

51447  
2026-2025

المعلومات المقدمة في هذا المجلد هي لأغراض إعلامية فقط ولا ينبغي استخدامها كإشارة على أي نوع من التوصيات أو الاستشارات. لا يمكن ضمان دقة المعلومات الواردة في هذا المجلد. لا يمكن ضمان دقة المعلومات الواردة في هذا المجلد. لا يمكن ضمان دقة المعلومات الواردة في هذا المجلد.

عزة الحارثي

أ.د. مالك الحارثي

مساحة المشرف:

المشرف:

مؤسسة الإماراتية للتعليم العالي  
جامعة الإمارات العربية المتحدة

2022100287

حبيب محمد سعيد الحارثي

2025041960

مهدي إبراهيم تاجي قاسم



البريد الإلكتروني: info@iuem.ac.ae  
البريد الإلكتروني: info@iuem.ac.ae



# مجلة الجامعة الإماراتية الدولية

artificial media.

The cybersecurity landscape is undergoing a radical transformation with the emergence of "Social Engineering 2.0." Attacks no longer rely solely on text manipulation but have expanded to employ generative artificial intelligence techniques, specifically "deepfakes," to create hyper-realistic audio-visual media. This research paper aims to analyze the risks arising from the integration of deepfakes in social engineering attacks, focusing on the current shortcomings of traditional defense mechanisms that fail to detect deepfakes in compressed environments and live communication channels. Through a critical review of recent literature and the proposal of a hybrid defense framework, the study discusses the importance of combining automated technical analysis with human behavioral verification. The findings conclude that technical solutions alone are insufficient in light of the development of competitive generative networks (GANs), recommending the adoption of "zero trust" strategies and out-of-band verification as essential for protecting institutional and societal assets in the age of artificial media.

## Abstract













HOW AI) لا سيما في الهندسة والتكنولوجيا والبرمجيات، والتي تتطلب العميق تعلم الآلة لتتفهم البيانات المعقدة وتتخذ قرارات دقيقة. كيف يمكن أن يكون:

### 3.6. الأثر الاجتماعي للذكاء الاصطناعي:

(Siva Krishna, 2025). الأثر الاجتماعي للذكاء الاصطناعي، بل الأهم من ذلك، هو قدرته على تغيير الطريقة التي نعيش بها.

أحد أكبر التحديات التي تواجهها المجتمعات الحديثة هي كيفية التعامل مع التغييرات التي تسببها التكنولوجيا. في حين أن الذكاء الاصطناعي قد يحل محل بعض الوظائف، فإنه يخلق أيضًا فرصًا جديدة للتعليم والتدريب.

في الوقت نفسه، فإن:

6. مستقبل الذكاء الاصطناعي: يتوقع أن يصبح الذكاء الاصطناعي أكثر تكاملًا مع الحياة اليومية، مما سيؤدي إلى تغييرات جذرية في العديد من المجالات.

المجالات:

5. الأمن السيبراني: مع زيادة الاعتماد على التكنولوجيا، أصبحت التهديدات الإلكترونية أكثر تعقيدًا، مما يتطلب حلولًا مبتكرة للتعامل معها.

4. الرعاية الصحية: يمكن للذكاء الاصطناعي تحليل كميات هائلة من البيانات لتشخيص الأمراض بدقة أكبر، مما يحسن من نتائج العلاج.

المجالات:

3. التوظيف: مع أتمتة المهام الروتينية، قد يفقد بعض الأشخاص وظائفهم، مما يتطلب برامج إعادة التدريب والتأهيل.

البيانات الضخمة والذكاء الاصطناعي.

2. الخصوصية والأمن: مع تزايد الاعتماد على التكنولوجيا، أصبحت البيانات الشخصية أكثر قيمة، مما يتطلب تدابير أمنية قوية لحمايةها.

(Phishing):

1. الأمان السيبراني: مع تزايد الاعتماد على التكنولوجيا، أصبحت البيانات الشخصية أكثر قيمة، مما يتطلب تدابير أمنية قوية لحمايةها.

هذه المجالات هي التي ستشهد أكبر تغييرات مع تطور الذكاء الاصطناعي. ومع ذلك، فإن التحديات التي تواجهها المجتمعات الحديثة هي كيفية التعامل مع التغييرات التي تسببها التكنولوجيا.

((Phishing))

Social Engineering 2.0 Deepfake and Deep Learning-Based Cyber-Attacks) (التهديدات السيبرانية القائمة على التعلم العميق والذكاء الاصطناعي)

الذكاء الاصطناعي (AI) هو مجال من مجالات التكنولوجيا الذي يهتم بتصميم وتطوير أجهزة وبرامج قادرة على محاكاة العمليات العقلية البشرية، مثل التعلم والتفكير وحل المشكلات.

### 3.5. الأثر الاجتماعي للذكاء الاصطناعي:

(Kristoffer Torngaard et al., 2025). الأثر الاجتماعي للذكاء الاصطناعي، بل الأهم من ذلك، هو قدرته على تغيير الطريقة التي نعيش بها.

أحد أكبر التحديات التي تواجهها المجتمعات الحديثة هي كيفية التعامل مع التغييرات التي تسببها التكنولوجيا. في حين أن الذكاء الاصطناعي قد يحل محل بعض الوظائف، فإنه يخلق أيضًا فرصًا جديدة للتعليم والتدريب.

في حين أن الذكاء الاصطناعي قد يحل محل بعض الوظائف، فإنه يخلق أيضًا فرصًا جديدة للتعليم والتدريب. ومع ذلك، فإن التحديات التي تواجهها المجتمعات الحديثة هي كيفية التعامل مع التغييرات التي تسببها التكنولوجيا.

أوامر مألوفة عن الذكاء الاصطناعي.







الجزء 4.6.1 نتائج الأداة النفسية: معدل الأداة 4.6.1

النتائج: النتائج النفسية المحددة: تم تحليل البيانات المجمعة من اختبار الأداة (KPIs) عبر المراحل الثلاثة للتحليل النفسي. فيما يلي تفصيل النتائج:

النتائج النفسية المحددة: تم تحليل البيانات المجمعة من اختبار الأداة (KPIs) عبر المراحل الثلاثة للتحليل النفسي. فيما يلي تفصيل النتائج:

النتائج النفسية المحددة: تم تحليل البيانات المجمعة من اختبار الأداة (KPIs) عبر المراحل الثلاثة للتحليل النفسي. فيما يلي تفصيل النتائج:

#### 4.6.1 نتائج الأداة النفسية: معدل الأداة

النتائج النفسية المحددة: تم تحليل البيانات المجمعة من اختبار الأداة (KPIs) عبر المراحل الثلاثة للتحليل النفسي. فيما يلي تفصيل النتائج:

النتائج النفسية المحددة: تم تحليل البيانات المجمعة من اختبار الأداة (KPIs) عبر المراحل الثلاثة للتحليل النفسي. فيما يلي تفصيل النتائج:

النتائج النفسية المحددة: تم تحليل البيانات المجمعة من اختبار الأداة (KPIs) عبر المراحل الثلاثة للتحليل النفسي. فيما يلي تفصيل النتائج:

النتائج النفسية المحددة: تم تحليل البيانات المجمعة من اختبار الأداة (KPIs) عبر المراحل الثلاثة للتحليل النفسي. فيما يلي تفصيل النتائج:

النتائج النفسية المحددة: تم تحليل البيانات المجمعة من اختبار الأداة (KPIs) عبر المراحل الثلاثة للتحليل النفسي. فيما يلي تفصيل النتائج:

النتائج النفسية المحددة: تم تحليل البيانات المجمعة من اختبار الأداة (KPIs) عبر المراحل الثلاثة للتحليل النفسي. فيما يلي تفصيل النتائج:

#### 4.5 المتاحون وأجزاء التقييم

النتائج النفسية المحددة: تم تحليل البيانات المجمعة من اختبار الأداة (KPIs) عبر المراحل الثلاثة للتحليل النفسي. فيما يلي تفصيل النتائج:

- المرحلة B (بعد الضغط): تمرير العينات عن مصادات اتصال شائعة (Zoom و WhatsApp) التي تحدث في الواقع.
- المرحلة A (العودة الجاهل): عرض الفيديو هات والموثبات والمزيفة بخلفية مائية مشابهة بعد التوليد.

النتائج النفسية المحددة: تم تحليل البيانات المجمعة من اختبار الأداة (KPIs) عبر المراحل الثلاثة للتحليل النفسي. فيما يلي تفصيل النتائج:

النتائج النفسية المحددة: تم تحليل البيانات المجمعة من اختبار الأداة (KPIs) عبر المراحل الثلاثة للتحليل النفسي. فيما يلي تفصيل النتائج:

النتائج النفسية المحددة: تم تحليل البيانات المجمعة من اختبار الأداة (KPIs) عبر المراحل الثلاثة للتحليل النفسي. فيما يلي تفصيل النتائج:

النتائج النفسية المحددة: تم تحليل البيانات المجمعة من اختبار الأداة (KPIs) عبر المراحل الثلاثة للتحليل النفسي. فيما يلي تفصيل النتائج:

النتائج النفسية المحددة: تم تحليل البيانات المجمعة من اختبار الأداة (KPIs) عبر المراحل الثلاثة للتحليل النفسي. فيما يلي تفصيل النتائج:



## الدراسات والبحوث

التي أجريتها في ٢٠١٤م. حيث بلغت نسبة الإجابة الصحيحة ٦٠% إلى أن كانت الإجابة الخاطئة ٤٠%.

أما فيما يتعلق بالدراسات والبحوث التي أجريتها في ٢٠١٤م، فقد كانت النتائج كالتالي:

- نسبة الإجابة الصحيحة على الأسئلة التي أجريتها في ٢٠١٤م كانت ٩٤%.
- نسبة الإجابة الخاطئة على الأسئلة التي أجريتها في ٢٠١٤م كانت ٦%.
- نسبة الإجابة الصحيحة على الأسئلة التي أجريتها في ٢٠١٤م كانت ٩٨.٥%.
- نسبة الإجابة الخاطئة على الأسئلة التي أجريتها في ٢٠١٤م كانت ١.٥%.

الدراسات والبحوث التي أجريتها في ٢٠١٤م كانت كالتالي:

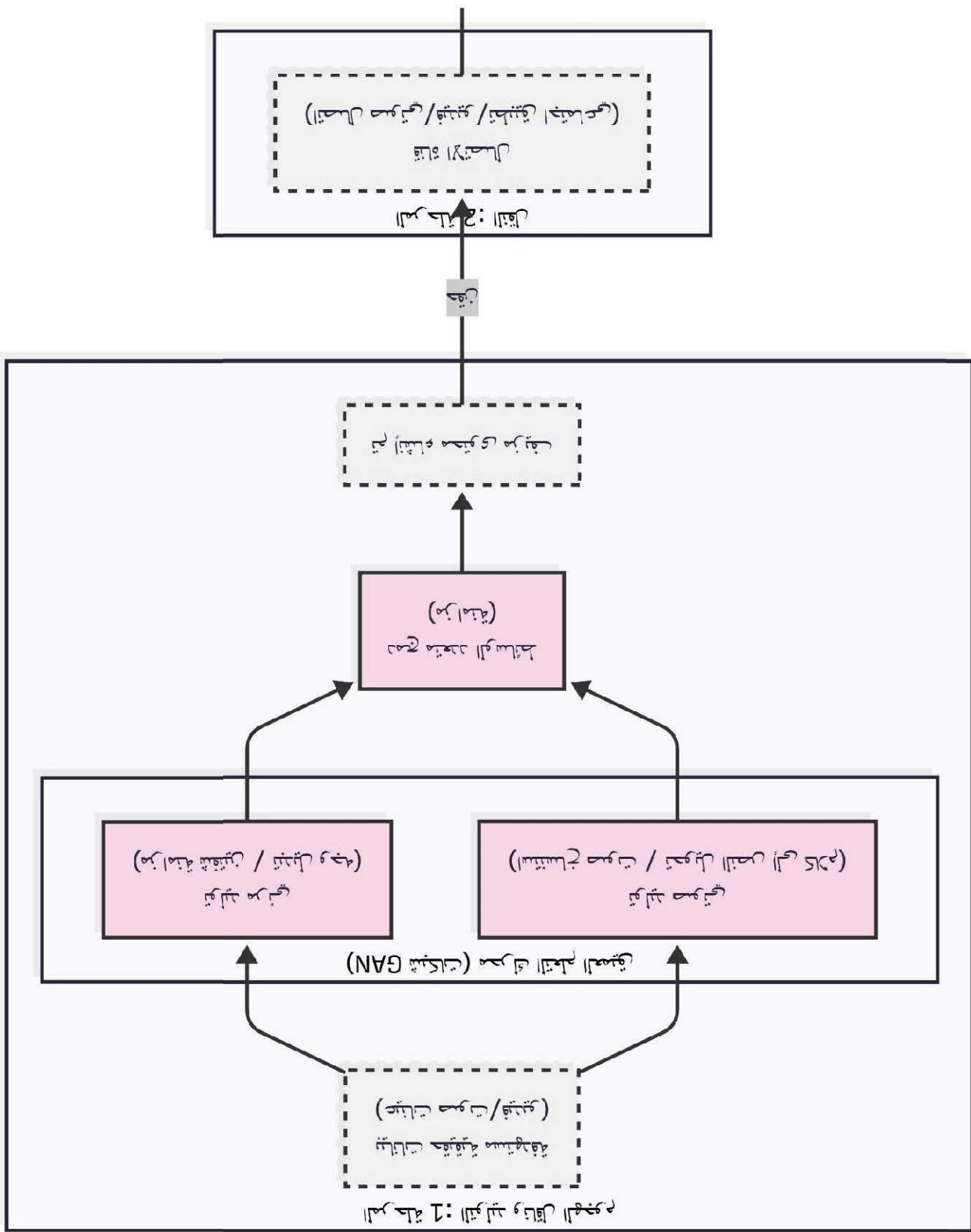
أما فيما يتعلق بالدراسات والبحوث التي أجريتها في ٢٠١٤م، فقد كانت النتائج كالتالي:

### ٤.٦.٣. نتائج الدراسات والبحوث

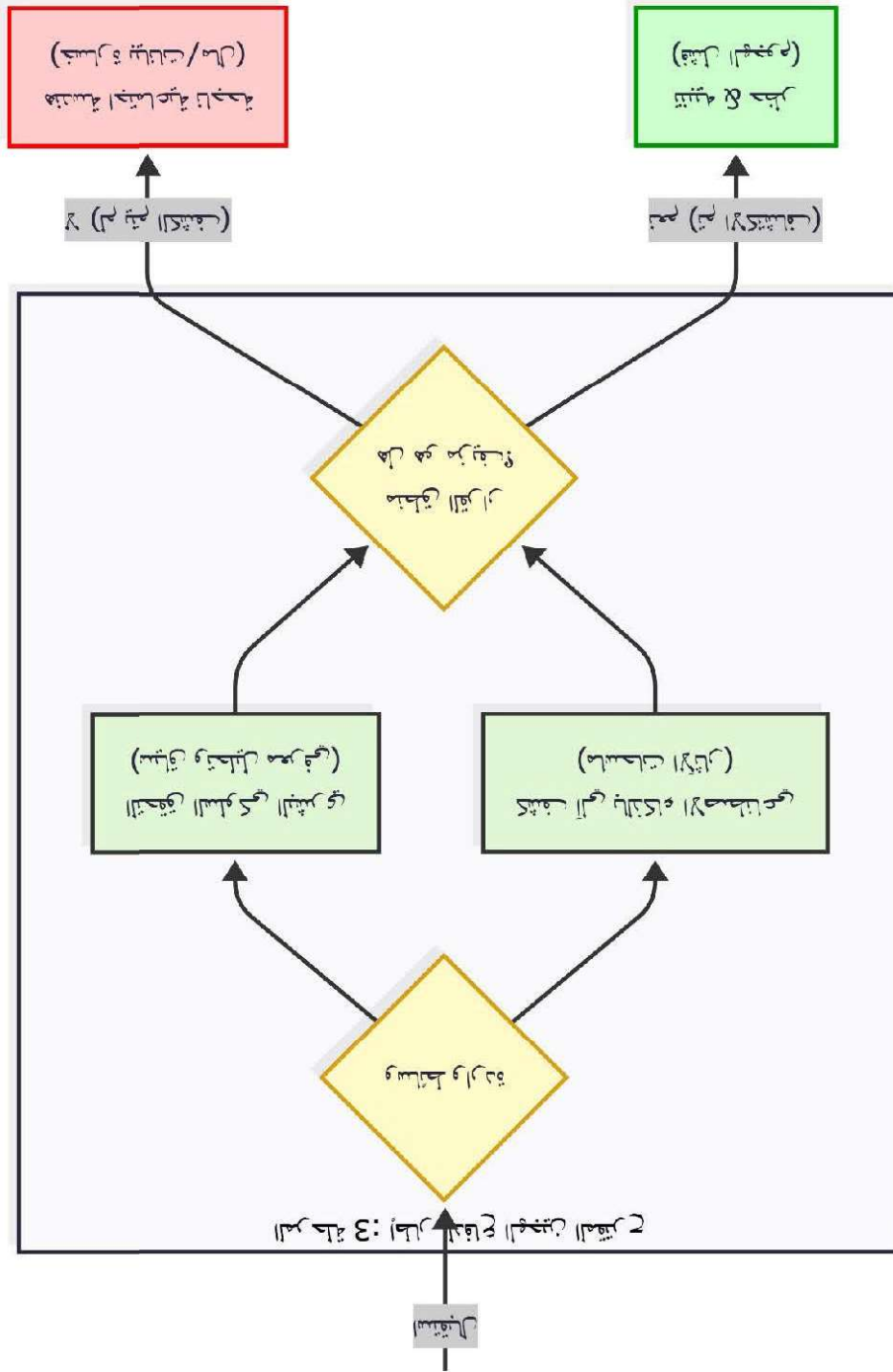
الدراسات والبحوث التي أجريتها في ٢٠١٤م كانت كالتالي:

مؤشر الأداء	الدراسات والبحوث التي أجريتها في ٢٠١٤م	الدراسات والبحوث التي أجريتها في ٢٠١٤م	الدراسات والبحوث التي أجريتها في ٢٠١٤م
مؤشر الأداء	٩٨.٥%	٩٧%	٤٤.٦%
مؤشر الأداء	١.٥%	٣%	٥٥.٤%
مؤشر الأداء	٩٤%	٩٧%	٤٤.٦%

### 5. خطوات العمل



الشكل 1: المخطط الآلي (بالتفصيل)









# مجلة الجامعة الإماراتية الدولية



4. النشر يبرع والحكومة الرقمية: نوصي بضرورة سد الفراغ النشر يبرع من خلال من خلال سن قنلة لاذر لاذر في المحتوى المولد بالاتصال بدمج "علامات رقمية" (Digital Watermarking) غير قنلة لاذر لاذر في المحتوى المولد بالاتصال بدمج "علامات رقمية" مما يسهل عملية الكشف والتتبع الخارجي.
5. النشر يبرع العميق ليس مجرد أداة اختراق عابرة، بل هو اختبار حقيقي لمدى مرونة مؤسساتنا وقدرتها على التكيف في بيئة رقمية لم تعد فيها "الزورقة" دابة كافيًا على "التصديقي".

- [1] Deepfake-Driven Social Engineering and AI-Generated Attacks: Redefining Threats and Defenses in the Age of Synthetic Media. 2025
- [2] Impact of Deepfake Technology on Social Media: Detection, Misinformation and Societal Implications. 2023
- [3] Partial Fake Speech Attacks in the Real World Using Deepfake Audio. 2025
- [4] Deepfake-Driven Social Engineering: Threats, Detection Techniques, and Defensive Strategies in Corporate Environments. 2025
- [5] Social Engineering 2.0 Deepfake and Deep Learning-Based Cyber-Attacks (Phishing). 2025
- [6] How AI and deepfakes are redefining social engineering threats. 2025
- [7] Goodfellow, I., et al. (2014). Generative Adversarial Nets. In Advances in Neural Information Processing Systems (NIPS).
- [8] Mirsky, Y., & Lee, W. (2021). The Creation and Detection of Deepfakes: A Survey. ACM Computing Surveys (CSUR), 54(1), 1-41.
- [9] FBI (Federal Bureau of Investigation). (2021). Malicious Actors Almost Certainly Will Leverage Synthetic Content for Cyber Operations. FBI Private Industry Notification.
- [10] Westerlund, M. (2019). The Emergence of Deepfake Technology: A Review. Technology Innovation Management Review, 9(11).
- [11] Agarwal, S., et al. (2019). Protecting World Leaders Against Deep Fakes. CVPR Workshops.
- [12] "التحديات الأمنية على الأمن السيبراني: دراسة تحليلية للتقنيات والآليات المخفية" مجلة الإماراتية الدولية، 2022.
- [13] "تحديات كشف التزييف العميق في الفيديو هات المضمون طية: دراسة تجريبية" أعمال المؤتمر السعوي للذكاء الاصطناعي، الرياض، السعودية، 2022.

## المراجع