التكنولوجيا الحديثة ودورها في تعزيز الأمن السيبراني

الباحـــث: علي عامر موسى كركوش العبيدي

جهة العمل: معهد يوم الوفاء العالي للعلوم والتقنية

البريد الإلكتروني:Ali.KarkoushAlobaidi@gmail.com الهاتف: 0919880101

ملخص البحث:

يشهد العالم تطورًا تكنولوجيًا متسارعًا أدى إلى توسع الاعتماد على الأنظمة الرقمية في مختلف القطاعات، مما جعل الأمن السيبراني عنصرًا حاسمًا لحماية البيانات والبنية التحتية المعلوماتية. تتناول هذه الدراسة دور التقنيات الحديثة، مثل الذكاء الاصطناعي وتقنيات التعلم الآلي، في كشف ومنع الهجمات الإلكترونية وتحليل الأنماط السلوكية للتهديدات.

يعتمد البحث على منهج وصفي تحليلي مدعوم بأسلوب كمي لقياس فعالية الحلول المقترحة، مع دراسة حالات واقعية لعمليات اختراق وكيفية التصدي لها. تتمثل إشكالية البحث في تزايد الهجمات المعقدة التي تتجاوز قدرات أنظمة الحماية التقليدية، والحاجة إلى حلول مبتكرة أكثر تطورًا.

يهدف البحث إلى وضع إطار تقني متكامل يعزز من قدرة المؤسسات على الاستجابة الفورية للتهديدات، وتطوير أنظمة إنذار مبكر تقلل من احتمالية حدوث الاختراقات.

كذلك تحسين مستوى الحماية الرقمية بنسبة ملحوظة، وتقليل زمن اكتشاف الهجمات، وتعزيز وعي المؤسسات بضرورة تبني استراتيجيات أمن سيبراني مستدامة. كما يسعى البحث إلى المساهمة في بناء بيئة رقمية آمنة تدعم الابتكار والنمو الاقتصادي.

الكلمات المفتاحية: التكنولوجيا، الأمن السيبراني، الذكاء الاصطناعي، حماية البيانات، التهديدات الرقمية

تطبيقات البحث والنتائج المتوقع تحقيقها

تطبيقات البحث:

- تطوير أنظمة إنذار مبكر للكشف عن الهجمات السيبرانية في مراحلها الأولى.
- استخدام الذكاء الاصطناعي لتحليل سلوك الشبكات واكتشاف الأنماط غير الطبيعية.
- تحسين أنظمة التحقق متعددة العوامل لتعزيز حماية الحسابات.
- دعم المؤسسات في وضع استراتيجيات شاملة لإدارة المخاطر الرقمية.

النتائج المتوقع تحقيقها:

- تقليل زمن اكتشاف التهديدات الإلكترونية بنسبة تتجاوز 40.%
- رفع مستوى الحماية الرقمية وتقليل فرص الاختراقات المعقدة.
- زيادة وعي المؤسسات والمستخدمين بأهمية الأمن السيبراني.
- تقديم نموذج عملي قابل للتطبيق في بيئات عمل مختلفة لتعزيز الحماية الرقمية.

Modern Technology and Its Role in Enhancing Cybersecurity

Researchers' Names: Ali Amer Mousa Karkoush Alobaidi

Affiliation: Yawm Al-Wafaa Institute of Higher Science and Technology

Email: Ali.KarkoushAlobaidi@gmail.com Mobile:0919880101

Abstract:

The world is witnessing rapid technological advancement, leading to increased reliance on digital systems across various sectors, making cybersecurity a critical element for protecting data and information infrastructure. This study explores the role of modern technologies, such as artificial intelligence and machine learning techniques, in detecting and preventing cyberattacks and analyzing behavioral patterns of threats.

The research adopts a descriptive-analytical approach supported by quantitative methods to measure the effectiveness of proposed solutions, along with case studies of real-world breaches and how to respond to them. The research problem lies in the growing complexity of attacks that exceed the capabilities of traditional security systems, highlighting the need for more advanced innovative solutions.

The study aims to establish an integrated technical framework that enhances institutions' ability to respond promptly to threats and develop early warning systems that reduce the likelihood of breaches. It also seeks to improve digital protection levels significantly, reduce threat detection time, and raise awareness among organizations about adopting sustainable cybersecurity strategies. Moreover, the research aims to contribute to building a secure digital environment that supports innovation and economic growth.

Keywords:

Technology, Cybersecurity, Artificial Intelligence, Data Protection, Digital Threats

Research Applications and Expected Outcomes:

Applications:

- Developing early warning systems to detect cyberattacks at initial stages.
- Using artificial intelligence to analyze network behavior and detect abnormal patterns.
- Enhancing multi-factor authentication systems to strengthen account security.
- Supporting organizations in developing comprehensive digital risk management strategies.

Expected Outcomes:

- Reducing electronic threat detection time by over 40%.
- Increasing digital protection levels and minimizing chances of complex breaches.
- Raising awareness among organizations and users about the importance of cybersecurity.
- Providing a practical model applicable in various work environments to enhance digital protection.