



Task 1 Research issues 3:Critical Review of Previous Studies in Cybersecurity

**Field:
Cybersecurity**

Prepared by

ALI MMADI, PhD student-Midocean University



Research Issues(3)

Task 1

ALI MMADI

PhD student - Midocean University

www.midocean.ae

Studies on Artificial Intelligence-Based Intrusion Detection

Hello everyone,

Today, I am going to present my assignment number 1, which consists of preparing a critical review of previous studies published in my research field, which is Information Technology, specializing in cybersecurity.

The objective of this review is to analyze existing research, identify its strengths and weaknesses, and highlight the gaps that require further scientific investigation.



1. Introduction to the field

Cybersecurity has become an essential field with global digital transformation. Businesses, governments, and individuals rely heavily on computer systems, which increases the risks associated with cyberattacks. According to the report published by IBM, the average global cost of a data breach continues to rise each year, highlighting the importance of strengthening protection mechanisms.

The main current threats include:

- ☐ Ransomware attacks
- ☐ Phishing
- ☐ Distributed denial-of-service attacks
- ☐ Insider threats

In this critical review, I will analyze three main research areas:

1. Artificial intelligence-based intrusion detection
2. Cloud computing security
3. Blockchain-based cybersecurity



2. Studies on Artificial Intelligence-Based Intrusion Detection

Several studies have investigated the use of Machine Learning and Deep Learning to improve intrusion detection systems.

An important study conducted by Ian Goodfellow in the field of Deep Learning demonstrated the effectiveness of neural networks in identifying complex attack patterns.

Key points:

- Use of large databases of real attacks
- High accuracy in threat detection
- Machine learning capability and continuous improvement

Weak points:

- High dependence on the quality of training data
- Problem of high false positives
- Significant computational cost
- Vulnerability to adversarial attacks

In addition, some studies have used the KDD Cup 99 dataset, which is outdated and does not reflect modern threats, limiting the validity of the results.

3. Studies on Cloud Computing Security

With the massive migration to the cloud, the security of cloud environments has become a priority. Research published by the National Institute of Standards and Technology has proposed risk management frameworks for cloud environments.

✓ Highlights:

- Structured approach to risk management
- Clear identification of responsibilities between supplier and client

- Implementation of international standards

✗ Weaknesses:

- Complexity of implementation in SMEs
- Lack of experimental studies in real environments

- Difficulty in managing internal threats

Some studies remain theoretical and lack large-scale practical evaluation.

4. Studies on blockchain in cybersecurity

Blockchain technology is being studied as a potential solution to improve the security of transactions and digital identities.

The concept introduced by Satoshi Nakamoto in the Bitcoin white paper: A Peer-to-Peer Electronic Cash System paved the way for many secure applications.

✓ Highlights:

- ❑ Transparency and traceability of transactions
- ❑ Resistance to data tampering
- ❑ Decentralization

✗ Weak points:

- Scalability issues
- High energy consumption
- Potential vulnerabilities in smart contracts

Furthermore, few studies analyze the actual integration of blockchain into existing infrastructures.

5.Global comparative analysis

By comparing these studies, several trends can be observed:

First, the majority of research shows promising results in the laboratory, but few are tested in large-scale real-world environments.

Second, there is a lack of integration between the different solutions. For example, few studies combine artificial intelligence, cloud, and blockchain in a unified approach.

Third, the issue of the human factor remains insufficiently studied, even though human error is one of the main causes of security incidents.

6. Identified gaps and future directions

From this critical review, several gaps emerge:

- ❖ Lack of recent and realistic datasets
- ❖ Insufficient experimentation in real-world conditions
- ❖ Limited consideration of emerging attacks
- ❖ Lack of hybrid approaches combining multiple technologies

Future research should focus on:

- ❖ Improving the robustness of AI models
- ❖ Reducing false positives
- ❖ Secure integration of multi-cloud environments
- ❖ Studying human behavior in cybersecurity

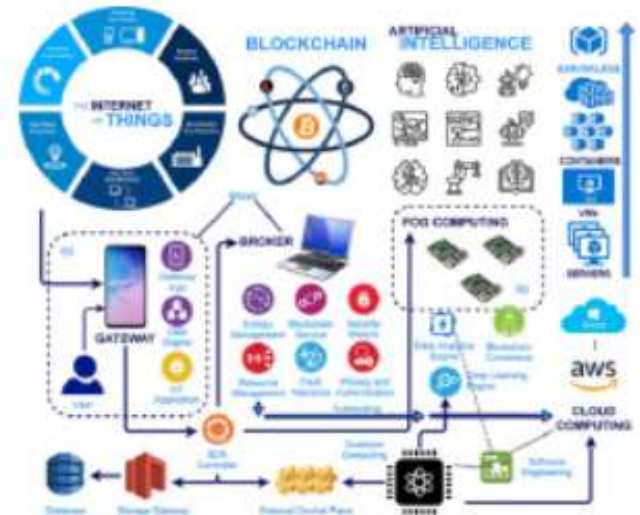
Conclusion

In conclusion, cybersecurity is a constantly evolving field. Existing studies offer significant advancements, particularly in artificial intelligence, cloud computing, and blockchain.

However, this research still has methodological and practical limitations.

This critical review has allowed me to identify current gaps and better guide my future research work toward more integrated, realistic, and suitable solutions for modern threats.

Thank you for your attention.



KEY REFERENCES

- 1) Research Issues 3 Course** by our professor Dr. Mohamed Gaber Al-Khouli at Midocean University
Course Title: An introductory lecture for the course: Research Issues 3 (2026)
- 2)** Ian Goodfellow, Bengio, Y., & Courville, A. (2016).
Deep Learning. MIT Press
- 3)** Mehdi Mirza & Simon Osindero (2014).
Conditional Generative Adversarial Nets. arXiv
- 4)** Mahbod Tavallaee et al. (2009).
A detailed analysis of the KDD CUP 99 dataset.
IEEE Symposium on Computational Intelligence for Security and Defense Applications
- 5)** Satoshi Nakamoto (2008).
Bitcoin: A Peer-to-Peer Electronic Cash System
- 7)** Arvind Narayanan et al. (2016).
Bitcoin and Cryptocurrency Technologies. Princeton University Press
- 8)** Joseph Bonneau et al. (2015).
SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies.
IEEE Symposium on Security and Privacy



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

