

العنوان باللغة العربية

تقييم تأثير التقنيات الناشئة (e.g., AI, IoT) على إدارة مخاطر الأمن السيبراني.

إعداد الطالب/ فهد بن احمد الهديان

إشراف/ د. وليد عبدالجواد سليمان صديق  
د. الفيصّل عبدالحميد محمد حسن

العام الدراسي:

2023

Introduction

In the fast-paced world of cybersecurity, staying ahead of threats is an ongoing battle. Moreover, the entire landscape of cyber threats has been reported to continually shift and even mutate thereby demanding a continuous adaptation from the ones who are tasked with protecting various forms of digital assets. On the other hand, two of the most transformative and disruptive forces in this ever-evolving realm are Artificial Intelligence (AI) and the Internet of Things (IoT). Their levels of integration into different facets of this modern life have undoubtedly ushered in significant benefits, but this entire technological progress has also ended up casting a shadow that is full of new and complex challenges within the realm of cyber security (Lee, 2020). The entire contemporary digital ecosystem is heavily influenced by these technological juggernauts. The implementation of AI has made its presence felt across the whole augmentation of various human capabilities thereby enabling various types of machines to process, analyze, and even learn from different amounts of data. Moreover, within the boundaries of cybersecurity, AI promises to revolutionize threat detection, incident response, and vulnerability management. It is the major pillar of hope most so in a world where issues that are associated with cyber-attacks have emerged to be increasingly sophisticated targeting everything right from critical infrastructure to personal information (Raban & Hauptman, 2018). Moreover, AI greatly empowers the use of predictive analytics thus providing the tantalizing prospect of preemptive security measures, allowing a vast range of organizations to anticipate and even prevent quite a number of potential breaches. On the other hand, The Internet of Things has woven itself into the fabric of its modern existence. Moreover, an intricate network of different types of interconnected devices, ranging from smart appliances and medical equipment to industrial sensors, has greatly transformed the manner in which we live, work, and even interact with our respective environments. This level of monumental integration has greatly unlocked a wealth that is full of various possibilities from enhancing healthcare to optimizing different types of industrial

processes and even scaling up the daily conveniences. On the other hand, the proliferation of such types of devices has ended up introducing a multitude of various vulnerabilities. The absence of a standardized security protocol accompanied by limited computational resources of IoT creates one of the most unique combinations of various risks that must be keenly addressed. As various forms of advanced technologies are currently on the verge of permeating our lives together with work environments, it is important to recognize that all these challenges that they pose to cyber security are not abstract concepts or even future possibilities. They are here, they are real and they are also demanding our immediate attention. This proposal therefore serves as a clear blueprint for a more comprehensive research project with one purpose: to assess the profound impact of these emerging technologies, namely AI and IoT, on the delicate and ever-critical domain of cybersecurity risk management.

## **Background of the Study**

### **Emerging Technologies: AI and IoT**

#### **AI within the boundaries of cyber security**

Artificial Intelligence has revolutionized cybersecurity in several ways. As a result, different types of AI-powered tools are in a position to detect various threats in an accurate manner within the shortest time possible when compared to traditional systems, automating threat detection, and incident response with vulnerability management (Radanliev et al., 2018). All these capabilities are essential in a world where cyber-attacks are emerging to be increasingly sophisticated. What is more interesting is that the use of AI also empowers predictive analytics, helping different types of organizations to anticipate and prevent any existing potential security breaches.

#### **IoT in Cybersecurity**

The Internet of Things, comprising connected devices such as smart appliances, medical devices, and industrial sensors, has transformed the way we live and work. However, these devices also bring on board quite a number of security challenges (Lee, 2021). With the IoT devices proliferating at a faster rate, they end up presenting new entry points for various cybercriminals. Again, the lack of standardized security protocols together with the limited computational resources of quite a number of IoT devices might also end up creating quite a number of unique vulnerabilities that must always be addressed.

### **Cybersecurity Risk Management**

Cyber risk management entails the identification, assessment, and mitigation of different risks that are associated with cyber threats. It majorly encompasses a wide range of strategies, and policies together with technologies that are perfectly designed for protecting an organization's digital assets, and data together with various systems (Radanliev et al., 2020). Developing a clear understanding of the impact of emerging technologies within the boundaries of cyber security risk management is very essential for different organizations to adapt and remain more secure in a constantly evolving threat landscape.

### **Research Objectives**

One of the primary objectives that is linked to this research project is to carry out the assessment of the overall impact of emerging technologies, specifically AI and IoT, on cybersecurity risk management. In order to ensure that the study is perfectly attained, it will address the following specific research objectives:

1. Carry out an analysis of how AI is currently being utilized in cybersecurity to detect, respond to, and mitigate threats.
2. Investigate different security implications that are associated with IoT devices in different sectors, including healthcare, industrial, and consumer applications.
3. To carry out an analysis of current practices in cybersecurity risk management within organizations.

### **Methodology**

In order to attain all the aforementioned research objectives, there will be the implementation of a mixed method approach including the use of both qualitative and quantitative data collection methods. As a result, the following methods will be utilized:

1. **Literature review:** A more comprehensive review of the existing literature on AI, IoT, and cybersecurity will offer one of the most foundational levels of understanding of the current state of the whole field.
2. **Surveys:** Surveys will be implemented for cybersecurity professionals, technology experts, and organizations that are actively using AI and IoT technologies. As a result, this will greatly help me develop a clear understanding of their respective experiences, and challenges together with some of the best practices.
3. **Interviews:** The implementation of in-depth interviews with various cybersecurity experts, AI and IoT technology developers, and IT decision-makers will offer quite a number of qualitative insights into various nuances alongside the challenges of integrating all these technologies.

### **Data Analysis**

The data that will be collected through the use of surveys and interviews will be adequately analyzed through the use of both quantitative and qualitative methods.

### Expected Contributions

The implementation of this research project majorly aims to make quite a number of contributions across the whole field of cybersecurity. Some of the contributions majorly entail the following;

1. **Enhanced Understanding:** By evaluating the role of AI within the boundaries of cybersecurity and the impact of IoT, this research will contribute to an enhanced understanding of how these emerging technologies influence cybersecurity risk management.
2. **Practical Insights:** The study will offer a variety of practical insights together with some of the best practices for organizations to be able to adapt to their cyber security risk management strategies in response to the evolving threat landscape.
3. **Policy and Regulatory Recommendations:** The research may also contribute to policy and regulatory recommendations, most so in different areas that are related to IoT security standards and AI ethics.
4. **Framework Development:** The whole project might also result in the development of an advanced framework for an effective integration of AI and IoT into cybersecurity risk management.

### Timeline

The entire research project is expected to be carried out over a period of 2 months with the following appropriate timelines:

| Activity                              | Period |
|---------------------------------------|--------|
| Literature review and research design | 1 Moth |

|                                                           |          |
|-----------------------------------------------------------|----------|
| Data collection through surveys and initial case studies. | 3 Weeks  |
| In-depth case studies and interviews.                     | 2 Months |
| Data analysis and synthesis of findings.                  | 1 Month  |
| Report writing and dissemination of results.              | 2 Months |

### Conclusion

In the relentless march of technology, the only constant is change, and this dynamic landscape extends its influence deep into the domain of cybersecurity. With the existence of every technological leap, the overall potential for progress and innovation is perfectly mirrored by the potential for new threats and vulnerabilities. Moreover, at the center of this ever-evolving struggle stand two formidable contenders: Artificial Intelligence (AI) and the Internet of Things (IoT). Again, the integration of all these technologies into different aspects of modern life has greatly transformed the manner in which we operate, work, and even communicate, heralding remarkable benefits and opportunities. However, all these transformative forces have also cast one of the most challenging and complex shadows over the entire realm of cyber security. The overall impact of AI on cybersecurity is profound. AI's capability to process and analyze different types of datasets in real time, learn from past incidents, and make decisions autonomously presents a game-changing opportunity for organizations to defend against cyber threats. Its capability to automate threat detection, incident response, and vulnerability management offers one of the most promising proactive and intelligent approaches to cybersecurity.

### References

Lee, I. (2020). Internet of Things (IoT) cybersecurity:

Literature review and IoT cyber risk  
management. *Future internet*, 12(9), 157.

Lee, I. (2021). Cybersecurity: Risk management

framework and investment cost analysis. *Business Horizons*, 64(5), 659-671.

Raban, Y., & Hauptman, A. (2018). Foresight of cyber security threat drivers and affecting  
technologies. *foresight*, 20(4), 353-363.

Radanliev, P., De Roure, D. C., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S., &  
Burnap, P. (2018). Future developments in cyber risk assessment for the internet of  
things. *Computers in industry*, 102, 14-22.

Radanliev, P., De Roure, D., Page, K., Nurse, J. R., Mantilla Montalvo, R., Santos, O., ... &  
Burnap, P. (2020). Cyber risk at the edge: current and future trends on cyber risk  
analytics and artificial intelligence in the industrial internet of things and industry  
4.0 supply chains. *Cybersecurity*, 3(1), 1-21.

**College of Management**

**Department of Risk management**

**Title in English**

**Assessing the impact of emerging technologies (e.g., AI, IoT) on  
cybersecurity risk management**

**Prepared by:**

**Fahad Ahmed Alhodayan**

**Supervised by:**

**PhD. Waleed sulaiman**

**PhD. Alfaisal Abdelhameed**

**Year:2023**