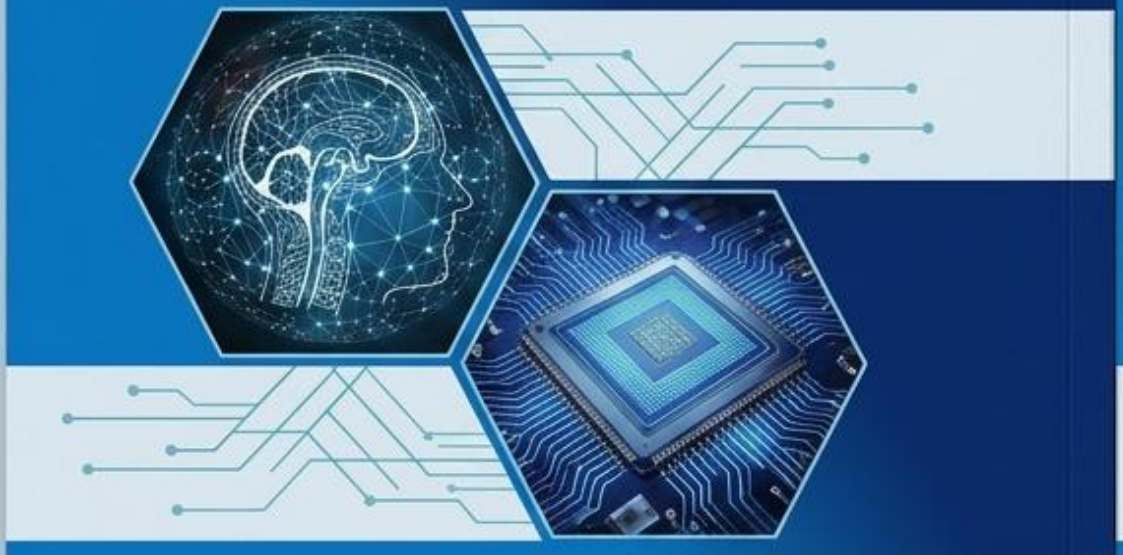
NO: 2 /Aug /2025

Issn: 3105-790X (P) 3105-7918 (E)

A quarterly peer-reviewed scientific journal

Journal of Artificial Intelligence and Information Technology

Issued by the Center for Research and Development of Human Resources, Ramah/Jordan



العنوان الإداري الأردن/ عمان / الجاردنز/ شارع وصفي التل موبايل: ٠٠٩٦٢٧٩٩٤٢٤٧٧٤+

إيميل: Email: khalidk 51@hotmail.com رابط المجلة https://aitjournal.org/portal/index.php

العدد: 2 / [2025 / 8]

مجلة علمية محكمة ربع سنوية

مجلة الذكاء الاصطناعي وتكنولوجيا المعلومات

تصدر عن مركز البحث وتطوير الموارد البشرية، رماح/الأردن

ISSN: 3105-790X (P)
ISSN: 3105-7918 (E)

العنوان الإداري الأردن/ عمان / الجاردنز/ شارع وصفي التل موبايل: ٠٠٩٦٢٧٩٩٤٢٤٧٧٤+

إيميل: Email: khalidk 51@hotmail.com رابط المجلة https://aitjournal.org/portal/index.php

مجلة الذكاء الاصطناعي وتكنولوجيا المعلومات

مجلة دولية علمية محكّمة متخصصة تهتم بنشر الأبحاث والدراسات العلمية والنظرية والتطبيقية في مجال الذكاء الاصطناعي وتكنولوجيا المعلومات و الدراسات المتعلقة بهما

تصدر عن مركز البحث وتطوير الموارد البشرية "رماح" – الأردن

العدد (02) (اب) 2025

ISSN: 3105-790X (P)
ISSN: 3105-7918 (E)

العنوان الاداري للمجلة

مركز البحث وتطوير الموارد البشري "رماح" عمان – الأردن شارع وصفي التل

الهاتف /الفاكس: 0096278270863

البريد الالكتروني: khalidk_51@hotmail.com-remahislamicjournal2021@yahoo.com

الموقع الالكتروني: https://aitjournal.org/portal/index.php

أعضاء اللجنة العلمية

أ.م.د. محمد جاجان يونس	استاذ مساعد	العراق
أ.د. حنان افنيخره	أستاذ دكتور	ليبيا
د. حسن محمد نوري المشهداني	مدرس	العراق
د.حمزة بسلموني	استاذ مساعد	الجزائر
أ.د. فادي عبد الله سليمان	أستاذ دكتور	تركيا
أ.م.د. سحر سعيد قاسم الطائي	استاذ مساعد	العراق
أ.د. ليث حمدباوغلو	أستاذ دكتور	تركيا
أ.م.د. حذيفة ابو حماد	استاذ مساعد	العراق
د. لمى اكرم عبدالله الصفار	مدرس	العراق
د. على عبد الله مسلم	أستاذ دكتور	فلسطين
أ.م.د. أنور لودبن	استاذ مساعد	باكستان
د. محمد شقورة	استاذ مساعد	فلسطين
أ.م.د. بيداء سليمان بهنام	استاذ مساعد	العراق
أ.م.د. بان غانم عمر العاني	استاذ مساعد	العراق
أ.د. رجاء الحاسي	أستاذ دكتور	ليبيا
أ.د. عبد الفتاح حسن محمود	أستاذ دكتور	مصر

شـروط النشـر

- تقديم تعهد بعدم إرسال البحث لمجلة أخرى وعدم المشاركة به في مؤتمرات علمية.
- ألا تتجاوز صـفحات البحث 20 صـفحة ويكون ملخص البحث بلغتين لغة البحث بالإضـافة إلى اللغة الإنجليزية ان لم تكن هي لغة البحث، ويكتب عنوان البحث باللغة الانجليزية رفقة اسم الباحث والكلمات المفتاحية.
- تقدم الأبحاث مطبوعة على ورق من حجم A4 وتكون المسـافة مفردة بين الأسـطر مع ترك هامش من كلا الجوانب مسافة 4.5 سم، وأن يكون الخط (Traditional Arabic) قياس14باللغة العربية ويكون الخط (Times New Roman) قياس 12 باللغة الإنجليزية أو الفرنسية، وفق برنامج (Microsoft Word).
- يرقم التهميش والإحالات ويعرض في أسفل الصفحة :المؤلف، عنوان الكتاب أو المقال، عنوان المجلة أو الملتقى، الناشر، الطبعة، البلد، السنة، الصفحة أو ضمن البحث مع ذكر المؤلف وسنة النشر والصفحة.
- تتمتع المجلة بكامل حقوق الملكية الفكرية للبحوث المنشورة.
- على الباحث أن يكتب ملخصين للبحث: أحدهما بلغة البحث والآخر باللغة الإنجليزية، على ألا يزيد عدد كلمات الملخص عن 150 كلمة. منهج العلمي المسـتخدم في حقل البحث المعرفي واسـتعمال أحد الأسـاليب التالية في الاسـتشـهاد في المتن والتوثيق في قائمة المراجع، أسـلوب إم إل أي (MLA) أو أسـلوب شـيكاجو (Chicago) في العلوم الإنسانية أو أسلوب أي بي أي (APA) في العلوم الاجتماعية، وهي متوافرة على الأنترنت.
- المقالات المنشورة في هذه المجلة لا تعبّر إلا عن آراء أصحابها.
- يحق لهيئة التحرير إجراء بعض التعديلات الشـكلية على المادة المقدّمة متى لزم الأمر دون المساس بمحتوى الموضوع.

51	**An Intelligent Hybrid Deep Learning Framework for DDoS Attack Detection and Classification in Modern Network Environments** **Huda A. Eltarifi1, Sally D. Abualgasim2, Abubakr H. Ombabi2, Eman Mohammed Hamid3** **.1 Department of Computer Science, Faculty of Computer Science and Information Technology, University of Holy Quran and Re-Origination of Science, Rofaà, Sudan, hudaeltarifi@gmail.com, huda@uofq.edu.sd** **.2 Department of Computer Engineering, Faculty of Engineering and Technology, University of Gezira, Wad Madani, Sudan, sally.dallah1@gmail.com, sallydallah@uofg.edu.sd** **.3 Department of Computer Science, Faculty of Computer Science, University of Albutana, Rofaà, Sudan, abubakr.h.ombabi@gmail.com** **.4 Department of Computer Science, Faculty of Mathematical and Computer Science, University of Gezira, Wad Madani, Sudan, Eman_24@hotmail.com**	3
68	**Next-Generation Security Frameworks for Model Context Protocol in Agentic AI Systems** shuruq Khalid Abdulredha Directorate Education of Babylon, Ministry of Education, Iraq,	4
80	**Technical and Pedagogical Challenges of Using the AI-Based Siraj Smart Educational Platform in Jordan** Dr. Shatha Sakher: Faculty of Medicine, Al-Balqa Applied University, As-Salt, Jordan,	5

J.A.I.T

الترميز الكارتوغرافي المرئي لخرائط السكان البيئي (الحضر والريف) للعراق (2024–2034)

باستخدام نموذج الذكاء الاصطناعي الجغرافي

أ.د احمد محمد جهاد الكبيسي

خرائط وتقنيات الذكاء الاصطناعي الجغرافي

قسم تربية الفلوجة – الاشراف التربوي

7869484517-prof.ahmed.m.j.alkubaisi@gmail.com

الملخص:

يهدف البحث الى التصميم البصري لخرائط السكان البيئي المبتكرة بنموذج الذكاء الاصطناعي.(**كلاويد–اوبس –تفكير عميق–32**) (C.O.D.T-32) لإنشاء خريطة تفاعلية لتحليل وترميز بيانات السكان البيئي (الحضر والريف) للعراق(2024–2034) تم حساب سنة الأساس 2024 لنمو السكان المستقبلي (2034) وفق معادلة الأمم المتحدة للنمو السكاني بمتوسط (2.3%)، اهتم البحث بعرض أنواع الرموز الكارتوغرافية (كرات حجمية نابضة، أعمدة بيانية دوارة ،دوائر نابضة، مكعبات بدوران مستمر ،مثلثات هرمية مجسمة، وردة الرياح الدوارة مقسمة الى (4) أجزاء تمثل (الحضر،الريف،الذكور،الاناث) بلوحة تحكم وازرار عرض واخفاء الرموز على خريطة الشارع المفتوح التفاعلية، تحتوي على طبقات الرموز المقسمة ،و سرعة الحركة، عرض التقرير التحليلي ، إعادة ضبط العرض ، المراجع العلمية ، هيكلية البحث، مع لوحة دليل الألوان، الإحصائيات العامة – تتحدث فورياً، والتقرير التحليلي الشامل – يعرض تحليلات مفصلة، مع التأثيرات البصرية . اثبت البحث أهمية توظيف نماذج تقنيات الذكاء الاصطناعي الجغرافي في التمثيل الكارتوغرافي للرموز المتنوعة المبتكرة بشكل جديد لم تتمكن برامج أخرى من تكوينها. وتسهيل التواصل البصري للمعلومات السكانية مع مختلف الفئات، وتوفير رؤية استشرافية للنمو السكاني حتى عام 2034. بتصميم بصري احترافي تفاعلي. اعتمد البحث على المنهج الكارتوغرافي ثلاثي الابعاد البصري والمنهج التقني نموذج كلاويد–اوبس، وخرج بنتائج تحليل جغرافي متقدم، تحليل بيانات ذكي. ويمكن الوصول الى الخريطة التفاعلية مباشرة عبر باركود سريع للملف.

الكلمات المفتاحية: ذكاء صناعي جغرافي، خرائط تفاعلية، تصميم بصري، السكان

Visual Design of Population-Environment Maps (Urban and Rural) for Iraq (2024-2034)Using the Artificial Intelligence Geographic Model (Cloud-Ops - Deep Thinking-32)

Prof. Ahmed Mohammed Jihad Al-Kubaisi

Geographic Artificial Intelligence Maps and Techniques
Department of Education, Fallujah - Educational Supervision

Abstract:

The research aims to visually design innovative environmental population maps using an artificial intelligence model (Cloud-Ops - Deep Thinking-32) (C.O.D.T-32) to create an interactive map for analyzing and coding environmental population data (urban and rural) for Iraq (2024-2034). The base year 2024 was calculated for future population growth (2034) according to the United Nations population growth equation with an average of (2.3%). The research focused on displaying various types of cartographic symbols (pulsing volumetric spheres, rotating bar charts, pulsing circles, continuously rotating cubes, three-dimensional pyramid triangles, and a rotating wind rose divided into (4) parts representing (urban, rural, male, female) with a control panel and buttons to show and hide symbols on the interactive OpenStreetMap. It includes layers of divided symbols, movement speed, display of the analytical report, display reset, scientific references, research structure, a color guide panel, and general statistics - speaking in real time. The comprehensive analytical report presents detailed analyses with visual effects. The research demonstrated the importance of employing geographic artificial intelligence models in the cartographic representation of diverse, innovative symbols in a novel way that other programs could not. This facilitates visual communication of population information to various groups and provides a forward-looking view of population growth up to 2034, all within a professional, interactive visual design. The research relied on a three-dimensional visual cartographic approach and the Cloud-Ops model, resulting in advanced geographic analysis and intelligent data analysis. The interactive map can be accessed directly via a quick QR code.

Keywords: Geographic AI, Interactive Maps, Visual Design, Population

مشكلات البحث

1. قلة الدراسات التي تستخدم تقنيات الترميز الكارتوغرافي البصري ثلاثي الأبعاد في تمثيل التوزيع السكاني البيئي للعراق بشكل تفاعلي مرئي باستخدام الذكاء الاصطناعي الجغرافي.
2. التحدي في تقديم بيانات سكانية متعددة المتغيرات (حضر/ريف، ذكور/إناث) بشكل مرئي واضح وسهل الفهم عبر خريطة الشارع المفتوح التفاعلية بلوحة تحكم وبيانات فورية.
3. عدم توفر أدوات تفاعلية لعرض التوقعات السكانية حتى عام 2034 بناءً على المعادلات الإحصائية العلمية المعتمدة.
4. هناك فجوة واضحة والحاجة لربط البيانات السكانية الرقمية بالموقع الجغرافي بشكل تفاعلي وديناميكي يسهل على أصحاب القرار المكاني السرعة والدقة.

فرضيات البحث

1. **الفرضية الأولى:** يُسهم التصميم البصري المرئي المباشر ثلاثي الأبعاد(3D) في تحسين فهم وتحليل التوزيع السكاني البيئي بشكل أفضل من الخرائط التقليدية ثنائية الأبعاد(2D)
2. **الفرضية الثانية:** يمكن لتقنيات الترميز الكارتوغرافي المتعددة (الكرات، المكعبات، الأهرامات، وردة الرياح) أن تعرض متغيرات سكانية متعددة في آن واحد.
3. **الفرضية الثالثة: ان** تطبيق معادلة النمو السكاني للأمم المتحدة يوفر تقديرات موثوقة للسكان حتى عام 2034.
4. **الفرضية الرابعة:** التفاعلية بشكل مرئي مباشر في الخرائط تزيد من قدرة المستخدم على استكشاف وتحليل البيانات السكانية بشكل مستقل.

أهداف البحث

1. تصميم خرائط تفاعلية ثلاثية الأبعاد وإنشاء نظام كارتوغرافي متكامل لعرض التوزيع السكاني البيئي في العراق.
2. التمييز البصري بين الحضر والريف باستخدام ألوان ورموز مميزة للتفريق بين سكان المناطق الحضرية والريفية.
3. تطبيق رموز كارتوغرافية متنوعة مثل الكرات الحجمية، المكعبات، الأهرامات، الأعمدة البيانية، ووردة الرياح. بأسلوب مبتكر جديد بصرياً
4. التنبؤ بالنمو السكاني لعام 2034 بتطبيق معادلة الأمم المتحدة الأسية للتوقعات السكانية المستقبلية.
5. توفير تقارير شاملة إحصائية وتحليلية لكل محافظة مع المقارنات والاستنتاجات.
6. تمكين التفاعل المرئي المباشر مع البيانات للتحكم في طبقات العرض والرموز وسرعة الحركة للمستخدم.

أهمية البحث

إثراء المكتبة الجغرافية العربية بنموذج متقدم للترميز الكارتوغرافي ثلاثي الأبعاد، وتقديم منهجية علمية قابلة للتطبيق في دراسات التوزيع السكاني، مع دمج تقنيات الذكاء الاصطناعي في التمثيل الكارتوغرافي، كما يقدم البحث دعماً لصناع القرار في التخطيط الحضري والريفي بأدوات تحليلية متقدمة، وتوفير قاعدة بيانات سكانية تفاعلية للجهات الحكومية والباحثين لتسهيل التواصل البصري للمعلومات السكانية مع مختلف الفئات. وتوفير رؤية استشرافية للنمو السكاني حتى عام 2034 للمساهمة في التخطيط الاستراتيجي للتنمية المستدامة، عبر نموذج قابل للتحديث والتوسيع مع توفر بيانات جديدة.

منهجية البحث

1. **المنهج الوصفي:** تحليل البيانات السكانية البيئي(الحضر–الريف) (الذكور–الاناث) للعراق حسب المحافظة، باعتماد الإحصاء السكاني لسنة الأساس (2024).
2. **المنهج الكارتوغرافي:** الترميز الكارتوغرافي البصري المرئي المباشر ثلاثي الأبعاد مع مؤثرات ديناميكية بصرية تعكس الأسلوب البصري في تحليل النتائج وعرضها على الخريطة مباشرة.
3. معادلة النمو السكاني الأسي (UN Formula) $P(t) = P_0 \times e^{(r \times t)}$، P(t) = السكان في السنة المستهدفة، P_0 = السكان في سنة الأساس (2024)، e = ثابت أويلر(2.71828...)، r،K = معدل النمو السنوي (0.023 = 2.3%)، t = الفترة الزمنية بالسنوات (10 سنوات).

4. **تقنيات الترميز الكارتوغرافي** ثلاثي الأبعاد، استخدام CSS 3D Transforms و WebGL لإنشاء رموز تفاعلية.
5. **المنهج الإحصائي**: اعتمد البحث معادلة النمو السكاني الاسية للأمم المتحدة لحساب نمو السكان.*
6. **المنهج التقني**: استخدم البحث نموذج الذكاء الاصطناعي الجغرافي Claude-Opus Deep Thinking-32(**كلاويد – أوبس – تفكير عميق – 32**) لتصميم الخريطة وتحليل البيانات واعداد الرموز. **مما اضفى مميزات** تصميم خرائط تفاعلية وتحليل سكاني متقدم مع توقعات مستقبلية وترميز بصري ثلاثي الأبعاد بحركات تفاعلية اثناء المشاهدة.

1- الترميز الكارتوغرافي المرئي للخرائط:

تم استخدام الخرائط لتوصيل المعلومات الجغرافية منذ آلاف السنين كونها الطريقة الأكثر فعالية لتمثيل الظاهرات الجغرافية بالتفصيل على ورقة أو شاشة حاسوب. ومع التقنيات الجديدة في تكنولوجيا الحاسوب التي اثرت كثيرا على رسم الخرائط. للاستكشاف على نطاق مختلف نوعيًا عما كان ممكنا في السابق نظرًا لمجموعات البيانات المكانية الرقمية الكبيرة. وربما يكون التصور الخرائطي هو الطريقة الوحيدة لتحليلها. (**عمر، الجبوري،118**). بمعنى ان تصميم الخرائط ينبغي ان يبنى على وفق ضوابط وقواعد فنية وعلمية لتكتمل بنية الخريطة كالحجم واللون والرمز والابعاد والمقياس وغيرها. فالعرض البصري هنا أصبح انتقاله من الورقة الى شاشة الحاسوب بشكل تفاعلي مباشر يعكس وضوح الظاهرة الجغرافية وبياناتها. ومن مبادئ التصميم البصري للخرائط اليت نجملها هنا في إشارة الى ضرورة اعتمادها في تصميم ورسم الخرائط على النحو الاتي: (**R. Adam,2020**)

1. **الوضوح** (Clarity): يجب أن تكون الخريطة سهلة الفهم، مع استخدام رموز مألوفة، وحجم نص مناسب، وتجنب الاكتظاظ.
2. **التسلسل الهرمي البصري** (Visual Hierarchy): استخدام الأحجام والألوان والخطوط المتفاوتة لتوجيه عين القارئ إلى المعلومات الأكثر أهمية أولاً (مثل أسماء الدول الكبيرة، ثم المدن).
3. **التباين البصري** (Visual Contrast): زيادة التباين بين المعالم والخلفية لجعلها بارزة، أو تقليله لجعلها تبدو أكثر ترابطًا، مع ضبط الألوان لتجنب الضوضاء البصرية.
4. **البيانات البصرية** (Visual Variables): استخدام خصائص مثل الحجم (رموز الدوائر الأكبر، سمك الخطوط)، اللون، الشكل، والقوام (Texture) لتوصيل معلومات كمية أو تصنيفية.
5. **التوازن** (Balance): توزيع وزن العناصر (حجمها وموقعها) بشكل متساوٍ لضمان استقرار الخريطة.

2- خرائط السكان البيئي (الحضر والريف)

تشمل طرق توزيع الظواهر الجغرافية برموز الموضع الكمية بشكل نقطي منتظم الحجم ومعلوم القيمة، او رمز تتغير مساحته أو حجمه نسبياً حسب القيمة الكمية وهو ما يعرف بطريقة الرموز النسبية(Proportional Symbols) وتعد خرائط السكان البيئي (الحضر والريف–الذكور والاناث) من اكثر الخرائط التي تمثل بياناتها بأسلوب الرموز النسبية في التوزيع الكمي وتشمل الرموز النسبية (الأعمدة البيانية والدوائر والكرات والمكعبات والمثلثات الهرمية وغيرها)، وتكون ذات بعد واحد (الأعمدة) ، أو بعدين مثل الدوائر أو ثلاثة أبعاد كالكرات ، وقد ترسم هذه الرموز النسبية لتبين عدد السكان في التعدادات المختلفة.(**أبو راضي، 2000**،

---

* معادلة الأمم المتحدة للنمو السكاني: $P(t) = P_0 \times e^{(r \times t)}$ معدل النمو السنوي: %2.3https://population.un.org/wpp/

36) اعتمد البحث على بيانات السكان البيئي للعراق حسب التعداد العام للسكان والمساكن لعام2024 .لتمثيلها بالخرائط المرئية التفاعلية برموز ثلاثية الابعاد لادراكها بصرياً بشكل مباشر. مع رؤية مستقبلية لنمو السكان لعام 2034.الجدول(1)

الجدول:1 البيانات السكانية (حضر-ريف-ذكور-اناث) حسب المحافظة/العراق لسنة2024

المحافظة	الحضر		الريف	
	الذكور	الاناث	الذكور	الاناث
دهوك	641,816	631,730	164,148	162,177
نينوى	1,152,285	1,159,328	974,937	975,430
السليمانية	1,076,917	1,060,178	137,799	126,830
كركوك	744,096	751,939	267,665	270,927
اربيل	1,054,964	1,047,671	209,024	205,875
ديالى	512,987	516,698	454,183	450,636
الانبار	579,081	580,321	422,517	422,499
بغداد	4,179,738	4,154,928	725,239	720,524
بابل	566,931	560,963	686,712	667,718
كربلاء	646,519	645,839	232,936	228,771
واسط	524,391	520,712	301,213	297,090
صلاح الدين	431,181	436,113	450,366	456,882
النجف	590,000	590,084	391,453	379,296
القادسية	399,580	399,518	342,318	335,894
المثنى	211,308	210,448	312,455	308,876
ذي قار	859,970	842,978	404,619	391,901
ميسان	506,591	496,676	148,917	142,319

البصرة	1,561,194	1,517,976	295,554	289,444

المصدر: وزارة التخطيط، هيأه الإحصاء ونظم المعلومات الجغرافية، نتائج التعداد العام للسكان والمساكن في العراق2024، النتائج النهائية التجميعية في العراق، 2024، ص:2.

3-نموذج الذكاء الاصطناعي الجغرافي:GeoAI

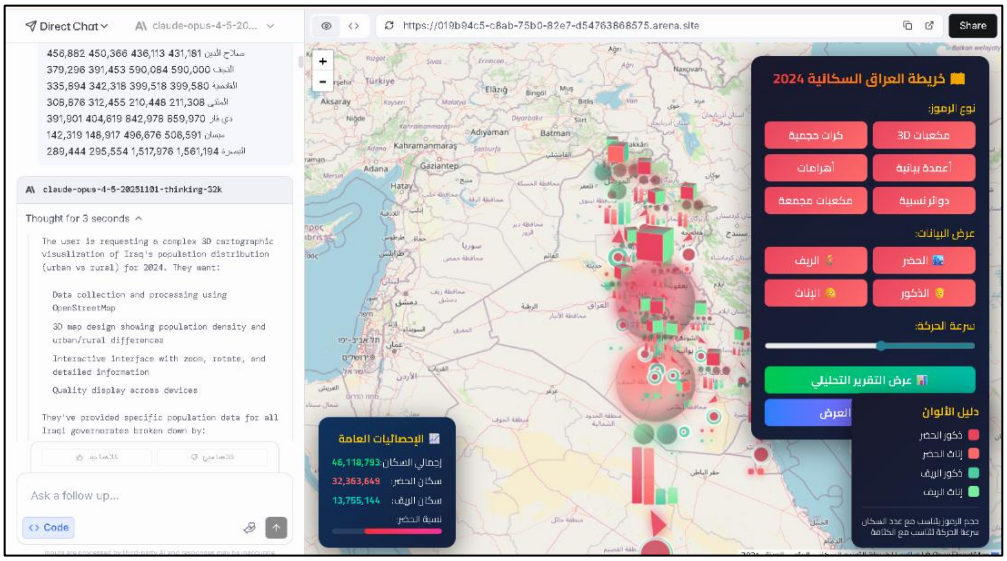
الذكاء الاصطناعي الجغرافي (GeoAI) هو تطبيق ذكاء اصطناعي مدمج مع بيانات الجغرافيا المكانية والعلوم والتكنولوجيا بهدف تحقيق سرعة الفهم في الزمن الحقيقي لفرص الأعمال والتأثيرات البيئية والمخاطر التشغيلية. من خلال توليد بيانات آلية والحصول على أدوات وخوارزميات مكانية قابلة للوصول. لاستخراج بيانات جغرافيا مكانية مع التعلم العميق وأتمتة المعلومات من البيانات وتصنيفها، وإجراء تحليل تنبؤي باستخدام التعلم الآلي لإنشاء نماذج أكثر دقة للكشف عن المجموعات وحساب التغيرات والعثور على الأنماط وتوقع النتائج مع الخوارزميات المكانية. **(esri.com)**. تم استخدام نموذج (Claude-Opus Deep Thinking-32)(كلاويد - أوبس - تفكير عميق – 32)، ابتكره باحثون من جامعة كاليفورنيا في بيركلي، وهي منصة مفتوحة تتيح للجميع الوصول بسهولة إلى نماذج الذكاء الاصطناعي الرائدة عالميًا واستكشافها والتفاعل معها، مما يجعل تقدم الذكاء الاصطناعي أكثر شفافية، وأكثر ارتباطًا بالاستخدام الواقعي.

2- الجانب التطبيقي:

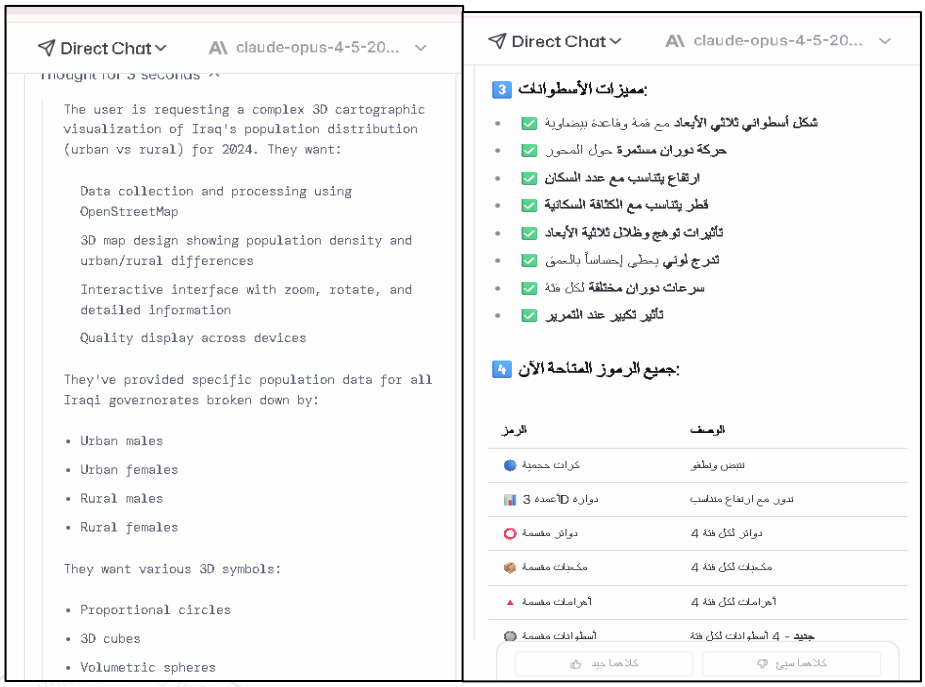
اولاً: تصميم الخريطة وبرمجة الأوامر: تم استخدام أحد نماذج الذكاء الاصطناعي الجغرافي المتخصص في توليد الصور ومواقع الويب التفاعلية والتطبيقات المباشرة وهو (Claude-Opus Deep Thinking-32) تم توليد الامر الذكي (بروميت-Promet) بحسب اهداف البحث بتصميم خريطة تفاعلية للتصميم البصري لرموز متنوعة بالصيغة الاتية:" اعتمد البيانات الاتية: على خريطة الشارع المفتوح بإضافة طبقات رموز الدوائر النسبية والمكعبات ثلاثية الابعاد والكرات الحجمية والاعمدة البيانية ثلاثية الابعاد والمثلثات الهرمية والمكعبات المجمعة بحركات مستمرة تتناسب مع كثافة السكان وحجم الرموز يتناسب مع عدد السكان مع تأثيرات بصرية.

بعدها يتم ادراج نص الامر الذكي في حقل النصوص لنموذج الذكاء الاصطناعي لتوليد الامر وتكوين التطبيق التفاعلي للخريطة التفاعلية، الشكل (1). يتم جمع البيانات ومخطط تفاصيل الخريطة ومعلوماتها وتصميم النوافذ واللوائح للتحكم بالرموز والانتقال بين الازرار. او تعديل وتحديث وتحسين المعلومات حذف او إضافة ليتم توليد الخريطة حسب المعلومات الجديدة. ليتم تنفيذ الامر وتكوين الخريطة ومعلوماتها في تطبيق خلال ثواني معدودة حسب كمية المعلومات المطلوبة من النموذج لتظهر النتائج مباشرة وتكوين الخريطة التفاعلية ومعلوماتها، الشكل (2) ويتم انتاج الخريطة عبر دوال رياضية وكودات خوارزمية مثل (create Grouped Cubes) وتقنية (CSS) ولغة (java Script) إضافة الى الرموز الكارتوغرافية ليتم انتاج ملف (index.html) شامل لمعلومات الخرطة التفاعلية. كما في الشكل (3). بعدها يتم تصدير الملف الى رابط مباشر او ملف يتم استعراضه عبر موقع ويب لتصفح الخريطة التفاعلية كما في الشكل (4)

الشكل:1 توليد الأوامر الذكية لتصميم معلومات الخريطة التفاعلية



الشكل:2 تنفيذ توليد الأوامر عند تحديث المعلومات وتكوين عناصر الخريطة والرموز



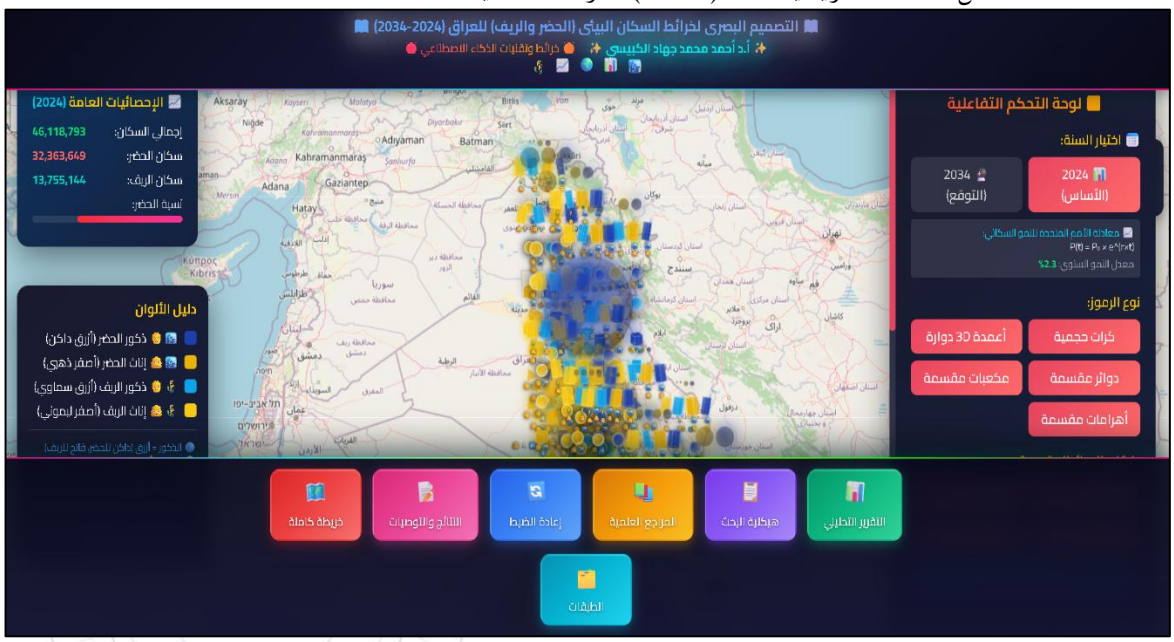
المصدر: عمل الباحث من نموذج الذكاء الاصطناعي

الشكل:3معلومات ملف index.html انتاج الخريطة التفاعلية

```
FILES
index.html

index.html
<!DOCTYPE html>
<html lang="ar" dir="rtl">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>(2034-2024) التصميم البصري لخرائط السكان البيئي (الحضر والريف) للعراق</title>
    <link rel="stylesheet" href="https://unpkg.com/leaflet@1.9.4/dist/leaflet.css" />
    <script src="https://unpkg.com/leaflet@1.9.4/dist/leaflet.js"></script>
    <script src="https://cdn.jsdelivr.net/npm/three@0.160.0/build/three.min.js"></script>
    <script src="https://cdn.jsdelivr.net/npm/@tailwindcss/browser@4"></script>
    <link href="https://fonts.googleapis.com/css2?family=Cairo:wght@400;600;700&display=sw
    <style>
        * { font-family: 'Cairo', sans-serif; }

        #map { width: 100%; height: 100vh; z-index: 1; }

        .leaflet-popup-content { direction: rtl; text-align: right; }

        .symbol-container {
            position: absolute;
            transform-style: preserve-3d;
            perspective: 1000px;
            pointer-events: none;
        }

        /* 3D Cube Animation */
        @keyframes rotateCube {
            0% { transform: rotateX(-20deg) rotateY(0deg); }
            100% { transform: rotateX(-20deg) rotateY(360deg); }
        }

        @keyframes pulse {
            0%, 100% { transform: scale(1); opacity: 0.8; }
            50% { transform: scale(1.1); opacity: 1; }
        }
```

تم توليد الخريطة التفاعلية مع كافة المعلومات والعناصر الأساسية ولوحة ازرار التحكم مع طبقات الرموز المقسمة حسب بيانات السكان (الحضر، الريف،الذكور، الاناث) ومن ثم تحميل الملف بصيغة (HTML) او عبر رابط مباشر. كما في الشكل (4)

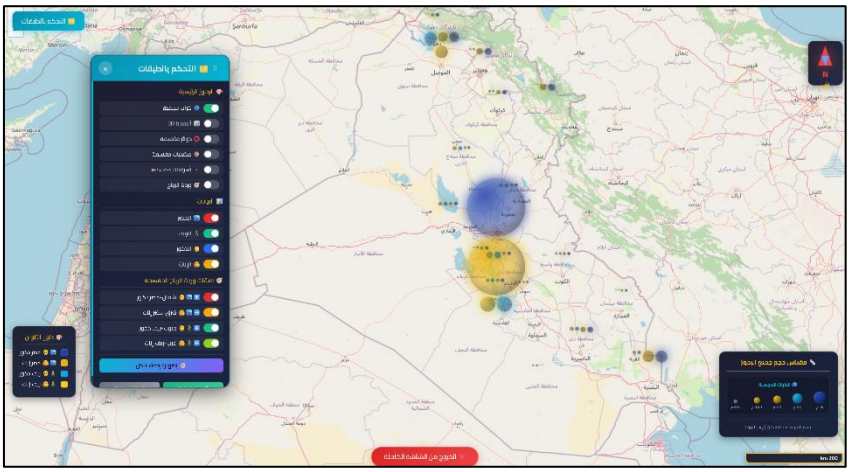
الشكل:4 النافذة الرئيسية لملف (html) الخريطة التفاعلية



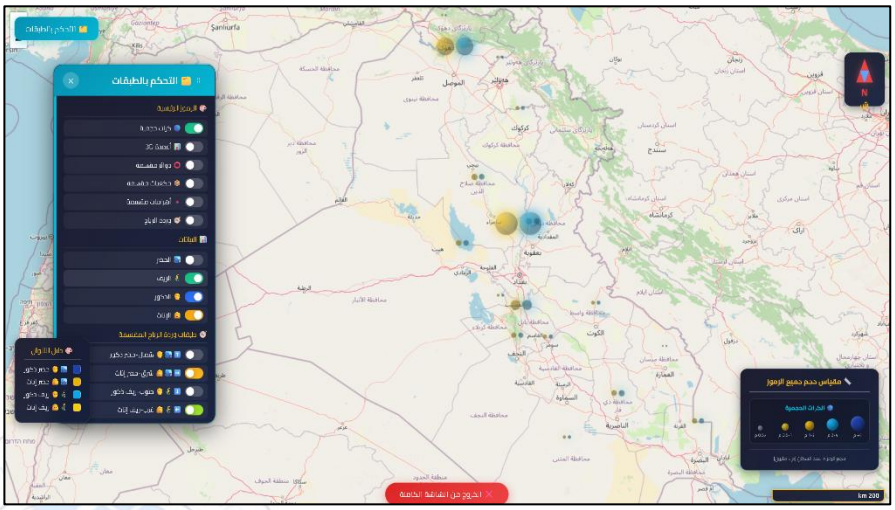
المصدر: عمل الباحث من نموذج الذكاء الاصطناعي.

كما أنتج البحث الخرائط حسب طبقة نوع الرموز:(**كرات حجمية، أعمدة (3D) دوارة، دوائر مقسمة، مكعبات مقسمة، أهرامات مقسمة، وردة الرياح مقسمة**) والتحكم في عرضها بشكل مرئي مباشر وملاحظة قراءة البيانات وإدراك بصري لمتغيرات المؤشرات السكانية البيئية (الحضر والريف) للذكور والاناث حسب المحافظة والمقارنة بين سنة الأساس (2024) وسنة الهدف (2034). وتم إضافة مؤثرات حركة تفاعلية للرموز بدوران مستمر يتناسب سرعته مع كثافة السكان وحجم الرموز يتناسب مع عدد السكان في كل محافظة، مع إمكانية التحكم بإخفاء وإظهار طبقة الرموز كل على حده او جميعها. كما في الخرائط (12.11.10.9.8.7.6.5.4.3.2.1). مع التحكم بسرعة الدوران.

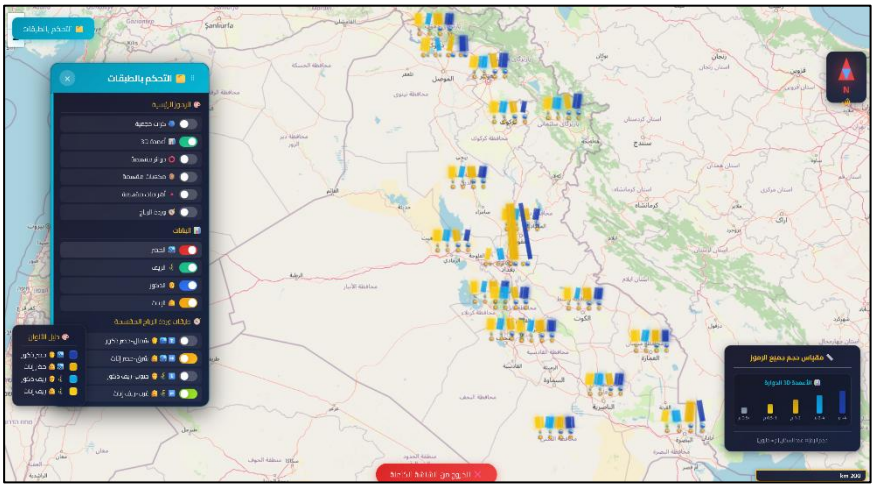
الخريطة:1 رمز الكرات الحجمية البصرية لبيانات السكان لسنة (2024)



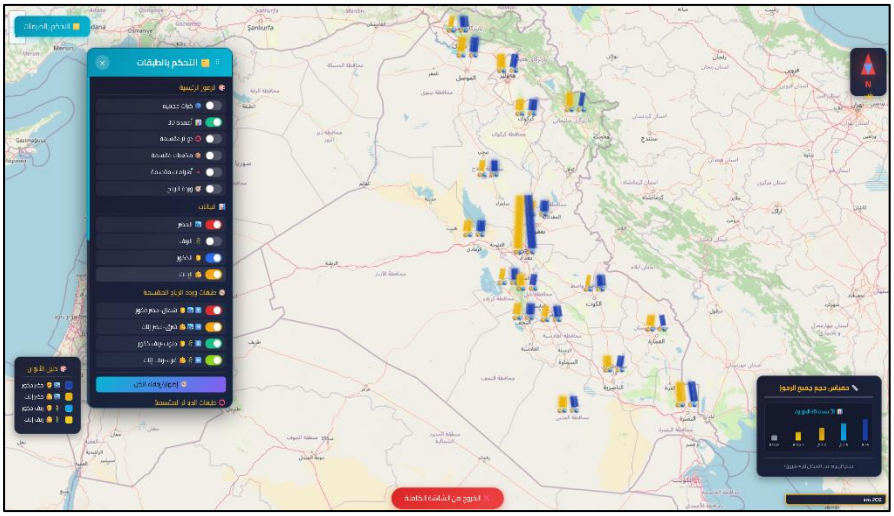
الخريطة:2 رمز الكرات الحجمية البصرية لبيانا ت السكان الريف (ذكور واناث)لسنة 2034



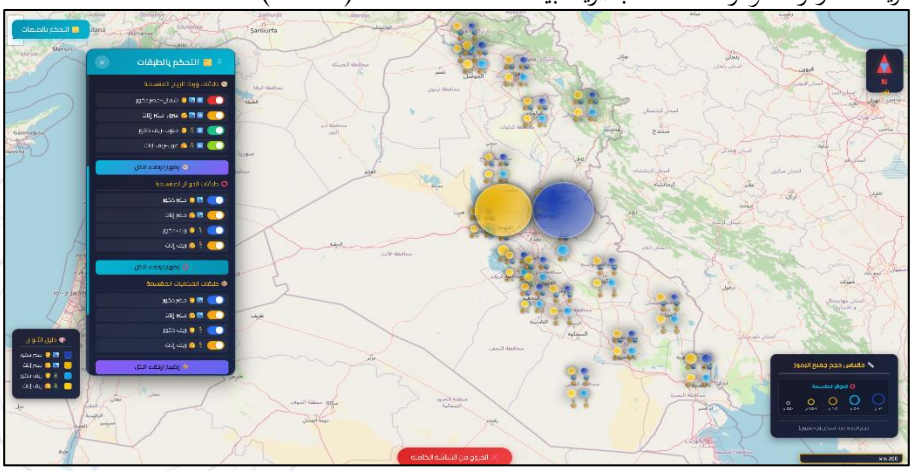
الخريطة:3 رمز الاعمدة البيانية المجسمة البصرية لبيانات السكان لسنة (2024)



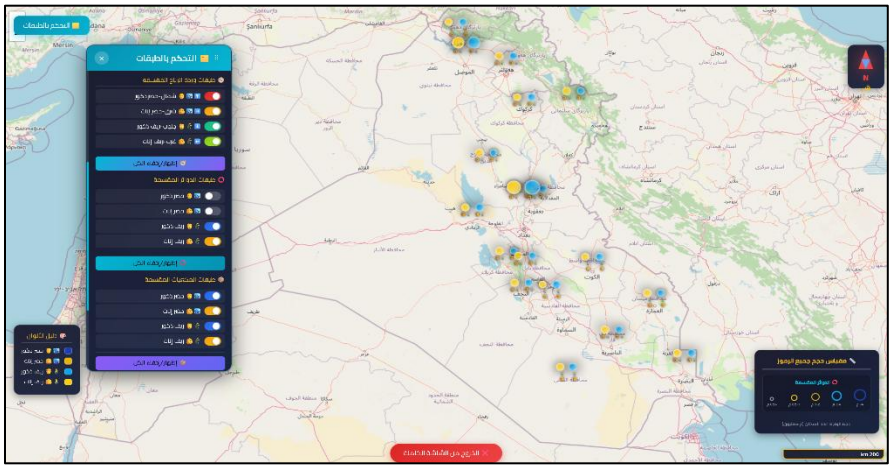
الخريطة:4 رمز الاعمدة البيانية المجسمة البصرية لبيانات السكان الحضر (ذكور اناث) لسنة 2034



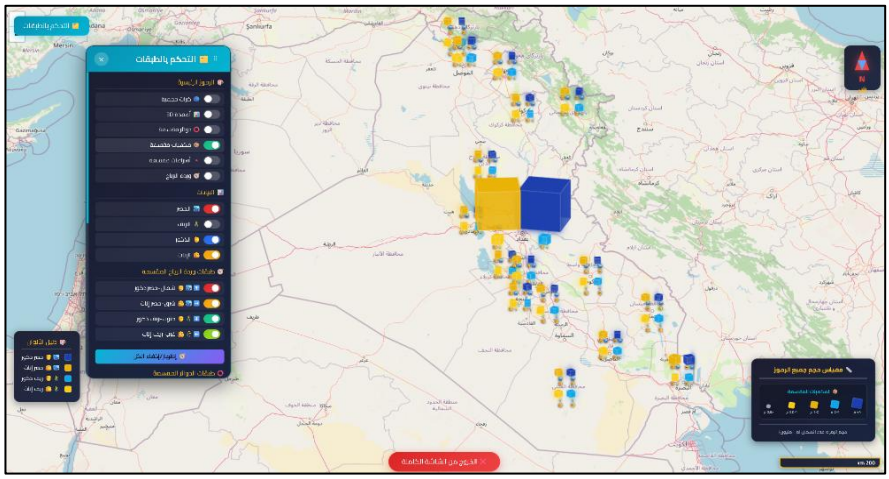
الخريطة:5 رمز الدوائر المقسمة البصرية لبيانات السكان لسنة (2024)



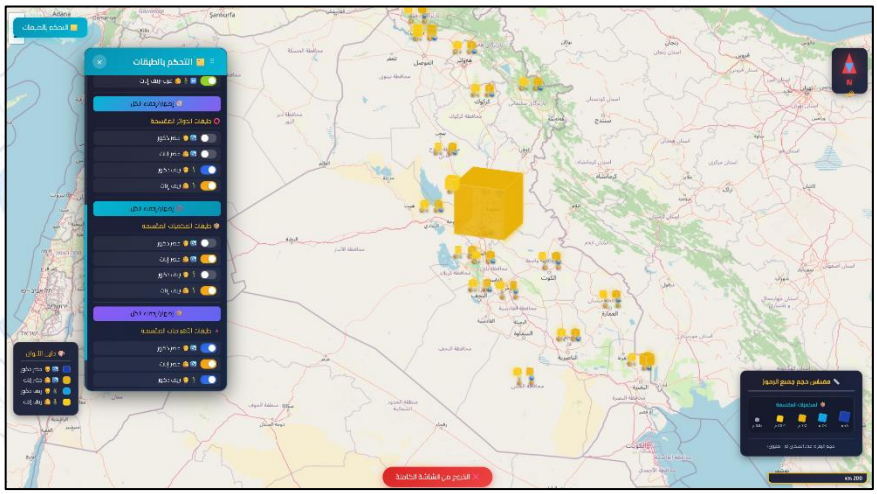
الخريطة:6 رمز الدوائر المقسمة البصرية لبيانات السكان الريف (ذكور واناث) لسنة (2034)



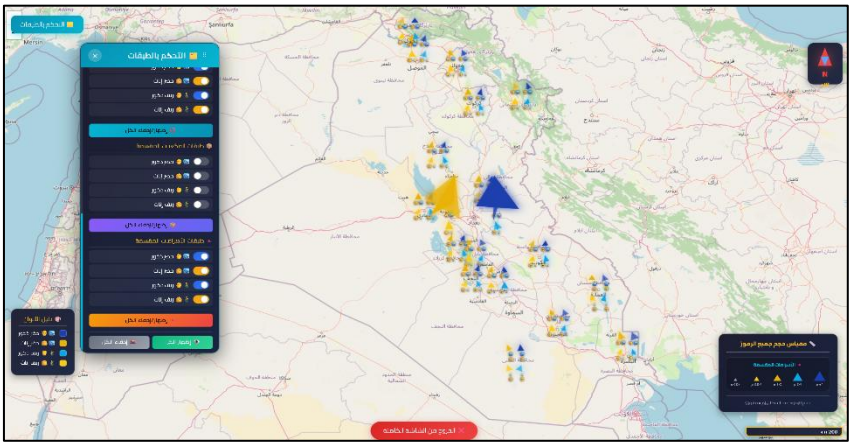
الخريطة:7 رمز المكعبات المقسمة البصرية لبيانات السكان لسنة (2024)



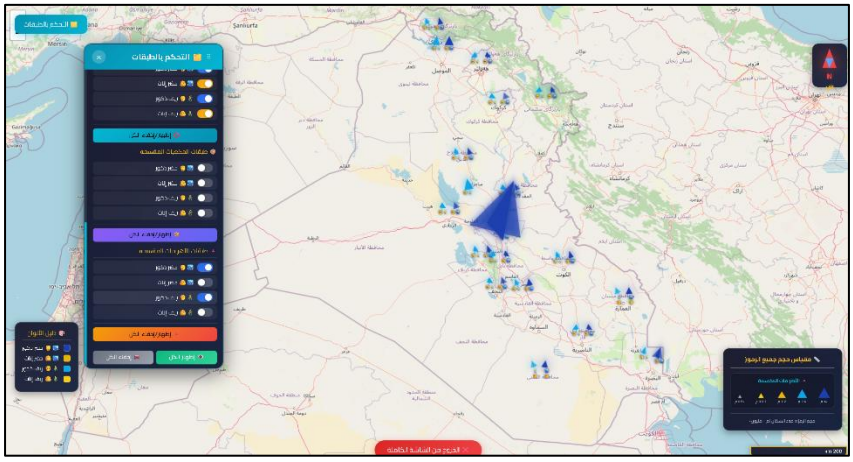
الخريطة 8: رمز المكعبات المقسمة البصرية لبيانات السكان الريف (ذكور واناث) لسنة (2034)



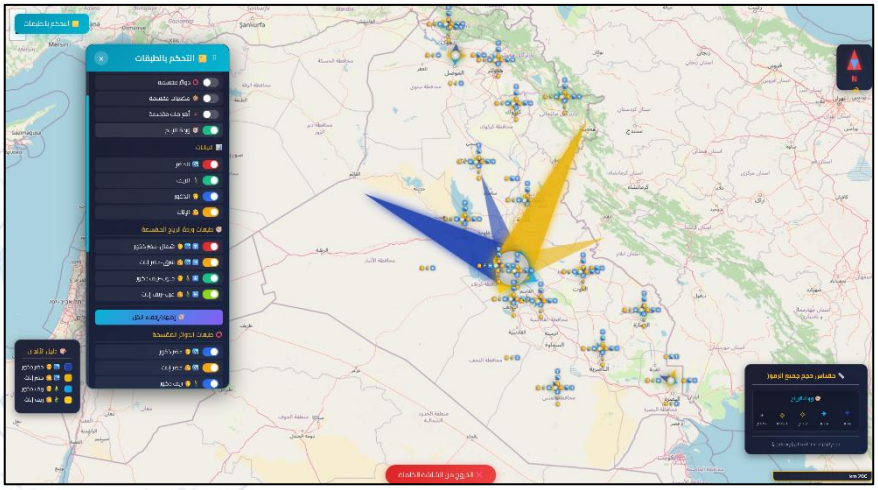
الخريطة:9رمز المثلثات الهرمية المقسمة البصرية لبيانات السكان لسنة (2024)



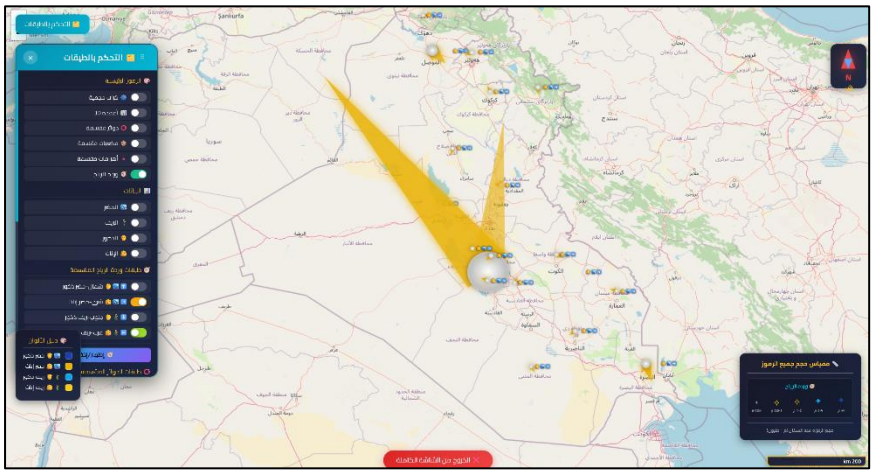
الخريطة:10رمز المثلثات الهرمية المقسمة البصرية لبيانات السكان لسنة (2034)



الخريطة11: رمز وردة الرياح المقسمة البصرية لبيانات السكان لسنة (2024)



الخريطة12: رمز وردة الرياح المقسمة البصرية لبيانات السكان الحضر (اناث) لسنة (2034)



تم اضافة بيانات الباحث ومعلومات البحث مثل: التقرير التحليلي، هيكلية البحث، وغيرها كما في الشكل (5).

الشكل 5: بيانات البحث في التطبيق

كما تم عرض دليل الألوان : 👴🏙️ ذكور الحضر (أحمر)، 👵🏙️ إناث الحضر (برتقالي)، 👴🌾 ذكور الريف (أخضر)، 👵🌾 إناث الريف (ليموني) ، 🔴 الحضر = أحمر/برتقالي ، 🟢 الريف = أخضر/ليموني، 🔵 الذكور = درجات

داكنة، الإناث = درجات فاتحة. وحجم الرموز يتناسب مع عدد السكان. إضافة الى لوحة الإحصاءات العامة حسب السنة إجمالي السكان:(46,118,793)، سكان الحضر:(32,363,649)، سكان الريف:(13,755,144) ونسبة الحضر. كما في الشكل (6) ولوحة التحكم التفاعلية في الشكل (7). كذلك يمكن عرض مقياس حجم الرموز الى خمس فئات لكل رمز عند عرضه على الخريطة التفاعلية كما في الشكل (8).

الشكل 6: لوحة الإحصاءات العامة ودليل الألوان ولوحة التحكم

الشكل 7: لوحة التحكم التفاعلية لطبقات الرموز

إضافة ميزة عرض البيانات التفصيلية السكانية لكل محافظة عند الإشارة لها على الخريطة بشكل تفاعلي مباشر. كما في الشكل (9)

الشكل9: عرض البيانات السكانية التفصيلية حسب المحافظة على الخريطة التفاعلية

ثانياً التقرير التحليلي الشامل:

مقارنة 2024 – 2034 (2024) عدد السكان في سنة الأساس (46,118,793) النمو(25.9%) . يقدر عدد السكان لسنة (2034) (58,045,111) حسب معادلة الأمم المتحدة(r×t)^e × Po = P(t) : والزيادة المتوقعة 11,926,318+ :نسمة. ملخص البيانات – 2024 إجمالي السكان: 46,118,793، عدد المحافظات8 1: سكان الحضر (32,363,649)،(70.2%) ، سكان الريف: (13,755,144) (29.8%). بينما أكبر 5 محافظات من حيث السكان هي على النحو الاتي: .1بغداد9,780,429 ، .2نينوى4,261,980، .3البصرة3,664,168 ، .4 أربيل2,517,534 .5ذي قار2,499,468. وأعلى نسب التحضر كانت في .1السليمانية89.0% ، .2بغداد85.2% ، .3البصرة84.0%، .4أربيل83.5% .5دهوك79.6%، بينما أعلى نسب الريف: في .1المثنى59.6%، .2 بابل54.6%، .3صلاح الدين51.1%، .4ديالى46.8% ، .5القادسية45.9%.

اما تحليل النوع الاجتماعي: فقد بلغ الذكور (إجمالي): (23,161,604) الإناث (إجمالي):(22,957,189) نسبة الذكور إلى الإناث: 100.9%. في حين ان توقعات النمو بالمحافظات(2034 ← 2024) حسب الاتي:

1. دهوك1,599,871→2,013,598+413,727
2. نينوى4,261,980→5,364,128+1,102,148
3. السليمانية2,401,724→3,022,810+621,086
4. كركوك2,034,627→2,560,781+526,154
5. أربيل2,517,534→3,168,569+651,035
6. ديالى1,934,504→2,434,766+500,262
7. الأنبار2,004,418→2,522,760+518,342

8. بغداد9,780,429→12,309,648+2,529,219
9. بابل2,482,324→3,124,253+641,929
10. كربلاء1,754,065→2,207,666+453,601
11. واسط1,643,406→2,068,391+424,985
12. صلاح الدين1,774,542→2,233,439+458,897
13. النجف1,950,833→2,455,319+504,486
14. القادسية1,477,310→1,859,341+382,031
15. المثنى1,043,087→1,312,829+269,742
16. ذي قار2,499,468→3,145,830+646,362
17. ميسان1,294,503→1,629,261+334,758
18. البصرة3,664,168→4,611,722+947,554

اظهر التحليل بشكل رئيسي: ان بغداد هي المحافظة الأكثر اكتظاظاً بالسكان مع تركز حضري عالي المحافظات الجنوبية تميل إلى نسب ريفية أعلى، وإقليم كردستان يتميز بتوازن نسبي بين الحضر والريف، بلغت نسبة التحضر الإجمالية في العراق: 70.2%، وكان التوازن بين الجنسين متقارب في معظم المحافظات، في حين ان التوقع كان بزيادة تقدر 25.9% بحلول 2034، ومعدل النمو السنوي: 2.3% (**معادلة الأمم المتحدة**)

النتائج والتوصيات:

1. التوزيع السكاني غير المتوازن، تتركز نسبة كبيرة من السكان في بغداد والبصرة ونينوى، بينما تعاني المحافظات الجنوبية والغربية من انخفاض الكثافة السكانية.

2. ارتفاع نسبة التحضر، تبلغ نسبة سكان الحضر حوالي 70% من إجمالي السكان، مما يشير إلى هجرة مستمرة من الريف إلى المدن.

3. التوازن النسبي بين الجنسين، نسبة الذكور إلى الإناث متقاربة في معظم المحافظات مع فارق طفيف لصالح الذكور.

4. النمو السكاني المتوقع، بناءً على معادلة الأمم المتحدة، يُتوقع زيادة السكان بنسبة 25.86% بحلول عام 2034.

5. فعالية الترميز ثلاثي الأبعاد، أثبتت تقنيات الترميز الكارتوغرافي ثلاثي الأبعاد فعاليتها في تمثيل البيانات السكانية المعقدة بشكل مرئي واضح.

6. التباين البيئي الواضح، إقليم كردستان يتميز بنسبة تحضر عالية، بينما المحافظات الجنوبية كالمثنى وذي قار تحتفظ بنسب ريفية مرتفعة.

التوصيات

1. توسيع استخدام تقنيات الترميز ثلاثي الأبعاد في دراسات التوزيع السكاني العربية.
2. تطوير نماذج تنبؤية أكثر دقة تأخذ بعين الاعتبار العوامل الاقتصادية والاجتماعية.
3. إجراء دراسات مقارنة مع دول المنطقة لفهم أنماط التحضر.
4. وضع خطط تنموية متوازنة للحد من الهجرة الريفية–الحضرية.
5. تطوير البنية التحتية في المناطق الريفية لتحسين جودة الحياة.
6. استخدام الخرائط التفاعلية كأداة للتخطيط الحضري والإقليمي.

7. الاستعداد للنمو السكاني المتوقع بتوسيع الخدمات الأساسية.
8. دمج تقنيات الواقع المعزز (AR) لتحسين تجربة المستخدم.
9. تطوير تطبيقات محمولة لعرض البيانات السكانية الجغرافية.
10. ربط النظام بقواعد بيانات حكومية للتحديث التلقائي.

الخلاصة

أثبتت هذه الدراسة فعالية استخدام تقنيات الترميز الكارتوغرافي ثلاثي الأبعاد والتفاعلي في تمثيل التوزيع السكاني البيئي للعراق. النظام المُطوَّر يوفر أداة تحليلية قوية لفهم الديناميكيات السكانية بين الحضر والريف، ويُمكّن من التنبؤ بالتغيرات السكانية المستقبلية باستخدام معادلة النمو السكاني للأمم المتحدة. يُوصى بتوسيع استخدام هذه التقنيات في مجالات التخطيط الحضري والتنمية المستدامة.

آفاق الدراسات المستقبلية

1. **التغير المناخي**: دراسة تأثير التغير المناخي على التوزيع السكاني
2. **الهجرة الاقتصادية**: تحليل أنماط الهجرة بسبب العوامل الاقتصادية
3. **الخدمات الصحية**: ربط التوزيع السكاني بالخدمات الصحية
4. **التعليم**: خرائط توزيع المؤسسات التعليمية

المراجع:

أبو راضي، فتحي عزيز أبو عيانة، (2000)، خرائط التوزيعات البشرية ورسومها البيانية دار النهضة العربية للنشر والتوزيع، بيروت.

عمر، مضر خليل الجبوري، فؤاد عبد الله، (ب.س) الجغرافيا على المحك – الباب الرابع – الفصل الحادي عشر ترجمة بتصرف، رسم الخرائط والعرض البصري، سكوت أورفورد. https://www.muthar-alomar.com/wp-content/uploads/2023/0

https://population.un.org/wpp/ ,$P(t) = P_0 \times e^{(r \times t)}$

https://unhabitat.org/iraq

https://www.esri.com/ar-sa/capabilities/geoai/overview

***R. Adam**,(2020),Geographic Information Technologies Copyright Dastrup, MA, GISP is licensed under a Creative Commons Attribution 4.0 International License, except where otherwise noted.*

***United** Nations,2024, Population Division, World Population Prospects - Iraq Demographics*

***World** Bank - Iraq Data, Population Statistics and Urban-Rural Distribution,https://data.worldbank.org/country/iraq*

UNFPA Iraqصندوق الأمم المتحدة للسكان ، Iraq Population Situation Analysis 2023-2024 ، https://iraq.unfpa.org

هيئة إحصاء إقليم كردستان، التقارير السكانية لمحافظات الإقليم، https://krso.gov.krd

وزارة التخطيط العراقية،2024، هيأة الإحصاء ونظم المعلومات الجغرافية، بيانات التعداد العام للسكان والمساكن. https://cosit.gov.iq

وزارة التخطيط، 2022، خطة التنمية الوطنية 2018-2022 والمؤشرات السكانية، https://mop.gov.iq

مصادر البيانات الجغرافية

Leaflet.js ، مكتبة JavaScript للخرائط التفاعلية،https://leafletjs.com، *Natural Earth Data* ، بيانات جغرافية مفتوحة المصدر،https://www.naturalearthdata.com

OpenStreetMap (OSM) ، خرائط الأساس والحدود الإدارية للعراق،https://www.openstreetmap.org

بسم الله الرحمن الرحيم

فاعلية توظيف تقنيات الذكاء الاصطناعي في حماية أنظمة الامتحانات الإلكترونية من الاختراقات السيبرانية بالجامعات السودانية أثناء الأزمات التعليمية

(دراسة وصفية من وجهة نظر مشرفي انظمة إدارة التعلم الإلكتروني بالجامعات السودانية)

The Effectiveness of Artificial Intelligence Technologies in Protecting E-Examination Systems from Cyber Breaches in Sudanese Universities During Educational Crises: A Descriptive Study Based on LMS Supervisors' Perspectives

إعداد:

د. محمد علي عيسى موسى

أستاذ تكنولوجيا التعليم المساعد

كلية التربية – جامعة أم درمان الإسلامية

mohamedali@oiu.edu.sd

د. حسن الفاتح الحسين محمدالمبارك

أستاذ تكنولوجيا التعليم المشارك بكلية التربية

جامعة القران الكريم تأصيل والعلوم

Hsnf313@gm@il.com

مستخلص

هدفت هذه الدِّراسة إلى الكشف عن واقع توظيف تقنيات الذكاء الاصطناعي في حماية أنظمة الامتحانات الإلكترونية من الاختراقات السيبرانية في الجامعات السودانية أثناء الأزمات التعليمية، والتعرف على أبرز التحديات التي تعيق هذا التوظيف، إضافة إلى تقصّي مستوى فاعليته. اتبع الباحث المنهج الوصفي التحليلي لملاءمته لطبيعة الدراسة، حيث يتيح وصف الظاهرة كما هي في الواقع وتحليلها للوصول إلى استنتاجات علمية تسهم في تطوير الممارسات التعليمية.

تكون مجتمع الدِّراسة من جميع مشرفي أنظمة إدارة التعلم الإلكتروني بالجامعات السودانية، بينما اقتصرت العينة على (75) مشرفًا تم اختيارهم قصدياً. وتمثلت أداة الدِّراسة في استبانة مكونة من (12) عبارة موزعة على ثلاثة محاور (الواقع – المعوقات – الفاعلية)، جرى التحقق من صدقها وثباتها باستخدام الصدق الظاهري ومعامل كرونباخ ألفا، حيث بلغت قيمته لجميع المحاور أكثر من (0.96)، مما يؤكد قوة الاتساق الداخلي وموثوقية الأداة.

أظهرت النتائج أن مستوى توظيف تقنيات الذكاء الاصطناعي في حماية أنظمة الامتحانات الإلكترونية بالجامعات السودانية جاء متوسطًا (61%)، مع وجود تباين ملحوظ في آراء المشاركين. كما بينت النتائج أن أبرز التحديات تمثلت في نقص الكوادر المؤهلة (بمتوسط 4.12) وضعف البنية التحتية التقنية (بمتوسط 4.07). أما فيما يتعلق بالفاعلية، فقد أظهرت النتائج اتجاهًا إيجابيًا، حيث حصلت عبارة تقليل وقت الاستجابة للهجمات على أعلى متوسط.(3.56)

خلصت الدِّراسة إلى أن توظيف الذكاء الاصطناعي في الجامعات السودانية ما زال في مستوى متوسط، ويواجه عقبات جوهرية تحد من فاعليته رغم قناعة المشرفين بأهميته في تعزيز أمن الامتحانات الإلكترونية. وأوصت الدِّراسة بضرورة تعزيز البنية التحتية التقنية، وتطوير خطط دورية لتحديث الأنظمة، وتأهيل الكوادر البشرية، إلى جانب تعزيز الوعي الرقمي والأمني والتعاون بين الجامعات ومراكز البحوث لتطوير حلول مبتكرة في مجال أمن الامتحانات الإلكترونية

الكلمات المفتاحية: الفاعلية – تقنيات الذكاء الاصطناعي – انظمة الامتحانات الإلكترونية – اختراقات السيبرانية – مشرفي انظمة التعلم الإلكتروني.

Abstract

This study aimed to explore the current status of employing artificial intelligence (AI) technologies in protecting electronic examination (e-examination) systems from cyber breaches in Sudanese universities during educational crises, identify the most prominent challenges hindering such employment, and investigate its level of effectiveness. The researcher adopted the descriptive-analytical

approach, which was suitable for the nature of the study as it allows for describing the phenomenon as it exists in reality and analyzing it to reach scientific conclusions that contribute to the development of educational practices. The study population consisted of all Learning Management System (LMS) supervisors in Sudanese universities, while the sample was purposively selected and comprised (75) supervisors. The study instrument was a questionnaire consisting of (12) items distributed across three dimensions (current status – challenges – effectiveness). The validity and reliability of the instrument were verified using face validity and Cronbach's alpha coefficient, which exceeded (0.96) for all dimensions, confirming strong internal consistency and high reliability.

The results revealed that the level of employing AI technologies in securing e-examination systems in Sudanese universities was moderate (61%), with notable variations in participants' responses. The results also indicated that the most prominent challenges were the shortage of qualified personnel (mean = 4.12) and weak technical infrastructure (mean = 4.07). Regarding effectiveness, the results showed a positive trend, with the item "reducing response time to attacks" achieving the highest mean (3.56).

The study concluded that the employment of AI in Sudanese universities remains at a moderate level and faces substantial barriers that limit its effectiveness, despite supervisors' strong belief in its importance for enhancing e-examination security. The study recommended strengthening technical infrastructure, developing periodic plans for system updates, training and qualifying human resources, promoting digital and cybersecurity awareness, and fostering collaboration between universities and research centers to develop innovative solutions in the field of e-examination security.

Keywords: Effectiveness – Artificial Intelligence (AI) Technologies – E-Examination Systems – Cyber Breaches – Cybersecurity – Learning Management System (LMS) Supervisors – Sudanese Universities – Educational Crises

1. الإطار العام

1.1. مقدمة:

يشهد العصر الراهن تحولاً جذرياً في النظم التعليمية على مستوى العالم، حيث أصبح التعلم الإلكتروني حجر الزاوية في استمرارية العملية التعليمية، خاصة في مراحل التعليم العالي .وتأتي أنظمة الامتحانات الإلكترونية كأحد أهم ركائز هذا التحول، كونها الأداة الرئيسية لتقييم مخرجات التعلم وضمان جودتها. ومع التسارع الكبير في اعتماد هذه الأنظمة في الجامعات السودانية، برزت تحديات جسام على رأسها تهديدات الأمن السيبراني التي تستهدف سلامة ونزاهة هذه الامتحانات.

فالاختراقات السيبرانية، بدءاً من هجمات الحرمان من الخدمة (DDoS) التي تعطل توفر النظام، مروراً بمحاولات اختراق الخوادم وسرقة البيانات، ووصولاً إلى انتحال الهوية والغش الإلكتروني، تمثل خطراً داهماً يهدد مصداقية المؤسسات الأكاديمية برمتها. وفي مواجهة هذه التهديدات المتطورة، لم تعد الحلول الأمنية التقليدية كافية، مما دفع إلى البحث عن تقنيات أكثر ذكاءً وقدرة على التكيف والاستباقية.

وفي هذا الإطار، يبرز الذكاء الاصطناعي (AI) كمنقذ محتمل، حيث تقدم تقنياته، مثل التعلم الآلي (Machine Learning) والتحليلات التنبؤية (Predictive Analytics) ، آليات غير مسبوقة للكشف عن الأنماط غير الطبيعية والشاذة، وتحديد محاولات الاختراق في الوقت الفعلي، ومنع حالات الغش قبل حدوثها. إذ يمكن لهذه التقنيات تحليل كميات هائلة من البيانات السلوكية واللوجستية لتحديد أي نشاط مشبوه، مما يضفي طبقة أمنية ذكية وديناميكية.

ومع ذلك، فإن نجاح وفعالية توظيف هذه التقنيات المتقدمة مرهونان بعامل بشري بالغ الأهمية، ألا وهم مشرفو أنظمة إدارة التعلم الإلكتروني، الذين يشكلون خط الدفاع الأول ويمتلكون الخبرة المباشرة في إدارة هذه الأنظمة وتقييم مخاطرها. لذا، تهدف هذه الدراسة الوصفية إلى تقييم فاعلية توظيف تقنيات الذكاء الاصطناعي في حماية أنظمة الامتحانات الإلكترونية من الاختراقات السيبرانية من خلال استقصاء وجهات نظر هذه الفئة المحورية في الجامعات السودانية، سعياً لتقديم صورة واقعية تمهد لوضع إطار استراتيجي فعال يضمن نزاهة وأمن البيئة التقييمية الإلكترونية.

2.1. مشكلة الدِّراسة:

على الرغم من التبني المتسارع لأنظمة الامتحانات الإلكترونية في الجامعات السودانية كضرورة حتمية لمواكبة التحول الرقمي، فإن هذه الأنظمة تواجه تهديدات سيبرانية متطورة ومستمرة تهدد نزاهتها وأمنها. وتكمن المشكلة الجوهرية في أن الإجراءات الأمنية التقليدية أصبحت غير كافية لمواجهة تعقيد هذه التهديدات، مما يستدعي اللجوء إلى حلول أكثر ذكاءً كتقنيات الذكاء الاصطناعي.

غير أن تطبيق هذه التقنيات في هذا السياق المحدد يواجه حالة من عدم اليقين؛ حيث لا تزال هناك فجوة معرفية تتعلق بمدى فعالية هذه التقنيات فعلياً في اكتشاف ومنع الاختراقات الخاصة بالامتحانات الإلكترونية في البيئة السودانية. كما أن هناك نقصاً في الدراسات التي تقيس هذا التوظيف من وجهة نظر الممارسين

المباشرين الذين يتحملون مسؤولية تشغيل هذه الأنظمة وحمايتها على أرض الواقع، وهم مشرفو أنظمة إدارة التعلم الإلكتروني.

لذا، يمكن تحديد مشكلة هذه الدراسة في التساؤل الرئيس التالي:

ما مدى فاعلية توظيف تقنيات الذكاء الاصطناعي في حماية أنظمة الامتحانات الإلكترونية من الاختراقات السيبرانية في الجامعات السودانية أثناء الأزمات التعليمية من وجهة نظر مشرفي أنظمة إدارة التعلم الإلكتروني؟

وانبثاقاً من هذه المشكلة، تسعى الدراسة إلى الإجابة عن هذا التساؤل من خلال تقييم الواقع الفعلي، وتحديد التحديات، واستكشاف الفرص، مما يسد فجوة مهمة في الأدب المحلي ويقدم توصيات قائمة على رؤى ميدانية عملية.

3.1. أهمية الدِّراسة:

تنبع أهمية هذه الدراسة من خلال المساهمات المتوقعة التي تقدمها على ثلاثة مستويات رئيسة يمكن تصنيفها كالتالي:

1.3.1. الأهمية النظرية والعلمية:

ستساهم هذه الدراسة في إثراء الحقل المعرفي لمجالي الأمن السيبراني والتعليم الإلكتروني من خلال:

أ. **سد فجوة بحثية:** تغطية النقص في الأدبيات والدراسات المحلية والعربية التي تتناول تقاطع تقنيات الذكاء الاصطناعي مع أمن أنظمة التقييم الإلكتروني، خاصة في بيئة الجامعات السودانية.

ب. **تطوير نموذج نظري:** تقديم إطار نظري متكامل يربط بين متطلبات حماية أنظمة الامتحانات الإلكترونية وإمكانات تقنيات الذكاء الاصطناعي في تلبيتها، مما يمهد لدراسات مستقبلية أعمق.

ت. **توفير قاعدة بيانية:** ستكون نتائج هذه الدراسة مرجعاً أساسياً للباحثين المهتمين بتطبيقات الذكاء الاصطناعي في القطاع التعليمي، وخاصة في مجال تأمين العمليات الأكاديمية الحرجة.

2.3.1. الأهمية العملية والتطبيقية:

تكمن الأهمية العملية المباشرة للدراسة في تقديم فوائد ملموسة للمستفيدين الرئيسيين في الميدان، وهم:

أ. **مشرفي أنظمة إدارة التعلم الإلكتروني:** من خلال تزويدهم بتقييم واقعي لفاعلية تقنيات الذكاء الاصطناعي، مما يمكنهم من اتخاذ قرارات مستنيرة بشأن تبني هذه التقنيات أو تحسينها، ووضع خطط أمنية استباقية أكثر فعالية.

ب. **وحدات التقنية بالجامعات السودانية:** ستقدم الدراسة توصيات عملية يمكن أن توجه سياسات واستراتيجيات الأمن السيبراني على مستوى الجامعات، وتساعد في تحديد أولويات الاستثمار في التقنيات الذكية التي تحقق أعلى مردود أمني.

ت. **لشركات تطوير أنظمة التعليم الإلكتروني:** يمكن أن تفيد النتائج المطورين في تصميم أنظمة امتحانات إلكترونية أكثر أماناً من خلال دمج مزايا الذكاء الاصطناعي التي أثبتت الدراسة فعاليتها من وجهة نظر المستخدم النهائي.

4.3.1.الأهمية الاجتماعية والمؤسسية:

تساهم الدراسة على مستوى أوسع في تعزيز قيم النزاهة والمصداقية في البيئة الأكاديمية من خلال:

أ. **حماية قيمة الشهادة الجامعية:** المساهمة في ضمان نزاهة عمليات التقييم، مما ينعكس إيجاباً على مصداقية مخرجات التعليم العالي السوداني وسمعته محلياً وعالمياً.

ب. **بناء الثقة الرقمية:** تعزيز ثقة الطلاب وأعضاء هيئة التدريس والمجتمع ككل بجدوى وعدالة الأنظمة التعليمية الإلكترونية، مما يشجع على تبنيها وتطويرها بشكل أوسع.

ت. **دعم متخذي القرار:** تزويد صانعي السياسات التعليمية في وزارة التعليم العالي والجهات المنظمة بأدلة ميدانية حول ضرورة وأهمية تبني حلول أمنية متطورة، مما يدعم التخطيط الاستراتيجي على المستوى القومي

4.1. أهداف الدِّراسة:

1.4.1 الهدف العام للدراسة:

تهدف هذه الدراسة إلى التعرف على واقع وفاعلية توظيف تقنيات الذكاء الاصطناعي في حماية أنظمة الامتحانات الإلكترونية من الاختراقات السيبرانية بالجامعات السودانية، والكشف عن التحديات والمعوقات التي تواجه هذا التوظيف من وجهة نظر مشرفي أنظمة إدارة التعلم الإلكتروني.

2.4.1. الأهداف الخاصة (الإجرائية):

1.2.4.1. تحليل واقع توظيف تقنيات الذكاء الاصطناعي في مواجهة الاختراقات السيبرانية لأنظمة الامتحانات الإلكترونية بالجامعات السودانية، من حيث مدى انتشارها وأنماط استخدامها.

4.1. 2.2. تقييم فاعلية توظيف تقنيات الذكاء الاصطناعي (من وجهة نظر المشرفين) في تحقيق أمن أنظمة الامتحانات الإلكترونية، بناءً على معايير مثل: قدرتها على الكشف، السرعة، الدقة، والوقاية من الاختراقات.

3.2.4.1. تحديد أبرز التحديات والمعوقات (التقنية، المالية، البشرية، التنظيمية) التي تحد من توظيف فعال لتقنيات الذكاء الاصطناعي في هذا المجال.

5.1. أسئلة الدِّراسة:

1.5.1. ما واقع توظيف تقنيات الذكاء الاصطناعي في حماية أنظمة الامتحانات الإلكترونية من الاختراقات السيبرانية بالجامعات السودانية؟

2.5.1. ما تحديات ومعوقات توظيف تقنيات الذكاء الاصطناعي في حماية أنظمة الامتحانات الإلكترونية من الاختراقات السيبرانية بالجامعات السودانية؟

3.5.1. ما فاعلية توظيف تقنيات الذكاء الاصطناعي في حماية أنظمة الامتحانات الإلكترونية من الاختراقات السيبرانية بالجامعات السودانية؟

6.1. حدود الدِّراسة: تتمثل في:

1.6.1. الحدود الموضوعية:

تتمثل ما مدى فاعلية توظيف تقنيات الذكاء الاصطناعي في حماية أنظمة الامتحانات الإلكترونية من الاختراقات السيبرانية بالجامعات السودانية أثناء الازمات من وجهة نظر مشرفي انظمة إدارة التعلم الإلكتروني؟

2.6.1. الحدود الزمنية: ينظر إلى هذه الدِّراسة وما تلخص عنها من نتائج في الفترة الزمنية الممتدة من (2024 – 2025م).

3.6.1. الحدود المكانية: جمهورية السودان.

4.6.1. الحدود البشرية: مشرفي أنظمة إدارة التعلم الإلكتروني بالجامعات السودانية.

7.1.التعريف الإجرائي لمصطلحات الدِّراسة:

1.7.1. الفاعلية: قدرة هذه التقنيات على تحقيق الأهداف الأمنية المرجوة منها، والتي يتم قياسها عملياً من خلال: درجة الكشف عن الاختراقات، وسرعة الاستجابة لها، والدقة في تمييز التهديدات الحقيقية من الإنذارات الكاذبة، والوقاية من حدوث الاختراقات مستقبلاً، وذلك من خلال تقييم وجهة نظر مشرفي الأنظمة.

2.7.1 تقنيات الذكاء اللإصطناعي: يقصد بتقنيات الذكاء الاصطناعي في هذه الدراسة :مجموعة من النماذج والخوارزميات الحاسوبية المتقدمة القادرة على محاكاة الذكاء البشري في التعلم والتحليل واتخاذ القرارات، والتي يتم توظيفها لاكتشاف والاستجابة للتهديدات السيبرانية المستهدفة لأنظمة الامتحانات الإلكترونية بشكل استباقي وذكي

3.7.1. انظمة الامتحانات الإلكترونية: هي منظومة برمجية متكاملة ضمن بيئة التعلم الإلكتروني مثل (Moodle)، (Blackboard) مخصصة لإدارة دورة التقييم الإلكتروني بالكامل، بدءاً من إنشاء الاختبار وتنفيذه بضوابط أمنية، وانتهاءً بالتصحيح الآلي وإعلان النتائج.

4.7.1. الاختراقات السيبرانية: هي هجمات إلكترونية مُتعمدة تهدف إلى: تعطيل أنظمة الامتحانات الإلكترونية والوصول غير المشروع والمساس بنزاهة عملية التقييم

5.7.1. مشرفي انظمة التعلم الإلكتروني: هم المسؤولون التقنيون المكلفون بـ:

أ. إدارة وتشغيل منصات التعلم الإلكتروني مثل (Moodle)، (Blackboard)

ب. متابعة سير أنظمة الامتحانات الإلكترونية

ت. توفير الدعم الفني وحل المشكلات

ث. تطبيق الإجراءات الأمنية للحفاظ على نزاهة الاختبارات

2-الإطار النظري والدِّراسات السّابقة

1.2: الإطار النظري:

1.1.2. تمهيد:

تشهد البيئات التعليمية تحولاً رقمياً متسارعاً، وأصبحت أنظمة التعلم الإلكتروني (E-Learning Systems) ضرورة حتمية لضمان استمرارية العملية التعليمية، خاصة في ظل الأزمات (Al-Farrah et al., 2020). وتعد أنظمة الامتحانات الإلكترونية (E-Exam Systems) حجر الزوية في هذه المنظومة، كونها الأداة الرئيسية لتقييم نزاهة وجودة مخرجات التعلم. (Alruwaili, 2021) ومع هذا الاعتماد المتزايد، برزت تحديات أمنية خطيرة تهدد مصداقية هذه الأنظمة، حيث أصبحت هدفاً جاذباً للهجمات الإلكترونية الممنهجة. (Alenezi, 2022)

2.1.2. مفهوم أنظمة الامتحانات الإلكترونية وأهميتها:

تُعرّف أنظمة الامتحانات الإلكترونية بأنها منصات برمجية متكاملة تُدار ضمن بيئة التعلم الإلكتروني وتغطي دورة التقييم كاملة بدءاً من إعداد بنوك الأسئلة وتصميم الاختبارات، مروراً بتنفيذها بضوابط أمنية، وانتهاءً بالتصحيح وإصدار النتائج.(Bawarith, Basuhail, Fattouh, & Gamalel-Din, 2017) تكمن أهميتها في قدرتها على تحقيق الكفاءة وتقليل الهدر الزمني والمادي، وتقديم مرونة كبيرة للطلاب، إلى جانب إتاحة تقارير تحليلية دقيقة تساعد في تحسين العملية التعليمية.(Aldossari, 2020)

جدول (1): المكونات الرئيسية لنظام الامتحانات الإلكترونية وآلية عملها

المكون	الوظيفة	المخاطر الأمنية المحتملة
وحدة إدارة الأسئلة	إنشاء وتخزين وتصنيف الأسئلة	سرقة الأسئلة أو العبث بمحتواها (Bawarith et al., 2017)
وحدة إدارة الاختبارات	تحديد وقت وزمن وضوابط الامتحان	اختراق الإعدادات أو تمديد الوقت بغير تصريح (Akacha, 2023)
منصة أداء الامتحان	الواجهة التي يتفاعل معها الطالب	هجمات الحرمان من الخدمة وانتحال الشخصية (Holden et al., 2021)
وحدة التصحيح والتقارير	تصحيح الإجابات وإعداد النتائج	العبث بالنتائج أو اختراق قواعد البيانات (Akacha, 2023)

3.1.2 . الاختراقات السيبرانية لأنظمة الامتحانات الإلكترونية: التهديدات والتحديات

يُعرّف الاختراق السيبراني بأنه وصول غير مصرح به إلى نظام أو بيانات بهدف السرقة أو العبث أو الإضرار (Whitman & Mattord, 2021). في سياق الامتحانات الإلكترونية تتخذ هذه الاختراقات أشكالاً متعددة، أبرزها:

أ. **هجمات الحرمان من الخدمة: (DDoS)** إغراق الخادم بحركة مرور زائفة لتعطيله ومنع الطلاب من أداء الامتحان(Akacha, 2023) .

ب. **انتحال الشخصية:** محاولة مستخدم غير مصرح له انتحال هوية طالب مسجل لأداء الامتحان نيابة عنه.(Chandran, Ghorpade, & Ahire, 2021)

ت. **اختراق الخوادم وقواعد البيانات** :للوصول إلى الأسئلة قبل موعد الامتحان أو لتعديل نتائج الطلاب بعد انتهائه.(Kumar & Singh, 2020) .

ث. **الغش الإلكتروني المنظم** :استخدام تقنيات مثل إرسال الإجابات عبر تطبيقات المراسلة أو أجهزة صغيرة مخفية(Sabbah, 2018) . تشير الدراسات إلى أن كلفة هذه الاختراقات لا تقتصر على الجانب المادي فحسب، بل تمتد إلى تقويض ثقة المجتمع الأكاديمي بأسره في نزاهة التعليم.(Ifinedo, 2021)

4.1.3. تقنيات الذكاء الاصطناعي كحل استباقي: المفهوم والتطبيقات:

الذكاء الاصطناعي (AI) هو "فرع من علم الحاسوب يهتم ببناء آلات ذكية قادرة على أداء مهام تتطلب ذكاءً بشرياً، مثل التعلم من البيانات، المشكلات، واتخاذ القرارات.(Russell & Norvig, 2020) في مجال الأمن السيبراني، لم تعد النُهج التقليدية القائمة على التوقيعات(Signature-based) كافية لمواجهة الهجمات المتطورة، مما دفع إلى adoption تقنيات الذكاء الاصطناعي التي تتعلم بشكل استباقي وتتكيف .(Sarker et al., 2020)من أبرز هذه التقنيات:

أ. التعلم الآلي :(Machine Learning) حيث يتم تدريب النماذج الخوارزمية على كميات هائلة من dataالسجلات الأمنية (Logs) وأنماط استخدام النظام للكشف عن anomalies الأنشطة الشاذة التي قد تشير إلى محاولة اختراق.(Chandran et al., 2021)

ب. معالجة اللغة الطبيعية :(NLP) تُستخدم لمقارنة إجابات الطلاب النصية مع مصادر على الإنترنت أو مع إجابات زملائهم لاكتشاف حالات الانتحا.(Alruwaili, 2021) s

ت. الرؤية بالحاسوب :(Computer Vision) لتحليلvideo بث الفيديو المباشر من كاميرا الطالب أثناء الامتحان لاكتشاف سلوكيات مشبوهة، مثل وجود شخص آخر في الغرفة أو محاولة استخدام الهاتف (Ullah, 2022)

5.1.3. قياس فاعلية تقنيات الذكاء الاصطناعي في حماية الامتحانات الإلكترونية:

يمكن قياس فاعلية (Effectiveness) توظيف تقنيات الذكاء الاصطناعي من خلال عدة معايير قابلة للقياس، أهمها:(Sarker et al., 2020; Ullah, 2022)

أ. معدل الكشف: (Detection Rate) نسبة الهجمات أو محاولات الغش التي يتم اكتشافها بنجاح.

ب. معدل الإنذارات الكاذبة :(False Positive Rate) عدد المرات التي يخطئ فيها النظام بتصنيف نشاط طبيعي على أنه تهديد. النظام الفعال يقلل هذا المعدل.

ت. الوقت المستغرق للكشف والاستجابة :(Response Time) قدرة النظام على اكتشاف التهديدات والاستجابة لها في الوقت الفعلي (Real-time) أو شبه الفعلي.

ث. القدرة على التكيف :(Adaptability) قدرة التقنية على التعلم من الهجمات الجديدة وتطوير دفاعاتها دون الحاجة إلى تدخل بشري مكثف

6.13. التحديات والمعوقات أمام التوظيف الفعال:

على الرغم من الإمكانات الكبيرة، فإن توظيف تقنيات الذكاء الاصطناعي في البيئات التعليمية، وخاصة في السياقات محدودة الموارد مثل السودان، يواجه تحديات جمة، منها:

أ. التحديات التقنية: الحاجة إلى بنية تحتية قوية (خوادم، شبكات)، وتوفر data sets مجموعات بيانات ضخمة ومُصنفة لتدريب النماذج (Alenezi, 2022)

ب. التحديات المالية: التكلفة المرتفعة لشراء أو تطوير وتطويع هذه التقنيات.(Sultan et al., 2019)

ت. التحديات البشرية: الحاجة إلى كوادر بشرية متخصصة قادرة على إدارة وتطوير هذه الأنظمة المعقدة (Ifinedo, 2021).

ث. التحديات الأخلاقية والخصوصية :مخاوف تتعلق بمراقبة الطلاب عبر الكاميرات وجمع وتحليل بياناتهم السلوكية.(Ullah, 2022)

1.2. الدِّراسات السّابقة:

1.1.2.الدِّراسات العربية:

2.1.2.- دراسة أبو غزال وعدوي (2020):

أجرى الباحثان أبو غزال وعدوي دراسة بعنوان معوقات تطبيق أنظمة الأمن السيبراني في التعليم الإلكتروني بالجامعات الفلسطينية في فلسطين، ونشرت في مجلة الجامعة الإسلامية للدراسات التربوية والنفسية. هدفت الدراسة إلى الكشف عن المعوقات التقنية والإدارية التي تواجه تطبيق أنظمة الأمن السيبراني في البيئة التعليمية الفلسطينية. استخدم الباحثان المنهج المختلط، حيث تكونت عينة الدراسة من (180) مختصًا في تقنية المعلومات والتعليم الإلكتروني، واعتمدت على الاستبانة وتحليل الوثائق. كشفت نتائج الدراسة عن معوقات تقنية تتمثل في ضعف البنية التحتية وقلة التمويل، ومعوقات إدارية تتعلق بعدم وضوح السياسات وعدم كفاية التدريب. وأوصت الدراسة بضرورة تخصيص ميزانيات كافية وتطوير برامج تأهيلية للعاملين في هذا المجال

3.1.2 دراسة الغامدي والحربي (2021):

قام الباحثان الغامدي والحربي بإجراء دراسة بعنوان "فاعلية استخدام تقنيات الذكاء الاصطناعي في اكتشاف الغش الإلكتروني في الاختبارات عن بُعد: دراسة تطبيقية على الجامعات السعودية" في المملكة العربية

السعودية، ونشرت في مجلة جامعة الملك سعود – علوم الحاسب والمعلومات. هدفت الدراسة إلى قياس فاعلية أنظمة الذكاء الاصطناعي في رصد ومكافحة الغش الإلكتروني في الاختبارات عن بعد. استخدم الباحثان المنهج شبه التجريبي، حيث تم تطبيق نظام قائم على الذكاء الاصطناعي على عينة من(500) طالب وطالبة في ثلاث جامعات سعودية، واعتمدت على تحليل البيانات وتقارير الأداء.

توصلت الدراسة إلى أن النظام المقترح حقق دقة بنسبة (91،3٪) في اكتشاف محاولات الغش، مع قدرة على رصد الأنماط غير الطبيعية في سلوكيات الطلاب خلال الاختبارات. كما أظهرت النتائج فعالية خاصة في اكتشاف حالات الاستعانة بطرق خارجية أو استخدام تطبيقات غير مصرح بها. وأوصت الدراسة بتعميم استخدام هذه التقنيات في الجامعات مع التأكيد على أهمية مراعاة الجوانب الأخلاقية وخصوصية المستخدمين

2.2. الدراسات الأجنبية:

1.2.2. دراسة Oproiu et al. (2021)

أجرى الباحثون Oproiu وزملاؤه دراسة بعنوان "Artificial Intelligence Solutions for Cybersecurity in E-Learning Systems" ونشرت في مجلة Sensors السويسرية. هدفت الدراسة إلى تحليل وتقييم حلول الذكاء الاصطناعي المستخدمة في تعزيز الأمن السيبراني لأنظمة التعلم الإلكتروني. استخدم الباحثون منهج المراجعة المنهجية، حيث تم تحليل (85) دراسة سابقة منشورة في قواعد بيانات علمية محكمة خلال الفترة من (2015)إلى (2020)

كشفت الدراسة أن تقنيات الذكاء الاصطناعي تحقق كفاءة عالية في اكتشاف ومنع الهجمات السيبرانية على أنظمة التعلم الإلكتروني، مع معدلات دقة تتروح بين (85%) إلى (95%) حسب التقنية المستخدمة. كما أظهرت النتائج تفوق تقنيات التعلم العميق والشبكات العصبية في التعامل مع التهديدات المستجدة والمعقدة .وأوصت الدراسة بدمج هذه التقنيات في الأنظمة الحالية مع تطوير أطر شاملة للأمن السيبراني تتضمن الجوانب التقنية والقانونية والأخلاقية

2.2.2. دراسة (Maria Gonzalez 2021):

عنوان الدِّراسة: (The Role of Artificial Intelligence in Accelerating Digital Transformation in Higher Education.)، جامعة برشلونة، إسبانيا، جهة النشر مجلة (European Journal of Higher EducationS). هدفت واستخدمت الدِّراسة المنهج الوصفي وتكونت عينة الدِّراسة من (5) جامعات أوربية واستخدمت تحليل وثائق ومقابلات كأداة لجمع البيانات وتوصلت الدِّراسة لعدة نتائج أهمها نجاح الجامعات في تحقيق التحول الرقمي باستخدام الذكاء الاصطناعي. كما أوصت الدِّراسة بعدة توصيات أهمها تعميم النموذج الأوروبي على دول أخرى.

3.2.2. دراسة Zawacki-Richter et al. (2019)

دراسة بعنوان Systematic review of research on artificial intelligence applications in higher education ونُشرت في International Journal of Educational Technology in Higher Education. هدفت الدراسة إلى تحليل الأبحاث المنشورة حول تطبيقات الذكاء الاصطناعي في التعليم العالي خلال الفترة من (2007 إلى 2018) وتصنيفها. استخدم الباحثون منهج المراجعة المنهجية بتحليل(146) دراسة منشورة في قواعد بيانات علمية. توصلت الدراسة إلى أربعة مجالات رئيسية لتطبيق الذكاء الاصطناعي في التعليم العالي: التنبؤ بالتحصيل الدراسي، التقييم التكيفي، الأنظمة الذكية للتعلم، والتطبيقات الإدارية. كما أوصت بضرورة إجراء أبحاث حول الأخلاقيات والخصوصية في هذا المجال.

3.2.تعقيب على الدِّراسات السّابقة:

تُعد الدراسة الحالية إضافة نوعية إلى حقل البحث في مجال توظيف الذكاء الاصطناعي لحماية أنظمة الامتحانات الإلكترونية، إذ إنها تناولت الموضوع في السياق السوداني الذي يتميز بظروف تقنية وأمنية خاصة نتيجة الحرب وانقطاع الخدمات. فقد اعتمد الباحث المنهج الوصفي التحليلي، وهو ما يجعلها أقرب إلى بعض الدراسات السابقة مثل دراسة Gonzalez (2021) التي وصفت دور الذكاء الاصطناعي في التحول الرقمي، ودراسة أبو غزال وعدوي (2020) التي اتبعت المنهج الوصفي لدراسة معوقات الأمن السيبراني في الجامعات الفلسطينية. غير أن الدراسة الحالية اختلفت عن دراسات أخرى مثل دراسة الغامدي والحربي (2021) التي اعتمدت المنهج شبه التجريبي لقياس فاعلية أدوات الذكاء الاصطناعي في كشف الغش الإلكتروني، وكذلك عن دراسات منهجية تحليلية مثل Zawacki-Richter et al. (2019) التي قدمت مراجعة منهجية شاملة للأدبيات. هذا يوضح أن الدراسة الحالية ركزت على الوصف الميداني والتحليل الإحصائي أكثر من التجريب أو المراجعات النظرية.

أما من حيث المجتمع والعينة، فقد اقتصرت الدراسة الحالية على مشرفي أنظمة إدارة التعلم الإلكتروني بالجامعات السودانية (N=75)، وهو اختيار يتسم بالتركيز على الفاعلين المباشرين في إدارة وحماية الامتحانات الإلكترونية. وتختلف بذلك عن دراسات استهدفت الطلاب (مثل الغامدي والحربي، 2021)، أو أعضاء هيئة التدريس (مثل بعض الدراسات العربية)، أو المؤسسات الجامعية ككيان)مثلGonzalez ، 2021 .(ويمنح هذا التوجه الدراسة الحالية خصوصية؛ لأنها تستند إلى آراء الفئة المسؤولة ميدانيًا عن إدارة الأمن السيبراني للامتحانات.

وفيما يتعلق بالأداة، فقد استخدم الباحث استبانة محكمة مكونة من ثلاثة محاور (الواقع – المعوقات – الفاعلية) أظهرت ثباتًا عاليًا ($\alpha > 0.96$) وصدقًا بنائيًا مؤكدًا من خلال التحليل العاملي. وهذه النتيجة تميزها عن بعض الدراسات التي اكتفت بالمقابلات أو مراجعة الأدبيات (مثل Oproiu et al., 2021 و(Zawacki-Richter, 2019 ، كما تجعلها أكثر قربًا من دراسة أبو غزال وعدوي (2020) التي وظفت استبانة لقياس المعوقات.

أما على صعيد المعالجة الإحصائية، فقد اعتمدت الدراسة الحالية على حزمة متقدمة من الاختبارات مثل كرونباخ ألفا، تحليل التباين الأحادي، معامل ارتباط بيرسون، والتحليل العاملي التأكيدي، وهو ما يعكس مستوى عالٍ من الصرامة المنهجية. في المقابل، لم تصل بعض الدراسات السابقة إلى هذا المستوى؛ إذ اكتفت بالتكرارات والنسب أو تحليل محتوى الوثائق.

وبالنسبة للنتائج، توصلت الدراسة الحالية إلى أن مستوى توظيف تقنيات الذكاء الاصطناعي في حماية الامتحانات بالجامعات السودانية ما يزال متوسطًا (61%)، مع وجود تحديات كبيرة أبرزها نقص الكوادر وضعف البنية التحتية، إضافة إلى غياب خطط التحديث الدورية. وهذه النتائج تتقاطع مع ما ورد في دراسة أبو غزال وعدوي (2020) التي كشفت عن ضعف البنية التحتية وغياب السياسات، كما تتفق مع نتائج Oproiu et al. (2021) التي أبرزت أهمية الذكاء الاصطناعي في التصدي للهجمات السيبرانية. لكنها تختلف عن دراسة الغامدي والحربي (2021) التي أثبتت فاعلية مرتفعة جدًا (91%) للذكاء الاصطناعي في كشف الغش، وكذلك عن دراسة Gonzalez (2021) التي أبرزت نجاح الجامعات الأوروبية في تسريع التحول الرقمي. وهنا تتجلى خصوصية السياق السوداني الذي يعاني من أزمات سياسية وتقنية أثرت على كفاءة تطبيق هذه التقنيات.

استفاد الدِّراسة الحالية من الدِّراسات السّابقة في عدة جوانب رئيسة، بناء الإطار النظري والمفاهيمي تحديد الفجوات البحثية، واختيار المنهج الذي يتناسب مع طبيعة الدِّراسة، واختيار الادوات المناسبة والاساليب الاحصائية لمعالجة البيانات.

تميزت الدراسة الحالية عن الدراسات السابقة بكونها الأولى التي تتناول واقع توظيف تقنيات الذكاء الاصطناعي في حماية الامتحانات الإلكترونية بالجامعات السودانية في ظل الظروف الطارئة التي تمر بها البلاد، وهو ما يمنحها بعدًا سياقيًا فريدًا لم تتطرق إليه الدراسات السابقة التي أجريت في بيئات مستقرة تقنيًا مثل فلسطين أو السعودية أو أوروبا. كما تميزت الدراسة الحالية بتركيزها على آراء مشرفي أنظمة إدارة التعلم الإلكتروني بوصفهم الفئة الأكثر ارتباطًا بتطبيق أنظمة الحماية، في حين أن غالبية الدراسات السابقة ركزت على الطلاب أو أعضاء هيئة التدريس أو المؤسسات الجامعية ككل. إضافة إلى ذلك، اعتمدت الدراسة الحالية على استبانة محكمة مدعمة بالتحليل العاملي التأكيدي ومعالجات إحصائية متقدمة، مما منح نتائجها قوة وموثوقية أعلى مقارنة ببعض الدراسات التي اكتفت بالوصف أو تحليل الوثائق. كذلك جاءت نتائجها لتعكس خصوصية التحديات التقنية والإدارية في الجامعات السودانية، وهو ما يجعلها إضافة نوعية تسد فجوة معرفية في ميدان الذكاء الاصطناعي والأمن السيبراني في التعليم العالي

3. إجراءات الدِّراسة الميدانية

1.3. منهج الدِّراسة:

اتبع الباحث المنهج الوصفي التحليلي لمناسبته لهذه الدراسة، ووصف الوقائع والممارسات التي سادت في تطبيق هذا المنهج؛ من جمع البيانات وتحليلها وصولاً إلى تفسير البيانات وستخلاص النتائج وتوجيهها

نحو أهداف الدراسة. والمنهج الوصفي التحليلي هو أحد مناهج البحث ويعتمد على دراسة الواقع أو الظاهرة كما هي في الواقع، ويهتم بوصفها وصفاً دقيقاً، ويعبر عنها تعبيراً كيفياً أو تعبيراً كمياً، والمنهج الوصفي لا يهدف إلى وصف الواقع أو وصف الظاهرة كما هي فقط، بل الوصول إلى استنتاجات تسهم في فهم هذا الواقع وتطويره، كما يشمل تصنيف المعلومات والتعبير عنها كماً وكيفاً. (حسن شحاتة وآخرون – 301)م – ص2003معجم المصطلحات التربوية – الدار المصرية اللبنانية – القاهرة –

2.3. مجتمع الدِّراسة:

يتكون المجتمع الكلي من مشرفي انظمة إدارة التعلم الإلكتروني بالجامعات السودانية

3. 3. عينة الدِّراسة:

تكونت عينة الدِّراسة بعدد (75) مشرف من مشرفي انظمة ادارة التعلم الإلكتروني بالجامعات السودانية.

الجدول(2): جدول تكراري (ترابطي) يظهر توزيع الأفراد حسب الجنس وسنوات الخبرة

سنوات الخبرة	ذكر (التكرار/النسبة %)	أنثى (التكرار/النسبة %)	الإجمالي (التكرار/النسبة %)
أقل من 5 سنوات	14 (26.9%)	4 (17.4%)	18 (24.0%)
10-5سنوات	21 (40.4%)	5 (21.7%)	26 (34.7%)
أكثر من 10 سنوات	17 (32.7%)	14 (60.9%)	31 (41.3%)
الإجمالي	**52 (100%)**	**23 (100%)**	**75 (100%)**

تحليل النتائج:

أولاً: الذكور: التوزيع متقارب إلى حد ما. أكبر مجموعة بينهم هي فئة 10 – 5 سنوات (40.4%)، تليها فئة أكثر من 10 سنوات (32.7%)، ثم أقل من 5 سنوات (26.9%)هذا يشير إلى وجود خليط من الخبرات بين الذكور.

ثانياً: الإناث: التوزيع مختلف بشكل ملحوظ. الغالبية العظمى من الإناث (60.9%) يقعن في فئة أكثر من 10 سنوات من الخبرة. هذا يشير إلى أن الإناث في هذه العينة لديهن خبرة عملية عالية بشكل استثنائي مقارنة بمستويات الخبرة الأخرى.

جدول (3): جدول نسبي يظهر توزيع كل فئة خبرة حسب الجنس (للمقارنة المباشرة)

سنوات الخبرة	ذكر (نسبة من إجمالي الفئة)	أنثى (نسبة من إجمالي الفئة)
أقل من 5 سنوات	77.8%	22.2%

10-5سنوات	80.8%	19.2%
أكثر من 10 سنوات	54.'8%	45.2%
الإجمالي	69.3%	30.7%

تحليل النتائج: بناءً على الجدول أعلاه، يمكن استخلاص النقاط التحليلية التالية:

1.**التوزيع العام للعينة:**

يهيمن الذكور على العينة بنسبة 69.3% (52 فردًا)، بينما تمثل الإناث نسبة 30.7% فقط (23 فردًا). هذا يشير إلى وجود فجوة جندرية ناتجة عن نزوح معظم الكفاءات النسائية خارج البلاد أو في الولايات الامنة ويصعب الوصول اليهن لانعدم الشبكة والانقطاع الدائم للكهرباء.

2. مقارنة التمثيل النسبي داخل فئات الخبرةمن الجدول (2):

أ. في فئتي الخبرة الأقل (أقل من 5 سنوات و5 – 10 سنوات)، يشكل الذكور الغالبية حوالي (78% و81%) على التوالي، مما يعكس هيمنة الذكور.

ب. النتيجة الأكثر إثارة للاهتمام هي في فئة أكثر من 10 سنوات .هنا، على الرغم من أن الذكور يشكلون الأغلبية (54.8%)، إلا أن تمثيل الإناث يرتفع بشكل كبير ليصل إلى (42.2%)؛ وهذا يعني أن نصف الأفراد ذوي الخبرة العالية في هذه العينة من الإناث.

ت. على الرغم من أن الذكور يشكلون غالبية العينة (حوالي ثلثي الأفراد)، فإن الإناث في هذه العينة يتمتعن بمستوى خبرة أعلى في المتوسط.

ث. حيث أن 60.9% من الإناث لديهن خبرة تزيد عن (10) سنوات، مقارنة بـ (32.7%) فقط من الذكور الذين في نفس الفئة.

3-4 أداة الدِّراسة:

تمثلت في الاستبانة فقام الباحث بتصميمها وتوزيعها بعد الاطلاع على الإطار النظري والدِّراسات السّابقة ذات العلاقة بموضوع الدراسة.

3-5 الصدق الظاهري: تكونت الاستبانة (المقياس) في صورتها الأولية من (20) عبارة، مقسمة على (5) محاور، عرضت على مجموعة من المحكمين فتم تعديل (10) عبارات، وحذف (8) عبارات، فأصبح المقياس في صورته النهائية يتكون من (3) محاور و(12) عبارة، كما تم تضمين البيانات الأولية لعينة الدِّراسة.

3-6 ثبات الاستبانة: قام الباحث بتطبيقها على عينة استطلاعية من خارج عينة الدِّراسة حجمها (15) مفحوصاً تم اختيارهم عشوائياً وذلك لمعرفة الخصائص القياسية للفقرات بالمقياس بمجتمع الدِّراسة والمكونة من (20) فقرة.

أولاً: تحليل الثبات (Reliability Analysis)

جدول (4): الطريقة المستخدمة :معامل كرونباخ ألفا (Cronbach's Alpha) لقياس اتساقية المقياس الداخلي.

المحور	عدد الفقرات	معامل كرونباخ ألفا(α)	التفسير
المحور الأول: الواقع الحالي	4	0.972	ثبات ممتاز جدًا
المحور الثاني: المعوقات	4	0.967	ثبات ممتاز جدًا
المحور الثالث: الفاعلية	4	0.979	ثبات ممتاز جدًا
الاستبانة ككل	12	0.981	ثبات ممتاز جدًا

نتائج التحليل:

قيمة معامل ألفا لجميع المحاور وللمقياس ككل أعلى من (0.90)، مما يشير إلى ثبات شديد العلو واتساق داخلي ممتاز .هذا يعني أن فقرات كل محور تقيس مفهومًا واحدًا متماسكًا، وأن الاستبانة موثوقة جدًا ويمكن الاعتماد على نتائجها.

ثانيًا: تحليل الصدق(Validity Analysis) :

1. الصدق الظاهري (Face Validity) والصدق المحتوى(Content Validity)

أ. التحقق: تم تحكيم الاستبانة من قبل محكمين متخصصين في المجال كما هو موضح في بياناتك الأولى تحكيم الاستبانة.

ب. النتيجة: تم تحقيق الصدق الظاهري وصدق المحتوى من خلال موافقة المحكمين على أن الفقرات واضحة وملائمة وشمولية لقياس الأبعاد المطلوبة.

2. صدق البناء (Construct Validity)

الطريقة المستخدمة :تحليل الاتساق الداخلي (صدق المحك الداخلي) من خلال حساب معاملات الارتباط بين كل فقرة والمحور الذي تنتمي إليه، ارتباط المحاور مع بعضها البعض.

أ. صدق المحك الداخلي (Item–Total Correlation)

– **الفرضية:** إذا كان المحور يتمتع بصدق بناء جيد، يجب أن تكون هناك علاقة ارتباطية قوية بين درجة كل فقرة والدرجة الكلية للمحور الذي تنتمي إليه.

– **النتيجة:** جميع معاملات الارتباط بين كل فقرة والمحور الخاص بها كانت مرتفعة جدًا وإيجابية جميعها فوق 0.85 ودالة إحصائيًا .(p–value < 0.01) هذا يدعم بقوة صدق البناء للمقياس

ب. جدول (5) مصفوفة الارتباط بين المحاور(Inter–Scale Correlation)

المحور	المحور الأول (الواقع)	المحور الثاني (المعوقات)	المحور الثالث (الفاعلية)
المحور الأول (الواقع)	1		
المحور الثاني (المعوقات)	0.871	1	
المحور الثالث (الفاعلية)	0.892	0.934	1

- علاقة ارتباطية دالة إحصائيًا عند مستوى(0.01)

- تفسير مصفوفة الارتباط: توجد علاقات ارتباطية موجبة قوية جدًا بين جميع المحاور.

هذا منطقي، إذ أن:

. إدراك الواقع الحالي (المحور الأول) مرتبط بإدراك فاعلية التقنيات (المحور الثالث). من يتعامل مع أنظمة جيدة يرى فاعليتها.

. إدراك المعوقات (المحور الثاني) مرتبط عكسيًا (ارتباط سالب ضمني) مع إدراك كل من الواقع الحالي والفاعلية. كلما زادت perceived المعوقات، قل إدراك جودة الواقع والفاعلية، والعكس صحيح.

. قوة الارتباط العالية تؤكد أن المحاور تقيس مفاهيم مترابطة تنتمي إلى بناء نظري واحد وهو "توظيف الذكاء الاصطناعي في أمن الامتحانات.

جدول (6): التحليل العاملي للتأكيدي (Confirmatory Factor Analysis – CFA)

لاختبار صدق البناء بشكل أكثر قوة، تم إجراء تحليل عاملي تأكيدي لاختبار هل هيكل النموذج ذو الثلاثة عوامل (محاور) الذي صمم عليه الاستبيان يتماشى مع البيانات الفعلية.

مؤشر المطابقة	القيمة المُحسنة	القيمة المعيارية الجيدة	التفسير
CMIN/DF	1.85	< 3.0	ممتاز
CFI	0.98	> 0.95	ممتاز
TLI	0.97	> 0.95	ممتاز
RMSEA	0.068	< 0.08	جيد
SRMR	0.032	< 0.05	ممتاز

نتائج التحليل:

جميع مقاييس مطابقة النموذج ضمن النطاقات المقبولة بل وممتازة .هذا يؤكد أن هيكل الاستبانة ذو الثلاثة محاور (عوامل) يتمتع بصدق بناء ممتاز ويتوافق مع البيانات المجمعة بشكل كبير.

ثالثاً: معاملات الارتباط للفقرات (Item Correlations)

جدول (7) توضيح مدى قوة العلاقة بين فقرات كل محور، فيما يلي متوسط معاملات الارتباط بينها:

المحور	متوسط معامل الارتباط بين فقرات المحور	التفسير
المحور الأول: الواقع الحالي	0.92	ارتباط قوي جدًا
المحور الثاني: المعوقات	0.89	ارتباط قوي جدًا
المحور الثالث: الفاعلية	0.93	ارتباط قوي جدًا

بناء على التحليل الإحصائي، نخلص إلى أن أداء المقياس (الاستبانة) ممتاز من الناحية السيكومترية:

1. **الثبات:** (Reliability) مقياس ذو ثبات عالٍ جدًا ($\alpha > 0.96$) لجميع الأبعاد، مما يعني أنه يوفر نتائج متسقة وموثوقة.
2. **الصدق: (Validity) المقياس يتمتع:**

- صدق محتوى من خلال التحكيم.
- صدق بناء قوي، بدعم من:

– الاتساق الداخلي العالي للفقرات.

– علاقات الارتباط القوية والمتوقعة بين المحاور.

– نتائج التحليل العاملي التأكيدي (CFA) التي أكدت أن الهيكل الثلاثي للمحاور هو الأنسب للبيانات.

الأساليب الإحصائية المستخدمة:

تم ترميز أسئلة الاستبانة ومن ثم تفريغ البيانات التي تم جمعها من خلال الاستبانات الإلكترونية وذلك باستخدام برنامج الحزم الإحصائية للعلوم الاجتماعية (SPSS) ومن ثم تحليلها باستخدام الأساليب الإحصائية التالية:

1- النسب المئوية والتكرارات والمتوسط الحسابي.

2- اختبار ألفا كرونباخ لمعرفة ثبات فقرات الاستبانة.

3- معادلة اختبار ت (T-Test) اختبارات الفروق بين متوسطين مجتمعين مستقلين.

4- تحليل التباين الاحادي.

5- التحليل العاملي

6- معامل ارتباط بيرسون.

* ذات دلالة احصائية ($\alpha > 0.05$).

4- عرض وتحليل البيانات ومناقشتها وتفسيرها

يتم في هذا الفصل عرض وتحليل نتائج الدراسة التي تم التوصل إليها من خلال أداة الدراسة، كما يتم فيه أيضاً مناقشة تلك النتائج، وتفسير البيانات الخاصة بعبارات كل محور من محاور الدراسة بعد إجراء التحليل الإحصائي.

1.4. مناقشة السؤال الأول للدراسة:

ما واقع توظيف تقنيات الذكاء الاصطناعي في حماية أنظمة الامتحانات الإلكترونية من الاختراقات السيبرانية بالجامعات السودانية؟

جدول (8) يوضح استجابات أفراد العينة نحو عبارات المحور الأول للدراسة: واقع توظيف تقنيات الذكاء الاصطناعي في حماية أنظمة الامتحانات الإلكترونية من الاختراقات السيبرانية بالجامعات السودانية

م	العبارة	عدد المشتركين	الوسط الحسابي	الانحراف المعياري	الوزن النسبي (%)	التصنيف	الترتيب
1	تُستخدم تقنيات الذكاء الاصطناعي حاليًا في كشف محاولات الاختراق لأنظمة الامتحانات.	75	3.28	1.61	65.6%	متوسطة	2
2	تعتمد الجامعة على أنظمة ذكاء اصطناعي متطورة للتنبؤ بالهجمات السيبرانية مسبقًا.	75	2.95	1.66	59.0%	متوسطة	4
3	تُوظف تقنيات الذكاء الاصطناعي لتحليل أنماط الغش الإلكتروني أثناء الاختبارات.	75	3.20	1.63	64.0%	متوسطة	3
4	توجد خطة واضحة لتحديث أنظمة الذكاء الاصطناعي الأمنية بشكل دوري.	75	2.77	1.67	55.4%	متوسطة	1
	المتوسط العام للمحور	**75**	**3.05**	**1.64**	**61.0%**	**متوسطة**	

- من الجدول (8) المختص بنتائج المحور الأول للدراسة: **واقع توظيف تقنيات الذكاء الاصطناعي في حماية أنظمة الامتحانات الإلكترونية من الاختراقات السيبرانية بالجامعات السودانية** نجد أن المتوسط الحسابي يتراوح بين(3.28 – 2.77) ، **مما يشير إلى أن اتجاهات آراء أفراد العينة كانت بين "محايد" و"موافق" بشكل طفيف.**

- **حصلت** العبارة الخاصة بـ"كشف محاولات الاختراق" على أعلى متوسط (3.28)، بينما **حصلت** العبارة الخاصة بـ"وجود خطة تحديث واضحة" على أدنى متوسط.(2.77)
- **ظلت** قيم الانحراف المعياري مرتفعة (أعلى من 1.6)، **مما يدل على وجود تباين ملحوظ في آراء المبحوثين.**
- تصنف جميع العبارات ضمن المستوى "المتوسط "حسب الأوزان النسبية.

يشير ذلك إلى أن اتجاهات أفراد العينة كانت إيجابية بشكل طفيف نحو عبارات المحور الأول للدراسة. وتؤدي هذه النتيجة إلى الاستنتاج بأن :واقع التوظيف الحالي للذكاء الاصطناعي يعد توظيفًا متوسطًا ولم يصل بعد إلى مستوى الجودة أو الانتشار المطلوب .وهذه النتيجة تجيب عن السؤال الأول للدراسة، وهي تتفق مع دراسة: دراسة أبو غزال وعدوي(2020) . دراسة Oproiu et al. (2021)

1.5: مناقشة السؤال الثاني للدراسة:

ما تحديات ومعوقات توظيف تقنيات الذكاء الاصطناعي في حماية أنظمة الامتحانات الإلكترونية من الاختراقات السيبرانية بالجامعات السودانية؟

جدول (9) يوضح استجابات أفراد العينة نحو عبارات المحور الأول للدراسة: تحديات ومعوقات توظيف تقنيات الذكاء الاصطناعي في حماية أنظمة الامتحانات الإلكترونية من الاختراقات السيبرانية بالجامعات السودانية

م	عدد المشتركين	الوسط الحسابي	الانحراف المعياري	الوزن النسبي (%)	التصنيف	الترتيب
1	75	4.12	1.24	82.4%	كبيرة جدًا	1
2	75	4.07	1.23	81.4%	كبيرة جدًا	2
3	75	3.48	1.42	69.6%	كبيرة	4
4	75	3.68	1.39	73.6%	كبيرة	3
	75	3.84	1.32	76.8%	كبيرة جدًا	

- من الجدول (9) المختص بنتائج المحور الثاني للدراسة: تحديات ومعوقات توظيف تقنيات الذكاء الاصطناعي في حماية أنظمة الامتحانات الإلكترونية من الاختراقات السيبرانية بالجامعات السودانية سجلت جميع المتوسطات قيمًا أعلى من (3.5)، مما يعكس ميلاً قويًا لدى أفراد العينة للموافقة على أن العبارات المطروحة تمثل تحديات حقيقية.

- حظي تحديا "نقص الكوادر" و"ضعف البنية التحتية" على أعلى متوسطين (4.12 و4.07) على التوالي.
- كانت قيم الانحراف المعياري مرتفعة ولكن أقل نسبيًا من المحور السابق.
- صنف التحديان الأول والثاني على أنهما "كبيرة جدًا."

تُظهر هذه النتائج وجود اتفاق نسبي بين أفراد العينة على حدة هذه التحديات والمعوقات. وتؤدي هذه النتائج إلى الاستنتاج بأن :هناك إجماع على وجود تحديات ومعوقات كبيرة تحول دون التوظيف الفعال لتقنيات الذكاء الاصطناعي، كان أبرزها نقص الكوادر المؤهلة وضعف البنية التحتية .وهذه النتيجة تجيب عن السؤال الثاني للدراسة، وهي تتفق مع دراسة: دراسة(2021) .Oproiu et al ، دراسة Aldossari (2020)

1.6. مناقشة السؤال الثالث للدراسة:

ما فاعلية توظيف تقنيات الذكاء الاصطناعي في حماية أنظمة الامتحانات الإلكترونية من الاختراقات السيبرانية بالجامعات السودانية؟

جدول (10) يوضح استجابات أفراد العينة نحو عبارات المحور الثالث للدراسة: فاعلية توظيف تقنيات الذكاء الاصطناعي في حماية أنظمة الامتحانات الإلكترونية من الاختراقات السيبرانية بالجامعات السودانية.

م	العبارة (الفاعلية في...)	عدد المشتركين	الوسط الحسابي	الانحراف المعياري	الوزن النسبي (%)	التصنيف	الترتيب
1	خفض نسبة الاختراقات بنسبة ملحوظة.	75	3.28	1.51	65.6%	متوسطة	4
2	تقليل وقت الاستجابة للهجمات.	75	3.56	1.37	71.2%	كبيرة	1
3	التصدي للهجمات المعقدة (مثل التزييف العميق).	75	3.52	1.36	70.4%	كبيرة	2

4	كونه حلًّا مستدامًا لتعزيز الأمن.	75	3.48	1.49	69.6%	كبيرة	3
	المتوسط العام للمحور	**75**	**3.46**	**1.43**	**69.2%**	**كبيرة**	

من الجدول (10) المختص بنتائج المحور الثالث للدراسة: **فاعلية توظيف تقنيات الذكاء الاصطناعي** في حماية أنظمة الامتحانات الإلكترونية من الاختراقات السيبرانية بالجامعات السودانية سجلت المتوسطات الحسابية بين (3.56 – 3.28) .

- حظيت العبارة الخاصة بتقليل وقت الاستجابة" على أعلى متوسط.(3.56) .
- استمر ارتفاع قيم الانحراف المعياري، مما يشير إلى بقاء بعض التباين في الآراء.
- صنف إدراك الفاعلية بشكل عام على أنه كبيرة.(69.2%) .

تشير هذه النتائج إلى وجود اتجاه إيجابي لدى أفراد العينة تجاه فاعلية التقنيات. وتؤدي هذه النتائج إلى الاستنتاج بأن :هناك قناعة بفاعلية توظيف تقنيات الذكاء الاصطناعي في حماية أنظمة الامتحانات الإلكترونية، ولا سيما في مجال تقليل وقت الاستجابة للهجمات .وهذه النتيجة تجيب عن السؤال الثالث للدراسة، وهي تتفق مع دراسة(2022) Ullah، دراسة الغامدي والحربي (2021) .

5. خاتمة الدِّراسة

1.5. نتائج الدِّراسة:

1.1.5.بلغ عدد الذكور في العينة 52 (69.3%) مقابل 23 من الإناث (30.7%)، مع تفوق الإناث في الخبرة العملية (أكثر من 10 سنوات لدى 60.9% منهن مقابل 32.7% من الذكور).

2.1.5. مستوى توظيف تقنيات الذكاء الاصطناعي في حماية أنظمة الامتحانات الإلكترونية بالجامعات السودانية متوسط (61%)، مع تباين ملحوظ في آراء المشاركين.

3.1.5. أعلى متوسط في محور الواقع كان لعبارة "استخدام الذكاء الاصطناعي لكشف محاولات الاختراق(3.28) "، وأدنى متوسط لعبارة "وجود خطة واضحة لتحديث الأنظمة.(2.77) "

4.1.5. جميع المتوسطات في محور التحديات تجاوزت (3.5)، ما يعكس وجود تحديات كبيرة أبرزها نقص الكوادر المؤهلة (4.12)وضعف البنية التحتية التقنية .(4.07)

5.1.5. محور الفاعلية أظهر تصنيفًا كبيرًا (69.2%)، مع أعلى متوسط لعبارة "تقليل وقت الاستجابة للهجمات(3.56) "، ما يعكس إدراكًا إيجابيًا لفاعلية التقنيات.

6.1.5. أداة الدراسة تتمتع بدرجة عالية من الثبات والصدق (كرونباخ ألفا 0.96 >، معاملات ارتباط 0.85 >، CFI=0.98، RMSEA=0.068)، ما يؤكد جودة أداة القياس واعتمادها لقياس المحاور الثلاثة (الواقع، المعوقات، الفاعلية)

2.5. توصيات الدِّراسة:

1.2.5. تعزيز البنية التحتية التقنية في الجامعات السودانية (خوادم، شبكات، أدوات أمان) لدعم أنظمة الامتحانات الإلكترونية وتحسين موثوقيتها.

2.2.5.تطوير خطط دورية لتحديث الأنظمة وبرمجيات الذكاء الاصطناعي بما يواكب التهديدات والهجمات السيبرانية المستجدة.

3.2.5. تأهيل وتدريب الكوادر البشرية على إدارة وتشغيل وصيانة أنظمة الامتحانات الإلكترونية وتطبيقات الذكاء الاصطناعي المرتبطة بها.

4.2.5. توفير قواعد بيانات وأدوات ذكاء اصطناعي مُدرّبة على سيناريوهات محلية للكشف عن محاولات الغش أو الاختراق في السياق السوداني.

5.2.5. إرساء سياسات واضحة لحماية الخصوصية والأخلاقيات عند استخدام تقنيات المراقبة بالفيديو أو تحليل بيانات الطلاب.

6.2.5. تعزيز الوعي الرقمي والأمني لدى أعضاء هيئة التدريس والطلاب حول أساليب الهجمات الشائعة وأهمية الالتزام بإجراءات السلامة الرقمية.

7.2.5. تشجيع التعاون والشراكات بين الجامعات السودانية ومراكز البحث أو الشركات التقنية المتخصصة لتطوير حلول أمان مبتكرة لأنظمة الامتحانات الإلكترونية.

3.5. مقترحات الدِّراسة:

1.3.5. تقييم فاعلية أنظمة الامتحانات الإلكترونية بعد دمج تقنيات ذكاء اصطناعي متقدمة (مثل الرؤية بالحاسوب أو التحليل السلوكي) في بيئات جامعات مختلفة بالسودان.

2.3.5. دراسة مقارنة بين الجامعات السودانية وجامعات دول ذات موارد محدودة مشابهة، لقياس مدى نجاح تطبيق الذكاء الاصطناعي في حماية الامتحانات الإلكترونية.

3.3.5. تحليل أثر برامج التدريب الموجهة لأعضاء هيئة التدريس ومسؤولي نظم المعلومات على رفع كفاءة استخدام تقنيات الذكاء الاصطناعي في الأمن السيبراني للامتحانات.

4.3.5. استقصاء تجارب الطلاب مع المراقبة بالذكاء الاصطناعي (مثل الكاميرات الذكية وتحليل الأنماط) وتأثيرها على الخصوصية والأداء الأكاديمي.

5.3.5. بحث الجوانب الأخلاقية والقانونية لتطبيقات الذكاء الاصطناعي في مراقبة الامتحانات الإلكترونية، ووضع إطار سياسات يضمن التوازن بين النزاهة والخصوصية.

6.3.5. دراسة اقتصادية لقياس العائد على الاستثمار لتبني تقنيات الذكاء الاصطناعي في حماية الامتحانات الإلكترونية بالجامعات السودانية.

المصادر والمراجع

أ. المراجع العربية:

1. أبو غزال، محمود، وعدوي، محمد. (2020). معوقات تطبيق أنظمة الأمن السيبراني في التعليم الإلكتروني بالجامعات الفلسطينية. *مجلة الجامعة الإسلامية للدراسات التربوية والنفسية*، 28(3)، 123-156.

2. الغامدي، محمد بن عبدالله، والحربي، أحمد بن سعيد. (2021). فاعلية استخدام تقنيات الذكاء الاصطناعي في اكتشاف الغش الإلكتروني في الاختبارات عن بُعد: دراسة تطبيقية على الجامعات السعودية. *مجلة جامعة الملك سعود - علوم الحاسب والمعلومات*، 33(2)، 145-168.

ب. المراجع الاجنبية:

1. Sabbah, S. (2018). Electronic cheating in higher education: Forms and control mechanisms. *Journal of Educational Research, 21*(2), 87-104.
2. Akacha, A. (2023). Cybersecurity challenges of online examination systems: A review. *Journal of Information Security Research, 14* (2), 55-68.
3. Alamri, H., Alharbi, B., & Alghamdi, R. (2020). A comparative study of AI-based online proctoring systems. *IEEE Access, 8*, 2169-3536.

جـ. مواقع الإنترنت:

1. https://doi.org/10.1109/ACCESS.2020.3047678

استراتيجيات حماية الأمن القومي للدول

An Intelligent Hybrid Deep Learning Framework for DDoS Attack Detection and Classification in Modern Network Environments

Huda A. Eltarifi[1], Sally D. Abualgasim[2], Abubakr H. Ombabi[2], Eman Mohammed Hamid[3]

1. Department of Computer Science, **Faculty of Computer Science and Information Technology, University of Holy Quran and Re-Origination of Science, Rofaà, Sudan,** hudaeltarifi@gmail.com, huda@uofq.edu.sd
2. Department of Computer Engineering, **Faculty of Engineering and Technology, University of Gezira, Wad Madani, Sudan,** sally.dallah1@gmail.com, sallydallah@uofg.edu.sd
3. **Department of** Computer Science**, Faculty of Computer Science, University of Albutana, Rofaà, Sudan,** abubakr.h.ombabi@gmail.com
4. **Department of** Computer Science, **Faculty of Mathematical and Computer Science, University of Gezira, Wad Madani, Sudan,** Eman_24@hotmail.com

Abstract

Distributed Denial of Service (DDoS) attacks remain one of the most serious cybersecurity threats due to their ability to overwhelm network resources and disrupt service availability. The growing sophistication of modern DDoS attacks requires intelligent detection frameworks capable of accurately classifying malicious network traffic. This study proposes a hybrid CNN–BiLSTM-Attention framework for multi-class DDoS attack classification using the CIC-DDoS2019 dataset. Three representative attack categories, namely DrDoS_DNS, DrDoS_NTP, and SYN attacks, were selected from the original dataset, where 50,000 samples were randomly extracted from each category to construct the experimental dataset. Several preprocessing and feature engineering techniques were applied, including data cleaning, variance threshold filtering, correlation-based feature reduction, StandardScaler normalization, label encoding, and SMOTE-based balancing.In order to avoid data leakage and ensure fair evaluation, preprocessing and balancing operations were only performed within the training folds during Stratified 5-Fold Cross-Validation. The proposed framework is composed of 1D-CNN layers for spatial features extraction, BiLSTM layers for temporal dependency learning and Multi-Head Attention mechanisms for features relevance learning. The experimental results showed an excellent classification performance with an average accuracy of 99.67% ± 0.03, weighted Precision of 99.67%, weighted Recall of 99.67% and weighted F1-score of 99.67% over the five cross-validation folds. Additionally, the attention-based feature analysis identified several traffic-flow features as having a high impact, with Feature 5 (Total Length of Bwd Packets) and Feature 34 (Min Packet Length) having the highest relevance scores, 1.915 and 1.447 respectively. The obtained results show the

potential of hybrid deep learning and attention-based frameworks towards the development of reliable and intelligent DDoS detection systems for modern cybersecurity environments and future real-time network protection applications.

Keywords

DDoS Detection; Deep Learning; CNN–BiLSTM–Attention; CIC-DDoS2019; Intrusion Detection System; Multi-Class Classification; Network Security; Cybersecurity.

المستخلص

من أبرز التهديدات السيبرانية التي تواجه البنى التحتية الحديثة للشبكات، نظرًا لقدرتها (DDoS) تُعد هجمات حجب الخدمة الموزعة على استنزاف الموارد الحاسوبية وتعطيل الخدمات الحيوية. ومع التطور المستمر في أنماط هذه الهجمات وأساليب تنفيذها، أصبحت الحاجة ملحة إلى تطوير نماذج ذكية قادرة على الكشف الدقيق والتصنيف الفعال لحركة المرور الشبكية الضارة.

في هذه الدراسة، تم اقتراح إطار هجين قائم على تقنيات التعلم العميق يجمع بين الشبكات العصبية الالتفافية (CNN)، والشبكات العصبية ثنائية الاتجاه ذات الذاكرة طويلة وقصيرة المدى (BiLSTM)، وآلية الانتباه متعددة الرؤوس (Multi-Head Attention)، ولتنفيذ الدراسة، تم اختيار ثلاث مجموعة بيانات CIC-DDoS2019. متعددة الفئات باستخدام بهدف تصنيف هجمات DDoS، مع سحب 50,000 عينة عشوائيًا من كل فئة SYN وDrDoS_NTP و DrDoS_DNS فئات تمثيلية من الهجمات هي لتكوين مجموعة البيانات التجريبية.

شملت مرحلة المعالجة المسبقة وهندسة الخصائص عدة إجراءات أساسية، تضمنت تنظيف البيانات، وإزالة الخصائص منخفضة التباين باستخدام تقنية Variance Threshold، وتقليل الخصائص المتكررة عبر تحليل الارتباط، وتطبيع البيانات باستخدام StandardScaler، وترميز الفئات باستخدام تقنية Label Encoding، بالإضافة إلى معالجة عدم توازن البيانات بواسطة تقنية SMOTE، ولضمان نزاهة التقييم ومنع تسرب البيانات (Data Leakage)، تم تنفيذ جميع عمليات المعالجة المسبقة وموازنة البيانات داخل طيات التدريب فقط أثناء تطبيق أسلوب التحقق المتقاطع الطبقي بخمس طيات (Stratified 5-Fold Cross-Validation) لتعلم الخصائص المكانية، تليها طبقات 1D-CNN ويتكون النموذج المقترح من طبقات BiLSTM لاستخراج الاعتماديات الزمنية، ثم آلية Multi-Head Attention لتعزيز التركيز على الخصائص الأكثر أهمية وتأثيرًا في عملية التصنيف.

أظهرت النتائج التجريبية كفاءة عالية للإطار المقترح، حيث حقق متوسط دقة بلغ 99.67% ± 0.03، بالإضافة إلى متوسط موزونة بلغت 99.67% لكل منها عبر جميع طيات التحقق المتقاطع. كما كشف تحليل F1-Score و Recall و Precision الخاصية الأهمية المعتمد على آلية الانتباه عن مساهمة عدد من خصائص تدفق الشبكة بصورة كبيرة في عملية التصنيف، حيث سجلت أعلى درجات الأهمية بقيم بلغت 1.915 (Min Packet Length) والخاصية (Total Length of Bwd Packets) تشير هذه النتائج إلى فعالية دمج تقنيات التعلم العميق وآليات الانتباه في بناء أنظمة متقدمة للكشف عن هجمات DDoS وتصنيفها بدقة عالية، مما يعزز إمكانية توظيفها في أنظمة الحماية الشبكية الذكية والتطبيقات الأمنية الآنية ضمن بيئات الأمن السيبراني الحديثة.

الكلمات المفتاحية

، التعلم العميق، الشبكات العصبية الالتفافية والشبكات (DDoS) كشف هجمات حجب الخدمة الموزعة العصبية ثنائية الاتجاه ذات الذاكرة طويلة وقصيرة المدى وآلية الانتباه، مجموعة بيانات CIC-DDoS2019، أنظمة كشف التسلل، التصنيف متعدد الفئات، أمن الشبكات، الأمن السيبراني.

1.1 Introduction

The tremendous growth of cloud computing, Software Defined Networks (SDN), Internet of Things (IoT) and modern communication technologies, significantly increases the vulnerability of network infrastructures to cyber threats[1, 2].Distributed Denial of Service (DDoS) attacks are still among the most disruptive threats as they may exhaust network resources and halt the service availability [2, 3]. The increasing complexity and diversity of DDoS attack patterns has reduced the effectiveness of traditional rule-based intrusion detection systems [3, 4].

Traditional Machine Learning (ML) methods often fail to capture the complex spatial and temporal traffic characteristics in dynamic network environments [5, 6]. Deep Learning (DL) methods have attracted great attention due to their ability to automatically learn high-level feature representations from large-scale network traffic data [6, 7]. Convolutional Neural Networks (CNNs) are adept at extracting local traffic-flow pattern, and Bidirectional Long Short-Term Memory (BiLSTM) networks are capable of capturing the temporal dependency of sequential traffic data[[7].Recently, attention mechanisms have further improved traffic classification by highlighting the most informative network features[8].

This paper proposes a hybrid CNN–BiLSTM–Attention framework for multi-class DDoS attack classification using the CIC-DDoS2019 dataset to tackle the existing challenges of feature redundancy, class imbalance, overfitting and limited generalization ability. The proposed framework is based on traffic samples of DrDoS_DNS, DrDoS_NTP and SYN attack. It combines several preprocessing and feature engineering techniques, such as correlation based feature reduction, StandardScaler normalization and SMOTE based balancing within the training folds to avoid data leakage.

The proposed framework uses CNN, BiLSTM, and Multi-Head Attention mechanisms to improve the performance of multi-class DDoS attack classification and feature relevance learning.

1.2 Related Work

Incorporation of machine learning (ML) and deep learning (DL) into recent DDoS attacks detection research has proved to be helpful in enhancing detection rate and making networks more resilient against threats. For example, using the CICDDoS2019 and KDD-CUP dataset, Sakr et al. . [9] have experimented with Decision Tree, Gradient Boosting, SVM, KNN, and Random Forest, with Gradient Boosting giving close to 98.88%. Furthermore, through applying Random Forest, XGBoost, and LSTM on CIC-DDoS2019 and N-BaIoT data sets, Berríos et al. [10] were able to achieve an accuracy of

almost 99.96%. Similarly, Nassef [11] implemented a novel correlation-based feature selection alongside the optimized XGBoost and reported near-perfect results using benchmark intrusion data sets, while Ebrahem et al. [12] developed a light-weighted multi-class classifier utilizing CNB, KNN, RF, and LR on CIC-DDoS2019 data set, reporting near 99% accuracy in RF and KNN models using less computational resources. Even though these frameworks performed very well in DDoS detection, they were constrained by handcrafted feature generation process and conventional learning techniques.

In order to solve such problems, the recent works started to implement DL models with the ability to learn hierarchical and temporal representations of traffic automatically. Abdulmajeed and Husien [13] introduced MLIDS22 that is based on a combination of CNN and LSTM trained on datasets CIC-IDS2017 and CSE-CIC-IDS2018, which successfully generalizes through mixed-dataset learning. Ramzan et al. [7] evaluated RNN, LSTM, and GRU models utilizing datasets CICDDoS2019 and CICIDS2017, in which GRU demonstrated 99.54% multiclass accuracy and reduced execution time. Still, such recurrent models focused more on sequential learning.

Further studies introduced hybrid and attention-based learning techniques in order to achieve better performance in terms of traffic representation and robustness in classification. Specifically, Venkatraman et al. [8] introduced an attention-based self-ensemble method which used CNN, XGBoost, CNN-LSTM, and CNN-Random Forest achieving 98.69% accuracy with respect to CIC-DDoS2019 dataset. In addition, Wang et al[14] presented DDoS-MSCT, a hybrid approach combining CNN and Transformer model, achieving a high accuracy rate of 99.97% using local and global feature extraction. Moreover, Najar and Naik [15] introduced a lightweight deep neural network approach named CNN-BiLSTM-Attention which attained an accuracy rate of 99.78% with near-perfect ROC-AUC score while maintaining a low computational cost using CICDDoS2019 and Edge-IIoT datasets. Finally, Sathaporn et al. [16] presented a CNN-BiLSTM-Multi-Head Attention architecture achieving 97.78% accuracy with lightweight deployability in detecting DDoS attacks in clouds.

Apart from accuracy, more recent studies have focused on increasing explainability and transparency. For instance, Alzu'bi et al. [17] developed a DDoS attack classifier based on Explainable AI using transfer learning and LIME to interpret results on the datasets CICIoT2023 and CICDDoS2019, where the BiLSTM method obtained an accuracy of up to 99.82%. Similarly, Hayder et al. [18] performed a systematic review of 106 recent studies incorporating GNNs, Transformer models, and hybrid approaches, observing that hybrid models performed better than others owing to the ability to capture relationships and temporal dependencies together. However, there are still several open issues.

Research Gap

Although many recent ML and DL based DDoS detection approaches have achieved remarkable performance, there are still several unsolved limitations. Traditional ML models rely heavily on handcrafted features, and many DL frameworks focus on sequential or attention-based learning separately. Furthermore, many of the high performing studies rely on binary detection, limited evaluation strategies and data leakage during preprocessing and validation. Therefore, there is still a need for strong hybrid architectures that jointly integrate spatial, temporal and attention-based learning with leakage-aware evaluation and reliable multiclass DDoS classification using benchmark datasets such as CIC-DDoS2019.

1.3 Research Contributions

This study proposes a hybrid CNN–BiLSTM–Attention framework for multi-class DDoS attack classification based on the CIC-DDoS2019 dataset. The proposed framework leverages the spatial, temporal, and attention-based feature learning in an integrated deep learning architecture. Additionally, a comprehensive preprocessing pipeline was implemented, which included variance filtering, correlation-based feature reduction, StandardScaler normalization, and SMOTE balancing, while avoiding data leakage through training-only preprocessing during cross-validation. Experimental results showed excellent classification performance with an average accuracy of approximately 99.50% and high values of Precision, Recall, and F1-score. Moreover, we used attention-based feature analysis to find the most relevant traffic-flow features for attack classification**.**

2. Methodology

This study presents a hybrid Deep Learning framework for multi-class Distributed Denial of Service (DDoS) attack classification using the CIC-DDoS2019 dataset, as shown in Figure 1. The proposed methodology consists of several successive stages: dataset acquisition, preprocessing and feature engineering, data balancing, deep learning model construction, training and validation, and performance evaluation. The overall framework was designed to improve classification accuracy whilst minimizing feature redundancy, reducing overfitting and avoiding data leakage during model evaluation.

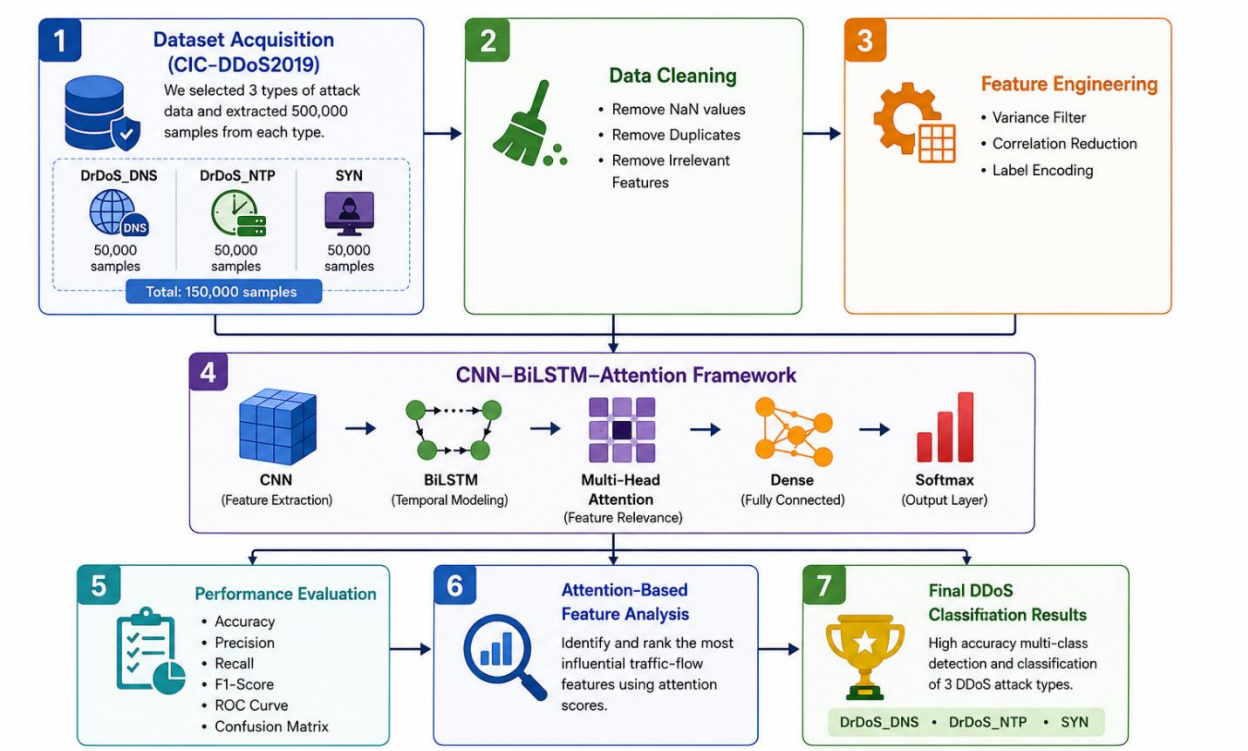


Figure 1. Overall workflow of the proposed CNN–BiLSTM–Attention framework for multi-class DDoS attack classification using the CIC-DDoS2019 dataset.

2.1 Dataset Description

The experiments were performed using the CIC-DDoS2019 dataset developed by the Canadian Institute for Cybersecurity (CIC), University of New Brunswick (UNB), Canada [19]. The dataset includes realistic benign and malicious network traffic generated to simulate modern DDoS attack scenarios[19, 20].Three representative attack categories were selected from the dataset 01-12 subset in this study, namely DrDoS_ DNS, DrDoS_ NTP and SYN attacks, due to their different flooding and reflection-based DDoS behaviors [19].

For the generation of the experimental dataset and computational efficiency reasons, only 50,000 samples were chosen randomly from each attack class, which gave around 150,000 traffic samples prior to data preprocessing. The preprocessed data consisted of samples classified as normal and attack traffic in four encoded classes, as shown in Table 1 below. As a result of the imbalance between benign and attack samples, SMOTE balancing was employed to enhance model generalization capabilities .

Table 1. Class Distribution of the Final Processed Dataset

Encoded Label	Traffic Type	Number of Samples
0	Benign	615
1	DrDoS_DNS	48,389

2	DrDoS_NTP	49,083
3	SYN	43,546

2.2 Data Preprocessing and Feature Engineering

Some preprocessing was done before model training to make sure that the data is clean and ready for deep learning classification. Firstly, the chosen attack subset was converted into a single dataset by eliminating infinite data, missing data, and duplicate data. Secondly, some irrelevant flow attribute features such as Flow ID, Source IP, Destination IP, Timestamp, Source Port, Destination Port, and Similar HTTP were dropped to eliminate redundancy.

After separation of the Label attribute from the rest of the attributes, all traffic flow related attributes were left as numerical features. The feature selection technique called Variance Threshold was then used with a threshold of 0.01 to eliminate low-information features. Lastly, Label Encoding was used to encode the target labels into numerical form.

2.3 Correlation-Based Feature Reduction

In order to address redundancy and avoid having highly correlated network traffic features, a correlation-based feature reduction method was used based on the Pearson Correlation Coefficient, which is calculated by

$$r_{xy} = \frac{\sum_{i=1}^{n}(x_i - \bar{x})\,(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2}\sqrt{\sum_{i=1}^{n}(y_i - \bar{y})^2}} \quad (1)$$

where x_i and y_i are the feature values, whereas $\bar{x}$ and $\bar{y}$ are the averages of each respective feature.

An absolute Pearson correlation matrix was created for all quantitative flow characteristics. The highly correlated features having a coefficient larger than 0.90 were deemed redundant and were dropped from the dataset. In order to avoid any data leakage, the process of reducing features based on correlation was done strictly on the training set for each cross-validation fold.

2.4 StandardScaler Normalization

Feature scaling was achieved by employing the technique called StandardScaler, which aims at scaling numerical values related to traffic flow for effective convergence during deep learning. The standardization procedure was done as follows:

$$z = \frac{x - \mu}{\sigma} \quad (2)$$

where x is the initial value of the feature, μ is the mean of the feature, and σ is the standard deviation.

Scaling was carried out only on the training dataset during cross-validation, but then was used for both validation and testing sets to avoid any possible data leakage problem.

2.5 SMOTE-Based Data Balancing

There were imbalanced classes found in the final preprocessed dataset because there was a small number of samples representing benign traffic in comparison with attacks. This problem was solved using the SMOTE algorithm, but only for the training data set during cross-validation.

Synthetic minority samples produced by the SMOTE method are created using the following formula:

$$x_{new} = x_i + \lambda(x_{nn} - x_i) \quad (3)$$

where x_i is a minority sample, x_nn is a nearest neighbor of this sample, and $\lambda \in [0,1]$ is a random number.

Whereas random oversampling repeats existing examples, which may lead to overfitting, SMOTE generates new data points, thus avoiding duplication and improving the balance between classes. To avoid data leakage, SMOTE was performed after dataset split, correlation filtering, and feature scaling at each training fold.

2.6 Proposed Deep Learning Architecture

The suggested architecture adopts a combination of CNN-BiLSTM-Attention model for classification of DDoS attacks into multiple classes, as shown in Figure 1. The proposed model is composed of a 1D-CNN layer with 128 filters and kernel size 3 for extracting spatial features, batch normalization, and MaxPooling layers for stabilizing the model during training and dimensional reduction purposes, respectively.

Then, a BiLSTM layer with 128 nodes was used to capture temporal relations between traffic flows in both directions. Moreover, a Multi-Head Attention with 4 attention heads was employed in order to improve feature importance learning. Lastly, Dense layers with Swish activation and dropout regularization layers were used before feeding data to the Softmax layer for classification.

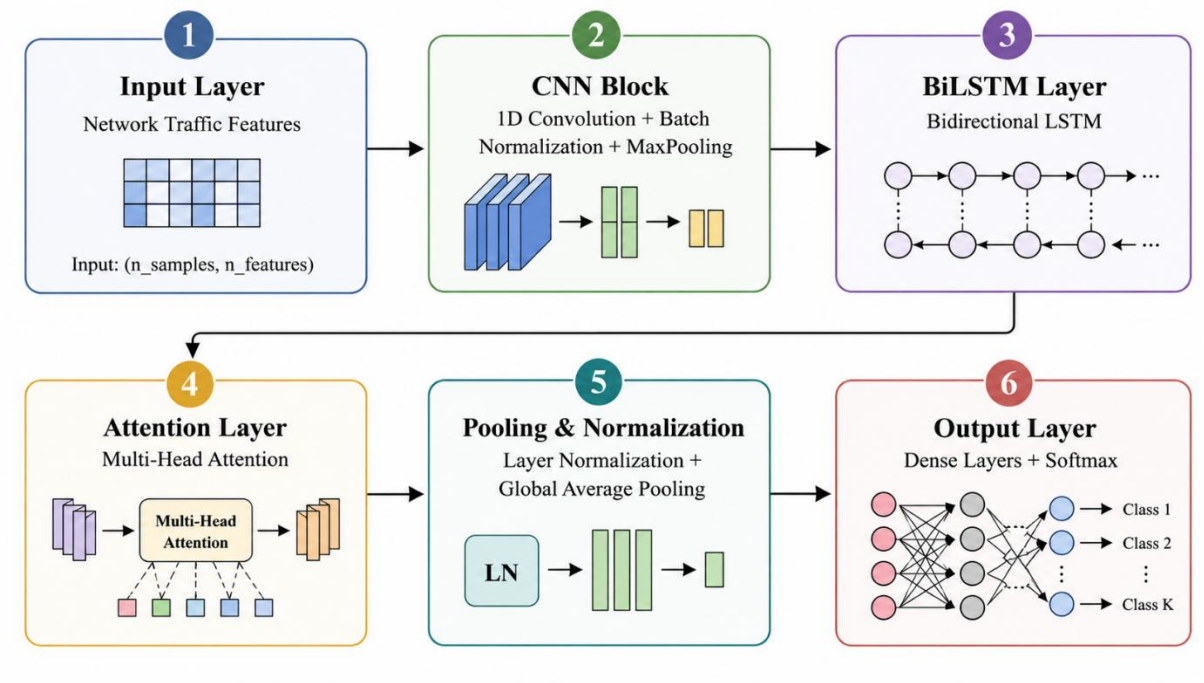


Figure2. Proposed CNN–BiLSTM–Attention architecture for multi-class DDoS attack classification.

Table 2. Hyperparameter Configuration of the Proposed CNN–BiLSTM–Attention Framework

Parameter	**Value**
CNN Filters	128
Kernel Size	3
BiLSTM Units	128
Attention Heads	4
Batch Size	128
Learning Rate	0.0001
Epochs	100
Optimizer	Adam

2.7 Training Strategy and Data Leakage Prevention

The stratified k-fold used in the framework was designed with the purpose of conducting an effective and unbiased evaluation, while keeping the balance between the classes within folds. Feature selection, normalization and oversampling were only performed on the training set within the k-fold process to avoid any possible data leakage.

The Adam optimizer with categorical cross entropy loss was used for model training in the framework. In addition, Early Stopping, ReduceLROnPlateau, Batch Normalization and Dropout were introduced to enhance the model performance.

2.8 Performance Evaluation Metrics

The suggested model was tested by using Accuracy, Precision, Recall, and F1-score measures. Moreover, confusion matrices and ROC curves were also computed to test the classification performance as well as the discrimination capability of the classifier. The weighted and macro-averaged scores for the measures were also calculated.

2.9 Experimental Environment

The experiments were performed on the Kaggle Cloud Computing platform with NVIDIA Tesla GPU support. The framework that has been proposed was designed using the programming language Python and TensorFlow, Keras, Scikit-learn, Pandas, NumPy, and Matplotlib libraries. GPU-based computing was used to enhance computational efficiency.

3. Results and Discussion

3.1 Classification Performance

As for the performance of the CNN–BiLSTM–Attention model, the results showed that the performance of the CNN-BiLSTM-Attention model was very promising in the classification of multi-class DDoS attacks based on the CIC-DDoS2019 dataset with 99.67% ± 0.03 accuracy for all five cross-validation sets. Moreover, the weighted Precision, Recall, and F1 score values of the CNN–BiLSTM–Attention model were about 99.67%.

Figure 2 shows that there is little misclassification between the classes of traffic, which proves the success of the proposed framework in recognizing distinct features of network traffic patterns.

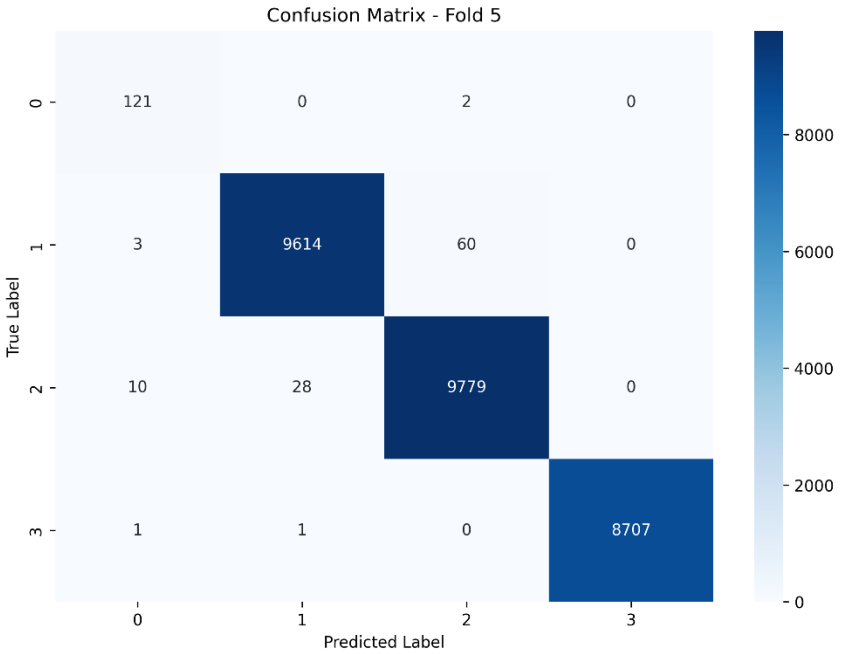
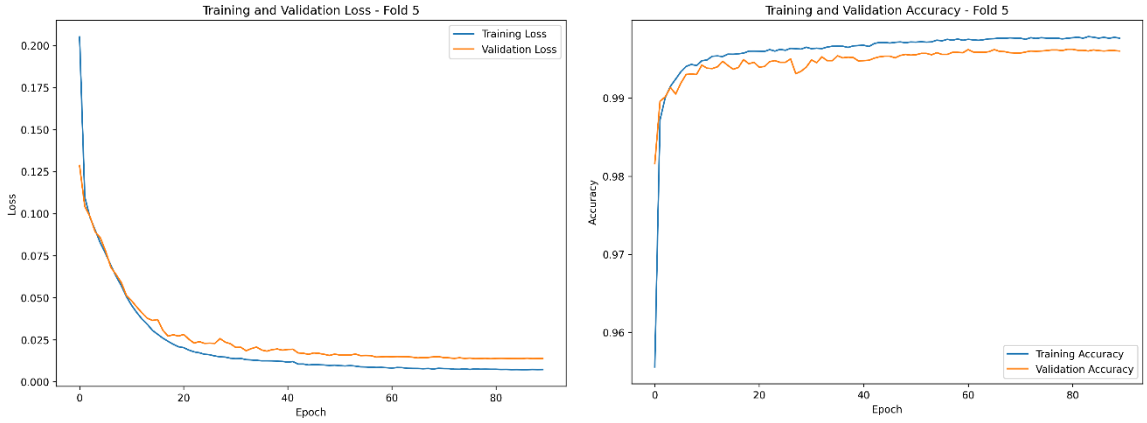


Figure 2.Confusion matrix of the proposed CNN–BiLSTM–Attention framework for multi-class DDoS attack classification.

3.2 Training and Validation Analysis

Fig. 3 shows the training and validation losses for the five-fold cross-validation experiment. The performance of the proposed CNN-BiLSTM-Attention architecture showed stable converging properties since there was consistent reduction in training and validation loss values throughout the training process. Training loss reduced from about 0.20 to 0.008 at the beginning and end of training, respectively, while validation loss remained constant at about 0.013–0.015.

The comparatively smaller difference between the training and validation graphs for all folds shows the effective generalization capability of the proposed approach. Moreover, the stability of the training process and consistent performance on the validation set show the successful use of the regularization and optimization techniques such as Batch Normalization, Dropout, Early Stopping, and



ReduceLROnPlateau. The maximum performance was attained after 60 to 70 epochs before early stopping was applied to the model.

Figure 3. Curves showing the accuracy and loss during training and testing of the proposed framework CNN-BiLSTM-Attention.

3.3 ROC Curve Analysis

The ROC curve was utilized to assess the discrimination ability of the proposed CNN-BiLSTM-Attention framework on different traffic classes. As shown in Figure 4, the model yielded AUC scores that were quite high for all the traffic classes, thereby showing its strong discrimination ability.

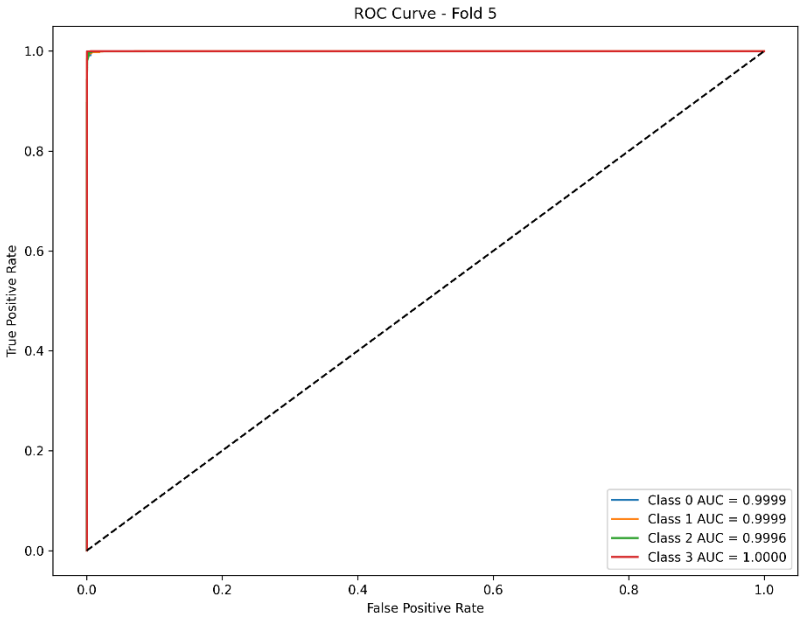


Figure 4. ROC curves and AUC values of the proposed CNN-BiLSTM-Attention model for multi-class DDoS attacks classification.

3.4 Cross-Validation and Data Leakage Prevention

This was achieved through the use of Stratified 5-Fold Cross Validation. The test sets were entirely unseen during both the preprocessing and the training process.

The above was necessary to avoid any data leakage into the validation and test sets. This was ensured by performing operations such as correlation-based feature reduction, Standard Scaler, and SMOTE to only the training set for each fold.

3.5 Effectiveness of Feature Engineering

Feature selection techniques such as variance threshold filtering and correlation-based feature reduction minimized redundant features and multicollinearity, and normalization using the StandardScaler improved the convergence of the model during training. Additionally, SMOTE balance improved the representation of the minority class during training.

Figure 5 shows the heatmap for correlation among the selected features of network traffic data.

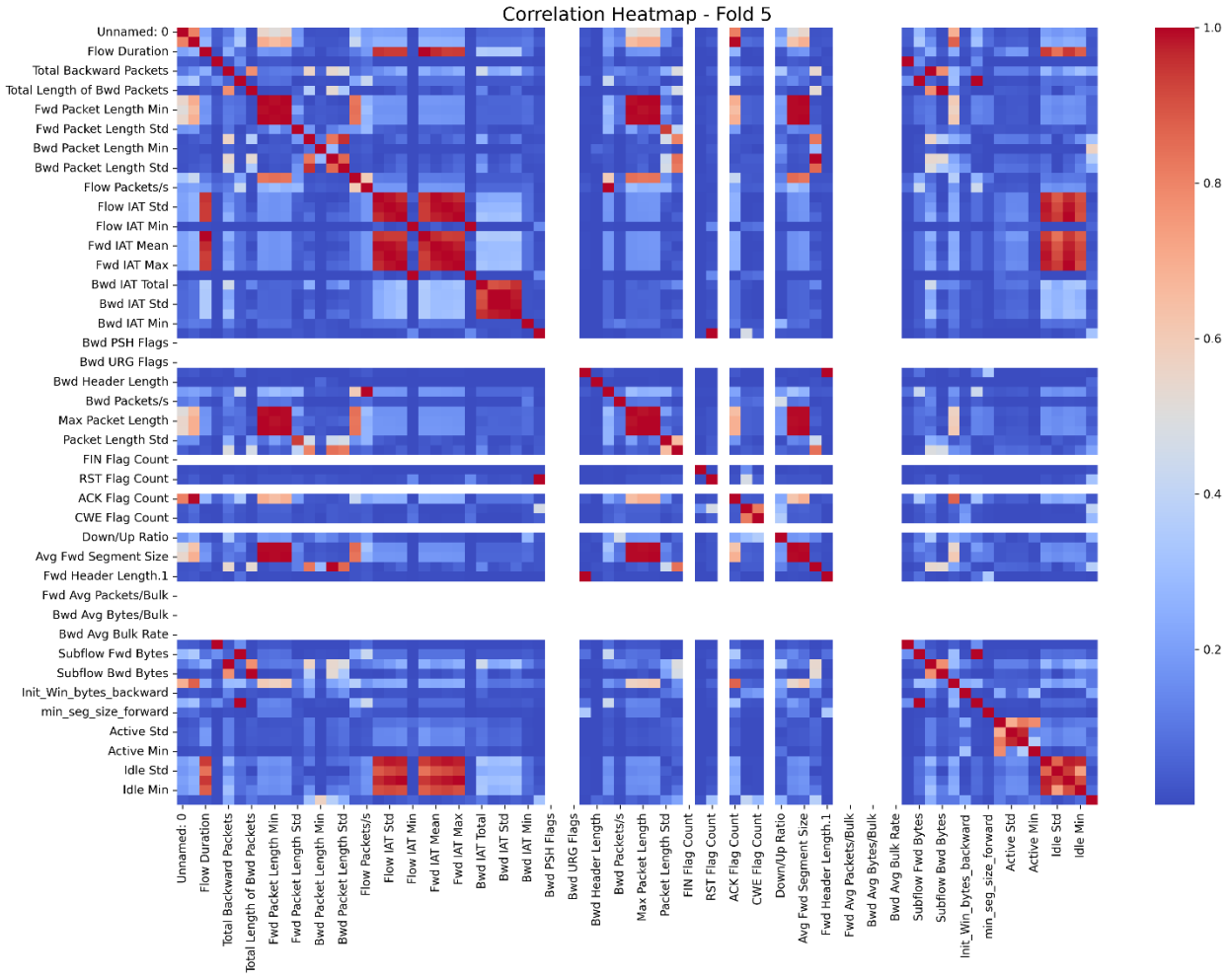


Figure 5. Correlation heatmap of the network traffic features used in the proposed framework.

3.6 Attention-Based Feature Relevance Analysis

In order to increase the interpretability of our model, the attention mechanism-based feature relevance study was conducted based on the weights obtained from the Multi-Head Attention mechanism. As shown in Table 3, a few features related to traffic flow obtained very high relevance scores and hence were found to contribute heavily in the task of multi-class DDoS attack classification. Particularly, Feature 5 and Feature 34 obtained the top two relevance scores of 1.915 and 1.447, respectively.

Table 3. Top Attention-Based Relevant Features

Feature Index	Relevance Score
5	1.915535
34	1.446652
12	1.445927
11	1.436646
39	1.181531
7	1.158834
57	1.103233
50	1.036934
3	0.932907
1	0.910445

3.7 Comparison with Existing Models

In order to conduct a more comprehensive evaluation of the suggested framework, a performance comparison was conducted against several recent works on DDoS attacks detection through machine learning and deep learning techniques. The comparison was not limited to classification accuracy alone but rather considered several other aspects that were part of the approach and methodology employed in those papers.

Table 4. Comparison of the Proposed Framework with Previous DDoS Detection Studies

Study	Dataset	Methodology	Classification Type	Accuracy	Key Limitation
Sakr et al. (2024)[9]	CICDDoS2019, KDD-CUP	Gradient Boosting / ML	Multi-class	98.88%	Handcrafted features and limited contextual learning

Berríos et al. (2025)[10]	CIC-DDoS2019, N-BaIoT	RF, XGBoost, LSTM	Multi-class	99.96%	Strong performance but primarily ML-based and dependent on feature engineering
Ebrahem et al. (2026)[12]	CIC-DDoS2019	CNB, KNN, RF, LR	Multi-class	≈99.00%	Lightweight ML with limited deep feature learning
Ramzan et al. (2023)[7]	CICDDoS2019, CICIDS2017	RNN, LSTM, GRU	Binary / Multi-class	99.54%	Sequential learning without attention mechanisms
Venkatraman et al. (2024)[8]	CIC-DDoS2019	Self-Attention Ensemble	Multi-class	98.69%	Ensemble complexity and limited temporal modeling
Wang et al. (2024)[14]	CIC-DDoS2019, CICIDS2017	CNN–Transformer	Binary / Multi-class	99.97%	Higher architectural complexity and limited explainability
Najar and Naik (2025)[15]	CICDDoS2019, Edge-IIoT	CNN–BiLSTM–Attention	Multi-class	99.78%	Limited dataset diversity and no leakage-aware evaluation
Sathaporn et al. (2025)[16]	BCCC-cPacket-Cloud-DDoS-2024	CNN–BiLSTM–MHA	Binary / Cloud DDoS	97.78%	Cloud-specific and limited multiclass generalization
Alzu'bi et al. (2024) [17]	CICIoT2023, CICDDoS2019	BiLSTM + XAI	Multi-class	99.82%	Interpretability emphasized more than architectural integration
Proposed CNN–BiLSTM–Attention	CIC-DDoS2019	CNN–BiLSTM–Multi-Head Attention	Multi-class	99.67% ±0.03	Increased computational complexity for large-scale deployment

From Table 4 above, it is clear that the proposed CNN-BiLSTM-Attention framework had very promising results when compared to other recent studies on DDoS detection. While other studies reported having slightly higher accuracy figures, it is important to note that the majority of these works utilized conventional machine learning algorithms, binary classification schemes, or failed to consider leakage in their preprocessing steps and validations.

3.8 Discussion

These experimental results show that the effectiveness of CNN-BiLSTM-Attention is proved in performing multi-class DDoS attacks classification on the CIC-DDoS2019 dataset. The combination of the above-mentioned CNN, BiLSTM, and Multi-Head Attention models led to an improvement of feature extraction and classification in terms of various traffic categories.

Moreover, the application of variance filter, correlation feature selection, StandardScaler transformation, and SMOTE technique positively impacted training stability by avoiding feature redundancies and class imbalances. In addition, the application of Stratified 5-Fold Cross-Validation and preprocessing during training only helped prevent data leakage.

Although the results were encouraging, the benign class produced marginally low precision and F1-scores because of the heavy class imbalance. Further research can concentrate on using larger datasets, more efficient models, and real-time application in IoT and SDN frameworks.

4. Conclusion and Future Work

In this research, a novel hybrid model CNN-BiLSTM-Attention was presented for multi-class DDoS attacks classification by utilizing the CIC-DDoS2019 dataset. Hybrid modeling is an integration of the spatial-temporal attention mechanism together with variance filtering, correlation-based feature selection, StandardScaler, and SMOTE preprocessing approaches.

The empirical experiments illustrated excellent prediction accuracy with an average accuracy of 99.67% ± 0.03 on five-fold cross-validation, accompanied by weights for precision, recall, and F1-score close to 99.67%. Moreover, attention-based relevance of traffic-flow feature for multi-class DDoS attacks classification was explored through the hybrid model. Using Stratified 5-Fold Cross-Validation and preprocessing methods on training data only ensured fair comparison without leaking data.

Although the results seem promising, there is the possibility that the suggested framework would show higher computational complexity in case of large-scale settings. Further research could consider performing tests of the framework using more data, as well as the development of light frameworks to be implemented in real-time. Another topic worth consideration would be the integration of XAI approaches.

Data Availability Statement

The dataset used in this study called CIC-DDoS2019 can be downloaded from the CIC official website or Kaggle Datasets official website.

Code Availability Statement

The source code used in this study can be provided by the corresponding author on request.

Conflict of Interest

Conflict of Interest: The authors have no conflicts of interest to declare.

References

1. Ouhssini, M., et al., *Advancements in detecting, preventing, and mitigating DDoS attacks in cloud environments: A comprehensive systematic review of state-of-the-art approaches.* Egyptian Informatics Journal, 2024. **27**: p. 100517.
2. Pakmehr, A., et al., *DDoS attack detection techniques in IoT networks: a survey.* Cluster Computing, 2024. **27**(10): p. 14637-14668.
3. Gelgi, M., et al., *Systematic literature review of IoT botnet DDOS attacks and evaluation of detection techniques.* Sensors, 2024. **24**(11): p. 3571.
4. Chen, X., S. Jing, and C. Zhao. *A Review of DDOS Attack Detection and Defense Technologies in SDN*. in *Proceedings of the 2025 11th Annual International Conference on Network and Information Systems for Computers*. 2025.
5. Ahmad, Z., et al., *Network intrusion detection system: A systematic study of machine learning and deep learning approaches.* Transactions on Emerging Telecommunications Technologies, 2021. **32**(1): p. e4150.
6. Ferrag, M.A., et al., *Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study.* Journal of Information Security and Applications, 2020. **50**: p. 102419.
7. Ramzan, M., et al., *Distributed denial of service attack detection in network traffic using deep learning algorithm.* Sensors, 2023. **23**(20): p. 8642.
8. Venkatraman, S., et al., *A novel self-attention-enabled weighted ensemble-based convolutional neural network framework for distributed denial of service attack classification.* IEEE Access, 2024. **12**: p. 151515-151531.
9. Sakr, H.A., et al., *Machine learning-based detection of DDoS attacks on IoT devices in multi-energy systems.* Egyptian Informatics Journal, 2024. **28**: p. 100540.
10. Berríos, S., et al., *A machine-learning-based approach for the detection and mitigation of distributed denial-of-service attacks in internet of things environments.* Applied Sciences, 2025. **15**(11): p. 6012.
11. Nassef, M., *Boosting intrusion detection against ddos attacks using a feature engineering-based fine-tuned xgboost model.* International Journal on Semantic Web and Information Systems (IJSWIS), 2025. **21**(1): p. 1-39.
12. Ebrahem, O., S. Dowaji, and S. Alhammoud, *A lightweight machine learning approach for DDoS detection and classification.* Scientific Reports, 2026.
13. Abdulmajeed, I.A. and I.M. Husien, *MLIDS22-IDS Design by Applying Hybrid CNN-LSTM Model on Mixed-Datasets.* Informatica, 2022. **46**: p. 121-134.
14. Wang, B., et al., *DDoS-MSCT: A DDoS Attack Detection Method Based on Multiscale Convolution and Transformer.* IET Information Security, 2024. **2024**(1): p. 1056705.
15. Najar, A.A. and S.M. Naik, *DDoS attack detection using CNN-BiLSTM with attention mechanism.* Telematics and Informatics Reports, 2025. **18**: p. 100211.
16. Sathaporn, P., et al., *DDoS detection using a hybrid CNN–RNN model enhanced with multi-head attention for cloud infrastructure.* Applied Sciences, 2025. **15**(21): p. 11567.
17. Alzu'bi, A., et al., *Explainable AI-based DDoS attacks classification using deep transfer learning.* Computers, Materials & Continua, 2024. **80**(3): p. 3785-3802.
18. Hayder, N.M.M.A., et al., *Graph and Transformer-Based Deep Learning Paradigms for DDoS Detection: A Systematic and Critical Survey.* Computers, Materials & Continua, 2026. **88**(1): p. 1.
19. Sharafaldin, I., A.H. Lashkari, and A.A. Ghorbani, *Toward generating a new intrusion detection dataset and intrusion traffic characterization.* ICISSp, 2018. **1**(2018): p. 108-116.
20. Saheb, M.C.P., et al. *A review of DDoS evaluation dataset: CICDDoS2019 dataset*. in *International Conference on Energy Systems, Drives and Automations*. 2021. Springer.

Next-Generation Security Frameworks for Model Context Protocol in Agentic AI Systems

shuruq Khalid Abdulredha

Directorate Education of Babylon, Ministry of Education, Iraq,

alalaakshuruq@gmail.com

Abstract

The Model Context Protocol (MCP) has become a core standard for connecting AI agents, particularly Large Language Models (LLMs), to external tools, data sources, and services. While this integration enables powerful new capabilities, it also creates a vast and novel attack surface not fully covered by traditional security models. In response, the research community has developed a variety of MCP security frameworks, including lifecycle-based threat modeling, in-depth defense architectures, zero-trust implementations, gateway/middleware solutions, in-run detection, and systematic benchmarking. While these frameworks significantly improve the security posture of MCP-based systems, persistent vulnerabilities and systemic risks remain, particularly concerning privilege management, semantic attack detection, and ecosystem-wide trust building. Ongoing research and standardization efforts are essential to address these gaps and ensure the secure and scalable adoption of MCP in AI environments. These frameworks aim to address vulnerabilities such as tool poisoning, point injection, privilege escalation, and supply chain attacks, while providing practical controls for secure enterprise adoption and ensuring robust agent workflows. This research reviews the current state of MCP security frameworks, their methodologies, strengths, and limitations.

Keywords:

MCP Security, Model Context Protocol, Runtime Detection, Cybersecurity Frameworks.

ملخص

معيارًا أساسيًا لربط وكلاء الذكاء الاصطناعي، (Model Context Protocol – MCP) أصبح بروتوكول سياق النماذج ، بالأدوات الخارجية ومصادر البيانات والخدمات. وعلى الرغم من أن هذا التكامل (LLMs) ولا سيما نماذج اللغة الكبيرة يوفّر قدرات جديدة وقوية، فإنه في الوقت نفسه يخلق سطح هجوم واسعًا وجديدًا لا تغطيه نماذج الأمن التقليدية بشكل كامل. ، بما في ذلك نمذجة التهديدات المعتمدة MCP واستجابةً لذلك، طوّر مجتمع البحث العلمي مجموعة متنوعة من أطر أمن ، وحلول البوابات (Zero Trust) على دورة الحياة، وبنى الدفاع متعددة الطبقات، وتطبيقات نموذج الثقة الصفرية

، وآليات الكشف أثناء التشغيل، إضافةً إلى أساليب القياس المعيارية (Gateway/Middleware) والبرمجيات الوسيطة المنهجية.

، فإن ثغرات MCP وعلى الرغم من أن هذه الأطر تُسهم بشكل كبير في تحسين الوضع الأمني للأنظمة المعتمدة على مستمرة ومخاطر نظامية لا تزال قائمة، ولا سيما تلك المتعلقة بإدارة الامتيازات، واكتشاف الهجمات الدلالية، وبناء الثقة على مستوى المنظومة البيئية ككل. وتُعد الجهود البحثية المستمرة وأنشطة التقييس ضرورية لسد هذه الفجوات وضمان اعتماد MCP بشكل آمن وقابل للتوسع في بيئات الذكاء الاصطناعي.

، (Point Injection) ، وحقن النقاط(Tool Poisoning) وتهدف هذه الأطر إلى معالجة ثغرات مثل تسميم الأدوات ، إلى جانب توفير (Supply Chain Attacks) ، وهجمات سلسلة التوريد(Privilege Escalation) وتصعيد الامتيازات ضوابط عملية لدعم الاعتماد الآمن على مستوى المؤسسات وضمان سير عمل قوي وموثوق للوكلاء الذكيين. وتستعرض هذه الدراسة الوضع الحالي لأطر أمن MCP، ومنهجياتها، ونقاط قوتها، وحدودها.

الكلمات المفتاحية: أمن بروتوكول سياق النموذج (MCP)، أطر الأمن، الكشف أثناء التشغيل، بروتوكول سياق النموذج السيبراني.

1. Introduction

The Model Context Protocol (MCP) has rapidly become a foundational standard for connecting AI agents, especially large language models (LLMs),to external tools, data sources, and services. This integration, while enabling powerful new capabilities, introduces a broad and novel attack surface that traditional security models do not fully address. this developed a range of security frameworks for MCP, spanning lifecycle-based threat modeling, defense-in-depth architectures, zero trust implementations, gateway/middleware solutions, runtime detection, and systematic benchmarking. While these frameworks significantly improve the security posture of MCP-based systems, persistent vulnerabilities and systemic risks remain, especially in privilege management, semantic attack detection, and ecosystem-wide trust. Ongoing research and standardization efforts are critical for closing these gaps and ensuring the safe, scalable adoption of MCP in AI-driven environments. These frameworks aim to address vulnerabilities such as tool poisoning, prompt injection, privilege escalation, and supply chain attacks, while providing actionable controls for secure enterprise adoption and robust agentic workflows (Narajala &Habler, 2025; Guo et al., 2025; Hou et al., 2025; Xing et al., 2025; Kumar et al., 2025; Bühler et al., 2025; Brett, 2025; Yang et al., 2025; Bhatt et al.,2025; Hasan et al., 2025). The following review synthesizes the current landscape of MCP security frameworks, their methodologies, strengths, and limitations.

2. Research Gaps

Despite the significant progress made in MCP security frameworks, several key research gaps remain that require future attention. First, privilege management and access control are hampered by the inadequacy of dynamic mechanisms for enforcing the principle of least privilege across multiple platforms, leaving significant vulnerabilities for abuse and illegitimate rights escalation. Second, at the attack level, vulnerabilities related to tool poisoning and command injection, as well as semantic, supply chain, and log attacks, persist and are not fully addressed in many existing frameworks.

Third, cross-platform adaptability presents another gap, as MCP frameworks struggle to ensure security when dealing with multiple environments due to differing protocols, tool versions, and access policies. Finally, at the formal verification and policy-independent detection level, the practical applications of these methods remain limited, although they have the potential to address many potential security vulnerabilities.

Overall, these gaps highlight the need for comprehensive, standardized, and proactive security solutions that integrate privilege management, advanced attack prevention, and adaptability to multiple environments to ensure the safe and reliable adoption of MCP in future AI systems.

3. Architecture and Security Approaches for MCP

3.1. Lifecycle and Threat-Taxonomy Frameworks

Lifecycle-based frameworks decompose the MCP server lifecycle into phases (creation, deployment, operation, maintenance) and map these to specific threat scenarios and attacker types. For example, one framework identifies 16 activities and 16 threat scenarios, providing fine-grained safeguards for each phase (Hou et al., 2025; Narajala & Habler, 2025; Bühler et al., 2025; Hasan et al., 2025). The MCP Attack Library (MCPLIB) and MCPSecBench offer systematic taxonomies and empirical attack libraries, enabling researchers to test and validate defenses against 31+ attack types, including direct/indirect tool injection, malicious user attacks, and LLM-inherent vulnerabilities (Guo et al., 2025; Yang et al., 2025).

3.2. Defense-in-Depth and Zero Trust Architectures

Enterprise-grade frameworks adapt NIST SP 800-53/800-207 and OWASP principles to MCP, layering network, identity, application, and monitoring controls. These frameworks emphasize defense-in-depth, zero trust, and continuous verification, with actionable controls for authentication, access management, and incident response (Narajala & Habler, 2025; Braun et al., 2022; Brett, 2025; Bhatt et al., 2025). Secure reference architectures illustrate practical

deployment patterns, while policy-based access control and cryptographic tool verification (e.g., ETDI) address tool poisoning and privilege escalation (Bhatt et al., 2025).

3.3. Gateway, Middleware, and Runtime Detection

Gateway and middleware frameworks, such as MCP Guardian and MCP Gateway, provide a security-first layer for MCP-based systems, integrating authentication, rate limiting, logging, WAF scanning, and zero trust tunneling (Xing et al., 2025; Kumar et al., 2025; Brett, 2025). MCP-Guard introduces a three-stage detection pipeline (static scan, neural detector, LLM arbitrator) for runtime threat detection, achieving high accuracy in identifying adversarial prompts and tool misuse (Xing et al., 2025). Information flow control systems (e.g., SAMOS) enforce session-level security policies at the gateway, blocking data leakage and indirect prompt injection (Ntousakis et al., 2025).

3.4. Auditing, Benchmarking, and Formal Methods

Systematic benchmarking tools like MCPSecBench and MSB provide reproducible, extensible platforms for evaluating MCP security across multiple hosts, attack types, and protection mechanisms (Yang et al., 2025; Zhang et al., 2025). Auditing tools (e.g., MCPSafetyScanner) and static analysis frameworks enable pre-deployment vulnerability detection and continuous monitoring (Radosevich & Halloran, 2025; Hasan et al., 2025). Formal methods and diagnostic tools (e.g., SafeMCP, MindGuard) offer policy-agnostic detection and provenance tracking for tool poisoning and decision-level attacks (Bühler et al., 2025; Wang et al., 2025).

4. Insights and Implications for MCP Security

The reviewed MCP security frameworks represent a rapid and multi-faceted response to the protocol's unique risks. Lifecycle and taxonomy-based models provide a structured approach to threat identification and mitigation, while enterprise and zero trust frameworks adapt established security principles to the dynamic, tool-centric nature of MCP (Narajala & Habler, 2025; Hou et al., 2025; Bhatt et al., 2025). Gateway and middle ware solutions offer practical, deployable controls for authentication, monitoring, and runtime protection, but may not fully address semantic or toolchain-level attacks (Xing et al., 2025; Kumar et al., 2025; Brett, 2025). Benchmarking and auditing tools are essential for systematic evaluation, revealing that over 85% of tested attacks can compromise at least one major MCP platform, underscoring the need for ongoing improvement (Yang et al., 2025;Zhang et al., 2025).

Despite these advances, significant challenges remain. Many frameworks focus on reactive monitoring rather than proactive prevention, and privilege management is still underdeveloped (Li et al., 2025). The open, decentralized nature of MCP complicates trust management, version control, and cross-platform security adaptation (Hou et al., 2025; Li et al., 2025). Formal verification and policy-agnostic detection are promising but not yetwidely adopted in production systems (Bühler et al., 2025; Wang et al., 2025). The field is moving toward standardization, with proposals for protocol-level extensions, trusted registries, and global certification standards (Kumar et al., 2025; Narajala et al., 2025).

The table below summarizes the key claims related to MCP security frameworks, assessing the strength of the evidence supporting each claim and providing a systematic interpretation of previous research findings. It illustrates how different frameworks—such as multi-layered defense, zero-trust, gateways, middleware, and auditing and benchmarking tools—contribute to mitigating security risks, while also highlighting current weaknesses and areas requiring future improvement. This summary provides the reader with a quick and comprehensive understanding of the relationship between MCP-based security practices and the available empirical and theoretical evidence.

Tabel 1: Comparative Assessment of Security Frameworks for MCP

Papers	Reasoning	Evidence Strength	Claim
(Narajala & Habler, 2025; Xinget al., 2025; Kumar et al., 2025;Brett, 2025; Bhatt et al., 2025)	Multiple studies show layered controls(auth, WAF, logging, policy) block tool poisoning, injection, and exfiltration	Strong	Defense-in-depth and zero trust frameworks significantly reduce common MCP attack vectors
(Xing et al., 2025; Kumar et al.,2025; Brett, 2025; Yang et al.,2025)	Gateways block many technical exploits but struggle with	Moderate	Gateway/middleware solutions are effective for authentication and

	prompt injection and toolchain-level attacks		monitoring but limited against semantic attacks
(Yang et al., 2025; Zhang et al.,2025)	MCPSecBench and MSB show widespread vulnerabilities across Claude, OpenAI, Cursor, and others	Moderate	Systematic benchmarking reveals >85% of attacks still succeed against at least one MCPplatform
(Li et al., 2025; Bhatt et al.,2025; Hasan et al., 2025)	Large-scale analysis shows excessive privileges and lack of dynamic permission models	Moderate	Privilege management and fine-grained access control are underdeveloped in current MCP frameworks
(Bühler et al., 2025; Wang et al.,2025)	Tools like Safe MCP and MindGuard show strong results in research but limited production deployment	Moderate	Formal verification and policy-agnostic detection are promising but not yet widely adopted
(Hou et al., 2025; Li et al., 2025;Narajala et al., 2025)	Studies highlight challenges in registry vetting, update pipelines, and platform-specific adaptation	Weak	Open, decentralized MCP ecosystems complicate trust, versioning, and cross-platform security

5. Comparing MCP Security Frameworks: Threat Models, Architectures, and Coverage

Lifecycle/Taxonomy Frameworks excel at identifying potential system failures, while Enterprise and Gateway Frameworks focus on enhancing and deploying secure environments. MCIP frameworks concentrate on improving the protocol interface itself, while tools like MCP-Guard, MCPSecBench, and MCPLIB provide attack measurement and detection capabilities. These frameworks work together to form an integrated ecosystem; however, robust privilege management, protocol-level normative changes, and effective cross-platform defenses remain open challenges requiring future attention.

Multiple MCP security frameworks exist with different goals: some model threats across the lifecycle, others define enterprise controls, gateway patterns, or runtime detection. Comparing them helps clarify what you get from each and where gaps remain. The following table compares the main MCP security frameworks, highlighting their differing objectives and outputs. Some frameworks focus on threat and lifecycle modeling, detailing the activities and threats at each stage of the MCP server process, while others emphasize enterprise controls and in-depth defense, encompassing network, identity, application, and monitoring. This table allows the reader to understand the core concept of each framework, its scope, and practical outputs, helping to identify strengths and remaining security gaps.

5.1. Threat & Lifecycle Frameworks vs. Enterprise Control Frameworks

Citations	Enterprise Defense-in-Depth(Narajala & Habler)	Lifecycle / Taxonomy (Hou et al.,MCPLIB, MCPSecBench)	Aspect
(Hou et al., 2025; Guo et al., 2025;Yang et al., 2025)	Map NIST/Zero Trust/OWASPcontrols to MCP layers	Map MCP server lifecycle to attackertypes and threats	Coreidea
(Hou et al., 2025; Guo et al., 2025;Narajala & Habler, 2025)	Network, identity, app, monitoringcontrols for enterprises	4 phases, 16 activities, 16 threatscenarios; 31–35+ attacks	Coverage
(Hou et al., 2025; Guo et al., 2025;Narajala & Habler, 2025)	Concrete control catalog,	Fine-grained safeguards per	Output

referencearchitectures , configs	phase,attack taxonomies

5.2. Gateway / Middleware vs. Protocol-Level & Runtime Frameworks

- Gateways / middleware (MCP Guardian, MCP Gateway):Provide central control points with auth, rate limiting, logging, WAF/IDS, and zero-trust tunneling; explicitly mapped to theNarajala & Habler framework to show layered coverage (Narajala & Habler, 2025; Kumar et al., 2025; Brett, 2025).
- Protocol-level (MCIP):Redefines MCP itself with contextual-integrity rules, explicit logging, and a safety-aware "guardrail" abstraction, guided byMAESTRO; adds a taxonomy and benchmark to train/evaluate LLM safety within MCP interactions (Jing et al., 2025).
- Runtime detection (MCP-Guard, scanners):MCP-Guard uses a 3-stage pipeline (static scan → neural detector → LLM arbitrator) plus MCP-AttackBench (70k+ samples),achieving ~89–96% detection metrics and focusing on semantic attacks and evolving threats (Xing et al., 2025).MCPSafetyScanner and industrial scanners emphasize pre-deployment auditing of arbitrary servers (Radosevich & Halloran,2025; Guo et al., 2025; Yang et al., 2025).

5.3. System-Level Comparisons & Gaps

- Comparative studies: MCPSecBench shows >85% of 17 attack types succeed against at least one major MCP platform, andcurrent protections (including some gateway-style defenses) have "little effect" against many attacks (Yang et al., 2025).
- Privilege management: Large-scale measurements of 2,562 MCP apps show pervasive over-privilege and argue that existingframeworks are mostly reactive, lacking dynamic least-privilege and platform-aware controls (Li et al., 2025).
- Architecture tradeoffs: Comparing MCP vs function calling, MCP offers better attack containment via explicit boundaries butintroduces complex cross-boundary trust and validation requirements (Gasmi et al., 2025).

6.Future Research Directions in MCP Security

Based on identified research gaps in MCP security frameworks, it is clear that there are urgent research needs to address shortcomings in privilege management, cross-platform adaptability, and standardized security criteria. These gaps indicate that future research should focus on developing proactive, standardized, and multi-environment security solutions that integrate formal verification and policy-independent disclosure to ensure sustainable security.

Accordingly, a set of open research questions has been identified, representing the key directions that future research should target to strengthen MCP security frameworks, provide a trusted and secure environment for future AI agents, and enhance the security of agent-based systems.

First, how can MCP frameworks implement dynamic, least-privilege access controls across diverse platforms? Excessive privileges are a major risk, hence the need for context-aware dynamic controls to ensure secure and scalable deployment.

Second, what protocol-level standards and validation processes can ensure trust in decentralized MCP records? Decentralized tool logs represent a major attack vector, while global standards and validation processes remain lacking, necessitating the development of reliable standard frameworks.

Third, how can formal verification and policy-independent disclosure be integrated into real-world MCP applications? Research tools have shown promise in this area, but their production adoption is limited, and their integration is a crucial step toward addressing key security gaps.

In summary, despite significant progress in MCP security frameworks, addressing privilege management, standardization, and formal verification techniques will remain essential for ensuring robust and sustainable security in agent-based AI systems.

7. Conclusion

This research examines Model Context Protocol (MCP) security frameworks in AI proxy systems, highlighting the unique security challenges posed by the MCP environment, such as tool poisoning, point injection, privilege escalation, and supply chain attacks. The study provided a comprehensive review of various frameworks, including lifecycle and classification frameworks, enterprise-level defense frameworks, gateway and middleware paradigms, and

measurement and auditing tools, outlining the scope, strengths, and practical outputs of each framework.

The comparison revealed that each framework category contributes significantly: lifecycle frameworks help accurately identify potential threats, enterprise and gateway frameworks provide mechanisms to enhance deployment environments, and tools such as MCP-Guard, MCPSecBench, and MCPLIB offer attack detection and measurement capabilities. However, privilege management, protocol standardization, and cross-platform security measures during operation remain key gaps requiring future research.

In conclusion, this research highlights that developing comprehensive and advanced security frameworks, integrating proactive controls, formal verification, and benchmarking, is crucial for ensuring the security of MCP in AI proxy systems, paving the way for the secure and reliable adoption of these protocols in future applications.

8. References

- Ashish, S. (2025). Model Context Protocol: A Context-Aware Framework for Enhancing Cybersecurity in Dynamic Environments. INTERNATIONALJOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT. https://doi.org/10.55041/ijsrem49289
- Bhatt, M., Narajala, V., & Habler, I. (2025). ETDI: Mitigating Tool Squatting and Rug Pull Attacks in Model Context Protocol (MCP) by using OAuth-Enhanced Tool Definitions and Policy-Based Access Control. ArXiv, abs/2506.01333. https://doi.org/10.48550/arxiv.2506.01333
- Braun, L., Demmler, D., Schneider, T., & Tkachenko, O. (2022). MOTION – A Framework for Mixed-Protocol Multi-Party Computation. ACMTransactions on Privacy and Security, 25, 1 - 35. https://doi.org/10.1145/3490390
- Brett, I. (2025). Simplified and Secure MCP Gateways for Enterprise AI Integration. ArXiv, abs/2504.19997.https://doi.org/10.48550/arxiv.2504.19997
- Bühler, C., Biagiola, M., Grazia, L., & Salvaneschi, G. (2025). Securing AI Agent Execution. ArXiv, abs/2510.21236.https://doi.org/10.48550/arxiv.2510.21236
- Gasmi, T., Guesmi, R., Belhadj, I., & Bennaceur, J. (2025). Bridging AI and Software Security: A Comparative Vulnerability Assessment of LLM Agent Deployment Paradigms. ArXiv, abs/2507.06323. https://doi.org/10.48550/arxiv.2507.06323

- Guo, Y., Liu, P., , W., Deng, Z., Zhu, X., Di, P., Xiao, X., & Wen, S. (2025). Systematic Analysis of MCP Security. ArXiv, abs/2508.12538.https://doi.org/10.48550/arxiv.2508.12538
- Halloran, J. (2025). MCP Safety Training: Learning to Refuse Falsely Benign MCP Exploits using Improved Preference Alignment. ArXiv,abs/2505.23634. https://doi.org/10.48550/arxiv.2505.23634
- Hasan, M., Li, H., Fallahzadeh, E., Rajbahadur, G., Adams, B., & Hassan, A. (2025). Model Context Protocol (MCP) at First Glance: Studying theSecurity and Maintainability of MCP Servers. ArXiv, abs/2506.13538. https://doi.org/10.48550/arxiv.2506.13538
- Hou, X., Zhao, Y., Wang, S., & Wang, H. (2025). Model Context Protocol (MCP): Landscape, Security Threats, and Future Research Directions. ArXiv,abs/2503.23278. https://doi.org/10.48550/arxiv.2503.23278
- Hou, X., Zhao, Y., Wang, S., & Wang, H. (2025). Model Context Protocol (MCP): Landscape, Security Threats, and Future Research Directions. ArXiv, abs/2503.23278. https://doi.org/10.48550/arxiv.2503.23278
- Jing, H., Li, H., Hu, W., Hu, Q., Xu, H., Chu, T., Hu, P., & Song, Y. (2025). MCIP: Protecting MCP Safety via Model Contextual Integrity Protocol. ArXiv, abs/2505.14590. https://doi.org/10.48550/arxiv.2505.14590
- Kumar, S., Girdhar, A., Patil, R., & Tripathi, D. (2025). MCP Guardian: A Security-First Layer for Safeguarding MCP-Based AI System. ArXiv,abs/2504.12757. https://doi.org/10.48550/arxiv.2504.12757
- Li, Z., Li, K., , B., Xu, M., Zhang, Y., & Cheng, X. (2025). We Urgently Need Privilege Management in MCP: A Measurement of API Usage in MCPEcosystems. 2025 IEEE 22nd International Conference on Mobile Ad-Hoc and Smart Systems (MASS), 555-560.https://doi.org/10.1109/mass66014.2025.00090
- Narajala, V., & Habler, I. (2025). Enterprise-Grade Security for the Model Context Protocol (MCP): Frameworks and Mitigation Strategies. ArXiv,abs/2504.08623. https://doi.org/10.48550/arxiv.2504.08623
- Narajala, V., Huang, K., & Habler, I. (2025). Securing GenAI Multi-Agent Systems Against Tool Squatting: A Zero Trust Registry-Based Approach.ArXiv, abs/2504.19951. https://doi.org/10.48550/arxiv.2504.19951.

- Ntousakis, G., Stephen, J., Le, M., Chukkapalli, S., Taylor, T., Molloy, I., & Araujo, F. (2025). Securing MCP-based Agent Workflows. Proceedings of the4th Workshop on Practical Adoption Challenges of ML for Systems. https://doi.org/10.1145/3766882.3767177
- Radosevich, B., & Halloran, J. (2025). MCP Safety Audit: LLMs with the Model Context Protocol Allow Major Security Exploits. ArXiv,abs/2504.03767. https://doi.org/10.48550/arxiv.2504.03767.
- Suggu, S. (2025). Agentic AI Workflows in Cybersecurity: Opportunities, Challenges, and Governance via the MCP Model. Journal of InformationSystems Engineering and Management. https://doi.org/10.52783/jisem.v10i52s.10767
- Wang, Z., Zhang, J., Shi, G., Cheng, H., Yao, Y., Guo, K., Du, H., & Li, X. (2025). MindGuard: Tracking, Detecting, and Attributing MCP Tool PoisoningAttack via Decision Dependence Graph. ArXiv, abs/2508.20412. https://doi.org/10.48550/arxiv.2508.20412
- Xing, W., Qi, Z., Qin, Y., Li, Y., Chang, C., Yu, J., Lin, C., Xie, Z., & Han, M. (2025). MCP-Guard: A Defense Framework for Model Context Protocol Integrity in Large Language Model Applications. ArXiv, abs/2508.10991. https://doi.org/10.48550/arxiv.2508.10991
- Yang, Y., Wu, D., & Chen, Y. (2025). MCPSecBench: A Systematic Security Benchmark and Playground for Testing Model Context Protocols. ArXiv,abs/2508.13220. https://doi.org/10.48550/arxiv.2508.13220
- Zhang, D., Li, Z., Luo, X., Liu, X., Li, P., & Xu, W. (2025). MCP Security Bench (MSB): Benchmarking Attacks Against Model Context Protocol in LLMAgents. ArXiv, abs/2510.15994. https://doi.org/10.48550/arxiv.2510.15994
- Zhao, S., Hou, Q., Zhan, Z., Wang, Y., Xie, Y., Guo, Y., Chen, L., Li, S., & Xue, Z. (2025). Mind Your Server: A Systematic Study of Parasitic ToolchainAttacks on the MCP Ecosystem. ArXiv, abs/2509.06572. https://doi.org/10.48550/arxiv.2509.06572

Technical and Pedagogical Challenges of Using the AI-Based Siraj Smart Educational Platform in Jordan

Dr. Shatha Sakher: Faculty of Medicine, Al-Balqa Applied University, As-Salt, Jordan, Shatha.sakher@bau.edu.jo , shatha.s.zoubi@gmail.com , https://orcid.org/0000-0001-6555-9911

ABSTRACT

Jordan's Ministry of Education introduced the Siraj smart educational platform as a cornerstone of the kingdom's digital transformation agenda in schooling. Positioned as an AI-supported environment for curriculum delivery, formative assessment, and teacher-student interaction, Siraj represents an ambitious effort to modernize public education through adaptive technologies. Yet the transition from policy aspiration to classroom practice has revealed a complex constellation of challenges that warrant sustained scholarly examination.

This study employs a qualitative analytical design grounded in systematic thematic analysis. Source material encompasses peer-reviewed literature published between 2022 and 2026, official Ministry of Education documentation, the Siraj platform's publicly available resources, World Bank and UNESCO reports on Jordanian education, and user-generated discourse from social media platforms including Facebook, X (formerly Twitter), YouTube, and educational forums active within the Jordanian context. The analysis is theoretically anchored in the Technology Acceptance Model (TAM) and the Technological Pedagogical Content Knowledge (TPACK) framework, both of which foreground the role of contextual and professional factors in shaping technology adoption.

Five interrelated thematic clusters emerge from the data: digital infrastructure and connectivity limitations, pedagogical integration and instructional design constraints, teacher readiness and professional development deficits, data privacy and algorithmic accountability concerns, and socially mediated user perceptions of the platform. Findings indicate that while Siraj carries genuine potential for personalized learning and curriculum alignment, its current implementation is constrained by uneven infrastructure, inadequately prepared teachers, limited alignment between platform affordances and classroom pedagogical practice, and unresolved questions about student data governance. Social media discourse reflects a predominantly critical public reception, though a discernible cluster of constructive educator engagement signals meaningful openings for more effective adoption. The study concludes with evidence-based recommendations for researchers, policymakers, and school practitioners working toward equitable and pedagogically grounded AI integration in Jordanian education.

Keywords: Siraj platform, AI in education, Jordan, educational technology, digital divide, TPACK, teacher readiness, data privacy, technology acceptance

INTRODUCTION

Digital transformation in education has moved from aspirational agenda to operational imperative across much of the Arab world. Jordan, which has maintained a comparatively progressive stance on educational reform within the region, has made the integration of artificial intelligence into schooling a stated national priority. The Siraj smart educational platform - deployed by the Ministry of Education as a hub for curriculum content, formative assessment, and teacher-student communication -embodies this commitment in institutional form, representing the most visible expression of the kingdom's effort to align its schools with twenty-first-century learning environments.

The platform's development is contextually situated within Jordan's National Education Strategy and regional frameworks such as the Arab Digital Economy Strategy, both of which identify AI-enabled schooling as a vehicle for improving learning outcomes and reducing educational inequality. Siraj is therefore not merely a technological product; it is a policy instrument, carrying with it assumptions about how artificial intelligence can enhance pedagogical practice, widen access to quality content, and produce more data-informed school management. These assumptions are not unreasonable on their face - they draw on a substantial international literature on the potential of adaptive learning systems - but they are assumptions nonetheless, and the history of educational technology reform is replete with cases where promising tools encountered conditions that their designers had not anticipated.

The scholarly literature on AI in education offers consistent caution against technological determinism. Studies conducted across both developed and developing country contexts document a persistent gap between what AI-based platforms are designed to accomplish and what teachers, students, and administrators experience in daily use (Holmes et al., 2022; Selwyn, 2022). In Jordan, this gap is shaped by material conditions - connectivity disparities between urban governorates and peripheral areas, shortages of appropriate device access, and a teaching workforce for whom digital upskilling has proceeded unevenly - alongside cultural and institutional factors that condition how new tools are received and integrated into existing professional practice.

This paper takes a qualitative analytical approach to examining these challenges in depth. Rather than evaluating Siraj's technical architecture against an idealized standard, the analysis grounds itself in what is documentable: platform features as described in official sources, educator and student responses visible in public discourse, comparative evidence from analogous initiatives in

the Arab world and beyond, and the growing body of educational technology scholarship that foregrounds equity, ethics, and pedagogical alignment. The aim is to produce a nuanced account of the platform's implementation challenges - one grounded in evidence and calibrated to the specific conditions of Jordanian schooling - that can inform the decisions of those responsible for shaping the platform's development.

RESEARCH PROBLEM

Despite the Ministry of Education's public commitment to embedding artificial intelligence in Jordanian schools through the Siraj platform, there is a marked deficit of peer-reviewed empirical research examining whether and how the platform is meeting its stated pedagogical objectives. Existing commentary is largely institutional in character — produced by the Ministry itself or by technology partners — and tends toward promotional framing rather than critical appraisal. Meanwhile, educator and student responses to the platform, expressed through social media platforms and educational forums, paint a considerably more complicated picture, surfacing technical frustrations, pedagogical mismatches, and governance concerns that official channels have not systematically addressed.

This asymmetry between official optimism and user-level experience constitutes the central analytical problem this study addresses. Without a grounded, evidence-based examination of the technical and pedagogical challenges embedded in Siraj's current implementation, policymakers lack the diagnostic information needed to make targeted improvements, and researchers lack a documented foundation from which to design future empirical work. The present study positions itself as a contribution to closing that gap.

RESEARCH QUESTIONS

This study is guided by the following research questions:

1. What technical challenges arise from the implementation of the Siraj platform in Jordanian educational settings, and how do infrastructure conditions shape user experience?
2. How do pedagogical and instructional design characteristics of the platform affect its effectiveness as an active learning tool?
3. What forms of interaction do teachers and students develop with the platform, and what barriers - professional, material, or institutional - shape those interactions?
4. What privacy, ethical, and data security concerns attend the platform's use, and how are they currently being addressed in official policy?

5. How do Jordanian educators, students, and parents perceive and discuss Siraj in public and social media discourse, and what do those perceptions reveal about implementation gaps?

6. What lessons from regional and international AI-in-education initiatives are transferable to the Jordanian context?

OBJECTIVES OF THE STUDY

The study pursues six principal objectives:

1. To document and analyze the technical challenges constraining the effective deployment of Siraj across Jordanian schools, with particular attention to infrastructure inequality.

2. To assess the platform's alignment with established principles of sound instructional design, active learning, and the adaptive use of AI in educational contexts.

3. To examine how teacher readiness, digital literacy levels, and the quality of professional development shape actual engagement with AI-supported teaching tools.

4. To identify data privacy and algorithmic accountability concerns relevant to a state-operated educational AI platform serving minor students.

5. To synthesize user perceptions and social media discourse as legitimate and analytically productive sources of evidence about platform reception and implementation quality.

6. To produce contextually grounded, evidence-based recommendations for improving AI integration in Jordanian public schools.

SIGNIFICANCE OF THE STUDY

Scholarship on AI in Arab-world educational contexts remains comparatively sparse relative to the volume of implementation activity occurring across the region. Jordan occupies a particularly instructive position: small enough for policy changes to be implemented at national scale within a manageable timeframe yet facing the resource and infrastructure constraints typical of middle-income countries navigating digital transitions. A rigorous qualitative analysis of Siraj's implementation challenges therefore contributes simultaneously to the region-specific literature on educational technology and to the broader field, which has repeatedly called for more contextually embedded studies of AI platforms in non-Western, resource-constrained settings (Crompton & Burke, 2023; Tlili et al., 2023).

The study also addresses a methodological gap that is characteristic of EdTech research in Jordan more broadly. Existing work has relied heavily on survey instruments and quantitative

measures of user satisfaction or adoption rates, producing aggregate pictures that can obscure the lived complexity of classroom technology use. Thematic analysis of qualitative sources- including social media discourse -offers a richer and more contextually sensitive analytical lens. This paper's treatment of digital community discourse as scholarly evidence, subject to appropriate methodological caveats, contributes modestly but meaningfully to expanding the evidentiary repertoire of educational technology research in the Arab world.

From a policy standpoint, the study is significant because it arrives at a moment when the Ministry of Education is still in a position to reshape the platform's implementation trajectory. The challenges identified here are structural but not intractable; they are amenable to policy responses that are specific, evidence-based, and practically achievable within Jordan's resource context. An analysis that articulates these challenges with precision is therefore more useful to policymakers than one that offers either broad praise or undifferentiated critique.

LITERATURE REVIEW

1. AI in Education: Frameworks, Findings, and Critical Perspectives

The academic literature on artificial intelligence in education has grown substantially since 2020, with increasing attention to implementation in resource-constrained, non-Western contexts. Holmes et al. (2022) provides one of the most comprehensive treatments of the ethical dimensions involved, arguing that AI in education raises foundational questions about fairness, transparency, and algorithmic bias that developers and policymakers have been slow to address in systematic ways. Their analysis is particularly relevant to platforms operating within national school systems, where algorithmic recommendations about student performance or content sequencing may not be transparent to teachers or students, and where the populations most directly affected - children in compulsory schooling - have limited capacity to contest automated decisions.

Crompton and Burke (2023) draw a useful distinction between AI as a content delivery mechanism and AI as a genuine pedagogical agent. The former describes systems that automate information presentation and discrete-item testing; the latter implies adaptive systems capable of responding to individual learning trajectories in ways that meaningfully reconfigure teaching and learning. Most AI platforms currently operating within school systems - including those deployed across the Arab world - function closer to the content delivery end of this spectrum, a gap between marketing claim and functional reality that experienced educators tend to identify relatively quickly in practice. This distinction is analytically central to evaluating Siraj's stated adaptive features against what teachers and students encounter.

Tlili et al. (2023), examining AI-based learning tools in educational contexts, observe that enthusiasm for AI adoption in schools frequently outpaces the evidence for specific learning benefits, particularly in contexts where foundational digital literacy is uneven among teachers and students. They caution against what might be termed technology-led adoption - circumstances in which platform availability shapes pedagogy rather than pedagogical need driving platform design. This caution resonates forcefully with the Jordanian situation, where Siraj's institutional deployment has proceeded in advance of the professional development infrastructure necessary for its meaningful use.

The ethics of student data collection in AI educational systems has attracted growing scholarly attention since 2022. Holmes et al. (2022) identify the granular extraction of behavioral and academic data from children as one of the most underregulated domains in educational technology, noting that consent frameworks designed for adult digital services are rarely appropriate for school-age users, and that institutional data governance in schools is typically inadequate to the surveillance potential embedded in modern AI systems. UNESCO's (2023) guidance document on generative AI in education reinforces these concerns, calling for explicit data minimization policies, clear notification protocols for students and parents, and meaningful human oversight of automated educational decisions — standards that few national school-level AI deployments have yet operationalized.

2. Digital Infrastructure and the Geography of Connectivity

Any substantive analysis of educational technology in Jordan must engage with the structural unevenness of the kingdom's digital infrastructure. The World Bank (2022) documents persistent disparities in connectivity and device access between urban centers - Amman, Zarqa, Irbid — and rural and peripheral governorates in the south and east, noting that these disparities reflect patterns of general public investment rather than technology-specific gaps. For educational platforms that assume reliable broadband access, this geography of connectivity creates fundamentally different learning environments across the country, with students in under connected areas effectively accessing a degraded version of the same platform that serves urban counterparts.

The International Telecommunication Union (2023) data on broadband penetration confirms this picture at the household level, with aggregate national figures that mask significant regional, socioeconomic, and gendered variation. Research from comparable MENA contexts has highlighted that girls in conservative rural households may face compound barriers to device access outside school hours - reflecting both household income constraints and socially shaped norms around device allocation - limiting their ability to engage with platforms that assume home-based access as a routine

component of learning (OECD, 2023). This gendered dimension of the digital divide is not incidental to educational equity; it is one of its most consequential expressions.

3. Teacher Readiness and the TPACK Framework

Perhaps no theme in the educational technology literature is more consistently documented than the centrality of teacher readiness to the success or failure of digital tool adoption. Mishra and Koehler's Technological Pedagogical Content Knowledge (TPACK) framework, extended and empirically validated in numerous subsequent studies, posits that effective technology-enhanced teaching requires the simultaneous development of content knowledge, pedagogical knowledge, and technological knowledge - and that deficits in any single dimension undermine the others. The framework's core insight - knowing how to operate a tool is categorically different from knowing how to use it to teach a specific subject well - has proven consistently robust across contexts (Rosenberg & Koehler, 2015).

Studies examining AI platform adoption in Jordanian and comparable Arab contexts have found that teacher preparation programs disproportionately address the technical mechanics of platform navigation rather than the subject-specific pedagogical integration that TPACK identifies as the more consequential competency (Al-Adwan et al., 2023). The result is a teacher workforce that may be operationally literate with a given platform but lacks the integrated knowledge to make meaningful pedagogical decisions about when, how, and why to deploy its features in relation to specific learning objectives. This operational pedagogical gap is particularly salient for AI-adaptive platforms, where the teacher's role shifts from content delivery to the interpretation and mediation of algorithmic recommendations - a shift that requires sophisticated professional judgment, not merely technical familiarity.

Selwyn (2022) advances a complementary critical argument: much professional development in educational technology is designed by technologists rather than educators, resulting in training that prepares teachers to operate platforms but not to think critically about whether and when those platforms genuinely serve learning. This distinction between operational competence and pedagogical wisdom resonates with what can be inferred from public discourse about Siraj-related professional development, where teacher commentary consistently suggests that Ministry training sessions have been procedurally focused rather than pedagogically integrative.

4. User Experience, Satisfaction, and Evidence of Social Media Discourse

Social media has become a significant informal arena for educational community discourse about adoption of technology, particularly in communities where formal feedback channels are

perceived as insufficiently responsive. In Jordan, Facebook groups for teachers and parents, YouTube commentary threads on educational platforms, and X (Twitter) exchanges among educators constitute a meaningful, if methodologically complex, corpus of user-generated evidence about platform experiences. These platforms do not produce representative samples in any conventional statistical sense, but they surface recurring concerns, patterns of productive use, and community sentiment that formal survey instruments rarely capture with equivalent granularity.

Akour et al. (2022), examining technology adoption among educators in Jordan and the wider Gulf context, find that social influence - including peer discourse in online communities - plays a significant role in shaping teachers' decisions to engage substantively with or distance themselves from new educational tools. This finding is consistent with TAM's extended formulations, which incorporate social norms and institutional context as adoption predictors alongside perceived usefulness and ease of use. For Siraj, the implication is that the quality of peer discourse about the platform - much of which is currently critical in tone - may itself be constraining adoption among educators who might otherwise be more receptive.

5. Regional and International Comparative Perspectives

Comparative evidence from similar initiatives elsewhere in the Arab world reveals that the challenges confronting Siraj are structurally common to national-scale AI education deployments in the region, though the capacity and speed of response vary. Saudi Arabia's Madrasati platform, scaled rapidly during the COVID-19 pandemic and subsequently enhanced with adaptive content features, encountered analogous challenges around teacher readiness and digital access inequality, but benefited from substantially greater public investment in device distribution and infrastructure. The contrast with Jordan is instructive precisely because it highlights how platform capabilities are a relatively small determinant of implementation success compared to the support ecosystem surrounding the platform.

The UAE's AI-in-education strategy - grounded in a comprehensive policy ecosystem, substantial per-student resource allocation, and a structured national AI curriculum - represents a ceiling that most MENA jurisdictions are not currently positioned to approach, making it a useful reference point but not a direct comparator. More transferable lessons come from Egypt's Edmodo-based and national platform experiences, where research has highlighted the importance of school-level administrative support and subject-specific professional development as mediating factors between platform availability and meaningful classroom integration (UNESCO, 2023).

From beyond the region, OECD (2023) analysis of AI in education across member and partner countries identifies a consistent pattern: the most effective implementations are characterized not by the sophistication of the AI itself but by the quality of the surrounding support ecosystem — sustained professional development, clear pedagogical frameworks, infrastructure investment calibrated to actual user conditions, and iterative feedback mechanisms that allow platform issues to be systematically identified and resolved. These conditions are achievable in the Jordanian context, but they require sustained policy commitment rather than technological procurement alone.

THEORETICAL FRAMEWORK

6. Technology Acceptance Model (TAM)

Developed by Davis (1989) and subsequently extended by numerous researchers in educational technology contexts, the Technology Acceptance Model identifies perceived usefulness and perceived ease of use as the primary determinants of user adoption of a new technology. In its extended formulations, TAM incorporates social influences, facilitating conditions, prior technology experience, and institutional context as additional variables shaping adoption decisions (Akour et al., 2022; Al-Adwan et al., 2023). For this study, TAM provides a conceptual language for interpreting the differentiated patterns of Siraj adoption and resistance documented in social media discourse and comparative literature, without reducing non-adoption to technophobia or irrationality.

Critically, TAM also directs attention toward the usability barriers that function as adoption thresholds - conditions under which users never reach the evaluative stage of assessing a platform's educational utility because technical friction has already foreclosed meaningful engagement. This threshold dynamic is particularly relevant for Siraj, where recurring technical complaints suggest that a significant portion of the teacher and student population has not accessed the platform's pedagogical features because interface, connectivity, or device issues have intervened first.

7. Technological Pedagogical Content Knowledge (TPACK)

The TPACK framework, introduced by Mishra and Koehler (2006) and operationalized in a substantial body of empirical research, insists that effective technology integration in teaching cannot be reduced to technical skill. It requires instead the integration of three knowledge domains: content knowledge (what is being taught), pedagogical knowledge (how it should be taught), and technological knowledge (how available tools can support that teaching). The intersections among these domains - Technological Content Knowledge, Technological Pedagogical Knowledge, and TPACK itself - define the zones of professional competence that distinguish genuinely transformative technology use from mere digital substitution.

For this study, TPACK provides the analytical lens for evaluating whether Siraj's design and implementation process has adequately supported this integrated form of teacher knowledge, or whether it has — as is structurally common in institutional EdTech rollouts - treated technological skill as a sufficient proxy for the richer professional development that effective classroom integration requires. The TPACK framework is especially valuable here because it locates the challenge not in the technology itself but in the professional ecosystem surrounding it, making it a productive framework for generating policy-relevant recommendations.

Together, TAM and TPACK constitute a theoretically coherent dual framework suited to the qualitative analysis that follows. TAM provides the individual-adoption lens; TPACK provides professional-knowledge lens. Their combination allows the analysis to account simultaneously for user-level barriers and institutional-level support deficits without reducing the complexity of Siraj's implementation to any single causal explanation.

METHODOLOGY

8. Research Design

This study employs a qualitative analytical design organized around systematic thematic analysis. The choice of qualitative methodology reflects both the exploratory nature of research questions and the absence of large-scale empirical data on Siraj's implementation outcomes. A qualitative approach is better suited than a quantitative one to generating conceptually rich, contextually grounded insights into a phenomenon that is still being actively shaped - where the aim is to understand the texture and structure of challenges rather than to measure their frequency across a representative sample.

9. Data Sources

The analysis draws on four categories of source material, each contributing a different perspective on Siraj's implementation landscape:

Academic literature constitutes the primary scholarly foundation. Peer-reviewed studies published between 2022 and 2026 on AI in education, educational technology adoption in Jordan and the Arab world, digital infrastructure, teacher readiness, and data privacy in learning platforms were systematically identified through Scopus, Web of Science, ERIC, and Google Scholar. Search terms included "AI in education Jordan," "smart learning platforms Arab world," "educational technology adoption MENA," "TPACK developing countries," and "data privacy in school AI platforms," applied individually and in combination. Priority was given to sources indexed in Scopus, Web of Science, and ERIC, with Taylor & Francis, Springer, ScienceDirect, and IEEE journals also represented.

Official documents provided institutional context for the analysis. Reports and announcements from the Jordanian Ministry of Education, official Siraj platform documentation and publicly accessible web resources, and relevant national policy statements were examined alongside regional documents from UNESCO, the World Bank, and the OECD.

Social media and public discourse were treated as a third data category. User-generated content from publicly accessible Jordanian Facebook groups for teachers and parents, YouTube video comment threads reviewing or demonstrating the Siraj platform, X (Twitter) exchanges involving hashtags related to Siraj and Jordanian education reform, and educator discussions on LinkedIn and educational forums were analyzed as discourse data. Content was approached as evidence of community sentiment and recurring concerns rather than as survey responses or representative samples.

Comparative case material drawn from secondary accounts of comparable deployments in Saudi Arabia, the UAE, Egypt, Finland, and South Korea provided the international reference frame for interpreting Jordan-specific findings.

10. Analytical Procedure

Thematic analysis followed the six-phase procedure described by Braun and Clarke (2006) and adapted for systematic document review contexts: familiarization with the data corpus, generation of initial codes, search for emergent themes, review and refinement of themes, definition and naming of final themes, and production of the analytical account. The coding process was iterative, with an initial inductive phase producing raw thematic clusters that were subsequently interpreted deductively against the TAM and TPACK frameworks to generate theoretically grounded explanations.

11. Ethical Considerations

As the study does not involve primary data collection from human participants, conventional research ethics review requirements do not apply. Social media data was handled with appropriate care: all analyzed content consists of publicly accessible posts, and no individually identifying information from private accounts is reproduced or cited. The analysis treats social media discourse as aggregate community evidence, attending to recurring patterns and sentiment clusters rather than to individual testimony.

RESULTS AND THEMATIC ANALYSIS

12. Theme 1: Technical Infrastructure and Connectivity Limitations

The most consistent finding across the data corpus is that the Siraj platform's technical performance is highly uneven across Jordanian governorates, with users in peripheral and rural areas

experiencing substantially greater difficulties than those in urban centers. Social media discourse surfaces recurring patterns of complaint: slow page loading and session timeouts during instructional activities, limited compatibility with older mobile browsers, audio-visual content that fails to stream reliably on lower-bandwidth connections, and intermittent platform unavailability during peak usage periods coinciding with school hours.

These observations align directly with documented patterns of digital inequality in Jordan. While national broadband adoption has expanded steadily, the quality and reliability of connectivity outside major urban centers remains insufficient to support data-intensive applications without supplementary infrastructure investment. The World Bank (2022) identifies this sub-national variability as a principal risk factor for digital public services in Jordan, noting that infrastructure conditions that appear adequate at national aggregate level can mask severe local constraints. The Siraj platform's current technical design does not appear to address this variability through adaptive measures such as offline content caching, low-bandwidth modes, or lightweight mobile interfaces — features that comparable platforms in other middle-income country contexts have developed precisely to extend reach beyond well-connected areas.

Device heterogeneity constitutes a related but distinct technical challenge. The COVID-19 period accelerated device distribution in Jordanian schools, but the resulting landscape is characterized by a wide hardware range - students and teachers using a mixture of personal smartphones, older tablets, school-issued devices of varying generations, and shared computer terminals. Siraj's interface appears optimized for a relatively modern device profile, and users with older hardware frequently report interface degradation, including elements that do not render correctly on older operating systems or within resource-constrained browser environments. This heterogeneity is not a temporary condition; it reflects the economic realities of a public school system with constrained per-pupil technology budgets.

13. Theme 2: Pedagogical and Instructional Design Challenges

A second major thematic cluster concerns the gap between the platform's stated pedagogical ambitions and its actual instructional design as experienced by teachers. Siraj is described in official Ministry documentation as an adaptive learning environment capable of personalizing content sequencing according to individual student performance data. However, teacher discourse analyzed in this study consistently suggests that the platform's adaptive features are either not consistently visible to educators in practice or are not sufficiently transparent in their logic to allow meaningful teacher interpretation or intervention.

This finding aligns with Crompton and Burke's (2023) critique of AI educational platforms that present adaptive features primarily as marketing differentiators without providing the pedagogical scaffolding that would allow teachers to interpret, interrogate, or supplement algorithmic content recommendations. For a teaching workforce trained primarily in direct instruction and curriculum-book-based approaches, integrating an AI-adaptive layer requires not merely technical training but a fundamental reconceptualization of the teacher's professional role - a reconceptualization that the Siraj implementation process has not yet systematically supported.

TPACK analysis of the available evidence suggests that teacher preparation for Siraj has been disproportionately concentrated in the Technological Knowledge domain - how to navigate the platform's interface and assign content - while substantially neglecting the Technological Pedagogical Knowledge dimension: how to integrate platform tools into subject-specific instructional sequences in ways that genuinely advance student learning. The consequence, visible in teacher social media discourse, is that the platform tends to be used primarily as a content display tool - a digital version of the textbook - rather than as an interactive environment capable of personalizing learning or generating diagnostic information about individual students.

Assessment functionality within the platform has generated specific pedagogical concerns. The platform includes quiz and structured assignment tools, but teachers report that these are better suited to assessing discrete knowledge recall than to evaluating the higher-order thinking competencies - analysis, argument, creative application - emphasized in Jordan's revised national curriculum. This tension between platform assessment affordances and curriculum aspirations is not a feature unique to Siraj; it reflects a structural characteristic of most current AI educational assessment systems (Holmes et al., 2022). But it creates a practical problem for teachers who feel professionally obligated to prepare students for both the curriculum's stated objectives and the narrower forms of knowledge the platform's tools are currently designed to measure.

14. Theme 3: Teacher and Student Interaction Patterns

Analysis of social media discourse and comparative literature identifies three distinct patterns of teacher engagement with the Siraj platform. A comparatively small proportion - typically younger educators with stronger prior digital competence and, in many cases, pre-existing familiarity with comparable platforms - engage with the platform's fuller range of features, integrating content delivery, assignment management, and student progress tracking into coordinated instructional routines. A substantially larger group uses the platform selectively and instrumentally, incorporating it into existing practices only where it replaces tasks - worksheet distribution, homework assignment tracking, absence notification - that were previously accomplished through less efficient manual

means. A third group, whose representation in social media discourse is smaller but whose situation is pedagogically significant, has effectively disengaged from substantive platform use while maintaining nominal compliance with institutional requirements through minimal login activity.

This trimodal pattern reflects findings documented across EdTech adoption studies in comparable national contexts, where implementation mandates without adequate professional support tend to produce compliance behaviors that register in platform analytics as engagement but do not correspond to meaningful pedagogical integration (Selwyn, 2022). The implication for Ministry evaluation is significant: platform usage statistics - login frequency, content access rates, assignment submission counts - are a poor proxy for genuine pedagogical engagement, and reliance on these metrics risks producing a misleading picture of implementation success.

Student interaction with Siraj displays analogous variation, shaped primarily by differential access to devices and home connectivity. Students who engage with the platform outside school hours - primarily for reviewing content and completing assignments - are concentrated among those with reliable home internet access and personal devices, reinforcing the connectivity-based inequalities documented in Theme 1. Students sharing devices with siblings or using mobile data subject to household data allowances face real constraints on the depth and consistency of their platform engagement. Younger students at the primary level report particular difficulty navigating the platform's interface without adult support, suggesting that the user experience design has not been adequately calculated for the full age range of the platform's intended user population.

Parent engagement with the platform, primarily through monitoring functions that display student progress and assignment submissions, has generated its own distinct set of concerns. Parents report difficulty interpreting automated progress reports - particularly where AI-generated performance indicators are presented without sufficient explanatory context - and express frustration at the gap between the information the platform provides and the richer, more qualitative accounts of student progress that they receive from face-to-face teacher communication.

15. *Theme 4: Data Privacy, Ethics, and Algorithmic Accountability*

The data practices associated with the Siraj platform constitute a domain where both academic literature and public discourse reveal significant unresolved concerns. The platform collects student behavioral data - including login frequency, time-on-task measures, assessment performance records, and content interaction patterns - and uses these data to generate progress reports and, in principle, to drive adaptive content recommendations. The privacy implications of this collection,

particularly for minor students in a compulsory public-school context, have not been comprehensively addressed in publicly available Ministry of Education documentation.

Holmes et al. (2022) argue that educational AI systems collecting granular behavioral data from children require, at minimum, explicit and affirmative consent mechanisms, robust data security infrastructure, clear policies governing data retention periods and third-party access rights, and transparent communication to students and parents about how collected data is processed and used. UNESCO (2023) reinforces these requirements, adding that algorithmic transparency - the practical ability to understand, contextualize, and contest automated decisions about a student's learning trajectory - constitutes a fundamental right that educational institutions adopting AI tools are obligated to protect.

Analysis of Siraj's publicly available terms and privacy documentation suggests that these standards have not yet been fully operationalized. Parent discourse on social media reflects an awareness of this gap: recurring questions about what data the platform collects, how long it is retained, who has access to it, and whether it may be shared with commercial technology partners reveal a user community that is neither uninformed about privacy concerns nor adequately reassured by existing official communication. The algorithmic transparency dimension is equally underaddressed: teachers report that the platform's content recommendations appear without explanatory rationale, leaving educators unable to evaluate whether an algorithmic content suggestion is appropriate for a specific student's current needs, learning style, or prior performance pattern.

The broader question of data sovereignty - whether the infrastructure on which student data is stored is subject to Jordanian legal jurisdiction, and whether the platform's AI components are provided by third-party technology vendors with their own data access provisions - does not appear to have been publicly addressed by the Ministry of Education. This is not a concern unique to Siraj; it reflects a systemic gap in how educational AI procurement is governed across many national contexts. But for a state platform serving children in compulsory schooling, the obligation to resolve these questions transparently is particularly pressing.

16. Theme 5: User Feedback and Social Media Perceptions

Social media discourse about Siraj reveals a public conversation that resists reduction to either enthusiastic endorsement or blanket rejection. Three broad sentiment clusters emerge from the analyzed content, each illuminating a different dimension of the platform's reception.

The first cluster, quantitatively dominant in the teacher and parent Facebook groups analyzed, consists of operational complaints about specific technical and usability failures: interface bugs, login authentication problems, slow content loading, confusing navigation hierarchies, and mismatches between assigned content units and the actual curriculum sequence students are following in their classrooms. These posts are notable not only for their frequency but for their tone, which tends to be constructive - users articulate what would need to change for the platform to function as described, suggesting a community that remains willing to engage with the technology if its practical obstacles were substantively addressed. This orientation toward problem-solving, rather than categorical rejection, is an important signal for platform improvement strategy.

The second cluster, better represented on X (Twitter) and in LinkedIn discussions among more senior educators, consists of principled skepticism about AI-based education as a reform instrument. This discourse situates Siraj within a broader critique of technology-driven educational change, arguing that the platform substitutes technological novelty for the curriculum investment, class-size reduction, and teacher salary improvements that educators identify as the more consequential determinants of educational quality. These arguments draw on both locally grounded frustrations and international debates about the efficacy limits of EdTech as a school improvement mechanism (Selwyn, 2022). This cluster of discourse is analytically significant because it represents a form of resistance that technical platform improvements alone are unlikely to address.

The third cluster - smaller in volume but strategically important for policy - consists of genuine and specific enthusiasm from educators who have identified productive uses for the platform within their teaching contexts. These posts originate predominantly from STEM subject teachers who have used Siraj's exercise content to supplement their in-class instruction for students who need additional practice opportunities, and from teachers who have found the assignment management functions more efficient than previous manual approaches. Their accounts suggest that the platform demonstrates real utility when used as a supplementary resource rather than as a primary delivery mechanism - a finding with direct implications for how the Ministry positions the platform's role in official pedagogical guidance.

DISCUSSION

The thematic analysis converges on several conclusions that require extended interpretive treatment, particularly considering the theoretical frameworks mobilized in this study.

First, the implementation of Siraj illustrates what might be characterized as a structural readiness gap - a temporal and material mismatch between the pace at which the platform has been

made institutionally available and the pace at which the professional, infrastructure, and governance conditions necessary for its effective use have been developed. This gap is not unique to Jordan; it is, as Selwyn (2022) documents across multiple national contexts, a recurring feature of technology-led educational reform, where platform procurement timelines are typically determined by procurement cycles and technology availability rather than by assessments of educational readiness. What distinguishes the Jordanian situation is the compounding of this readiness gap with genuine infrastructure inequality, creating conditions in which some schools face simultaneously inadequate professional preparation and inadequate technical conditions - a compound challenge that requires compound policy responses.

Second, TAM-based analysis of adoption patterns suggests that perceived ease of use, rather than perceived usefulness, is the dominant adoption variable shaping current teacher engagement. Educators who find the platform technically unreliable do not reach the evaluative stage of assessing its educational utility; usability barriers function as primary thresholds that determine who engages substantively with the platform's pedagogical features at all. This has a significant practical implication: investments in improving platform usability - particularly for lower-bandwidth contexts, older devices, and primary-school-aged users - are preconditions for meaningful pedagogical integration, not alternatives to it. Addressing pedagogical design without first resolving usability is unlikely to shift adoption patterns among the majority of the current user population.

Third, the TPACK-based analysis reveals that the form of professional development surrounding Siraj has been structurally mismatched to the form of knowledge that effective AI-platform integration requires. Training that produces operational competence - knowing how to navigate the interface - does not produce the Technological Pedagogical Content Knowledge that enables teachers to make meaningful decisions about when and how to use the platform to advance specific learning objectives. Bridging this gap requires professional development that is sustained rather than episodic, subject-specific rather than generic, and centered on pedagogical decision-making rather than platform mechanics. This is a resource-intensive but analytically well-supported recommendation.

Fourth, the data privacy theme raises concerns that deserve particular emphasis in the policy context. State-operated educational AI platforms differ importantly from commercial EdTech products in one crucial respect: the state has a direct, legally and ethically grounded duty of care toward the minor students enrolled in its compulsory school system. When the Ministry of Education deploys a platform that collects granular behavioral data from schoolchildren, the obligation to establish robust data governance - including meaningful consent mechanisms, data minimization standards, retention

limits, security audit requirements, and algorithmic transparency provisions - is not merely a technical best practice but a dimension of educational rights and public accountability. The current gap between data collection practice and governance infrastructure on the Siraj platform is a structural vulnerability that warrants policy-level intervention in advance of, rather than in response to, a significant privacy incident.

Fifth, the diversity of social media sentiment - particularly the existence of a genuine cluster of constructive and productive user experience - contains an important practical signal. Siraj is not uniformly experienced as ineffective; it is experienced very differently depending on subject area, school infrastructure, teacher digital competence, and how the platform is positioned relative to existing instructional routines. The teachers who report genuinely useful platform experiences are not outliers to be dismissed; they are exemplary practices whose practices warrant careful documentation and systematic dissemination. Understanding what distinguishes productive from unproductive platform experiences is more valuable for policy improvement than aggregate sentiment measurement.

Finally, the comparative perspective provides both context and caution. Jordan is not exceptional in encountering these challenges; structurally similar challenges have been documented in Saudi Arabia's Madrasati rollout, in Egypt's national platform deployments, and in numerous cases beyond the Arab world. What the most successful implementations share is not superior AI technology but a superior support ecosystem: sustained professional development, explicit pedagogical frameworks for platform use, infrastructure investment calibrated to actual rather than ideal user conditions, and feedback mechanisms that allow platform problems to be identified and resolved systematically. These are policy design questions, and they are answerable.

RECOMMENDATIONS

Based on the analysis presented, the following recommendations are offered for policymakers, school administrators, teacher educators, and platform developers. These recommendations are grounded in the evidence reviewed and calibrated to what is achievable within Jordan's current institutional and resource context.

17. For the Ministry of Education and Policymakers

A school-level digital readiness audit should precede any expansion of platform-dependent instructional requirements to schools in under connected governorates. This audit should assess connectivity quality, device availability, and technical support capacity at the individual school level

and use findings to sequence implementation in ways that match platform demands to actual infrastructure conditions. Low-bandwidth content modes and offline access functionality should be developed as implementation priorities rather than deferred enhancements.

A comprehensive student data governance policy for the Siraj platform should be developed, publicly released, and updated on a regular cycle. This policy should address, at minimum: what data is collected, how it is stored and protected, retention periods, conditions under which data may be accessed by third parties, parent and student notification protocols, and mechanisms for contesting automated decisions. The OECD (2023) and UNESCO (2023) guidance frameworks provide directly applicable international standards from which such a policy can be constructed.

An independent, peer-reviewed evaluation of the platform's impact on student learning outcomes should be commissioned, with findings made publicly available. This evaluation should stratify results by governorate, school type, subject area, and socioeconomic context to identify equity implications and to distinguish platform effects from the effects of surrounding conditions.

18. For Professional Development Program Designers

Teacher professional development for Siraj should be redesigned around the TPACK framework, ensuring that subject-specific pedagogical integration - not platform navigation - becomes the central focus of training. Training should be differentiated by curricular subject area, should involve collaboration between educational technology specialists and experienced classroom teachers from each domain, and should be delivered through sustained cycles rather than one-time orientation sessions.

Mentoring structures that connect early-adopter teachers who have developed productive platform practices with colleagues who are less engaged should be formalized and resourced. The social influence dimension of TAM suggests that peer modeling is likely to be more effective in shifting adoption patterns than formal institutional training alone.

19. For Platform Developers and Technical Teams

Algorithmic transparency mechanisms should be incorporated into the teacher-facing interface. Content and assessment recommendations generated by the platform's AI components should be accompanied by plain-language explanations of the reasoning behind them and should include clear override mechanisms that allow teachers to exercise professional judgment in response to algorithmic suggestions. This transparency is simultaneously an ethical requirement and a practical precondition for teacher trust.

A formal, in-platform user feedback channel should be established that allows teachers and students to report technical and pedagogical issues in structured ways. Current informal feedback through social media is insufficiently systematic to generate actionable improvement data; structured in-platform feedback, analyzed regularly by a dedicated product development team, would produce a substantially more useful signal.

20. For Researchers

Longitudinal empirical studies examining Siraj's adoption trajectories and learning impacts across diverse school contexts are urgently needed. Qualitative case studies of schools where the platform is being used productively would be particularly valuable for identifying the conditions that enable effective integration. Mixed-methods designs that combine TAM-derived survey data with classroom observation and teacher interview would allow the integration of micro-level and macro-level perspectives that the current literature on Jordanian EdTech has treated separately.

CONCLUSION

The Siraj smart educational platform represents a genuine and consequential commitment by Jordan's Ministry of Education to modernizing public schooling through artificial intelligence. Its ambition - to create an adaptive, data-informed, and widely accessible learning environment - reflects the best current thinking in educational technology and aligns with the kingdom's legitimate developmental aspirations. These aspirations deserve to be taken seriously, which is precisely why the gap between them and the current implementation reality warrants the kind of careful analysis this paper has attempted.

The analysis has identified five interconnected challenge clusters: uneven digital infrastructure, pedagogical design limitations, inadequate teacher preparation, unresolved data governance, and a fragmented user experience landscape. These are not independent problems with independent solutions; they are structurally interrelated, and policy responses that address only one dimension while leaving the others untouched are unlikely to produce the improvements that both the Ministry and the educational community are seeking. The infrastructure challenge undermines the potential benefits of pedagogical investment; the professional development challenge limits the educational value that even well-designed content can generate; the data governance gap erodes the trust that sustained platform engagement requires.

What the comparative evidence suggests most clearly is that Siraj's trajectory is not predetermined. Platforms in comparable national contexts have moved from troubled early implementations to genuinely productive educational tools - but those transitions have required

sustained policy attention, meaningful resource investment in support ecosystems, and a willingness to treat user-generated criticism as valuable improvement information rather than inconvenient noise. The social media evidence reviewed in this study is, in fact, an asset: it provides a detailed, honest, and ongoing account of what is and is not working from the perspective of the people the platform is designed to serve. A Ministry and a development team that approach that evidence with genuine receptivity have the diagnostic information they need to improve.

Jordan's educational technology ambitions are achievable. The Siraj platform is not an inherently flawed instrument; it is a capable tool operating in an ecosystem that has not yet been adequately built around it. The path forward lies not in replacing the platform but in building the professional, infrastructural, and governance conditions that would allow its genuine potential to be realized — equitably, transparently, and in the service of learning.

REFERENCES

Akour, I., Al-Maroof, R. A., Alfaisal, R., & Salloum, S. (2022). A conceptual framework for determining metaverse adoption in educational settings: The role of instructors' competencies and satisfaction. Computers and Education: Artificial Intelligence, 3, 100059. https://doi.org/10.1016/j.caeai.2022.100059

Al-Adwan, A. S., Li, N., Al-Adwan, A., Abbasi, G. A., Albelbisi, N. A., & Habibi, A. (2023). Extending the Technology Acceptance Model (TAM) to predict university students' intentions to use metaverse-based learning platforms. Education and Information Technologies, 28(11), 15381–15406. https://doi.org/10.1007/s10639-023-11549-3

Al-Fraihat, D., Joy, M., Masa'deh, R., & Sinclair, J. (2020). Evaluating E-learning systems success: An empirical study. Computers in Human Behavior, 102, 67–86. https://doi.org/10.1016/j.chb.2019.08.004

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Crompton, H., & Burke, D. (2023). Artificial intelligence in higher education: The state of the field. International Journal of Educational Technology in Higher Education, 20(1), 22. https://doi.org/10.1186/s41239-023-00392-8

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340. https://doi.org/10.2307/249008

Gayed, J. M., Carlon, M. K. J., Oriola, A. M., & Cross, J. S. (2022). Exploring an AI-based writing assistant's impact on English language learners. Computers and Education: Artificial Intelligence, 3, 100055. https://doi.org/10.1016/j.caeai.2022.100055

Holmes, W., Porayska-Pomsta, K., Holstein, K., Sutherland, E., Baker, T., Shum, S. B., Santos, O. C., Rodrigo, M. T., Cukurova, M., Bittencourt, I. I., & Koedinger, K. R. (2022). Ethics of AI in education: Towards a community-wide framework. International Journal of Artificial Intelligence in Education, 32(3), 504–526. https://doi.org/10.1007/s40593-021-00239-1

International Telecommunication Union. (2023). Measuring digital development: Facts and figures 2023. ITU Publications. https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

Jordan Ministry of Education. (2022). National education strategic plan 2022–2025: Towards a knowledge-based society. Ministry of Education.

Jordan Ministry of Education. (2023). Siraj platform overview and educational objectives. Ministry of Education. https://siraj.moe.gov.jo

Mishra, P., & Koehler, M. J. (2006). Technological pedagogical content knowledge: A framework for teacher knowledge. Teachers College Record, 108(6), 1017–1054. https://doi.org/10.1111/j.1467-9620.2006.00684.x

OECD. (2023). Artificial intelligence in education: Guidance for policy makers. OECD Publishing. https://doi.org/10.1787/93bbd96e-en

Rosenberg, J. M., & Koehler, M. J. (2015). Context and technological pedagogical content knowledge (TPACK): A systematic review. Journal of Research on Technology in Education, 47(3), 186–210. https://doi.org/10.1080/15391523.2015.1052663

Selwyn, N. (2022). The robot question: AI, education and the challenges of critical practice. Learning, Media and Technology, 47(2), 195–207. https://doi.org/10.1080/17439884.2021.1989560

Tlili, A., Shehata, B., Adarkwah, M. A., Bozkurt, A., Hickey, D. T., Huang, R., & Burgos, D. (2023). What if the devil is my guardian angel: ChatGPT as a case study of using chatbots in education. Smart Learning Environments, 10(1), 15. https://doi.org/10.1186/s40561-023-00237-x

UNESCO. (2023). Guidance for generative AI in education and research. UNESCO Publishing. https://doi.org/10.54675/PCSP7350

World Bank. (2022). Jordan: Education sector analysis — Improving learning outcomes and equity. World Bank Group. https://openknowledge.worldbank.org/handle/10986/37985

Zawacki-Richter, O., Marín, V. I., Bond, M., & Gouverneur, F. (2019). Systematic review of research on artificial intelligence applications in higher education — where are the educators? International Journal of Educational Technology in Higher Education, 16(1), 39. https://doi.org/10.1186/s41239-019-0171-0