

جامعة ميداو شن
كلية علوم الحاسوب

سد الفجوة بين الكشف التقليدي والاستجابة الذكية في الأمن السيبراني
البنكي

اسم الطالب: عبدالله الفيفي
اسم المادة: منهجية البحث في علوم الحاسوب
اسم المحاضر: د. محمد عنبر

جدول المحتويات

1. عنوان البحث
2. بيان المشكلة
3. أهداف البحث
4. المراجعة الأدبية
5. المراجع

1- عنوان البحث

تطوير إطار عمل هجين يعتمد على التعلم الآلي لتعزيز دقة كشف الاحتيال ورفع كفاءة مراكز العمليات الأمنية (SOC) في البنوك السعودية.

2- بيان المشكلة

بصفتي ممارساً في إدارة المشاريع التقنية ضمن بيئتي مركز عمليات الشبكة (NOC) ومركز العمليات الأمنية (SOC)، نلاحظ بشكل يومي اتساع الفجوة بين قدرات الأنظمة التقليدية وطبيعة التهديدات السيبرانية الحديثة. الواقع العملي يوضح أن الأنظمة القائمة على القواعد (Rule-based)، والتي لا تزال تشكل العمود الفقري في كثير من البيئات البنكية، لم تعد قادرة على مواكبة الأساليب المتغيرة والمتسارعة للاحتيال والهجمات. النتيجة المباشرة لذلك هي تضخم عدد الإنذارات الكاذبة، واستنزاف وقت وجهد المحللين في متابعة أحداث غير ذات قيمة، مقابل احتمالية تفويت تهديدات حقيقية أكثر تعقيداً.

تكمن المشكلة بشكل أوضح داخل بيئة الـ SOC ، حيث نتعامل مع تدفقات ضخمة من البيانات اللحظية التي تتطلب تحليلاً فورياً ودقيقاً. ذلك لأن الأنظمة التقليدية المعتمدة على التوقيعات المسبقة (Signature-based) تُظهر محدودية واضحة في قدرتها على التوسع أو التنبؤ بالهجمات الجديدة، خاصة تلك التي لا تترك أنماطاً معروفة مسبقاً. هذا القصور لا يؤثر فقط على كفاءة العمليات، بل يضعف من قدرتنا على تبني نهج أمني استباقي.

تزداد حساسية هذه الإشكالية في القطاع المالي السعودي، الذي أصبح هدفاً رئيسياً للهجمات المنظمة، خصوصاً مع التوجه المتسارع نحو المصرفية المفتوحة. في هذا السياق، أي تأخير في اكتشاف التهديدات أو الاستجابة لها قد يترتب عليه خسائر مالية كبيرة، بالإضافة إلى التأثير المباشر على ثقة العملاء، والذي يعد من أهم الأصول في المؤسسات المالية.

ومن واقع الممارسة، فإن الاعتماد الكبير على التدخل البشري والتحليل اليدوي لم يعد خياراً فعالاً في ظل هذا الحجم والتعقيد. العمليات الحالية تستهلك وقتاً طويلاً ولا توفر الدقة المطلوبة بشكل مستدام. لذلك، تبرز الحاجة إلى تبني نماذج تعلم آلي قادرة على التعلم المستمر من البيانات الحية، وتحليل الأنماط السلوكية بشكل ديناميكي، بما يساهم في تقليل الإنذارات الكاذبة، وتسريع زمن الاستجابة، ورفع جودة القرار الأمني، مع الالتزام بالمتطلبات التنظيمية الصارمة الصادرة عن البنك المركزي السعودي (SAMA).

3- أهداف البحث

الهدف العام من هذا البحث يتمثل في تصميم إطار عمل ذكي يدمج تقنيات التعلم الآلي ضمن سير العمل التشغيلي في مركزي عمليات (SOC/NOC)، بما يعزز القدرة على الاستجابة للتهديدات بشكل أكثر مرونة وفعالية، وينتقل بالمنظومة الأمنية من النمط التفاعلي إلى النمط الاستباقي.

وانطلاقاً من هذا الهدف، يمكن تفصيل الأهداف الإجرائية بشكل يعكس واقع الممارسة الميدانية على النحو التالي:

يتمثل **الهدف الأول** في تحليل نقاط الضعف في الأنظمة الأمنية الحالية داخل البيئة البنكية، مع التركيز على مدى اعتمادها على القواعد الثابتة وتأخرها في اكتشاف الأنماط الاحتمالية المعقدة والحديثة المبتكرة. هذا التحليل لا يقتصر على الجانب التقني فقط، بل يشمل أيضاً أثر هذه الأنظمة على كفاءة المحللين وحجم الإنذارات الكاذبة الناتجة عنها.

أما **الهدف الثاني** فهو تصميم نموذج تعلم آلي متقدم يركز على كشف الشذوذ (Anomaly Detection) في العمليات المالية اللحظية، بحيث يكون قادراً على التعلم من البيانات الحية والتكيف مع السلوكيات الجديدة، بدلاً من الاعتماد على التوقعات أو السيناريوهات المعرفة مسبقاً.

ويأتي **الهدف الثالث** في تقييم أداء النموذج المقترح بشكل عملي، من خلال مقارنته بالأنظمة التقليدية المستخدمة حالياً، وذلك من حيث سرعة اكتشاف التهديدات، ودقة النتائج، وانخفاض معدل الإنذارات غير الصحيحة، بما يعكس القيمة الفعلية للنموذج في بيئة العمل الحقيقية.

وأخيراً، يركز **الهدف الرابع** على تطوير خارطة طريق تقنية واضحة لدمج هذه النماذج الذكية ضمن البنية التحتية القائمة في مركزي العمليات (SOC/NOC)، مع مراعاة متطلبات التكامل، واستمرارية الأعمال، والامتثال للضوابط التنظيمية، بما في ذلك متطلبات البنك المركزي السعودي (SAMA)، لضمان إمكانية تطبيق الحل بشكل عملي ومستدام.

4- المراجعة الأدبية

من واقع الخبرة العملية، مدعومة بما ورد في الأدبيات الأكاديمية، يتضح أن التحدي في تبني تقنيات التعلم الآلي داخل البيانات الحساسة لا يقتصر على تحقيق دقة عالية في التنبؤ فقط، بل يمتد ليشمل مسألة "قابلية التفسير" (Explainability).

فالنماذج التي تعمل كـ "صناديق سوداء" قد تقدم نتائج دقيقة، لكنها تفتقر إلى الشفافية المطلوبة لاتخاذ قرارات تشغيلية أو تنظيمية حساسة. وفي هذا السياق، يشير (Reddy, 2022) إلى أن القطاعات الحيوية مثل القطاعين الطبي والمالي تحتاج إلى أنظمة ذكاء اصطناعي قادرة على تقديم مبررات واضحة ومنطقية لقراراتها، بما يدعم الثقة ويعزز الامتثال للمتطلبات التنظيمية.

من جانب آخر، تؤكد الدراسات الحديثة (Zhang & Lu, 2021) أن الانتقال من نموذج الأمن التفاعلي إلى الأمن الاستباقي لا يمكن تحقيقه بمعزل عن تكامل عميق بين خوارزميات التعلم العميق والبنية التحتية للشبكات. هذا التكامل يتطلب إعادة التفكير في كيفية تدفق البيانات، وآليات التحليل اللحظي، ودور الأنظمة الذكية داخل منظومة التشغيل اليومية.

وانطلاقاً من ذلك، يسعى هذا البحث إلى سد الفجوة بين الطرح الأكاديمي والتطبيق العملي، من خلال تقديم نموذج يجمع بين الكفاءة التقنية وقابلية التفسير، ويأخذ بعين الاعتبار متطلبات التشغيل الفعلي داخل بيئات الـ SOC والـ NOC. الهدف ليس فقط بناء نموذج دقيق، بل تقديم حل يمكن الوثوق به وتفسيره ودمجه بسلاسة ضمن الأنظمة القائمة، بما يحقق قيمة تشغيلية حقيقية ويتمشى مع الأسس التنظيمية المعتمدة.

5- المراجع

- Reddy, S. (2022). *Explainability and artificial intelligence in medicine and finance systems*.
- Zhang, C., & Lu, Y. (2021). *Study on artificial intelligence: The state of the art and future prospects*.
- Lazar, J., et al. (2017). *Research methods in human-computer interaction*.
- Goddard, W., & Melville, S. (2004). *Research methodology: An introduction*.