعضدي ومشاطري أفراحي
وأحزاني.

إلى زوجتي.... أسمى رموز الإخلاص والوفاء ورفيقة
الدرب

إلى أولادي..... فلذات الأكباد.

إلى جميع الأخلاء؛ أهدي إليكم بحثي العلمي في
استخدام الذكاء الاصطناعي في كشف الجرائم
السيبرانية



الموضوع

ما هو الذكاء الاصطناعي؟

الذكاء الاصطناعي هو فرع من فروع علوم الحاسوب يهدف إلى تطوير أنظمة وبرامج قادرة على محاكاة القدرات الذهنية البشرية، مثل التعلم والاستنتاج وحل المشكلات. يتميز الذكاء الاصطناعي بقدرته على تحليل كميات هائلة من البيانات واكتشاف الأنماط والشذوذات التي يصعب على الإنسان ملاحظتها، مما يجعله أداة فعالة في الكشف عن الجرائم الإلكترونية ومنعها.



كيف يُستخدم الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية؟

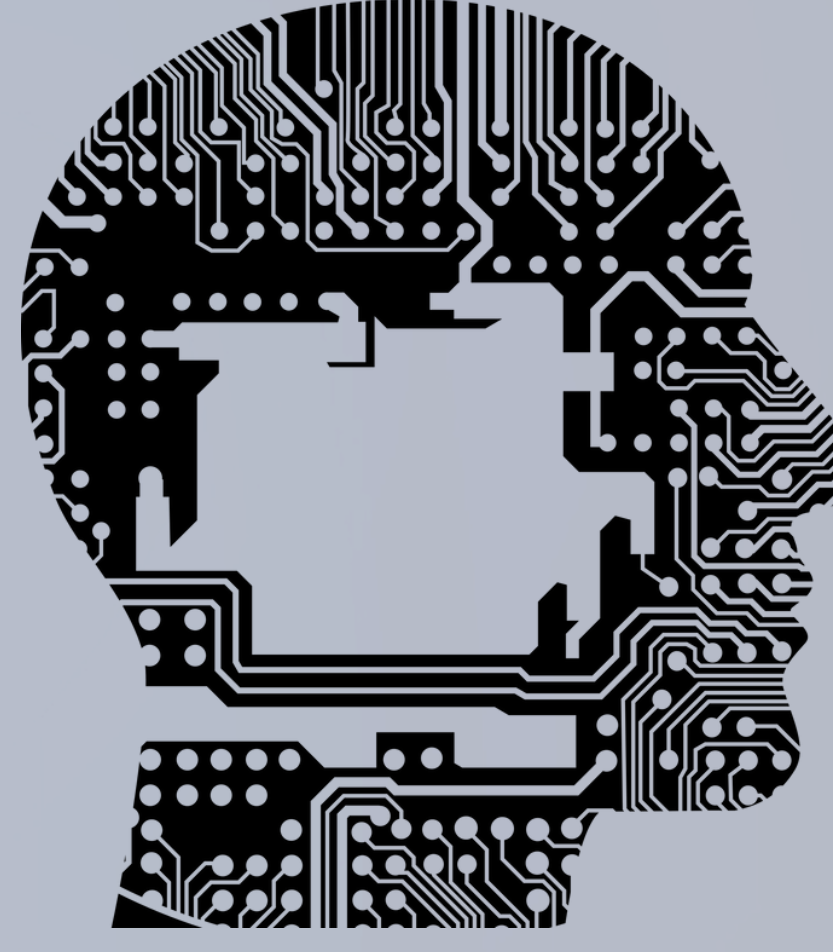
تحليل حركة المرور على الشبكة

الكشف عن البرامج الضارة

تحسين أنظمة المراقبة

الكشف عن الاحتيال المالي

مكافحة التصيد الاحتيالي



الموضوع

كيف يُستخدم الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية؟
يُستخدم الذكاء الاصطناعي في مجموعة متنوعة من التطبيقات الأمنية، بما في ذلك:

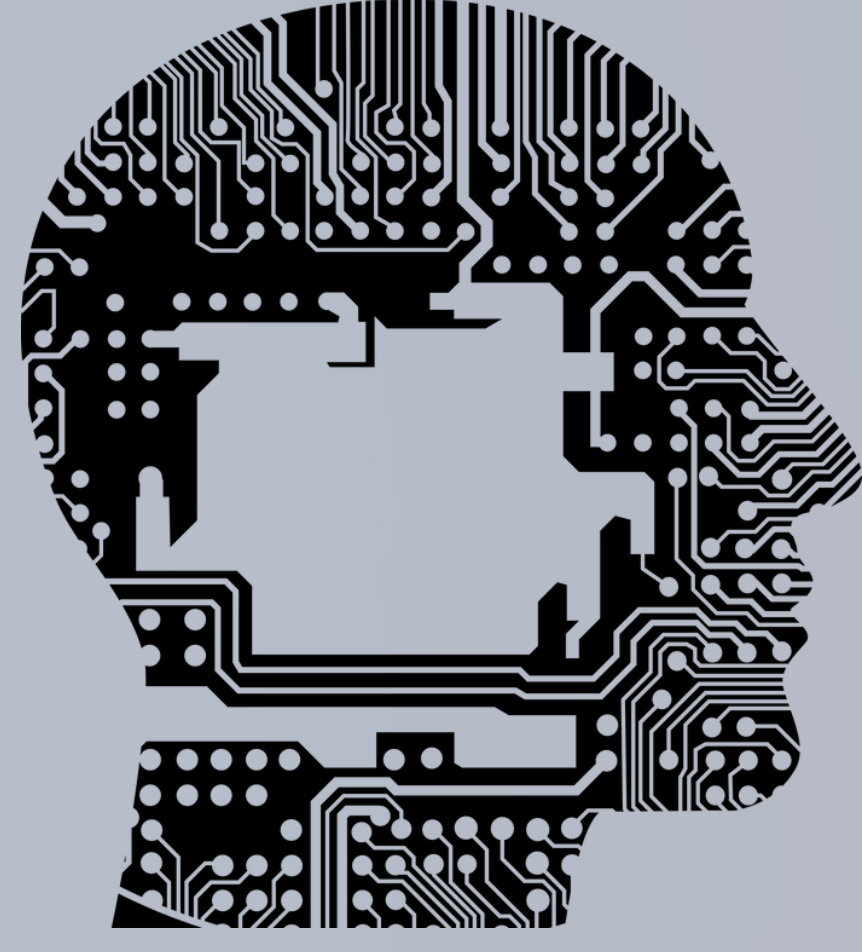
الكشف عن البرامج الضارة: تستخدم أنظمة الذكاء الاصطناعي تقنيات التعلم الآلي لتحليل سلوك البرامج وتحديد ما إذا كانت ضارة أم لا. يمكن لهذه الأنظمة اكتشاف البرامج الضارة الجديدة التي لم يتم التعرف عليها من قبل، مما يوفر حماية أفضل ضد التهديدات الحديثة.

تحليل حركة المرور على الشبكة: يمكن للذكاء الاصطناعي تحليل أنماط حركة المرور على الشبكة للكشف عن الأنشطة المشبوهة، مثل محاولات الاختراق وهجمات حجب الخدمة.

مكافحة التصيد الاحتيالي: يمكن للذكاء الاصطناعي تحليل رسائل البريد الإلكتروني والمواقع الإلكترونية لتحديد ما إذا كانت تنطوي على محاولات تصيد احتيالي، وتنبيه المستخدمين إلى ذلك.

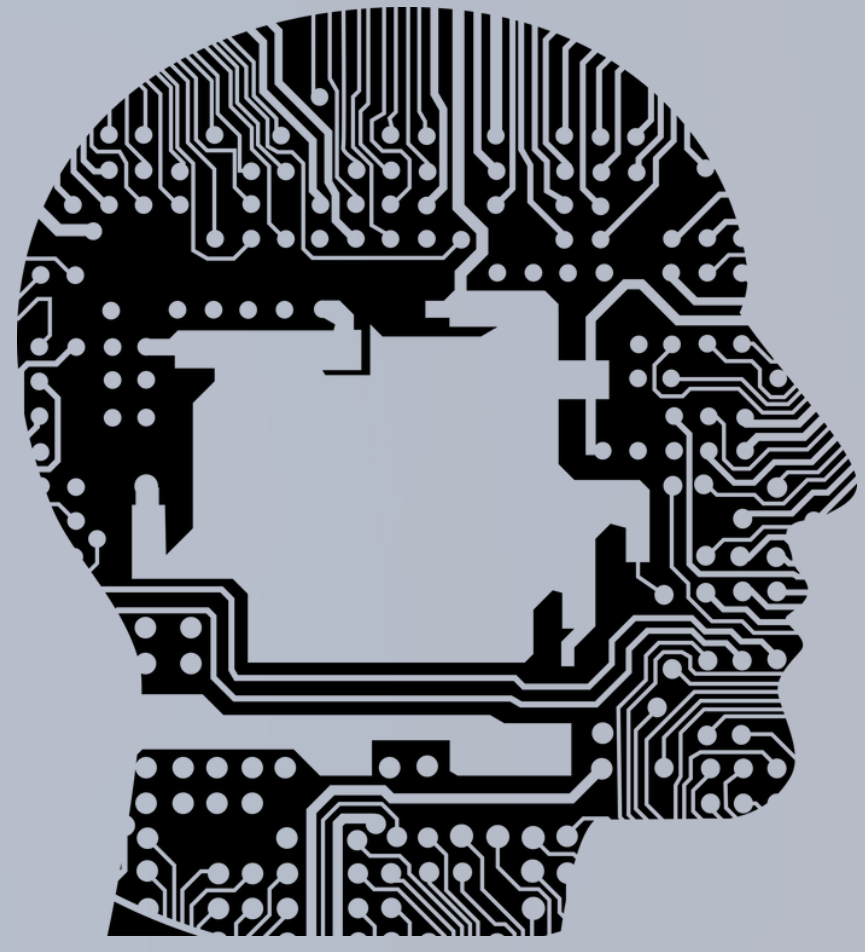
الكشف عن الاحتيال المالي: يمكن للذكاء الاصطناعي تحليل المعاملات المالية للكشف عن الأنشطة الاحتيالية، مثل استخدام بطاقات الائتمان المسروقة.

تحسين أنظمة المراقبة: يمكن دمج تقنيات الذكاء الاصطناعي في أنظمة المراقبة لتحليل لقطات الفيديو والكشف عن الأنشطة المشبوهة، مثل عمليات السرقة والتخريب.



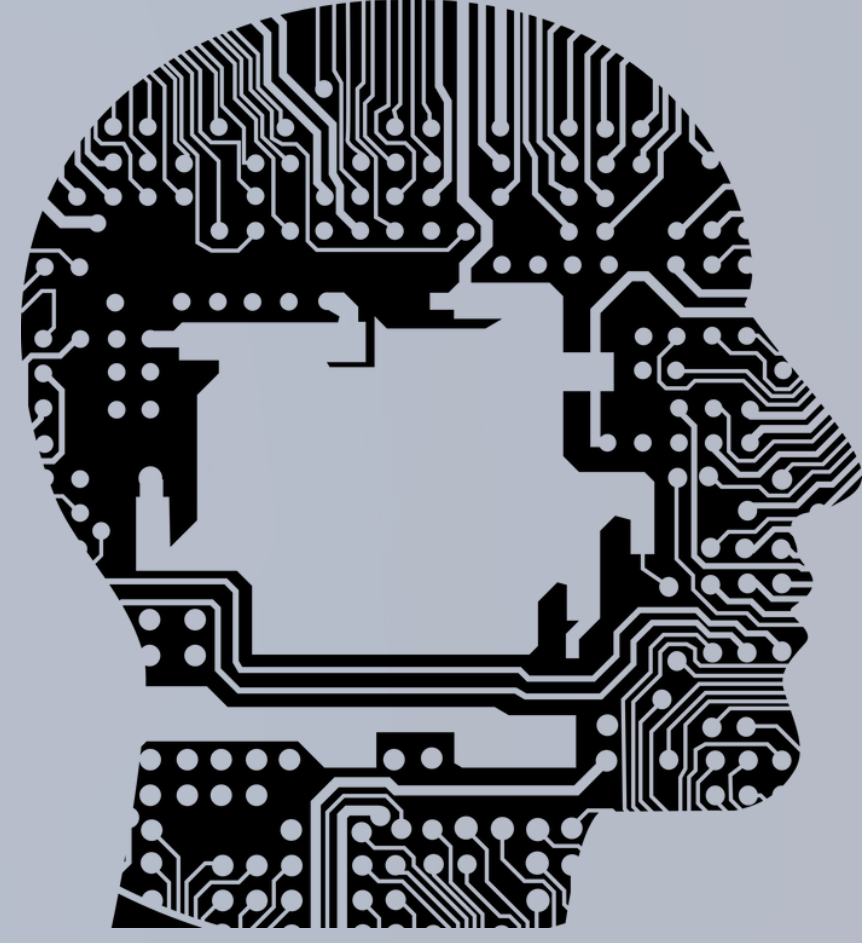
الموضوع

تحديات استخدام الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية على الرغم من الفوائد الكبيرة التي يقدمها الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، إلا أنه يواجه بعض التحديات، بما في ذلك: تكلفة التطوير والتنفيذ: قد تكون تكلفة تطوير وتنفيذ أنظمة الذكاء الاصطناعي للأمن السيبراني مرتفعة. الحاجة إلى بيانات ضخمة: تتطلب أنظمة الذكاء الاصطناعي كميات هائلة من البيانات لتدريبها وتحسين أدائها. نقص الكفاءات: هناك نقص في المتخصصين في مجال الذكاء الاصطناعي والأمن السيبراني. تطور أساليب الهجوم: يتطور مجرمو الإنترنت باستمرار ويطورون أساليب جديدة للهجوم، مما يتطلب تحديث وتطوير أنظمة الذكاء الاصطناعي بشكل مستمر.



الخاتمة

نصل معكم إلى نهاية بحثنا هذا الذي تناولنا فيه (موضوع البحث أو عنوان البحث)، حيث تطرقنا لعدد وافر من المعلومات الهامة والتفاصيل الفريدة المرتبطة بالموضوع، وقد ألقينا الضوء في مضموننا على (استخدام الذكاء الاصطناعي في كشف الجرائم السيبرانية)، وبالإضافة إلى ذلك، حيث ركزنا في هذا البحث على استعراض أبرز الحلول وا لتوصيات ا لمناسبة التي تم تحليلها وتقييمها بعناية لتمكين القارئ من اختيار ما يتلاءم مع احتياجاته وظروفه.



الفهرس

