

دراسات نقدية

إعداد
خليل إبراهيم المويل

دراسة نقدية لبحث

AI-Enhanced IT Governance and Cybersecurity Auditing in
Saudi Higher Education Universities: Policy, Risk, Educational
Leadership, and Institutional Behavior

حوكمة تكنولوجيا المعلومات المعززة بالذكاء الاصطناعي وتدقيق الأمن
السيبراني في جامعات التعليم العالي السعودية: السياسة، والمخاطر، والقيادة
التربوية، والسلوك المؤسسي



**AI-Enhanced IT Governance and Cybersecurity Auditing in
Saudi Higher Education Universities: Policy, Risk, Educational
Leadership, and Institutional Behavior**

التكليف الثاني

AI-Enhanced IT Governance and Cybersecurity Auditing in Saudi higher education universities: Policy, risk, educational leadership, and institutional behavior

Haifa Ibrahim Alodan^a, Aisha Abdallah^b, Saad Alateeq^c, Aeshah A. Almutairi^d, Abdullah Alotaibi^e, Ala'a M. Al-Momani^f, Reem Abdullah Almoeather^g, and Malik Bader Alazzam^g

^aDepartment of Teaching and Learning, Princess Nourah Bint Abdul Rahman University, Riyadh, Kingdom of Saudi Arabia; ^bDepartment of Health Information Management and Technology (HIMT), College of Medical and Applied Sciences, University of Hafr Al Batin, Hafar Al-Batin, Kingdom of Saudi Arabia; ^cSocial Studies Department, College of Humanities and Social Sciences, King Saud University, Riyadh, Saudi Arabia; ^dDepartment of Information Technology, College of Computer, Qassim University, Buraydah, Saudi Arabia; ^eEducational Technology, College of Education, King Saud University, Riyadh, Saudi Arabia; ^fDepartment of Management Information Systems, Amman Arab University, Amman, Jordan; ^gFaculty of Information Technology, Jadara University, Irbid, Jordan

ABSTRACT

The growing application of artificial intelligence in the domain of cybersecurity has improved threat detection and response mechanisms simultaneously, and this has also raised concerns about governance, policy, and risk management, especially in the domain of higher education. This paper examines the application of AI-Enhanced IT Governance and Cybersecurity Auditing in Saudi Arabian higher education, focusing on its association with policy clarity and effectiveness, AI-based cybersecurity risk management, and its educational aspects. This paper uses the theories and frameworks of governance and risk management and fills an important gap in existing literature, which has focused on the Western world and its application in the domain of higher education. A mixed-methods approach has been adopted, and this includes the survey method, which has targeted 200 professionals, including IT and cybersecurity experts, administrative staff, and education staff, and has also conducted semi-structured interviews. The quantitative results have been analyzed through the application of descriptive statistics, reliability, and regression analysis, and the qualitative results have also undergone the process of thematic analysis. The results have shown that there is moderate to high application of AI-Enhanced IT Governance and Cybersecurity Auditing in Saudi Arabian higher education.

7. Conclusion

This research focused on AI-Enhanced IT Governance and Cybersecurity Auditing in Saudi Arabian Higher Educational Institutions and its implications on policy clarity, management of AI-based cybersecurity risk, and educational outcomes. Utilizing a mixed research methodology, this research work empirically validates that the maturity of AI-Enhanced IT Governance and Cybersecurity Auditing in Saudi Arabian Higher Educational Institutions is moderate to high, which is a positive outcome of their digital transformation strategy.

Analysis of the findings shows that the impact of governance of AI cybersecurity is strongly positive on the transparency of policies and the governance of risks associated with the use of AI cybersecurity. The governance of the institution is likely to be associated with policies and processes that are clear and enforceable, as well as having an effective mechanism for evaluating risks associated with the use of AI cybersecurity. The findings confirm the governance theory.

To conclude, the research has verified that AI-Enhanced IT Governance and Cybersecurity Auditing represent an essential institutional capability that influences the efficiency of policy, risk maturity, and preparedness for educational events in HEIs. The findings from the Saudi-based research help to better comprehend the subject of cybersecurity and the requirement for an education-focused perspective on AI-Enhanced IT Governance and Cybersecurity Auditing.

7.1. Recommendations

From the findings, the following recommendations can be proposed:

- (1) Creating clear guidelines for AI-based cybersecurity: A specific governance structure for cyberse-

دراسة نقدية لمصطلحات الدراسة

اعتمدت الدراسة على مجموعة من المصطلحات الحديثة والمتخصصة في مجالات الذكاء الاصطناعي والأمن السيبراني وحوكمة تقنية المعلومات، وكان من أبرزها:

(حوكمة تقنية المعلومات المعززة بالذكاء الاصطناعي). AI-Enhanced IT Governance

(تدقيق الأمن السيبراني). Cybersecurity Auditing

(إدارة مخاطر الأمن السيبراني القائمة على الذكاء الاصطناعي). AI-Based Cybersecurity Risk Management

(وضوح السياسات وفعاليتها). Policy Clarity and Effectiveness

(الآثار أو الانعكاسات التعليمية). Educational Implications

(السلوك المؤسسي). Institutional Behavior

وتُعد هذه المصطلحات مناسبة لموضوع الدراسة وتعكس طبيعة التحول الرقمي والتطورات الحديثة في إدارة الأمن السيبراني داخل مؤسسات التعليم العالي.

دراسة نقدية لمصطلحات الدراسة

الدراسة استخدمت بعض المصطلحات المركبة والمعقدة دون تقديم تعريفات نظرية وإجرائية كافية في بداية البحث، وخاصة مصطلح AI-Enhanced IT Governance and Cybersecurity Auditing الذي يجمع بين ثلاثة مفاهيم مستقلة: حوكمة تقنية المعلومات، والذكاء الاصطناعي، والتدقيق السيبراني. وقد يؤدي هذا الدمج إلى صعوبة في التمييز بين حدود كل مفهوم ودوره في النموذج البحثي. كما أن الدراسة تعاملت مع هذا المصطلح كمفهوم واحد رغم أنه يتضمن أبعاداً متعددة تحتاج إلى توضيح أكبر.

بعض المصطلحات مثل Policy Clarity and Effectiveness و Institutional و Educational Implications Behavior جاءت بصيغة عامة وواسعة، ولم يتم تحديد أبعادها أو مؤشرات قياسها بصورة واضحة قبل استخدامها في الفرضيات والتحليل الإحصائي. فمثلاً، لم توضح الدراسة بشكل كافٍ ما المقصود بالسلوك المؤسسي تحديداً، وهل يتعلق بثقافة المؤسسة أم بعمليات اتخاذ القرار أم بالالتزام التنظيمي. كذلك فإن مفهوم الآثار التعليمية جاء عاماً دون تحديد الجوانب التعليمية المستهدفة بشكل دقيق.

دراسة نقدية لمصطلحات الدراسة

ومن ناحية أخرى، استخدمت الدراسة عدداً كبيراً من المصطلحات التقنية الحديثة مثل Machine Learning (ML) و Deep Learning (DL) و Graph Neural Networks (GNNs) و Explainable AI (XAI)، وهو ما يعكس حداثة المراجع المستخدمة، إلا أن التركيز على الجوانب التقنية كان أكبر من توضيح ارتباط هذه المفاهيم بالإطار الإداري والحوكومي للدراسة، مما أوجد نوعاً من التباين بين الجانب التقني والجانب الإداري في العرض النظري

3. Literature review

3.1. AI-Enhanced IT Governance and Cybersecurity Auditing

Artificial intelligence (AI), especially machine learning (ML) and deep learning (DL), is increasingly being utilized to enhance and improve major cybersecurity capabilities that require fast recognition of patterns and scalable decision-making. One of the major application domains of AI is related to intrusion detection systems (IDS), where AI algorithms are trained to recognize malicious behavior based on learned patterns from data to perform detection with higher effectiveness than traditional signature-based methods (Sowmya & Mary Anita, 2023). Current research trends reveal an increasing focus of IDS research action on new computing domains such as cloud computing, edge computing, and IoT, where DL-based detection of malicious activity is made possible with high-volume data (Pinto Neto et al., 2025).

Besides the conventional deep learning techniques, new architectures, such as Graph Neural Networks (GNNs), are being increasingly used in the development of intrusion detection systems because of the ability of GNNs to represent the relationships between different entities, such as hosts, flows, and events, which may not be properly handled by the conventional deep learning approaches (Zhong et al., 2024).

Artificial Intelligence is also widely utilized in the classification and detection of malware, with application of DL techniques on various platforms and formats, such as text, binary, and image-based models for malware. It has shown effective detection power, yet highly dependent on the quality and criteria of the datasets utilized (Bensaoud et al., 2024). Phishing site detection is another key use of AI, with ML and DL approaches being used for phishing site detection based on pattern detection from URLs and site content features. Systematic reviews indicate a significant use of ML detection mechanisms in recent studies (Safi & Singh, 2023). More recently, AI approaches are being investigated for ransomware detection with promising uses of DL and big-data analysis for dealing with ransomware threats (Bello et al., 2021).

Despite the improvement in detection capabilities and automation, the literature identifies the threats associated with trustworthiness and functionality in the literature. The most important threat associated with trustworthiness is the vulnerability of the models to adversarial attacks like poisoning attacks and evasion attacks (Bountakas et al., 2023).

Another important risk is related to the opacity or lack of explainability in complex AI models. For critical cybersecurity applications, the trust of cybersecurity experts in the decisions made by “black box” systems for intrusion detection can be affected negatively by the opacity of these systems’ decision-making processes. Therefore, the application of explainable AI in IDS is increasingly being sought after for increased transparency in decision-making processes (Samed & Sagiroglu, 2025).

studies (Safi & Singh, 2023). More recently, AI approaches are being investigated for ransomware detection, with promising uses of DL and big-data analysis for dealing with ransomware threats (Bello et al., 2021).

Despite the improvement in detection capabilities and automation, the literature identifies the threats associated with trustworthiness and functionality in the literature. The most important threat associated with trustworthiness is the vulnerability of the models to adversarial attacks like poisoning attacks and evasion attacks (Bountakas et al., 2023).

Another important risk is related to the opacity or lack of explainability in complex AI models. For critical cybersecurity applications, the trust of cybersecurity experts in the decisions made by “black box” systems for intrusion detection can be affected negatively by the opacity of these systems’ decision-making processes. Therefore, the application of explainable AI in IDS is increasingly being sought after for increased transparency in decision-making processes (Samed & Sagiroglu, 2025).

However, there are also challenges with regard to deployment. The deployment of IDS systems based on deep learning is also faced with challenges of high rates of false positives, lack of generalization from controlled benchmark datasets to realistic deployment scenarios, as well as challenges of operationalization of models for continuous detection within dynamic settings (Pinto Neto et al., 2025). In the context of malware detection, there is emphasis placed upon challenges of benchmarking, generalization to unseen threats, as well as challenges of the effects of adversarial attacks upon robustness of deep learning classifiers (Bensaoud et al., 2024). In research related to phishing detection, there is also emphasis placed upon sensitivity of results to sources as well as designs of machine learning models for phishing detection, with emphasis placed upon governance-aware deployment (Safi & Singh, 2023). All these challenges further strengthen the argument for AI systems for security to be governed with emphasis placed upon validation, transparency, monitoring, and resilience.

دراسة نقدية للدراسات السابقة

جاءت الدراسات السابقة في البحث واسعة وحديثة، حيث تناولت عدة محاور مرتبطة بموضوع الدراسة، مثل تطبيقات الذكاء الاصطناعي في كشف التسلل والبرمجيات الخبيثة والتصيد الإلكتروني، وحوكمة الأمن السيبراني في مؤسسات التعليم العالي، والسياسات التنظيمية، وإدارة المخاطر، والآثار التعليمية. وهذا يدل على أن الباحثين حاولوا بناء خلفية علمية شاملة تربط بين الذكاء الاصطناعي والأمن السيبراني والحوكمة في الجامعات السعودية.

ومن نقاط القوة أن الدراسات السابقة اعتمدت على مراجع حديثة في الغالب، خاصة من الأعوام 2020 إلى 2025، وهذا مناسب لطبيعة الموضوع لأنه من المجالات المتغيرة بسرعة. كما أن تقسيم المراجعة إلى محاور فرعية مثل-AI :
**‘Cybersecurity Governance in Enhanced IT Governance and Cybersecurity Auditing،
Higher Education Institutions، Cyber Risk Management، وEducational Implications** ساعد في تنظيم العرض وربط الأدبيات بمتغيرات البحث الرئيسية .

دراسة نقدية للدراسات السابقة

- إلا أن الملاحظة النقدية الأبرز هي أن عرض الدراسات السابقة جاء في معظمه وصفيًا تجميعيًا أكثر من كونه تحليليًا نقديًا؛ إذ ركز الباحثون على تلخيص ما توصلت إليه الدراسات السابقة دون مناقشة كافية لأوجه الاتفاق والاختلاف بينها، أو نقد مناهجها، أو بيان حدودها العلمية. فمثلاً، ذُكرت دراسات حول التعلم العميق، والشبكات العصبية، واكتشاف البرمجيات الخبيثة، لكنها لم تُناقش بعمق من حيث مدى ارتباطها المباشر بحوكمة تقنية المعلومات أو البيئة الجامعية السعودية.
- كما يلاحظ أن بعض الدراسات السابقة ذات طابع تقني بحت، بينما موضوع البحث يتناول أيضاً أبعاداً إدارية وتنظيمية وتعليمية مثل السياسات، وإدارة المخاطر، والقيادة التعليمية، والسلوك المؤسسي. لذلك كان من الأفضل أن يوضح الباحثون بشكل أدق كيف تخدم كل دراسة من الدراسات السابقة بناء النموذج المفاهيمي والفرضيات البحثية، بدلاً من الاكتفاء بعرض عام للموضوعات

دراسة نقدية للدراسات السابقة

من الجوانب الإيجابية أن البحث حدد فجوة بحثية واضحة، وهي قلة الدراسات التجريبية التي تناولت حوكمة الأمن السيبراني المعتمدة على الذكاء الاصطناعي في مؤسسات التعليم العالي السعودية. غير أن هذه الفجوة كان يمكن دعمها بصورة أقوى من خلال مقارنة مباشرة بين الدراسات العالمية والدراسات السعودية أو الخليجية، وبيان لماذا لا تكفي نتائج الدراسات الأجنبية لتفسير واقع الجامعات السعودية.

دراسة نقدية للدراسات السابقة

الخلاصة

اتسمت الدراسات السابقة بالحدائثة والتنوع والتنظيم الجيد، وأسهمت في بناء إطار نظري مناسب لموضوع الدراسة. إلا أن عرضها جاء أقرب إلى السرد الوصفي منه إلى التحليل النقدي، حيث لم تتم مناقشة أوجه الاتفاق والاختلاف بين الدراسات بصورة معمقة، كما أن الربط بين نتائج الدراسات السابقة ومتغيرات البحث وفروضه لم يكن واضحًا بالقدر الكافي، إضافة إلى محدودية التركيز على الدراسات السعودية والخليجية ذات العلاقة.



Thank You