Developing a Hybrid Algorithm that Combine Rule-based and Machine Learning Methods to Detect Social Engineering Attacks

تطوير خوارزمية نظام هجين يجمع بين الأساليب القائمة على القواعد والتعلُّم الآلي لكشف هجمات الهندسة الاجتماعية

دانا نجيب لجامعة الافتراضية السورية

باسل الخطيب : وزارة التعليم العالي، الجامعة الافتراضية السورية، جامعة دمشق_سوريا.

عنوان التواصل: dana_najeeb_300318@svuonline.org – t_balkhatib@svuonline.org

تاريخ التسليم: ٢٠ تموز ٢٠٢٦ – **تاريخ القبول:** ١٥ تشرين الاول ٢٠٢٦

ABSTRACT

Social engineering is a science that utilizes social interaction to persuade an individual or organization to comply with an attacker's request via a computer-related entity. Recently, social engineering attacks have grown rapidly, exploiting human naivety to gain unauthorized access to systems and information. Many models have been developed to address this problem. The hybrid algorithm proposed in this study is based on automating most cases of the optimized model for manual detection of social engineering attacks, while applying a dynamic blacklist algorithm to verify each line of text generated by a potential attacker, matching with dynamic topic blacklist, and employing natural language processing and machine learning, the proposed hybrid system successfully automated the detection of social engineering attacks. This achieved substantial operational efficiency, demonstrating the efficacy of the proposed algorithm as a defensive tool. The dataset used consists of 50,000 emails, collected from the public repository (Kaggle), balanced samples were integrated into a unified test file to feed the proposed hybrid system and measure its security response. The accuracy reached 0.9740 despite ignoring other features, which is considered excellent.

Keywords: Cybersecurity, Social Engineering Attacks, Attack Detection Techniques, Machine Learning, Artificial Intelligence Technologies.

الملخص

الهندسة الاجتماعية علم يعتمد التفاعل الاجتماعي وسيلةً لإقناع فرد أو منظمة بالامتثال لطلب مهاجم عبر كيان مرتبط بالحاسوب. برزت هجمات الهندسة الاجتماعية مؤخراً كتهديد متزايد للأمن السيبراني. استغل المهاجمون نقاط الضعف البشرية للوصول غير المصرح به للأنظمة والمعلومات الحساسة. تم تطوير نماذج متعددة لمعالجة هذه المشكلة. خوارزمية النظام الهجين المقترحة في هذه الدراسة قائمة على أتمتة معظم حالات النموذج المُحسَّن للكشف اليدوي عن هجمات الهندسة الاجتماعية، وتطبيق خوارزمية القوائم السوداء الديناميكية بالمطابقة مع نص أنشأه مهاجم محتمل، وباستخدام معالجة اللغة الطبيعية والتعلم الآلي، تمكن النظام الهجين المقترح من اكتشاف هجمات الهندسة الاجتماعية آليا، وحقق كفاءة تشغيلية ملموسة أثبتت كفاءة الخوارزمية المقترحة كأداة دفاعية لكشف هجمات الهندسة الاجتماعية. مجموعة البيانات المستخدمة (50.000) رسالة بريد الكتروني. جُمعت من مستودعات (Kaggle) العامة. دمجت العينات المتوازنة بملف اختبار موحد مغذي للنظام الهجين المقترح لقياس استجابته الأمنية. بلغت الدقة 0.9740، وتُعتبر جيدة، بسبب الاكتفاء بالمقارنة النصية لنص البريد في هذا الاختبار.

الكلمات المفتاحية: الأمن السيبراني، هجمات الهندسة الاجتماعية، تقنيات الكشف عن الهجمات، التعلُّم الآلي، تقنيات الذكاء الاصطناعي.

CC BY

المقدمة

شهد القرن الحادي والعشرين اندماجاً كاملاً لتكنولوجيا المعلومات (IT) في بنية المجتمعات المعاصرة، وركيزة أساسية لإدارة القطاعات الحيوية الحكومية والمالية والصحة والتعليم والاتصالات وغيرها. هذا الاعتماد الرقمي الشامل فتح افاقاً جديدة للتهديدات السيبرانية، وحول التكنولوجيا نفسها الى أداة لإلحاق الضرر بالمؤسسات والأفراد. برز أمن المعلومات (IS) كخدمة استراتيجية لحماية البيانات أثناء حفظها واستخدامها ونقلها من التهديدات الداخلية والخارجية. ورغم التطور الهائل للتقنيات الدفاعية للبرمجيات وأجهزة مكافحة الثغرات الرقمية، الا أن المهاجمين وجدوا في العنصر البشري منفذاً أكثر فاعلية عبر ما يعرف بالهندسة الاجتماعية (SE) التي تعتمد استغلال الخطأ البشري، والتلاعب النفسي والثقة لخداع المستخدمين واستدراجهم لكشف بيانات حساسة (كلمات مرور، حسابات بنكية) وتسهيل اختراق الأنظمة المحظورة. تؤكد الإحصاءات خطورة هذا التهديد، وتشير التقارير الأمنية لعام 2026 الى دور العنصر البشري في أغلب خروقات البيانات العالمية، وتُستخدم تقنيات «القرصنة البشرية» بشكل شائع في الجرائم الإلكترونية لخداع المستخدمين لكشف معلومات محمية، أو نشر إصابات ببرامج ضارة، أو منح الوصول إلى أنظمة محظورة. هذه التقنيات تستغل عدم وعي الانسان ليؤدي عملاً يفتح ثغرة أمنية أو يفضي بمعلومات سرية. وقد تستخدم في عمليات احتيال عبر الإنترنت أو على أرض الواقع، وقد تمكّن المهندس الاجتماعي (المهاجم) من اختراق المباني أو الأنظمة أو الحسابات لتحقيق منافع معنوية أو مادية أو أمنية، دون الحاجة إلى مهارات تقنية عالية كما هي الحال في «الهاكرز» و«الكراكرز» الذين يتميزون بمهارات برمجية ومعرفة حاسوبية واسعة بالعتاد وأنظمة التشغيل والشبكات وثغراتها الأمنية. ما يحتاجه المهاجم هنا فقط مهارات اجتماعية ومهارات تسويق، لإقناع الضحية وأخذ ما يريده دون إثارة شبهات. نعرّف الهندسة الاجتماعية (SE) أنها تقنية يستخدمها المهاجمون للتلاعب بالأفراد لإفشاء معلومات حساسة أو القيام بأعمال يمكن أن تعرض أمن المؤسسة للخطر، ويعد الاحتيال الالكتروني (Phishing) التطبيق التقني الأكثر انتشاراً لها. تتزايد هجمات الهندسة الاجتماعية (SE) بسبب نقص المعلومات حول الموضوع [1]. هناك حاجة للمزيد من البحث في هذا القطاع لرفع مستوى الوعي بشأن هجمات الهندسة الاجتماعية (SE). أصبحت هجمات الهندسة الاجتماعية (SE) معقدة بشكل يصعب اكتشافه. يتم تطوير نماذج قائمة على القواعد (RBS) والتعلم الآلي (ML) والشبكات العصبونية الاصطناعية (ANN) ومعالجة اللغة الطبيعية (NLP) لمعالجة هذه المشكلة باستمرار، لكنها تغفل دور المستخدم. تهدف هذه المقالة البحثية الى تطوير خوارزمية نظام هجين يجمع بين الأساليب القائمة على القواعد (الذكاء الاصطناعي الرمزي) والتعلم الآلي والطريقة اليدوية لتمكين المستخدم، وكشف هجمات الهندسة الاجتماعية (SE). الشق الأول هو تطوير نموذج للكشف عن هجمات الهندسة الاجتماعية بالطريقة اليدوية الأقل تكلفة، معتمد على الإنسان، يمكن استخدامه لتعليم الناس كيفية حماية أنفسهم من بعض أنواع الهجمات. الشق الثاني الكشف بالطريقة الآلية الأكثر تكلفةً وتعقيداً، ومعتمد على النظام. وفي هذا السياق، يقترح البحث أسلوبًا يستخدم خوارزمية القوائم السوداء الديناميكية للموضوعات (Topic Blacklist–TBL) للتحقق من موضوعات النقاش لكل سطر من نص أنشأه مهاجم محتمل. وباستخدام تقنيات معالجة اللغة الطبيعية والتعلم الآلي، يمكن للنظام اكتشاف هجمات الهندسة الاجتماعية (SE) ألياً. النموذج الهجين المقترح مبني على أساس أتمتة أجزاء من خوارزمية الكشف اليدوي، للوصول الى تكامل معرفي يدمج اليات الكشف الالي ضمن حالات خوارزمية الكشف اليدوي.

الجدول1 قائمة الاختصارات

IT	Information Technology	تقنية المعلومات
IS	Information Security	أمن المعلومات
SE	Social Engineering	الهندسة الاجتماعية
ML	machine learning	التعلم الالي
AI	Artificial intelligence	الذكاء الاصطناعي
DL	Deep Learning	التعلم العميق
NLP	Natural Language Processing	معالجة اللغة الطبيعية
ANN	Artificial Neurons Networks	اشبكة العصبونية الاصطناعية
SEADM	Social Engineering Attacks Detection Model	نموذج كشف هجمات الهندسة الاجتماعية
TBL	Topic BlackList	القائمة السوداء الديناميكية للموضوعات
SAI	Symbolic AI	الذكاء الاصطناعي الرمزي
RBS	Rule- based systems	الأنظمة المعتمدة على القواعد
URL	Uniform Resource Locator	محدد موقع الموارد المحدد (رابط ويب)

الدراسات المرجعية

أُجريت العديد من الدراسات البحثية لتعزيز فاعلية تقنيات الكشف عن هجمات الهندسة الاجتماعية (SE)، ومنعها. ومع ذلك، لم تتمكن هذه الدراسات من القضاء على عيوب هذه التقنيات بالكامل. تم تصنيف أكثر الطرق شيوعاً للكشف عن هجمات الهندسة الاجتماعية (SE) إلى ثلاثة أنواع: اجتماعية، وتقنية، وهجينة (Hybrid) [2]. تعتمد الطرق الاجتماعية للكشف اليدوي على الإنسان لكشف الهجوم [3،4،5]، أما الطرق التقنية الآلية فتعتمد على النظام لكشف الهجوم باستخدام التقنيات وأدوات الذكاء الاصطناعي (AI). جميع استراتيجيات الكشف المستخدمة حاليًا هي خيارات قابلة للتطبيق لاكتشاف هجمات الهندسة الاجتماعية (SE) أو منعها. لكنها تحوي نقاط ضعف تستدعي التحديث بانتظام لمواكبة التغيرات السريعة. أيضا معظمها تعتمد على بنية تحتية مكلفة بدلاً من حلول موجهة للمستخدم (هدف الهجوم)، لذلك حتى الشركات التكنولوجية الضخمة التي تنفق الكثير على الأمن عرضة لهجمات الهندسة الاجتماعية (SE). ان اغفال دمج وعي المستخدم لتعزيز الطرق التقنية المتاحة هو الفجوة المعرفية التي تهدف هذه الدراسة لمعالجتها كحجر أساس للنموذج المقترح.

CC BY



الشكل رقم 1 تصنيف تقنيات الكشف عن هجمات الهندسة الاجتماعية (SE)

الجدول٢ تصنيف التقنيات المستخدمة في الكشف عن هجمات الهندسة الاجتماعية (SE)

التقنية أو النهج	الحلول	الإيجابيات والسلبيات	المراجع
النهج الاجتماعي	تثقيف وتدريب المستخدمين أثناء وبعد التوظيف على الأمن السيبراني ونقاط ضعفه	يُعتبر النهج الاجتماعي تدخلاً مُركّزاً على الإنسان. تُركّز حلول الكشف عن الاحتيال الإلكتروني المعتمد على الهندسة الاجتماعية (SE) والوقاية منه على آليات الحماية من تلاعبات المستخدمين بدلاً من التلاعب المباشر بالنظام. يُتيح النهج الاجتماعي للمستخدمين سبل حماية أنفسهم والعواقب المترتبة على عدم حمايتهم. على الرغم من دقة وفعالية هذه التقنية الاجتماعية، لا يزال المتسللون يجدون طريقهم للتلاعب بالمستخدمين نظرًا للطبيعة المتطورة لهجمات الاحتيال الالكتروني والحالة النفسية للمستخدم وقت الهجوم	[4،5،3]
التعلم الآلي	استخدام تقنيات الذكاء الاصطناعي (AI) (التعلم الآلي، الشبكات العصبية الاصطناعية (ANN)، التعلم العميق، معالجة اللغة الطبيعية، الشبكات العصبية التلافيفية، الغابة العشوائية)	يُعد هذا النهج الأكثر شيوعًا في الكشف الفني عن الاحتيال الإلكتروني المعتمد على الهندسة الاجتماعية (SE)، لمرونته واعتماده خوارزميات تصنيف البيانات. لا يُعد حلاً مثالياً لمكافحة هذه الهجمات، لأنه يغفل العامل البشري. تتراوح دقة هذه الخوارزميات بين 92% و99.68%. فالخوارزميات لا تستطيع محاكاة سلوك الإنسان بدقة تامة	[6,7,8]
قوائم الحظر Blacklist Whitelist Blocklist Phishtank	قاعدة بيانات حالات الاحتيال الالكتروني المبلغ عنها والكلمات والمواضيع الدالة على الهجوم	تشتهر هذه المواقع الإلكترونية بدقة معلوماتها عن حالات الاحتيال الإلكتروني المبلغ عنها، الا ان المشكلة تكمن في تشتت البيانات التي توفرها هذه المواقع. فمثلاً، قد يصنف أحد المواقع موقعاً ما على أنه موقع احتيالي، بينما لا يحتوي موقع آخر أي معلومات عنه. مما يصعب على المستخدم اكتشاف هذه المواقع الاحتيالية.	[9]
هيكلية/ محتوى الموقع الإلكتروني	تطابق المحتوى الموجود في صفحات الويب مع محتوى الصفحات الأخرى	يعمل تحليل محتوى المواقع الإلكترونية وطريقة مقارنة التشابه بشكل جيد في مكافحة عمليات الاحتيال التي تهدف الى تقليد صفحات الإنترنت. إلا أن هذه الطريقة قد لا تتمكن من اكتشاف عمليات الاحتيال الالكتروني التي تستخدم محتوى ونظام تصميم مشابهين لمواقع الإنترنت الأصلية.	[10,11]
تشابه عناوين (URL)	مقارنة عناوين (URL) للصفحات الإلكترونية المشبوهة بعناوين الصفحات الإلكترونية الموثوقة	يعمل هذا النهج بشكل جيد في مكافحة عمليات الاحتيال الإلكتروني التي تستخدم عناوين مواقع ويب مزيفة عبر تقليد عناوين المواقع الأصلية. إلا أن هذا النهج لا يُمكنه الكشف عن عمليات الاحتيال الالكتروني التي تستخدم عناوين فريدة وغير مكررة.	[12,13]
سجل عمليات الوصول إلى الموقع الالكتروني	تطابق عناوين (URL) لصفحات الويب مع سجل الوصول الذي يوفره الخادم.	هذا النهج عملي لمستخدمين على نفس الخادم الذي تم إنشاء سجل الوصول إليه. وليكون النظام فعالاً، يجب أن يتضمن سجل الوصول بيانات من جميع خوادم الويب.	[14,8]
متعدد المستويات	جمع المؤلفون بين اثنين أو أكثر من تدخلات النظام وبين تدخل المستخدم.	يبدو أن هذا النهج هو الأنسب للكشف عن عمليات الاحتيال الإلكتروني المعتمد على الهندسة الاجتماعية (SE)، يجمع بين التدخلات التقنية وتدخلات المستخدمين. الا أن التحدي يكمن في تحديد أفضل الاستراتيجيات لتحقيق أفضل النتائج	[2,15,16]
النهج الهجين Hybrid) (Approach	جمع المؤلفون بين نهجين أو أكثر	يعتمد هذا النهج دمج خوارزميتين أو أكثر من خوارزميات التعلم الآلي، بالإضافة إلى منهجية للحد من مخاطر الاحتيال الالكتروني، بهدف تعزيز دقة تصنيف الالكتروني. وتقتصر تلك الدراسات السابقة في هذا النهج على عمليات الاحتيال حلول تقنية صرفة دون دمج آليات تفاعلية لحماية وتوعية المستخدمين النهائيين.	[2,15,17]

يوضح الجدول 2 الدراسات الحديثة مصنفةً حسب الاجتماعية (SE)، والايجابيات والسلبيات المتعلقة بها. التقنيات المستخدمة في الكشف عن هجمات الهندسة

المواد والطرائق

تتمثل منهجية النظام المقترح الهجين من خلال دمج تقنية النهج الاجتماعي بخوارزمية القوائم السوداء الديناميكية للموضوعات (TBL) والتعلم الآلي لكشف هجمات الهندسة الاجتماعية (SE). بناءً على ذلك، تم تطوير خوارزمية النموذج المقترح المخصص للكشف اليدوي عن هجمات الهندسة الاجتماعية (SE) أولا، وبعد تحليل كافة العوامل السيكولوجية المتوفرة في الدراسات المرجعية. ولاختباره بشكل فعال، تم استخدام سيناريو بريد ذريعة (احتيال الكتروني) ثم استبيان موافق لأسئلة النموذج اليدوي التي تعتبر بوابات النموذج. في قسم آخر من الدراسة تم استعراض الإطار النظري لأنواع من هجمات الهندسة الاجتماعية (SE) والتقنيات المستندة للتعلم الآلي في كشفها (النهج التقني) والمتوفرة في الدراسات المرجعية. ثم تم الاستعانة ببرمجية مفتوحة المصدر على (GitHub) [18] وقاعدة بيانات متوازنة مكونة من (11.000) سطر من الروابط الخبيثة المتوفرة على (Data Mendeley) [19]، لدراسة وتحليل واختبار فاعلية التعلم الآلي [20] في اكتشاف أهم ميزات الروابط الاحتيالية (URL) المستخدمة في هجمات الاحتيال الالكتروني بالاعتماد على الذكاء الاصطناعي (AI). أيضا تمت دراسة فاعلية القوائم السوداء الديناميكية للموضوعات (TBL) لتعزيز أليات الفحص الذكي، كما تم تطوير أداة توعوية كنموذج أولي (prototype) لتوضيح فكرة القوائم السوداء الديناميكية للموضوعات (TBL) [21] ، وكيفية تفاعل المستخدم مع القوائم بالإضافة والحذف عبر تطبيق جافا سكريبت كواجهة تفاعلية حية. في النهاية تم استخدام مجموعة بيانات ضخمة متوازنة من نصوص البريد الالكتروني [24]، لتدريب نموذج التعلم الآلي. وأخيرا تم الحصول على نموذج هجين يجمع بين خوارزمية القوائم السوداء الديناميكية للموضوعات (TBL) القابلة لتدخل المستخدم مع خوارزميات التعلم الآلي لكشف رسائل الاحتيال الالكتروني، وتجربة النموذج الهجين المقترح على تطبيق بايثون سحابي [22].

خوارزمية النموذج المقترح المخصص للكشف اليدوي عن هجمات الهندسة الاجتماعية (SE)

يهتم النموذج المقترح بتعديل الإصدار الأول والثاني لخوارزمية (SEADM)، ويستخدم من قبل الأفراد لتثقيف أنفسهم حول أساليب الخداع والهجوم. يعتمد النموذج المقترح على القواعد (RBS) والمحاكمة المنطقية لبعض المعايير كالاستعجال، الخوف والفضول، وإضافة بعض القواعد كالثقة والصلاحيات، المعاملة بالمثل، الالحاح، والتحيز في الإدراك، بهدف رفع وعي المستخدم لكشف هجمات الهندسة الاجتماعية (SE). يساعد النموذج المحسن المقترح الأفراد في طرح أسئلة تقييم ذاتية لحماية أنفسهم من أنواع مختلفة من هجمات الهندسة الاجتماعية (SE). يعتمد النموذج المقترح شجرة قرار متعددة المستويات لتكون عملية اتخاذ القرار أكثر مرونة وقابلية للإدارة. يعرض النموذج تدفق الإجراءات وكيف يجب على «المستلم» التعامل مع أشكال الطلب الواردة. تم تصميم حالات النموذج للوصول إلى إحدى الحالتين الرئيسيتين، إيقاف الطلب (SF) أو تنفيذ الطلب (SS). يعزى هذا الاختزال الاجرائي للمخرجات لغرض الدراسة واعتبار الرسائل المؤجلة مدخلات جديدة، تعود الى بداية شجرة القرار للتحقق، ليكون المخرج الحتمي النهائي ثنائي التصنيف ينحصر في الإيقاف التام او التنفيذ الامن.

–الحالة SF: أوقف الطلب: هذا هو شرط النتيجة السلبية (اكتشاف هجوم هندسة اجتماعية (SE)).

–الحالة SS: تنفيذ الطلب: هذه هي حالة النتيجة الإيجابية للنموذج (لا يعتبر هجوما).

–الحالة S1: فهم الطلب: تقوم هذه الحالة بتقييم ما إذا كان مستلم الطلب يفهم الطلب تمامًا.

–الحالة S2: طلب معلومات لفهم الطلب أكثر.

–الحالة S3: هل يحاول مقدم الطلب خلق شعور بالإلحاح؟

–الحالة S4: هل يمكن للمستلم أن يبطئ الطلب ويتأكد من شرعيته؟

–الحالة S5: هل يحث مقدم الطلب على فتح مرفق أو النقر فوق رابط ويب (URL)؟

–الحالة S6: هل يستطيع المستلم التحقق من المرفق أو رابط الويب (URL) قبل النقر عليه؟

–الحالة S7: هل الطلب وصل بشكل غير متوقع أو يجيب على سؤال لم يطرح ويطلب معلومات شخصية؟

–الحالة S8: هل يتمتع المستلم بسلطة تنفيذ الطلب؟

–الحالة S9: هل الإجراء أو المعلومات المطلوبة متاحة للعامة؟

–الحالة S10: هل يمكن التحقق من هوية مقدم الطلب؟

–الحالة S11: هل يتمتع مقدم الطلب بالسلطة اللازمة لطلب الإجراء أو المعلومات؟

تتكامل هذه الحالات (S1–S11) لتشكل معاً بناءً منهجياً ينقسم لأربع بوابات أمنية تتوزع على مستويات خدمة استراتيجية الدفاع العميق (Defense–in–Depth):

–المستوى الادراكي: تقييم وضوح الطلب الوارد ويشمل الحالات S1, S2)).

–المستوى النفسي السلوكي: رصد الضغوط السيكولوجية ويشمل الحالات S3, S4)).

–المستوى الفني (التقني): كشف المؤشرات التقنية كالروابط والمرفقات الخبيثة ويشمل الحالات S5, S6,S7)).

–المستوى الإداري التنظيمي: يفحص صلاحيات وهوية مقدم الطلب وشرعية تداول البيانات مؤسساتياً ويشمل الحالات S8,S9,S10,S11)).

يفيد التقسيم المنهجي في تتبع السلوك الأمني لتحديد المستوى الأمني الذي تم رصد هجوم هندسة اجتماعية (SE) فيه أو فشل اكتشافه. بناءً على تحليل البيانات وتوصيات خبراء الهندسة الاجتماعية (SE)، تم تطوير الإرشادات المنهجية التالية:

القاعدة 1: كن حذرًا إذا طلب مقدم الطلب معلومات حساسة –كمعلوماتك الشخصية أو بيانات غير عامة.

–القاعدة 2: كن متشككًا إذا حاول مقدم الطلب خلق شعور إلحاح، كالتهديد بتجميد حسابك إذا أهملت المعلومات.

–القاعدة 3: كن حذرًا إذا حثك مقدم الطلب على فتح مرفق أو النقر على رابط (URL) بدافع الخوف أو الفضول.

–القاعدة 4: كن حذرًا إذا كان مقدم الطلب يستخدم اسمًا أو عنوان بريد إلكتروني مزيف.

–القاعدة 5: كن حذرًا إذا هددك مقدم الطلب أو حاول تخويفك.

المجتمع والعينة وأدوات جمع البيانات

محاكاة الاحتيال الالكتروني (Phishing Simulation) هي تقنية تدريب لاختبار قدرة الناس وجاهزيتهم للتعرف على هجمات الاحتيال الالكتروني والإبلاغ عنها، وتعد وسيلة فعالة لتحسين الوعي الأمني وتقليل مخاطر هجمات الاحتيال الالكتروني. تم استخدام سيناريو بريد الذريعة كأحد أمثلة الهجمات الواقعية للاحتيال الالكتروني، والذي قد يمثل هجوم هندسة اجتماعية أو مجرد رسالة الكترونية حقيقية. في هذه الدراسة تتمثل الذريعة بدعوة الطلاب للمشاركة بندوة علمية ونشر أبحاث حول دراستهم وتحفزهم بأن المشاركة سترفع درجتهم النهائية. بعد موافقة مدير برنامج الدراسات العليا في علوم الويب/ الجامعة الافتراضية السورية، ودكتور مادة أمن المعلومات/ الجامعة الدولية الخاصة، تم ارسال النص التالي عبر بريد الكتروني صمم خصيصاً للهدف البحثي باسم مشابه لبريد الجامعة الافتراضية السورية الالكتروني (svu.symp.adm@gmail.com)، ليوحي

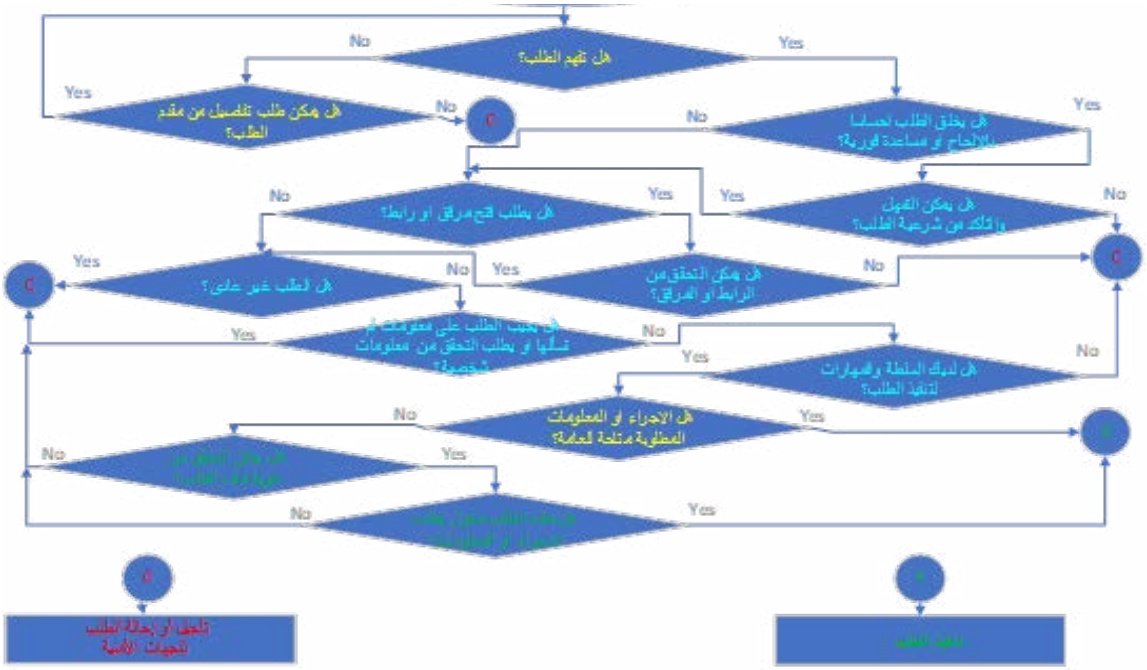
CC BY

the Use of Artificial Intelligence Technologies
- Cybersecurity
- Social Engineering
- Cloud Computing: Containers and Virtual Servers
- Sub-solutions for AI Technologies in Web Applications
- Data Storage, Sharing, and Retrieval and Big Data Processing on the Web
- Other topics.

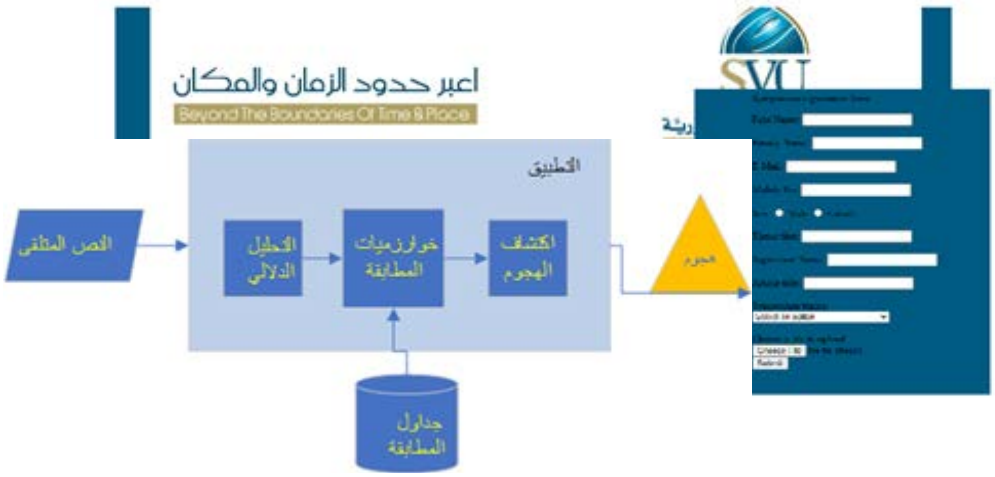
To register, please fill out the student's information and the research to be submitted via the following link: (www.svu-srf.kesug.com) username: admin password: 1234

للمستلم أنه من الجهة الناظمة للندوة العلمية. بالطبع الهدف إحصاء عدد الطلاب الذين استخدموا رابط الويب (URL) للولوج الى الموقع الوهمي البسيط والذي لا يحوي أي نوع من أنواع الهجمات اطلاقاً [23]، ولا يحتفظ بأي معلومة يتم إدخالها من قبل المشاركين. نص رسالة بريد الذريعة:

We invite you to participate in the Scientific Symposium on various topics in web science, scheduled to be held at the Syrian Virtual University on Thursday, December 18 2025 Participating research and articles should reflect summaries or the current portion of each student's research, based on the specific thesis topic. The symposium will cover the following topics:
- Web Application Development and



الشكل رقم 2: الخوارزمية المقترحة للكشف اليدوي عن هجمات الهندسة الاجتماعية (SE)



الشكل رقم 3: صفحة الرابط المرفق

خوارزميات القوائم السوداء الديناميكية للموضوعات (TBL–Top–ic–blacklists)

تنتمي هذه الخوارزميات الى النهج التقني لكشف الاحتيال الالكتروني المعتمد على الهندسة الاجتماعية (SE)، يستخدم النموذج الهجين المقترح الخوارزميات التقنية التالية للكشف عن الهجوم:

خوارزمية الكشف عن الهندسة الاجتماعية (SE) بالاعتماد على (TBL)

حلقة خارجية تمسح كل سطر في نص أرسله مهاجم محتمل (TEXT)، تتكرر الحلقة الداخلية خلال كل إدخال (n في TBL). يستدعي السطر 3 خوارزمية تحدد إذا كان موضوع الإدخال (n) موجودًا في السطر الأول. عند المطابقة يتم اكتشاف هجوم وعرض رسالة تحذير.

1. For each l Є TEXT.
2. For each n Є TBL.
3. If Match Topic (l,n).
4. ATTACK_DETECTED.

خوارزمية تطابق الموضوع بالاعتماد على (TBL)

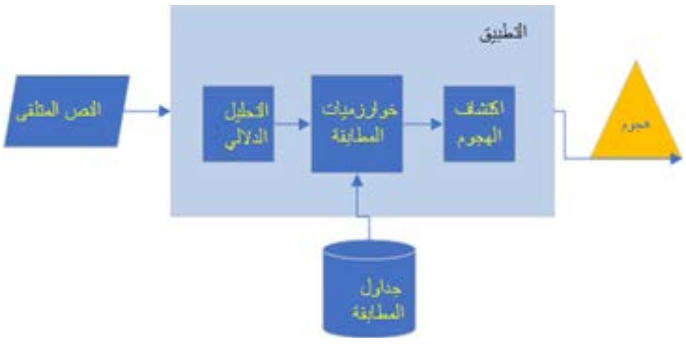
الغرض من الحلقة الخارجية (السطر 1) هو فحص كل رمز مميز في السطر ومقارنته بـ (n.action)، الفعل المرتبط بإدخال (n في TBL) . يتم إجراء المقارنة مع (n.action) في (السطر 2) . إذا تم العثور على الفعل، فسيتم الدخول للحلقة الداخلية (السطر 3) لمسح الرموز المميزة المتبقية على السطر ومقارنتها بـ (n.resource)، المورد الموافق. إذا تم العثور على كل من الفعل والمورد، فسترجع الدالة (TRUE) في (السطر 5). تقوم دالة المقارنة التي يتم استدعاؤها في (السطرين 2 و4) بإجراء مقارنة سلسلة، ولكنها تقارن أيضًا الوسيطة الأولى بأي مرادفات للوسيطة الثانية

1. For i = 0 to | token in l |
2. If Compare (l[i], n.action).
3. For j = I + 1 to |token in l|.
4. If Compare (l[j], n.resource).
5. Return TRUE.
6. Return FALSE.

يتفاعل المستخدم مع القوائم السوداء الديناميكية (TBL) المضمنة داخل نظامه بالإضافة والحذف، مما يزيد مناعة نظامه ويرفع وعيه ومسؤوليته الرقمية. القوائم المقترحة محلياً ضمن (TBL) هي جداول من أفعال ومصادر تنتمي دلالياً وسياقيا الى عوامل الخوارزمية الهجينة المقترحة بعد الاستفادة من خوارزمية (SEADM) الإصدار الأول والثاني، واضافة عوامل أخرى تؤشر الى هجمات بالهندسة الاجتماعية (SE)، كالاستعجال وطلب المال وتجاوز الصلاحيات وانتحال السلطة وغيرها. تقترح الدراسة دمج مجموعة من خوارزميات معالجة اللغة الطبيعية (NLP) لتقطيع النص الى أسطر ثم الى كلمات، ثم التنظيف والتجذير، وخوارزمية مطابقة الكلمات مع القوائم السوداء الديناميكية للموضوعات (TBL)، ثم إطلاق التحذيرات الملائمة في الوقت الفعلي، بالطبع الفكرة مرنة قابلة للتطبيق على مختلف نواقل الهجوم (اتصال احادي او غير مباشر كنص بريد الكتروني، أو ثنائي الاتجاه كالدردشات). تستخدم عادةً برامج جدر الحماية (Firewall) وأيضاً مصفاة البريد الالكتروني الأمن (Email Filter) وغيرها، جميعها تستخدم خوارزمية القوائم السوداء الديناميكية للموضوعات (TBL) يتم تحديثها باستمرار بالمواقع والخوادم والروابط الخبيثة وبصمات الملفات المكتشفة دوريا وغيرها الكثير، مثل قواعد بيانات ارقام الهواتف الاحتيالية. تبنى هذه القوائم والمكتبات وتتحدث باستمرار من قبل أهم شركات الأمن السيبراني في العالم، مثالها (Phish Tank, Open Phish , Virus Total). يقوم النظام الهجين المقترح على أتمتة أغلب حالات النموذج المحسن للكشف اليدوي (الاجتماعي) عن الهجمات بالهندسة الاجتماعية (SE)، عبر المطابقة مع القوائم السوداء الديناميكية للموضوعات (TBL) المنتمية دلالياً الى حالات النموذج المحسن للكشف اليدوي (الاجتماعي)، بالطبع يمكن تحميل قوائم سوداء ديناميكية للموضوعات (TBL) ومكتبات محلياً ومجاناً داخل النظام البرمجي. أو التواصل مع خوادم الفحص السحابية العالمية، أو استعمال تقنية (Bloom Filter). يمكن استخدام بعض أو جميع ما ذكر بحسب أهمية المؤسسة، مع مراعاة خصوصية وسرية وفيدرالية البيانات، والأخذ بعين الاعتبار أن الامن مقدم على التأخير. برمجياً كل هذا متاح ليخدم الهدف البحثي للدراسة الحالية. تم تصميم تطبيق جافا سكريبت أولي كمنصة تفاعلية لشرح الفكرة.

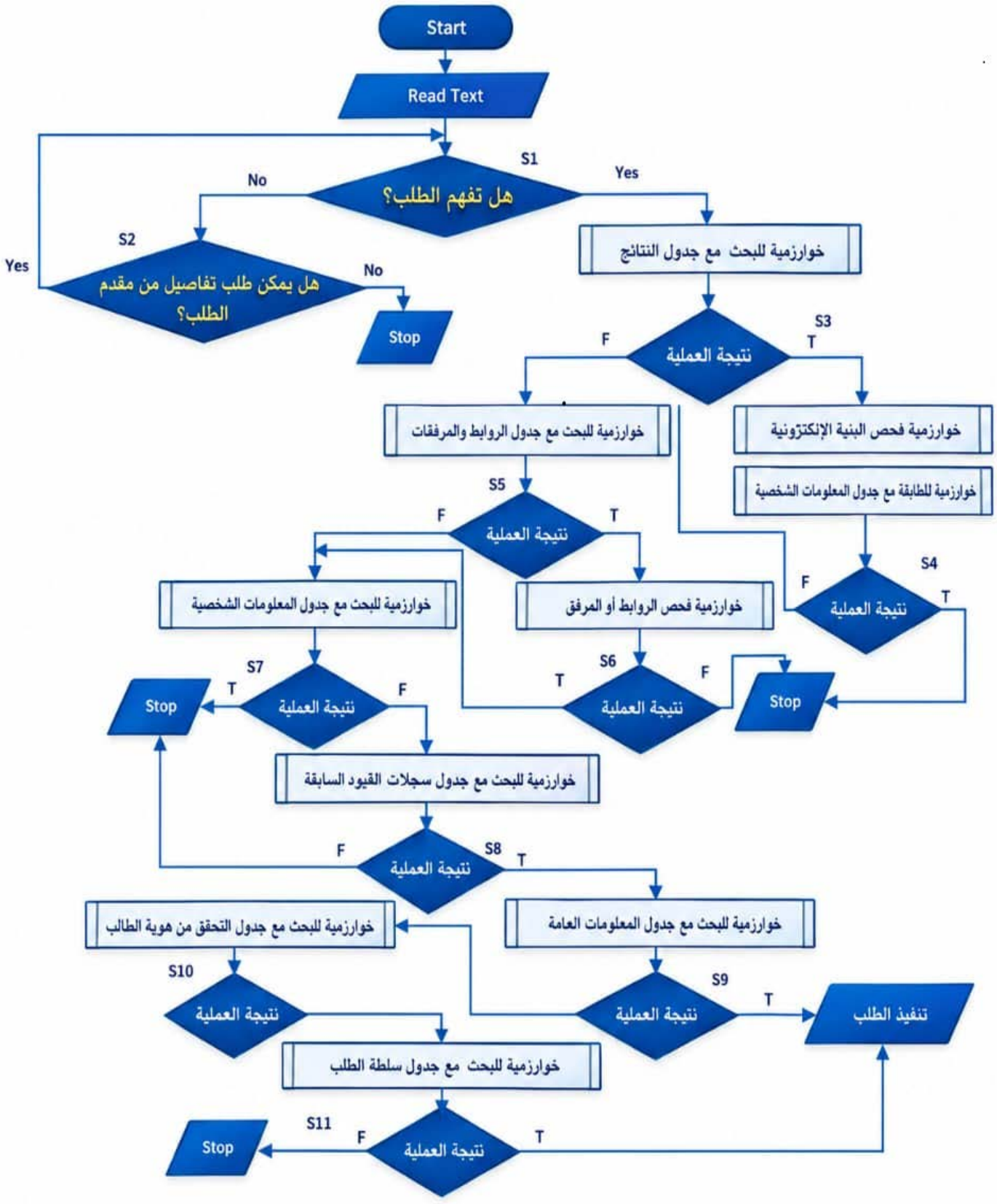
النظام الهجين المقترح

تعتمد الأنظمة المعتمدةعلى القواعد (RBS) والذكاء الاصطناعي الرمزي (SAI) على مجموعة قواعد محددة مسبقًا لتحديد هجمات الهندسة الاجتماعية (SE). تستند هذه القواعد إلى أنماط الهجوم والسلوكيات المعروفة. وتعتمد حظر تلقائي مؤقت لكلمات ومواضيع معينة في الوقت الفعلي، بناءً على سياق الأحداث أو سلوك المستخدمين. من خلال هذا المنحى، يقترح البحث نموذجاً قائماً على القواعد والتعلم الآلي ومعالجة اللغة الطبيعية، محسن ومخصص وقائم على المحاكمة المنطقية لبعض القواعد والمعايير مثل: قلة الوعي، الاستعجال، الثقة، الخوف والفضول، وتعديل خوارزمية(SEADM) بإضافة بعض القواعد عليها، كالثقة والصلاحيات، المعاملة بالمثل والالحاح، التحيز في الإدراك، بهدف رفع وعي المستخدم لكشف هجمات الهندسة الاجتماعية (SE). يقوم النظام الهجين المقترح بتطبيق خوارزمية القوائم السوداء الديناميكية للموضوعات (TBL) للمطابقة مع جداول الحظر، حسب الحالة في النموذج اليدوي، حيث تمثل كل حالة (جدول) قائمة موضوعات مستقلة ضمن (TBL)، للتحقق من موضوعات المناقشة لكل سطر من نص أنشأه مهاجم محتمل، واستخدام معالجة اللغة الطبيعية والتعلم الآلي، لاكتشاف هجمات الهندسة الاجتماعية (SE) آليا. يقترح البحث طريقة لاكتشاف هجمات الهندسة الاجتماعية (SE) عبر إجراء تحليل دلالي لجميع النصوص المرسلة إلى الضحية لتخمين المواضيع والكلمات المحظورة التي تتم مناقشتها في كل سطر ومقارنتها مع الكلمات المخزنة في القوائم حسب الحالة. ثم التحقق والتأكد من المعالجة والإجابة الآلية لاتخاذ القرار المناسب والانتقال للحالة التالية حسب الخوارزمية الهجينة المقترحة، إذا تم اكتشاف هجوم، فسيتم إنشاء رسالة تحذير للضحية.



الشكل رقم 4: المخطط العام لنظام الكشف الهجين المقترح

خوارزمية النظام الهجين المقترحة



جداول الحالات

تبنى الجداول الديناميكية على أهداف هجوم الهندسة الاجتماعية (SE) الشائعة. وترتبط كل كلمة جذر في بمجموعة مرادفات.

الجدول 3 القائمة السوداء للموضوع	
الفعل (الطلب)	الموارد
إرسال	الأموال
إرسال	البيانات الحساسة
اتصل	بالرقم
زيارة	الموقع

الجدول 4 الإلحاح	
#	الكلمات الدالة على الالحاح
1	فورا
2	عاجل
3	سريع
4	التصرف الآن
5	موعد نهائي
6	حد زمني
7	مدة محددة

الجدول 5 الأفعال المرتبطة بالإلحاح	
الموارد	الفعل (الطلب)
الحساب	تجميد
الحساب	تعطيل
الحساب	إيقاف
انذار	توجيه
الخدمات	انهاء
الراتب	خصم
الترقية	تأخير

الجدول ٦ المعلومات الشخصية	
#	الكلمات الدالة على المعلومات الشخصية
1	كلمة المرور
2	رقم بطاقة الائتمان
3	عنوان السكن
4	عدد افراد الأسرة
5	مدارس الأولاد
6	الراتب الشهري
7	الحالة الاجتماعية
8	البريد الالكتروني الشخصي
9	الحساب البنكي
10	الجنس

الجدول 7الروابط والمرفقات (URL)	
الفعل (الطلب)	الموارد
افتح	المرفق
افتح	الملف
افتح	الرابط
افتح	صفحة الويب
انقر	الرابط
حمل	المرفق
نزل	المرفق
انتقل	للصفحة
أملئ	الاستبيان
أملئ	النموذج

الجدول8 صلاحيات التنفيذ (للمستلم)	
رقم الموظف	
المنشور على العام S9	
الاذن ١	
الاذن ٢	

الجدول 9 المعلومات المتاحة للعامة	
يشمل هذا الجدول قائمة عناوين المواضيع والمعلومات المتاحة للعامة، والفقرات المنشورة على الموقع الالكتروني للمؤسسة.	
#	البند
١	من نحن
٢	اهدافنا
٣	رؤيتنا
٤	مشاريعنا
٥	منتجاتنا
٦	عروضنا
٧	الاتصال بنا

الجدول ١٠ التحقق من هوية مقدم الطلب	
الرقم	
الاسم	
الهاتف	
البريد الالكتروني	
صورة الهوية	

الجدول ١١ سلطات مقدم الطلب	
الرقم	
سلطة مستوى ١	
سلطة مستوى ٢	
سلطة مستوى ٣	

CC BY

لتقييم خوارزمية الكشف اليدوي المقترحة في القسم 3.1. تم ارسال بريد الذريعة لعدد 140 طالب، 60 طالب منهم ماجستير علوم الويب في الجامعة الافتراضية السورية. تم جذب 25 ضحية من أصل 60 طالب، أي بنسبة بلغت 41,67 % من اجمالي عينة المجموعة الأولى، وعند ارسال الرسالة الى عدد 80 طالب سنة رابعة وخامسة هندسة معلوماتية / الجامعة الدولية الخاصة، تم جذب 50 ضحية أي بنسبة بلغت 62.50 % من اجمالي عينة المجموعة الثانية، مما يؤكد زيادة احتمال نجاح الهجوم وجذب ضحايا أكثر في مجتمعات أقل خبرةً في حال تغيير نص الذريعة ليناسب مجتمعات متنوعة بحسب اهتماماتها، ويثبت مرونة ناقل الهجوم حيث لا يقتصر بالضرورة على رسائل البريد الإلكتروني، بل يمتد ليشمل النصوص المنشورة على منصات التواصل الاجتماعي المختلفة. لاحقاً، تم اجراء استبيان لمعرفة مدى استفادة الطلاب من التجربة البحثية، ولمعرفة في أي مرحلة من حالات النموذج تبين للمستلم انه كان بريداً وهمياً، حيث أن أسئلة الاستبيان تمثل الحالات المنهجية للنموذج المقترح (S1–S11). لدينا 75 حالة هجوم محتمل في العالم الحقيقي بين مجموعة من الاختصاصيين. النتيجة المرجوة من هذا الاختبار هي توجيه المستلمين لاتخاذ قرار إيقاف الطلب (SF) لجميع الحالات الخمس والسبعين، مما يرفع الوعي الأمني للمستلم لاتخاذ القرار المناسب. يعرض الجدول التالي أسئلة الاستبيان:

الجدول 12 أسئلة الاستبيان

رقم القاعدة	القاعدة	الطلب المؤجل		تنفيذ الطلب
		نعم	لا	
S1	هل تفهم ما هو المطلوب؟	66	9	لا
S2	هل يمكن طلب تقديم تفاصيل أكثر عن الطلب من مقدم الطلب؟	57	18	
S3	هل يحاول مقدم الطلب خلق شعور إلحاح؟	29	46	
S4	هل يمكن للمستلم أن يبطئ ويتأكد من شرعية الطلب؟	58	17	
S5	هل يحثك مقدم الطلب على فتح مرفق أو النقر على رابط (URL)؟	42	33	
S6	هل تستطيع التحقق من المرفق أو الرابط (URL) قبل الضغط عليه؟	53	22	
S7	هل الطلب غير عادي ووصل بشكل غير متوقع أو يجيب على سؤال لم يطرح ويطلب معلومات شخصية؟	26	49	
S8	هل لدى المستلم صلاحية تنفيذ الطلب؟	53	22	
S9	هل الإجراء أو المعلومات المطلوبة متاحة للعامة؟	41	34	
S10	هل يمكن التحقق من هوية مقدم الطالب؟	50	25	
S11	هل يمتلك مقدم الطلب السلطة اللازمة لطلب الإجراء أو المعلومات؟	42	33	

المناقشة

نجح تسلسل أسئلة الاستبيان في تصفية المخاطر تدريجياً، ورفع مستوى وعي المشاركين لرفض الطلب في النهاية، لأن الأسئلة مصممة بالفعل لتثير الشك بوجود ثغرات قد تؤدي لهجوم حقيقي. سلط النموذج الضوء على سلوكيات التلاعب السيكولوجي بالمستخدمين بدلاً من التلاعب بالنظام، ورفع وعي المستخدمين بدلاً من التركيز التقليدي على التقنيات والأجهزة المكلفة. وبناءً عليه يمكننا استخدام النموذج السلوكي المحسن المقترح للدفاع ضد هجمات الهندسة الاجتماعية (SE) كأداة لرفع وعي المستخدمين، ورفع أداء التقنيات السيبرانية لمواجهة الهجمات. ان القيمة الابتكارية المضافة تكمن في دمج النهج السلوكي مع خوارزمية القوائم السوداء الديناميكية للموضوعات (TBL) والتعلم الالي (ML) كفكرة رائدة لإشراك وعي المستخدم في رفع كفاءة التقنيات لمواجهة الهجمات، تنجح هذه البنية الهجينة في سد الفجوة البحثية، حيث اكتفت الدراسات السابقة بالحل التقني او دمج مجموعة تقنيات أو دراسة نظرية للعوامل الاجتماعية والسيكولوجية المسببة للهجوم دون حلول إجرائية. لاختبار الكفاءة الإجرائية وصحة المنطق البرمجي صمم تطبيق جافا سكريبت يحاكي ألية الكشف باستخدام خوارزمية القوائم السوداء الديناميكية للموضوعات (TBL) الممثلة للأنظمة المعتمدة على القواعد (RBS) والذكاء الاصطناعي الرمزي (SAI). تتسم بنية النموذج الهجين المقترح بقدرتها الاستيعابية على دمج خوارزميات التعلم الآلي (ML)، لمعالجة المشكلة على نطاق أوسع، ومرونتها التصميمية البرمجية. لذلك، تم بناء مجموعة بيانات متوازنة مؤلفة من (50.000) رسالة بريد الكتروني مرمزة ثنائياً (0) رسالة شرعية، (1) رسالة احتيال الكتروني. تم توزيعها مناصفةً (50:50) لضمان توازن البيانات. جُمعت عينات مجموعة البيانات الكلية (Dataset) من المستودعات القياسية العامة كالتالي: (25.000) رسالة بريد إلكتروني شرعية من بيانات شركة إنرون القياسية Enron (Email Corpus) وهي أشهر قاعدة بيانات عالمية تحوي مئات الألاف من رسائل البريد الالكتروني الحقيقية، و(25.000) رسالة احتيال الكتروني من بيانات نازاريو القياسيةNazario Phishing) (Corpus التي تحوي مئات ألاف رسائل الهندسة الاجتماعية (SE) الحقيقية التي استهدفت الضحايا بأساليب الخداع النفسي، والروابط الخبيثة وطلب البيانات. دمجت العينات وتم اكمال النقص بتوازن من (Spam Assassin Public Corpus) وعينات (Kaggle) العامة لتكوين ملف بيانات موحد ومغذٍ للتطبيق البرمجي المطور، لقياس استجابته الأمنية. وبعد اجراء المعالجة اللغوية للنصوص كتجريد الرموز وتوحيد حالات الأحرف، تم تطبيق تقنيةTF–IDF) (Vectorizerلاستخلاص الميزات النصية مع وضع قيود معيارية على أقصى حجم للميزات لمنع ظواهر الافراط في التخصيص (overfitting) والتسريب المعرفي وفرط التدريب، قُسّمت مجموعة البيانات الاجمالية عشوائياً بنسبة 80% (40,000 رسالة) لغرض التدريب و20% (10,000 رسالة) المتبقية لغرض الاختبار، وتم اخضاع خوارزميات التصنيف المتنافسة للتحليل المعمق عبر مصفوفة الارتباك (confusion matrices) الخاصة بمجموعة الاختبار المعزولة والبالغة (10,000) رسالة. تعتمد الخوارزمية المقترحة آلية تكامل هجين، أولاً، تتم مقاطعة الكلمات(Tokens)

CC BY

عبر استعلامات مباشرة مع الجدول المعرفية الديناميكية (الفحص القائم على القواعد (RBS–Matching)) لرصد أفعال الطلب ومواردها ومرادفاتها المرتبطة بالإلحاح أو المعلومات الشخصية والروابط الحساسة ، التي تشير مباشرةً الى هجوم هندسة اجتماعية، حيث تستخلص هذه الميزات بشكل مستقل لكل رسالة لتجنب تسرب البيانات (Data Leakage) . ثانياً، تشغيل مصفوفة التردد العكسي لاستخلاص الأوزان الإحصائية للكلمات والأنماط الدلالية للرسالة. تُربط مخرجات المسارين معاً عبر الية التكديس الافقي لتوليد متجه ميزات هجين(Hybrid Feature Vector) ، ليغذي هذا المتجه الهجين المتكامل خوارزميات التعلم الآلي الكلاسيكي المقارنة، حيث يتم تدريبها واختبار كفاءتها على المجموعات المعزولة مسبقاً لضمان دقة التقييم وقدرة النماذج على التعميم. يوضح الجدول13 أداء أبرز الخوارزميات في حالتي التدريب والاختبار.

الجدول ١٣ نتيجة دقة التدريب والاختبار للمصنفات الأربعة للنموذج الهجين المقترح

نموذج التعلم الآلي	دقة التدريب على 40000 رسالة	دقة الاختبار على 10000 رسالة
Support Vector Machines (SVM)	**0.9850**	**0.9740**
Naive Bayes	**0.9780**	**0.9630**
K-Nearest	**0.9620**	**0.9410**
Decision Tree	**0.9450**	**0.9120**

تظهر القراءة التحليلية للنتائج تفوقاً واضحاً للنماذج الخطية في التصنيف النصي ثنائي الفئة. فقد سجلت خوارزمية (SVM) أعلى دقة اختبار بلغت 97.40% متفوقةً بفارق ضئيل على مصنف (Naive Bayes) الذي حقق 96.30%. في المقابل، سجل مصنف (K–Nearest) دقة اختبار متزنة بلغت 94.10%، متقدماً على نموذج (Decision Tree) الذي استقر عند دقة اختبار واقعية بلغت 91.20%. إن تراجع أداء شجرة القرار يُعد سلوكاً منطقياً متسقاً مع المراجع العلمية[25] ، حيث يميل التصنيف المعتمد على شجرة القرار إلى ارتكاب أخطاء تصنيفية عندما تكون الحدود الفاصلة بين الكلمات متداخلة وكثيفة. يلاحظ من مراجعة قيم الفوارق الإحصائية بين دقة التدريب ودقة الاختبار ثبات مؤشر القدرة التعميمية لجميع النماذج، حيث انحصر الفارق في نطاق آمن منضبط (بين 1.1% إلى 2.1%)، مما يقلل بشكل كبير من احتمال حدوث إفراط في التخصيص(Overfitting) . خضعت مخرجات الخوارزميات التصنيفية المتنافسة لتحليل معمق عبر مصفوفة الارتباك (confusion matrices) على مستوى عينة الاختبار المستقلة البالغة 10,000 رسالة. تُلاحظ كفاءة خوارزمية(SVM) التي تربع أداؤها على قمة التصنيف، في تقليص الإنذارات الخاطئة وفشل الكشف، حيث نجحت في تحديد 4,870 رسالة تصيد بشكل صحيح من أصل 5,000 عينة (True Positives)، وانحصر فشل الكشف في 130 رسالة فقط تسللت عبر النظام (False Negatives)، وأظهرت مرونة أمنية عالية برصد 4,870 رسالة عمل شرعية (True Negatives)، ولم تسجل سوى 130 إنذار خاطئ تسبب في حجز بريد شرعي (False Positives)، مما يمنح النموذج وثوقية عالية للعمل كخط دفاع أول دون تعطيل أعمال الموظفين. في المرتبة الثانية، أظهر مصنف (Naive Bayes) سلوكاً قريباً جداً من (SVM)، وانحصرت الأخطاء التصنيفية لديه في 185 عينة خطأ لكل فئة من أصل عينات فحص الاختبار المستهدفة. يُعزى هذا الاستقرار والمعدل المنخفض للإنذارات الخاطئة لدى بايز الساذج إلى حساسيته الاحتمالية العالية لتكرار الكلمات، حيث تمكن بكفاءة من تصفية الميزات اللغوية التي يستغلها المهاجمون لإثارة الضغط النفسي[26] (عناصر الإلحاح). في المقابل، أظهر نموذج الجار الأقرب ميلاً واضحاً لارتكاب أخطاء من النوع الثاني (فشل كشف الاحتيال الالكتروني)، وأخفق في كشف ما يقارب 300 رسالة احتيالية لاعتماده على المسافات الإقليدية المتداخلة في الفضاءات الرقمية متعددة الأبعاد[27]. أما مصنف شجرة القرار، فقد عانى من تشتت إحصائي انعكس صراحةً في مصفوفة الارتباك الخاصة به، حيث سجل أعلى معدل أخطاء إجمالي في التجربة، تمثل في وقوع حوالي 440 عينة خطأ موزعة بين إنذارات خاطئة وفشل كشف. هذا القصور يبرهن عملياً على أن أشجار القرار المنفردة تميل إلى اتخاذ قرارات حادة وجامدة عند مواجهة نصوص تحتوي على تكرار وتداخل سياقي متعمد من قبل المهاجمين، مما يجعلها أقل مرونة من النماذج الخطية والاحتمالية عند التعامل مع تعقيد وتطور هجمات الهندسة الاجتماعية (SE) المعاصرة[28] . يعرض الجدول14 صياغة نموذجية لنتائج النماذج الأفضل في الدراسة. القراءة التحليلية للنتائج المدرجة في الجدول 41 تثبت علمياً أن الخوارزميات الكلاسيكية، عند ضبط معاملاتها الفائقة وتغذيتها ببيانات متوازنة بدقة، تمتلك قدرة تنافسية عالية تضاهي الأنظمة الأمنية الحديثة في التمييز القاطع بين أنماط رسائل العمل الشرعية ورسائل الهندسة الاجتماعية(ES) الموجهة، يلاحظ أيضاً تطابق قيم المؤشرات الإحصائية ، هذا التساوي الرياضي يعزى لتوازن توزيع فئات عينة الاختبار، وتناظر الأخطاء التصنيفية المستخرجة من مصفوفة الارتباك، مما يعكس استقراراً هيكلياً في أداء المصنفات. بناءً على تحليل البيانات والنتائج، والمقارنة مع الدراسات المرجعية، نجح النموذج الهجين المقترح في كشف هجمات الهندسة الاجتماعية(ES) على عدة مستويات، وسد الفجوة البحثية المتروكة في الدراسات المرجعية، وحقق الهدف المعرفي للدراسة بالوصول الى نموذج كشف هجين يدمج بين الجداول المعرفية الديناميكية و أليات الكشف الآلي المتطورة ضمن حالات خوارزمية الكشف اليدوي، وساهم في اشراك المستخدمين ورفع وعيهم لكشف هجمات الهندسة الاجتماعية(ES).

جدول 14: نتائج المقاييس الإحصائية على عينة الاختبار (10,000) رسالة للنماذج الأفضل في الدراسة

النموذج	حجم ومصدر مجموعة البيانات	Accuracy الدقة	Precision الضبط	F1-Score التوازن
(SVM)	50,000 رسالة (Enron+Nazario+Combined)	0.9740	0.9740	0.9740
Naive Bayes	50,000 رسالة (Enron+Nazario+Combined)	0.9630	0.9630	0.9630

الاستنتاجات والتوصيات

يبرهن هذا البحث أن الحلول التقنيّة الصرفة تبقى قاصرة في مواجهة هجمات الهندسة الاجتماعية (SE)، مالم تراع التحديث البرمجي الدائم والتدريب والتوعية لتعزيز دفاعات المستخدمين، نظراً لتزايد انتشار هجمات الهندسة الاجتماعية (SE). هناك حاجة ملحة لدعم الأشخاص بحسب خياراتهم ومهنتهم وقدراتهم. نجح النظام الهجين المقترح بسد هذه الفجوة عبر أتمتة أغلب حالات النموذج المحسن للكشف اليدوي عن هجمات الهندسة الاجتماعية (SE)، وتطبيق خوارزمية القوائم السوداء الديناميكية (TBL) على نص أنشأه مهاجم محتمل، وباستخدام تقنيات معالجة اللغة الطبيعية (NLP) والتعلم الآلي (ML)، تمكن النظام الهجين المقترح من اكتشاف هجمات الهندسة الاجتماعية (SE) آليا، وحقق كفاءة تشغيلية ملموسة، مما يثبت كفاءة الخوارزمية المقترحة كأداة دفاعية في كشف هجمات الهندسة الاجتماعية (SE). ولتوسيع نطاق الاستفادة من النموذج الهجين المقترح، توصي هذه الدراسة مستقبلا بتوسيع الطاقة الاستيعابية للنموذج بدراسته على منصات التراسل الفوري وشبكات التواصل الاجتماعي لضمان مرونة التصنيف في بيئات تواصل متنوعة. كما يوصي البحث بدعم الأنظمة متعددة اللغات، والتحول نحو نماذج اللغة الضخمة (LLMs)، وتضمين خوارزميات التعلم العميق (DL) لمعالجة النوايا ورصد الحالة العاطفية للمستخدم عند تطوير النموذج الهجين المقترح مستقبلاً، أيضاً توصي الدراسة بالبحث في معالجة تحدي الهواتف النقالة، حيث توفرت معظم المؤشرات الأمنية لشاشات الحواسب، بينما ما يزال حجم شاشة الهواتف النقالة لا يسمح بذلك.

المراجع

[1] Nagaraj K, Bhattacharjee B, Sridhar A, Sharvani GS. Detection of Phishing Websites Using a Novel Twofold Ensemble Model. Journal of Systems and Information Technology. 2018 Oct;20(4):392-411. Available from: https://doi.org/10.1108/JSIT-09-2017-0074.

[2] Aonzo S, Merlo A, Tavella G, Fratantonio Y. Phishing Attacks on Modern Android. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security; 2018 Oct 15-19; Toronto, Canada. New York: ACM; 2018. p. 1793-1806. Available from: https://doi.org/10.1145/3243734.3243778.

[3] Lastdrager EE. Achieving a consensual definition of phishing based on a systematic review of the literature. Crime Sci. 2014 Sep 3;3:9. Available from: https://doi.org/10.1186/s40163-014-0009-y.

[4] Alsufyani AA, Alzahrani SM. Social Engineering Attack Detection Using Machine Learning: Text Phishing Attack. Indian J Comput Sci Eng. 2021 Jun;12(3):743-751. Available from: https://doi.org/10.21817/indjcse/2021/v12i3/211203298.

[5] Iuga C, Nurse JRC, Erola A. Baiting the hook: factors impacting susceptibility to phishing attacks. Hum Cent Comput Inf Sci. 2016 Dec;6:8. Available from: https://doi.org/10.1186/s13673-016-0065-2.

[6] Adu-Manu K, Ahiable R. Detecting Phishing Using a Multi-Layered Social Engineering Framework. J Comput Sci. 2023;5:13-32. Available from: ProQuest; https://www.proquest.com/openview/08a4c605b57abbcae828fbb328f25bc0/1?pq-origsite=gscholar&cbl=4585457 [Accessed 2026 Jul 6]. doi:10.32604/jcs.2023.043359.

[7] Waelchli S, Walter Y. Reducing the Risk of Social Engineering Attacks Using SOAR Measures in a Real World Environment: A Case Study. Comput Secur. 2025 Jan;148:104137. Available from: https://doi.org/10.1016/j.cose.2024.104137.

[8] Bell S, Komisarczuk P. An Analysis of Phishing Blacklists: Google Safe Browsing, OpenPhish, and PhishTank. In: Proceedings of the Australasian Computer Science Week Multiconference; 2020 Feb 4-6; Melbourne, Australia. New York: ACM; 2020. p. 1-11. Available from: https://doi.org/10.1145/3373017.3373020.

[9] Venkatesha S, Reddy KR, Chandavarkar BR. Social Engineering Attacks During the COVID-19 Pandemic. SN Comput Sci. 2021 Mar;2(2):78. Available from: https://doi.org/10.1007/s42979-020-00443-1.

[10] Hijji M, Alam G. A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions. IEEE Access. 2021;9:7152-7169. Available from: https://doi.org [11] "How Experts Detect Phishing Scam Emails." https://doi.org/10.1145/3415231.

[11] Pan Y, Ding X. Phishing page detection via learning classifiers from page layout features. EURASIP J Wirel Commun Netw. 2019 Feb 20;2019(1):33. Available from: doi:10.1186/s13638-019-1361-0

[12] Malloy T, Ferreira MJ, Fang F, Gonzalez C. Training Users Against Human and GPT-4 Generated Social Engineering Attacks. arXiv [Preprint]. 2025 Feb 3 [cited 2026 Oct 5]:arXiv:2502.01764 [cs.HC]. Available from: https://doi.org/10.48550/arXiv.2502.01764.

[13] Sahingoz OK, Buber E, Demir O, Diri B. Machine Learning Based Phishing Detection from URLs. Expert Syst Appl. 2019 Mar;117:345-357. Available from: doi:10.1016/j.eswa.2018.09.029

[14] Adebowale MA, Lwin KT, Hossain MA. Intelligent phishing detection scheme algorithms using deep learning. J

الاختصارات:

الجدول رقم 1

اساهمات المؤلفين الإطار المفاهيمي: باسل الخطيب– دانا نجيب

المنهجية: دانا نجيب

التحقيقات: باسل الخطيب– دانا نجيب

إدارة المشروع: باسل الخطيب

الإشراف: باسل الخطيب

الكتابة – المسودة الأصلية: دانا نجيب

الكتابة – المراجعة والتحرير :باسل الخطيب– دانا نجيب

تضارب المصالح:يعلن المؤلفون أنه ليس لديهم أي مصالح متضاربة.

توافر البيانات والمواد:جميع البيانات متوفرة في النص الرئيس عدا الأشكال والمراجع.

المواد التكميلية: قائمة المراجع – قائمة الأشكال – قائمة الجداول (المدرجة في النص).

التمويل: لا يوجد

Enterprise Inf Manag. 2020 May 20;34(3):849-868. Available from: https://doi.org/10.1108/JEIM-01-2020-0036
[15] Zamir A, Khan H, Iqbal T, Yousaf N, Aslam F, Anjum A, et al. Phishing web site detection using diverse machine learning algorithms. Electron Libr. 2020 Jun 25;38(3):543-564. Available from: https://doi.org/10.1108/EL-05-2019-0118
[16] Soyemi J, Mudasiru H. An enhanced authentication scheme for preventing phishing attacks on WhatsApp accounts. In: Proceedings of the 2nd International Conference on Science, Technology, Engineering and Management (ICSTEM); 2020 Nov 10-11; Ilaro, Nigeria. FPI; 2020. p. 45-53. Available from: https://erepository.federalpolyilaro.edu.ng/handle/123456789/1627
[17] Roy SS, Thota P, Naragam KV, Nilizadeh S. From Chatbots to Phishbots?: Phishing Scam Generation in Commercial Large Language Models. In: Proceedings of the 2024 IEEE Symposium on Security and Privacy (SP); 2024 May 19-23; San Francisco, CA, USA. Piscataway: IEEE; 2024. p. 36-54. Available from: https://doi.org/10.1109/SP54263.2024.00182
[18] Najeeb D. Forked Repository [Software on the Internet]. Zenodo; 2026. Available from: https://doi.org/10.5281/zenodo.23168960
[19] Hannousse A, Yahiouche S. Web page phishing detection [Dataset]. Mendeley Data; 2021. Available from: Mendeley Data; 2021. doi:10.17632/c2gw7fy2j4.3.
[20] Najeeb D. Phishing Features Detection and Analysis Code [Computer Program on the Internet]. Google Colab; 2026 [cited 2026 Oct 5]. Available from: https://colab.research.google.com/drive/1CSNK2zKcS7CxYTi2Yi_B5HLMhKApkM0O?usp=sharing
[21] Najeeb D. JavaScript Application [Software on the Internet]. Zenodo; 2026. Available from: https://doi.org/10.5281/zenodo.23168848
[22] Najeeb D. Win [Software on the Internet]. Zenodo; 2026. Available from: https://doi.org/10.5281/zenodo.23168574
Najeeb D. Social Engineering Detection and Feature Engineering Code [Computer Program on the Internet]. Google Colab; 2026 [cited 2026 Oct 5]. Available from: https://colab.research.google.com/drive/13kySjOAxcyvoCaNzOQ-WiXolLsu5c0Qt?usp=sharing
[23] Najeeb D. Web Page [Internet]. Zenodo; 2026. Available from: https://doi.org/10.5281/zenodo.23169057
[24] Alam NA. Phishing Email Dataset [Dataset]. Kaggle; 2024 [cited 2026 Oct 5]. Available from: https://www.kaggle.com/datasets/naserabdullahalam/phishing-email-dataset
[25] Napierala K, Stefanowski J. Types of minority class examples and their influence on learning classifiers. J Intell Inf Syst. 2016;46(3):563-597. doi: 10.1007/s10844-015-0368
[26] Salloum SA, Al-Emran M, Monem AA, Shaalan K. A survey of text mining in social media: highlights and trends. Int J Inf Manag Data Insights. 2021;1(2):100028. doi:10.1016/j.jjimei.2021.100028
[27] Cvetko T. The Curse Of Dimensionality in KNN Classifiers. Towards AI. 2023;12(4):102-115. doi:10.21384/tai.knn.2023.04
[28] Trevisan T. Machine Learning and Text Classification: Stability and Overfitting of Single Decision Trees. Politesi. 2026;14(2):112-126. doi:10.1057/pol.dt.2026.03.