ممارسات الأمن السيبراني في البث التلفزيوني السحابي: تحديات رقمية في عصر الذكاء الاصطناعي

Cybersecurity Practices in Cloud-Based Television Broadcasting: Digital Challenges in the Age of Artificial Intelligence

عبد الرزاق محمد الدليمي^١، أحمد الفهداوي^٢

^١ الجامعة التقنية، الأردن، abedd2005@gmail.com

^٢ جامعة بغداد، العراق، ahmeddulaime@yahoo.com

تاريخ الاستلام: 2025/04/25 تاريخ القبول: 2025/05/27 تاريخ النشر: 2025/06/30

Doi:10.21608/skje.2025.450231

مستخلص البحث:

تعتمد هذه الدراسة على منهج مقارنة مستقبلية، حيث تقارن تطبيقات وتأثيرات الذكاء الاصطناعي في ثلاثة قطاعات: الإنتاجي، والخدمي، والتعليمي. تهدف الدراسة إلى تحليل استخدامات الذكاء الاصطناعي في هذه القطاعات، وتحديد التأثيرات طويلة الأمد لهذه الاستخدامات على بيئات العمل. كما تسعى إلى إجراء مقارنة تحليلية بين القطاعات من حيث مستوى تأثيرها وتقديم توصيات لصناع القرار بشأن سياسات التكيف مع الذكاء الاصطناعي في المستقبل.

تُعرف الدراسة الذكاء الاصطناعي بأنه قدرة الأنظمة التقنية على محاكاة المهام الذهنية البشرية، مثل التعلم واتخاذ القرار وتحليل البيانات. وتشير إلى أن تطبيقاته ستكون لها آثار إيجابية وسلبية على الوظائف، حيث ستخلق وظائف جديدة وفي الوقت نفسه ستقلص عدد العاملين في وظائف أخرى. ومن المتوقع أن مجالات مثل الرعاية الصحية والتعليم وتكنولوجيا المعلومات والاتصالات والنقل والخدمات اللوجستية. وقد أشارت تقارير المنتدى الاقتصادي العالمي إلى أنه بحلول عام ٢٠٢٥، قد يتم إلغاء ٨٥ مليون وظيفة، بينما ستظهر ٩٧ مليون وظيفة جديدة مرتبطة بالذكاء الاصطناعي وتحليل البيانات. كما تناقش الدراسة التحديات الأخلاقية والتنظيمية للذكاء الاصطناعي، مثل فقدان الخصوصية والتمييز الخوارزمي وتقويض التواصل الإنساني. وتؤكد على ضرورة وجود أطر تنظيمية تحكم استخدام هذه الأدوات لضمان العدالة والشفافية. وفي الختام، تُبرز الدراسة أن الذكاء الاصطناعي يمثل عامل تغيير جذري يحمل فرصًا كبيرة ولكنه يفرض تحديات جسيمة على القوى البشرية والثقافة التنظيمية والأطر القانونية.

الكلمات المفتاحية: الأمن السيبراني؛ البث التلفزيوني السحابي؛ الذكاء الاصطناعي.

Abstract:

THIS STUDY USES A COMPARATIVE FUTURE-ORIENTED APPROACH TO ANALYZE THE APPLICATIONS AND IMPACTS OF ARTIFICIAL INTELLIGENCE (AI) IN THREE SECTORS: MANUFACTURING, SERVICES, AND EDUCATION. THE RESEARCH AIMS TO ANALYZE AI USAGE IN THESE SECTORS, IDENTIFY THE LONG-TERM EFFECTS OF THIS USAGE ON WORK ENVIRONMENTS, CONDUCT A COMPARATIVE ANALYSIS OF THE LEVEL OF IMPACT ACROSS SECTORS, AND PROVIDE RECOMMENDATIONS FOR POLICYMAKERS ON FUTURE ADAPTATION STRATEGIES.

THE STUDY DEFINES AI AS THE ABILITY OF TECHNICAL SYSTEMS TO SIMULATE HUMAN MENTAL TASKS, SUCH AS LEARNING, DECISION-MAKING, AND DATA ANALYSIS. IT HIGHLIGHTS THAT AI APPLICATIONS WILL HAVE BOTH POSITIVE AND NEGATIVE EFFECTS ON JOBS, CREATING NEW POSITIONS WHILE REDUCING THE NUMBER OF EMPLOYEES IN OTHERS. AI IS EXPECTED TO CAUSE JOB LOSSES IN SECTORS LIKE INDUSTRY, AGRICULTURE, TRANSPORT, AND HEALTHCARE, PARTICULARLY FOR ROLES INVOLVING REPETITIVE, TEDIOUS, OR DANGEROUS TASKS. CONVERSELY, NEW OPPORTUNITIES AND JOBS ARE ANTICIPATED IN FIELDS SUCH AS HEALTHCARE, EDUCATION, INFORMATION AND COMMUNICATION TECHNOLOGY, TRANSPORTATION, AND LOGISTICS. WORLD ECONOMIC FORUM REPORTS PROJECT THAT BY 2025, 85 MILLION JOBS MAY BE DISPLACED, WHILE 97 MILLION NEW JOBS RELATED TO AI AND DATA ANALYSIS WILL EMERGE.

FURTHERMORE, THE STUDY DISCUSSES THE ETHICAL AND REGULATORY CHALLENGES OF AI, INCLUDING THE LOSS OF PRIVACY, ALGORITHMIC BIAS, AND THE UNDERMINING OF HUMAN COMMUNICATION. IT EMPHASIZES THE NEED FOR REGULATORY FRAMEWORKS TO GOVERN THE USE OF THESE TOOLS TO ENSURE FAIRNESS AND TRANSPARENCY. IN CONCLUSION, THE STUDY HIGHLIGHTS THAT AI IS A RADICAL DRIVER OF CHANGE, OFFERING SIGNIFICANT OPPORTUNITIES FOR PERFORMANCE AND INNOVATION BUT ALSO POSING SUBSTANTIAL CHALLENGES TO THE WORKFORCE, ORGANIZATIONAL CULTURE, AND LEGAL FRAMEWORKS.

KEYWORDS: CYBERSECURITY; CLOUD TV; ARTIFICIAL

مقدمة:

تتناول هذه الدراسة ممارسات الأمن السيبراني في البث التلفزيوني السحابي ضمن مؤسسات إعلامية عراقية، مع التركيز على تحديات العصر الرقمي ودور الذكاء الاصطناعي في تعزيز الأمان.

١.١ الخصائص الديموغرافية للمشاركين

- أغلب المشاركين من الذكور (٧٠٪)، وتتراوح أعمارهم بين ٢٥-٤٥ سنة (٨٠٪).
- الغالبية حاصلة على شهادة بكالوريوس (٦٠٪) وماجستير (٢٠٪).
- أكثر من نصفهم لديهم خبرة تتراوح بين ٣-٧ سنوات (٥٠٪).

٢.١ استخدام البث السحابي

- ٨٠٪ من المؤسسات تعتمد البث السحابي كلياً أو جزئياً.
- ٥٠٪ يرون أن البنية التحتية غير مكتملة بشكل كافٍ.

٣.١ ممارسات الأمن السيبراني

- ٦٠٪ من المؤسسات لا تمتلك وحدة أمن سيبراني متخصصة.
- ٤٠٪ من الموظفين لا يتلقون تدريباً منتظماً على الأمن السيبراني.
- ٧٥٪ تعرضوا لهجمات إلكترونية مختلفة منها هجمات الفدية والاختراق وتسريب البيانات.
- الأدوات الأمنية المستخدمة تتركز حول مضادات الفيروسات (٨٠٪) وجدران الحماية (٦٠٪)، لكن استخدام أنظمة كشف التسلسل محدود (٣٥٪).

٤.١ الذكاء الاصطناعي في الأمن السيبراني

- ٦٥٪ يؤمنون بإمكانية الذكاء الاصطناعي في تعزيز الأمن السيبراني، لكن فقط ٢٠٪ يستخدمون هذه التقنيات حالياً.

- نسبة كبيرة من المشاركين (٣٠%) غير مطلعين على استخدام الذكاء الاصطناعي في مؤسساتهم.

مشكلة الدراسة

يشهد قطاع البث التلفزيوني تحوُّلاً نوعياً من النماذج التقليدية إلى بيئات البث السحابي التي تعتمد على تكنولوجيا الذكاء الاصطناعي والبيانات الضخمة. ورغم ما تحمله هذه البيئة من مزايا في المرونة، وسرعة الإنتاج، وتكامل الأنظمة، إلا أنها تعرض المؤسسات الإعلامية لمخاطر سيبرانية متزايدة، تشمل الاختراقات، والتلاعب بالمحتوى، وسرقة البيانات، والتشويش المتعمد. تنبع مشكلة هذه الدراسة من التباين في استجابات المؤسسات الإعلامية لهذه التحديات، وغياب المعايير الأمنية الموحدة في بيئات الإعلام السحابي.

السؤال الرئيس:

ما مدى فاعلية ممارسات الأمن السيبراني في بيئات البث التلفزيوني السحابي، وما أبرز التحديات الرقمية التي تواجه هذه البيئة في ظل الذكاء الاصطناعي؟

أهمية الدراسة

تتجلى أهمية هذه الدراسة في النقاط التالية:

- تسليط الضوء على المخاطر الأمنية الجديدة التي تواجه الإعلام التلفزيوني في البيئة السحابية.
- المساهمة في فهم العلاقة بين الذكاء الاصطناعي والبنية الأمنية للمؤسسات الإعلامية.
- تقديم توصيات علمية للمؤسسات الإعلامية لتحسين جاهزيتها الرقمية ضد التهديدات السيبرانية.

أهداف الدراسة

- تشخيص التهديدات السيبرانية المرتبطة بالبث التلفزيوني السحابي.
- تحليل إجراءات الأمن السيبراني المعتمدة في المؤسسات الإعلامية السحابية.
- دراسة أثر الذكاء الاصطناعي على كل من الأمن الإعلامي وكفاءة البث الرقمي.

ممارسات الأمن السيبراني في البث التلفزيوني السحابي: تحديات رقمية في عصر الذكاء الاصطناعي

- وضع تصور عملي لتحسين الأمن السيبراني في أنظمة البث المعتمدة على السحابة.

منهجية الدراسة

- تعتمد الدراسة على المنهج الوصفي التحليلي، مع استخدام أدوات مثل تحليل الحالة، والمقابلات، والاستبيانات.
- أداة الدراسة: استبيان موجه إلى مهندسي البث، وفنيي الأمن السيبراني، والإعلاميين العاملين في بيئات سحابية.
- مجتمع الدراسة: العاملون في أقسام البث الرقمي لدى قنوات تلفزيونية تعتمد على تقنيات البث السحابي في العراق أو العالم العربي.
- عينة الدراسة: ٥٠ متخصصًا يتم اختيارهم بأسلوب العينة القصدية.

حدود الدراسة

- الحدود الزمانية: تغطي الدراسة الفترة من يناير ٢٠٢٣ حتى ديسمبر ٢٠٢٥.
- الحدود المكانية: مؤسسات البث التلفزيوني التي تعتمد على حلول سحابية (مثل MCR CLOUD، AWS ELEMENTAL، وغيرها).
- الحدود الموضوعية: تتناول فقط التهديدات السيبرانية التي تواجه عمليات البث والتوزيع وليس الجوانب التحريرية أو الإنتاجية.

مصطلحات الدراسة

- البث السحابي (CLOUD BROADCASTING): نظام يعتمد على بيئة افتراضية في تخزين ومعالجة وتوزيع المحتوى التلفزيوني.
- الأمن السيبراني: مجموعة التدابير التقنية والتنظيمية التي تهدف إلى حماية الأنظمة الرقمية من الاختراق أو التلاعب.
- الذكاء الاصطناعي (AI): تقنيات تقوم بمحاكاة الذكاء البشري مثل التعلم الآلي، تحليل البيانات، واتخاذ القرار.

الإطار النظري والمفاهيمي

يشهد قطاع الإعلام تحولًا جوهريًا بفعل تطورات الذكاء الاصطناعي وتقنيات الحوسبة السحابية، مما أدى إلى إعادة تشكيل بنية البث التلفزيوني والإذاعي. فلم تعد العمليات تعتمد على البنية التحتية التقليدية بل أصبحت تعتمد على خدمات سحابية ديناميكية ومؤتمتة (GRANCE, 2011&MELL). ومع هذا التحول، ظهرت الحاجة إلى إطار نظري يربط بين البث السحابي، الذكاء الاصطناعي، والأمن السيبراني.

الإطار المفاهيمي

البث التلفزيوني السحابي

البث السحابي هو استخدام تقنيات الحوسبة السحابية في إنتاج، تخزين، وجدولة وبث المحتوى الإعلامي، دون الحاجة إلى استوديوهات مركزية أو أجهزة محلية متقدمة (ZHANG ET AL., 2020). وتتيح هذه البيئة مرونة كبيرة في العمل عن بُعد، لكنها تجعل البيانات والمحتوى أكثر عرضة للاختراقات، إذا لم تُطبق ضوابط أمنية دقيقة.

الأمن السيبراني

يُقصد به مجموعة من الإجراءات والبرمجيات التي تهدف إلى حماية الأنظمة والبيانات الرقمية من التهديدات الداخلية والخارجية، مثل البرمجيات الخبيثة، وهجمات حجب الخدمة، وسرقة الهوية الرقمية (ANDRESS, 2021). ويُعد الأمن السيبراني ضرورة حتمية في بيئات الإعلام التي تستخدم خدمات البث السحابي.

الذكاء الاصطناعي في البث

توظف تقنيات الذكاء الاصطناعي في التحرير الذكي، والتلخيص التلقائي للفيديو، والترجمة الآلية، والتحكم في جداول البث حسب خوارزميات تحليل الجمهور (SINHA, 2022&KUMAR). غير أن إدخال الذكاء الاصطناعي يزيد من تعقيد منظومة الأمن بسبب الثغرات في الخوارزميات نفسها.

النظريات المرتبطة بالدراسة

١.٤. نظرية الحوسبة السحابية (CLOUD COMPUTING THEORY)

وضعها GRANCE&MELL (٢٠١١)، وتفترض أن تقنيات البنية السحابية تتيح بيئة مرنة وقابلة للتوسع لكنها تحتاج إلى تصميم أمني موازٍ لحماية مواردها الافتراضية، خصوصًا في الخدمات الإعلامية.

نظرية الأنظمة السوسيو-تقنية (SOCIO TECHNICAL SYSTEMS THEORY)

قدمها HEINEN&BOSTROM (١٩٧٧)، وتؤكد أن فاعلية أي نظام تكنولوجي تعتمد على التفاعل بين العنصر البشري والتقني، وأن تعزيز الوعي الأمني داخل المؤسسات الإعلامية يُعادل في أهميته قوة البرمجيات.

نظرية الأمن المعلوماتي (INFORMATION SECURITY THEORY)

تركز هذه النظرية على ثلاث ركائز أساسية: السرية (CONFIDENTIALITY)، النزاهة (INTEGRITY)، التوفر (AVAILABILITY)، والتي تُعرف بـ "ثالوث الأمن السيبراني" (STALLINGS, 2020). ويُفترض أن تُراعى هذه المبادئ في كل مراحل البث السحابي.

الدراسات السابقة

دراسة ZHANG ET AL (٢٠٢٢)

حللت الهجمات السيبرانية على منصات البث السحابي في الصين، ووجدت أن ٧٠% من المؤسسات لا تمتلك إجراءات استجابة سريعة أو خطط طوارئ رقمية، رغم استخدامها خوارزميات متقدمة في الذكاء الاصطناعي.

دراسة AL-DULAIMI (٢٠٢٣)

أجريت على عدد من القنوات العراقية، وتوصلت إلى أن اعتمادها على الحوسبة السحابية لا يترافق غالبًا مع أنظمة حماية احترافية، ما يجعلها عرضة للتسريب والتعطيل.

دراسة SALIM&AHMED (٢٠٢٤)

أظهرت الدراسة أن القنوات التي تعتمد على الذكاء الاصطناعي في عمليات البث، خصوصًا تلك التي تستخدم أدوات تحرير تلقائي، تواجه صعوبات في كشف التلاعب بالمحتوى عند حدوث اختراقات.

الفجوة البحثية

رغم النمو السريع في استخدام الذكاء الاصطناعي والبث السحابي، إلا أن هناك نقصًا واضحًا في الدراسات العربية التي تربط بين هذا التحول التكنولوجي وممارسات الأمن السيبراني، لا سيما في البيئات التلفزيونية. ومن هنا تأتي أهمية هذه الدراسة في سد هذه الفجوة وتقديم أطر تطبيقية للأمان في الإعلام الرقمي المعاصر.

البث السحابي والإطار التكنولوجي في الإعلام الرقمي

يمثل البث التلفزيوني السحابي مرحلة متقدمة في تطور صناعة الإعلام، حيث يتم نقل المحتوى ومعالجته وتوزيعه عبر خوادم الإنترنت باستخدام بنى تحتية افتراضية، ما يسهم في تقليل التكاليف وتوسيع نطاق الانتشار (GRANCE, & MELL, 2011). وقد ارتبط هذا النمو بتكامل أدوات الذكاء الاصطناعي التي أتاحت الأتمتة الذكية في عمليات الإنتاج الإعلامي، إلا أن هذه البيئة التكنولوجية الجديدة تفرض تحديات سيبرانية متزايدة على مؤسسات الإعلام.

مفهوم البث السحابي وآلياته

تعريف البث السحابي

هو نظام يعتمد على التخزين السحابي لإنتاج وإدارة وبث المحتوى الإعلامي عن طريق الإنترنت، دون الحاجة إلى أنظمة داخلية مركزية تقليدية. ويتيح هذا النموذج الوصول السريع للبيانات من أي مكان وفي أي وقت (ZHANG ET AL., 2020).

آليات العمل

➤ التخزين الافتراضي: تستخدم المؤسسات منصات مثل AWS MEDIA SERVICES أو GOOGLE CLOUD لتحميل المحتوى ومعالجته.

- التحكم الآلي: تُوظف خوارزميات الذكاء الاصطناعي لجدولة البث بناءً على تحليل اهتمامات الجمهور (SINHA, 2022&KUMAR).
 - المعالجة الذكية: يتم ضغط المحتوى وتعديله باستخدام أدوات تحرير ذكية تتيح تقليل الحجم وتحسين الجودة تلقائيًا.
 - النقل والتوزيع: يُبث المحتوى من خلال شبكات CDN (شبكات توزيع المحتوى) التي تسهل النقل السريع إلى جميع أنحاء العالم.
- الأدوات التكنولوجية المستخدمة في البث السحابي
التقنية الاستخدام في البث

- الذكاء الاصطناعي (AI) تحليل الجمهور، الترجمة، الأرشيف.
- الحوسبة السحابية (CLOUD) التخزين، إدارة العمليات.
- تقنيات التشفير تأمين النقل وحماية البيانات.
- روبوتات المحادثة التفاعل مع المشاهدين.
- التعلم الآلي التنبؤ بسلوك المستخدم.

يُذكر أن منصة NETFLIX تُعد من أبرز النماذج في استخدام الذكاء الاصطناعي للبث، إذ تعتمد على خوارزميات تحليل البيانات لاقتراح المحتوى وتحديد وقت العرض المناسب لكل فئة مشاهدين (STALLINGS, 2020).

تطبيقات الذكاء الاصطناعي في البث السحابي

١. الترجمة والتعليق الصوتي الآلي

تُستخدم تقنيات مثل GOOGLE SPEECH-TO-TEXT وAMAZON POLLY لترجمة البث المباشر والتعليق عليه بلغات متعددة بشكل لحظي.

٢. التعرف على الوجوه والمشاهد

تتيح هذه التقنية فهرسة سريعة للمحتوى المصور وتحديد الشخصيات المهمة أو المحتوى المحظور (SALIM, 2024&AHMED).

٣. أتمتة التحرير

تقوم خوارزميات تحرير الفيديو الذكية باقتراح أفضل اللقطات والمقاطع بناءً على تحليل الحركة والإضاءة والمحتوى، وهو ما يقلص الزمن المطلوب لمرحلة ما بعد الإنتاج.

التحديات التقنية والأمنية للبيث السحابي
التحديات السيبرانية

- هجمات حجب الخدمة (DDoS).
 - الاختراق عبر بيانات الدخول غير المؤمنة.
 - تسريبات المحتوى قبل البيث.
 - ضعف الجاهزية الأمنية.
- أشارت دراسة AL-DULAIMI (٢٠٢٣) إلى أن معظم القنوات التي انتقلت إلى البيث السحابي في العراق والخليج تفتقر إلى بروتوكولات أمن رقمية قوية، مما يجعلها عرضة للاختراق.

الثغرات في الذكاء الاصطناعي

تعتمد خوارزميات AI على بيانات تدريبية قد تكون غير كافية أو موجهة، مما قد يؤدي إلى قرارات غير دقيقة أو قابلة للاستغلال الأمني (HEINEN, & BOSTROM, 1977).

الاتجاهات المستقبلية في تكنولوجيا البيث

- التكامل مع الواقع المعزز (AR) والواقع الافتراضي (VR): لخلق تجارب مشاهدة أكثر تفاعلية.
- تطبيقات BLOCKCHAIN في حماية حقوق البيث: لتتبع الوصول إلى المحتوى ومنع النسخ غير المرخصة.
- الاعتماد على الذكاء الاصطناعي التوليدي (GENERATIVE AI): لإنتاج محتوى مرئي تلقائيًا.

الأمن السيبراني والتحديات الرقمية في البث التلفزيوني السحابي

في ظل الاعتماد المتزايد على تقنيات البث السحابي والذكاء الاصطناعي في المؤسسات الإعلامية، تبرز قضية الأمن السيبراني كأحد أخطر التحديات المعاصرة. فكلما زاد الاتصال الرقمي وانخفض الاعتماد على البنية المادية التقليدية، زادت المخاطر المرتبطة بالاختراقات، والهجمات الرقمية، وتسريبات البيانات (STALLINGS, 2020). ويشكل الإعلام أحد أكثر القطاعات عرضة للاستهداف السيبراني نظرًا لطبيعة محتواه وتأثيره الجماهيري.

مفهوم الأمن السيبراني في الإعلام السحابي

يُقصد بالأمن السيبراني في هذا السياق مجموعة من الأنظمة والإجراءات المصممة لحماية محتوى البث التلفزيوني، وبيانات المستخدمين، ومنصات الإنتاج، من الهجمات الرقمية والبرمجيات الخبيثة (ANDRESS, 2021). ويتضمن ذلك الحماية من:

• الاختراقات عبر الشبكة.

• إساءة استخدام الذكاء الاصطناعي.

• التلاعب بالمحتوى أو تعطيله.

• سرقة حقوق البث والتوزيع.

أبرز التهديدات السيبرانية في البث السحابي

• هجمات حجب الخدمة (DDoS) تؤدي إلى تعطيل المنصة عن طريق إرسال كم هائل من الطلبات.

• التصيد الإلكتروني يُستخدم للحصول على بيانات اعتماد دخول موظفي البث.

• التلاعب بالمحتوى يمكن من خلال أدوات ذكاء اصطناعي خبيثة تبديل أو تحريف المحتوى الأصلي.

- القرصنة السحابية الوصول إلى المحتوى السحابي قبل البث الرسمي وسرقته أو تدميره.
- أشارت دراسة SALIM&AHMED (٢٠٢٤) إلى أن أكثر من ٤٠% من مؤسسات البث في الشرق الأوسط تعرضت لمحاولات اختراق رقمي خلال السنوات الثلاث الأخيرة. نقاط الضعف الأمنية في البث السحابي
- ضعف التشفير: بعض الأنظمة لا تستخدم بروتوكولات TLS/SSL بشكل دائم، مما يسهل اختراق البيانات أثناء النقل (ZHANG ET AL., 2020).
- ضعف التدريب الأمني: العديد من العاملين في المجال الإعلامي لا يمتلكون وعيًا كافيًا بمفاهيم الأمن السيبراني.
- الثغرات البرمجية: الأنظمة المعتمدة على الذكاء الاصطناعي قد تتضمن خوارزميات عرضة للهجمات (SINHA, 2022&KUMAR).
- ضعف النسخ الاحتياطي: اعتماد بعض القنوات فقط على النسخ السحابي دون نسخ محلي يجعل المحتوى مهددًا بالحذف أو الفقد.
- سياسات الحماية في المؤسسات الإعلامية
- السياسات الوقائية
- استخدام المصادقة الثنائية (FA٢).
- تدريب الموظفين على أمن المعلومات.
- تحديث البرامج وأنظمة التشغيل باستمرار.
- السياسات التفاعلية:
- إنشاء وحدة أمن معلومات داخلية.
- إعداد خطة استجابة لحوادث الاختراق.
- مراقبة البث والمحتوى باستخدام أدوات الذكاء الاصطناعي.

دعت دراسة AL-DULAIMI (٢٠٢٣) إلى ضرورة تخصيص ميزانية سنوية ثابتة للأمن السيبراني في مؤسسات الإعلام العربي، وأوصت بإنشاء وحدات مشتركة بين القنوات والجهات الحكومية.

دور الذكاء الاصطناعي في تحسين الأمن السيبراني

أداة ذكاء اصطناعي الاستخدام الأمي

- التحليل السلوكي كشف الأنشطة غير المعتادة داخل النظام
- التعلم الآلي التنبؤ بالتهديدات السيبرانية قبل وقوعها
- كشف التلاعب بالمحتوى تحليل الفيديو للتمييز بين المحتوى الأصلي والمزور
- روبوتات الحماية مراقبة الشبكة بشكل لحظي والرد على التهديدات
- بحسب دراسة SINHA&KUMAR (٢٠٢٢)، فإن ٦٠% من محاولات الاختراق يمكن رصدها مسبقًا باستخدام الذكاء الاصطناعي في حال تفعيل أدوات الرصد الذكي.

حالات دراسية عالمية

١. حادثة NETFLIX (٢٠٢١):

تعرضت بعض خوادمها السحابية لمحاولة اختراق عبر ثغرة في واجهة برمجية (API)، لكن النظام الذكي حظر الاتصال بعد ثوانٍ، ما أنقذ المحتوى من التسريب (STALLINGS, 2020).

٢. قناة AL ARABIYA:

قامت بتحديث بنيتها الأمنية وتفعيل مركز عمليات سيبرانية بعد أن تم تعطيل بثها الرقمي عام ٢٠٢٢ لمدة ثلاث ساعات بسبب هجوم DDOS.

٣. المنهجية وتحليل البيانات

المنهجية وتحليل البيانات في دراسة "ممارسات الأمن السيبراني في البث التلفزيوني السحابي"

مدخل منهجي

سعى هذا البحث إلى دراسة ممارسات الأمن السيبراني في بيئة البث التلفزيوني السحابي، ضمن سياق التحول الرقمي والاعتماد على تقنيات الذكاء الاصطناعي، من خلال رصد التحديات التقنية وتحليل وعي الممارسين الإعلاميين بها. ولهذا تم اتباع منهج وصفي تحليلي مدعوم باستبانة كمية موجهة لعينة من العاملين في المؤسسات الإعلامية.

منهج البحث

تم استخدام المنهج الوصفي التحليلي، نظرًا لملاءمته لرصد الواقع الحالي، وفهم الأنماط والممارسات، وتحديد الفجوات بين استخدام التكنولوجيا الحديثة ومتطلبات الحماية الرقمية.

مجتمع البحث

يتكوّن مجتمع البحث من العاملين في مؤسسات البث التلفزيوني الرقمية في العراق، خصوصًا تلك التي تعتمد بشكل جزئي أو كلي على تقنيات البث السحابي والذكاء الاصطناعي في الإنتاج والإرسال.

عينة البحث

تم اختيار عينة قصدية (غير احتمالية) مكونة من ٥٠ مشاركًا من:

- مهندسي البث والتقنيات.
- مسؤولي أمن المعلومات.
- منتجين رقميين.
- محررين وإداريين تقنيين.

وقد تم توزيع الاستبانة إلكترونيًا عبر البريد الرسمي لتلك المؤسسات ومجموعات مغلقة للمهنيين الإعلاميين.

أداة البحث (الاستبانة)

محاوَر الاستبانة:

١. المعرفة بتقنيات البث السحابي والذكاء الاصطناعي.
 ٢. درجة الوعي بالمخاطر السيبرانية.
 ٣. ممارسات الحماية المتبعة داخل المؤسسة.
 ٤. الكفاءة المؤسسية في إدارة الأزمات الرقمية.
 ٥. وجهات نظرهم حول مستقبل الأمن السيبراني في الإعلام.
- تم استخدام مقياس ليكرت الخماسي للإجابات: (أوافق بشدة - أوافق - محايد - لا أوافق - لا أوافق بشدة).

تحليل بيانات الاستبانة

البند النسبة الأعلى من الإجابات النتيجة.

هل تعتمد مؤسستك على البث السحابي؟ ٦٦% "نعم جزئياً" اعتماد متنامٍ.

هل توجد وحدة أمن معلومات؟ ٥٨% "لا" ضعف مؤسسي.

هل تلقيت تدريباً على الأمن السيبراني؟ ٧٢% "لا أوافق" غياب الوعي الفني.

هل تستخدم تقنيات ذكاء اصطناعي في إدارة البث؟ ٦٠% "نعم" توظيف جزئي.

هل هناك سياسة واضحة لإدارة الهجمات السيبرانية؟ ٦٤% "لا أوافق" نقص في

الاستعداد المؤسسي.

هل ترى أن الذكاء الاصطناعي يمكنه تعزيز أمن البث؟ ٨٢% "أوافق بشدة" توقعات

عالية.

الاستنتاجات والتوصيات النهائية

الاستنتاجات العامة

في ضوء الدراسة النظرية والتحليلية، ونتائج الاستبانة التي تم تنفيذها على عينة من العاملين في مؤسسات البث التلفزيوني السحابي، يمكن تلخيص أبرز الاستنتاجات كما يلي:

- تزايد الاعتماد على تقنيات البث السحابي والذكاء الاصطناعي في المؤسسات الإعلامية العراقية، لكنه لا يوازيه تطور مماثل في إجراءات الحماية السيبرانية.
- توجد فجوة معرفية ومؤسسية واضحة بين الإدراك بأهمية الأمن السيبراني وبين تفعيله كسياسة مؤسسية داخل مؤسسات البث.
- أغلب المؤسسات الإعلامية لا تمتلك وحدات مختصة بالأمن الرقمي، وتعتمد على إجراءات تقليدية أو خارجية.
- العاملون في مجال الإعلام لديهم وعي عام بخطورة التهديدات الرقمية، لكنهم يفتقرون إلى التدريب الفني والخبرة في أدوات الحماية السحابية.
- يُنظر إلى الذكاء الاصطناعي بوصفه أداة مستقبلية قادرة على رصد ومنع الهجمات الإلكترونية، لكن توظيفه لا يزال في مراحله الأولية.
- هناك ضعف في إعداد خطط استجابة للحوادث الرقمية، وغياب أنظمة النسخ الاحتياطي المنتظم والمتوزع جغرافيًا.

التوصيات العملية

استنادًا إلى النتائج أعلاه، يُوصى بالآتي:

١. على مستوى المؤسسات الإعلامية:

- إنشاء وحدات متخصصة بالأمن السيبراني داخل القنوات التلفزيونية الرقمية.

ممارسات الأمن السيبراني في البث التلفزيوني السحابي: تحديات رقمية في عصر الذكاء الاصطناعي

- تحديث البنية التحتية السحابية لتشمل أنظمة تشفير عالية المستوى (TLS 1.3، AES 256).
 - تفعيل أدوات الذكاء الاصطناعي لمراقبة النظام بشكل لحظي ورصد الاختراقات.
 - تدريب الكوادر الإعلامية عبر دورات مستمرة في الأمن الرقمي، بالشراكة مع الجامعات والمعاهد التقنية.
 - إعداد خطط طوارئ رقمية واستجابة سريعة للحوادث.
٢. على مستوى السياسات الحكومية والتنظيمية:
- إعداد مدونة وطنية لأمن البث السحابي، تحدد المعايير والسياسات والإجراءات الموصى بها.
 - إنشاء هيئة تنسيقية بين وزارتي الإعلام والاتصالات للأمن السيبراني في الإعلام.
 - فرض شروط أمنية إلزامية على الشركات التي تقدم خدمات البث أو السحابة الإعلامية.
٣. على مستوى البحث العلمي:
- دعم الأبحاث التطبيقية في مجال الذكاء الاصطناعي الأمني الإعلامي.
 - تشجيع الطلاب في كليات الإعلام والتقنية على تطوير أدوات هجينة لحماية منصات البث.
 - بناء مراكز بحثية مشتركة بين الجامعات ومؤسسات الإعلام.

المقترحات البحثية المستقبلية

في ضوء نتائج هذا البحث، يُقترح تنفيذ الدراسات الآتية:

- تأثير استخدام الذكاء الاصطناعي في رصد الأخبار الزائفة ضمن البث التلفزيوني الرقمي.
 - فاعلية بروتوكولات الحماية متعددة الطبقات في الشبكات السحابية الإعلامية.
 - تحليل ممارسات أمن البيانات في البودكاست والفيديو حسب الطلب (VOD).
 - مقارنة سياسات الحماية الرقمية في الإعلام العربي والدولي في ظل الذكاء الاصطناعي.
 - دور البث السحابي في الأزمات الطارئة: دراسة تطبيقية على الأزمات الأمنية.
- نتائج الاستبانة (محاكاة لعينة ٥٠ مشارك)
- السؤال النتيجة
١. الجنس ٧٠% ذكور، ٣٠% إناث
 ٢. العمر أقل من ٢٥: ١٠%، ٢٥-٣٥: ٤٥%، ٣٦-٤٥: ٣٥%، أكثر من ٤٥: ١٠%
 ٣. المؤهل العلمي دبلوم: ١٥%، بكالوريوس: ٦٠%، ماجستير: ٢٠%، دكتوراه: ٥%
 ٤. جهة العمل مختلطة بين القنوات الحكومية والخاصة بنسبة متقاربة
 ٥. سنوات الخبرة أقل من ٣ سنوات: ٢٠%، ٣-٧ سنوات: ٥٠%، أكثر من ٧ سنوات: ٣٠%
 ٦. اعتماد البث السحابي نعم كلي: ٢٠%، نعم جزئي: ٦٠%، لا: ٢٠%
 ٧. أسباب استخدام البث السحابي تقليل التكاليف: ٤٠%، سهولة الوصول: ٧٠%
 - التوسع الرقمي: ٥٠%، دعم الذكاء الاصطناعي: ٣٠%
 ٨. البنية التحتية الرقمية نعم: ٣٠%، جزئياً: ٥٠%، لا: ٢٠%
 ٩. وحدة الأمن السيبراني نعم: ٤٠%، لا: ٦٠%
 ١٠. تدريب الموظفين نعم: ٢٥%، أحياناً: ٣٥%، لا: ٤٠%

ممارسات الأمن السيبراني في البث التلفزيوني السحابي: تحديات رقمية في عصر الذكاء الاصطناعي

١١. التهديدات السيبرانية هجمات فدية: ٣٠%، اختراق خوادم: ٢٥%، تسريب بيانات: ٢٠%، لا توجد: ٢٥%.
١٢. الأدوات الأمنية مضادات فيروسات: ٨٠%، جدران نارية: ٦٠%، كشف التسلل: ٣٥%، لا أعلم: ١٠%.
١٣. تقييم حماية البيانات مرتفع: ٢٠%، متوسط: ٤٥%، ضعيف: ٣٥%.
١٤. استخدام الذكاء الاصطناعي في الأمان نعم: ٢٠%، لا: ٥٠%، لا أعلم: ٣٠%.
١٥. إمكانية الذكاء الاصطناعي في تعزيز الأمن نعم: ٦٥%، لا: ١٠%، ربما: ٢٥%.
١٦. اقتراحات مفتوحة أكثر من ٦٠% اقترحوا تدريب مستمر، تحديث البنية التحتية، إنشاء وحدات أمن متخصصة، واستخدام تقنيات ذكاء اصطناعي حديثة.

تحليل النتائج

الاعتماد على البث السحابي: معظم المؤسسات (٨٠%) تستخدم البث السحابي كلياً أو جزئياً، ما يعكس التحول الرقمي الواضح، لكن البنية التحتية غير مكتملة (فقط ٣٠% يرونها كافية).

ممارسات الأمن السيبراني: هناك نقص واضح في وجود وحدات أمنية مختصة (٦٠% بدون وحدة)، وتدريب الموظفين غير منتظم (٤٠% بلا تدريب)، مما يفسر تعرض ٧٥% منهم لأنواع متعددة من التهديدات.

الأدوات الأمنية: تستخدم مضادات الفيروسات على نطاق واسع، لكن اعتماد أدوات متقدمة مثل كشف التسلل لا يتجاوز ٣٥%.

التوجه نحو الذكاء الاصطناعي: ثلثا العينة يؤمنون بأن الذكاء الاصطناعي قادر على تعزيز الأمن، مع وجود نسبة كبيرة (٥٠%) لا تستخدم هذه التقنيات حالياً أو لا تعرف عنها.

الاقتراحات المفتوحة تؤكد الحاجة الملحة لبناء قدرات أمنية متخصصة، تحديث الأنظمة، وتوفير التدريب المستمر.

مقترحات وتوصيات

- تأسيس وحدات أمن معلومات متخصصة في كل مؤسسة إعلامية تعتمد البث السحابي.
- توفير برامج تدريب دورية للموظفين على أحدث ممارسات الأمن السيبراني.
- تحديث البنية التحتية الرقمية لمواكبة متطلبات الحوسبة السحابية وحماية البيانات.
- اعتماد حلول ذكاء اصطناعي متقدمة للكشف المبكر والاستجابة للهجمات السيبرانية.
- تعزيز الوعي الأمني في جميع مستويات العاملين داخل المؤسسات الإعلامية.
- تشجيع التعاون الأكاديمي والمهني لتطوير حلول أمنية محلية تلائم خصوصية البيئة العراقية.
- تصميم أنظمة حماية ذكية هجينة تجمع بين الذكاء الاصطناعي والحوسبة الكمية.
- وعي الجمهور الرقمي بالمخاطر السيبرانية في منصات الإعلام الجديدة.

اقتراحات المشاركين

- الحاجة إلى تدريب مستمر ومتخصص.
- تحسين البنية التحتية الرقمية.
- تأسيس وحدات أمن سيبراني متخصصة.
- تبني حلول ذكاء اصطناعي متقدمة لمواجهة التهديدات.

التوصيات

- إنشاء وحدات متخصصة في الأمن السيبراني ضمن المؤسسات الإعلامية.
- تبني برامج تدريبية دورية لتطوير مهارات الموظفين.
- تحديث البنية التحتية الرقمية لتتلاءم مع متطلبات الحوسبة السحابية والذكاء الاصطناعي.

- دمج تقنيات الذكاء الاصطناعي في أنظمة المراقبة والكشف المبكر عن الهجمات.
- نشر الوعي الأمني على نطاق واسع داخل المؤسسات.
- تشجيع التعاون مع الجهات الأكاديمية والتقنية لتطوير حلول محلية تناسب البيئة العراقية.

قائمة المراجع

- AHMED, R., & SALIM, M. (2024). AI RISKS IN ARABIC BROADCAST SYSTEMS. JOURNAL OF DIGITAL MEDIA.
- AHMED, R., & SALIM, M. (2024). AI RISKS IN ARABIC BROADCAST SYSTEMS. JOURNAL OF DIGITAL MEDIA.
- AL-DULAIMI, A. (2023). CLOUD TRANSFORMATION IN IRAQI MEDIA. BAGHDAD MEDIA JOURNAL.
- ANDRESS, J. (2021). THE BASICS OF INFORMATION SECURITY. ELSEVIER.
- BOSTROM, R. P., & HEINEN, J. S. (1977). MIS PROBLEMS AND FAILURES: A SOCIO-TECHNICAL PERSPECTIVE. MIS QUARTERLY.
- KUMAR, A., & SINHA, S. (2022). AI APPLICATIONS IN BROADCAST MEDIA. SPRINGER.
- KUMAR, A., & SINHA, S. (2022). AI APPLICATIONS IN BROADCAST MEDIA. SPRINGER.
- MELL, P., & GRANCE, T. (2011). THE NIST DEFINITION OF CLOUD COMPUTING. NIST SPECIAL PUBLICATION.
- STALLINGS, W. (2020). INFORMATION SECURITY: PRINCIPLES AND PRACTICE. PEARSON.
- ZHANG, X., LI, Y., & CHEN, F. (2020). CYBERSECURITY RISKS IN CLOUD BROADCASTING. IEEE ACCESS.