



توظيف تقنيات التعلم العميق للكشف المبكر عن الهجمات السيبرانية وتحسين أمن الأنظمة الرقمية



الفصل الأول

مقدمة

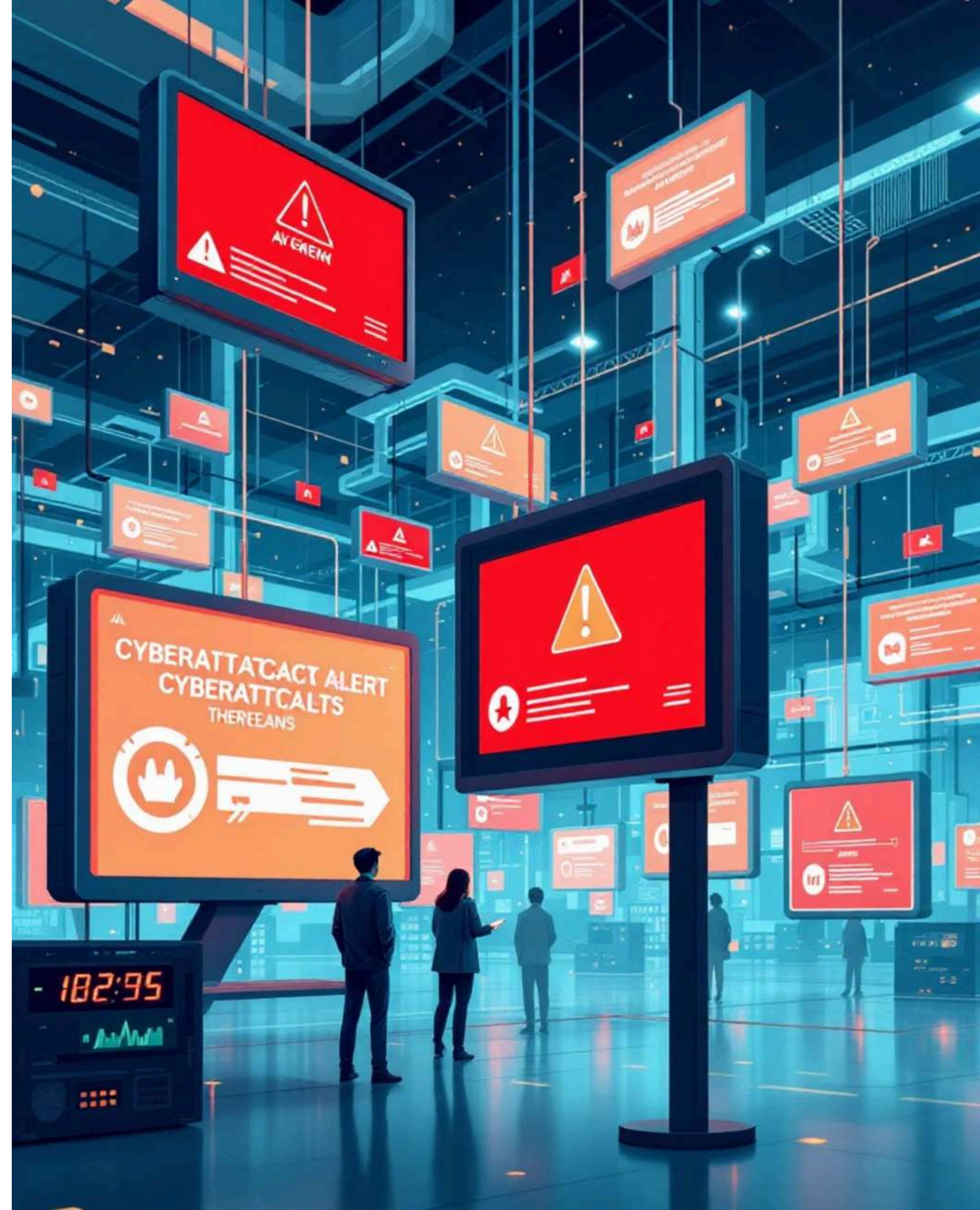
يشهد العالم تطورًا متسارعًا في التقنيات الرقمية، ومع هذا التطور تزداد الهجمات السيبرانية تعقيدًا وانتشارًا، مما يجعل الأنظمة التقليدية في كشف الهجمات أقل قدرة على المواجهة.

تسعى المؤسسات اليوم إلى تحسين قدراتها الأمنية باستخدام تقنيات الذكاء الاصطناعي والتعلم العميق، نظرًا لقدرتها على تحليل البيانات الضخمة والتعرف على الأنماط الشاذة بدقة عالية وفي وقت قصير.

مشكلة الدراسة

تعاني الأنظمة الأمنية التقليدية من صعوبة في الكشف المبكر عن الهجمات السيبرانية المتقدمة، خصوصًا تلك التي لا تعتمد على توقعات ثابتة.

هذا يؤدي إلى خسائر كبيرة مالية وتشغيلية. لذلك تظهر الحاجة إلى حلول ذكية قادرة على التنبؤ والكشف عن التهديدات قبل حدوثها.



أهداف الدراسة

تهدف هذه الدراسة إلى:

01

استكشاف دور تقنيات التعلم العميق

استكشاف دور تقنيات التعلم العميق في كشف الهجمات السيبرانية.

03

اقتراح نموذج أولي

اقتراح نموذج أولي يعتمد على الشبكات العصبية لاكتشاف الهجمات مبكرًا.

02

مقارنة الأداء

مقارنة أداء أنظمة الذكاء الاصطناعي مع الأنظمة التقليدية في الأمن السيبراني.

04

تحسين الدقة

تحسين مستوى الدقة وتقليل عدد الإنذارات الخاطئة.

أهمية الدراسة



وطنيًا

تدعم توجهات التحول الرقمي وحماية البنية التحتية الحيوية.



عمليًا

تساعد المؤسسات على تعزيز أنظمتها الدفاعية وتقليل المخاطر الأمنية.



علميًا

تساهم الدراسة في إثراء الأدبيات المرتبطة بتطبيق الذكاء الاصطناعي في الأمن السيبراني.

حدود الدراسة

1

تركز الدراسة على الهجمات الشبكية

تركز الدراسة على الهجمات الشبكية وليس جميع أنواع الهجمات السيبرانية.

2

الاعتماد على بيانات عامة

تعتمد الدراسة على بيانات تم جمعها من قواعد بيانات عامة.

3

مؤشرات تقييم محددة

يتم تقييم النموذج وفق مجموعة محددة من المؤشرات.



٦

مراجعة الأدبيات

أشارت العديد من الدراسات الحديثة إلى أن تقنيات التعلم العميق مثل **LSTM** و **CNN** أثبتت كفاءتها في كشف الهجمات خصوصًا **DDoS** و **Malware Detection**، مقارنة بأنظمة الكشف التقليدية.

وفي المقابل، ما زالت بعض التحديات قائمة مثل الحاجة إلى بيانات كبيرة، وزمن التدريب الطويل.

المنهجية المقترحة



بناء النموذج

بناء نموذج تعلم عميق (LSTM / CNN).



معالجة البيانات

معالجة البيانات وتنظيفها.



جمع البيانات

جمع بيانات هجمات سيبرانية من مصادر موثوقة (مثل KDD99 Dataset أو NSL-KDD).



التحليل

تحليل النتائج واستخلاص التوصيات.



المقارنة

مقارنة النتائج مع أنظمة الكشف التقليدية.



التدريب والاختبار

تدريب النموذج واختباره.

النتائج المتوقعة والجدول الزمني

النتائج المتوقعة

1. تحقيق دقة أعلى في الكشف مقارنة بالطرق التقليدية.
1. تقليل نسبة الإنذارات الكاذبة.
1. تحسين سرعة الاستجابة الأمنية.
1. تقديم نموذج يمكن تطويره وتطبيقه عمليًا.

الجدول الزمني

المدة	المرحلة
أسبوعان	جمع البيانات
أسبوع	معالجة البيانات
أسبوعان	بناء النموذج
أسبوعان	التجارب والتقييم
أسبوع	كتابة التقرير النهائي

التوصيات المستقبلية

1

تطوير النموذج

تطوير النموذج ليشمل أنواعًا متعددة من الهجمات.

2

توسيع قاعدة البيانات

توسيع قاعدة البيانات المستخدمة.

3

الدمج مع الأنظمة المتقدمة

دمج الذكاء الاصطناعي مع أنظمة أمنية متقدمة.

4

التعلم المستمر

استخدام التعلم المستمر لمواكبة التهديدات الجديدة.