

Research Issues RSC811-Assignment 7

Prepared by
Abdulaziz Alarfaj



Part

1

Research Title : العنوان

Title : "Harnessing GPT-4 for generation of cybersecurity GRC policies: A focus on ransomware attack mitigation “

Research Area: The paper focuses on using GPT-4 to generate cybersecurity policies, specifically for mitigating ransomware attacks involving data exfiltration. This is a compelling and contemporary topic, given the rapid advancements in AI and increasing cyber threats.

Variables:

Independent: Use of GPT-4 for policy generation.

Dependent: Effectiveness, efficiency, completeness, and ethical compliance of the generated policies.

Application Domain: Governance, Risk, and Compliance (GRC) in cybersecurity.

Introduction : المقدمة

The introduction effectively outlines the importance of GRC in cybersecurity and the challenges organizations face.

GPT-4 is introduced as a potential solution to enhance GRC policy efficiency and effectiveness.

Strengths: Comprehensive and well-linked to the research problem.

Weaknesses: More detail on how effectiveness/efficiency are measured could be added.

Part

3

Problem Statement : مشكلة الدراسة

Gaps in Literature: Clearly identified, such as the lack of comprehensive studies on AI models in GRC, especially against modern ransomware threats.

Problem Formulation: Key research questions are posed, e.g.:

How do GPT-4-generated policies compare to human-generated ones in terms of effectiveness?

What are the ethical/legal challenges of using GPT-4 for GRC?

Proposed Solutions: Game theory and quantitative analysis are used for policy comparison.

Part

4

Significance of the Study : أهمية الدراسة :

Theoretical: Provides a novel framework for evaluating AI-generated cybersecurity policies, opening avenues for future research.

Practical: Offers actionable recommendations for organizations integrating GPT-4 into GRC decision-making, with ethical/legal considerations.

Value: Bridges theory and practice, benefiting academics and practitioners.

Part

5

Objectives of the Study : أهداف الدراسة

Clear and achievable objectives, e.g.:

Compare GPT-4 and human-generated policies.

Develop a comparison framework using game theory.

Identify strengths/weaknesses of GPT-4 policies.

Feasibility: Objectives align with the methodology.

Achievement of Objectives: The study achieves its objectives

مفاهيم وتعريفات الدراسة : Concepts and Definitions

Variables: Well-defined, e.g.:

Effectiveness: Policy's ability to achieve goals.

Efficiency: Resource utilization.

Ethical Compliance: Adherence to laws/standards.

الدراسات السابقة: Literature review

Recency: Most cited studies are recent (2020–2023), reflecting current AI/cybersecurity trends.

Agreements/Disagreements:

Agreement on GPT's potential in GRC automation.

Disagreement on ethical/legal challenges.

Theoretical Proposals: Used to formulate hypotheses, e.g., GPT-4's superiority in certain contexts.

Part

8

Hypotheses : فرضيات الدراسة

Main Hypotheses:

GPT-4 policies are more effective/efficient than human ones in specific contexts.

Tailored prompts improve GPT-4's performance.

Alignment with Objectives: Hypotheses support the study's goals (e.g., policy comparison).

Strengths: Clear and testable.

Weaknesses: Could include hypotheses on ethical/legal challenges.

Part

9

Study Model : نموذج الدراسة

Theoretical Framework: Based on game theory and quantitative analysis (e.g., cost-benefit).

Clarity: The model illustrates relationships between variables (e.g., how GPT-4 policies influence attacker/defender decisions).

Hypothesis Testing: Done via quantitative comparison.

Methodology and Statistical Analysis: منهجية الدراسة و التحليل الاحصائي

Data Sources: Reports from NIST, Trend Micro, etc.

Sample: Policies from cybersecurity vendors and government agencies.

Data Collection: GPT-4 generates policies based on problem descriptions.

Strengths: Comprehensive, multi-method approach.

Weaknesses: Reliance on non-sensitive data may limit generalizability.

Discussion of Results and Recommendations : مناقشة النتائج والتوصيات

Results:

GPT-4 policies outperformed human ones in effectiveness/efficiency with tailored prompts.

Ethical/legal challenges require further exploration.

Interpretation: Results align with some literature but highlight caution in AI adoption.

Recommendations:

Human review of AI-generated policies is essential.

Develop best-practice guidelines for GPT-4 use.

Future Research: Expand GPT-4's application in GRC, improve transparency/accountability.

Part

12

Overall Assessments :

The study makes a valuable contribution to cybersecurity by integrating AI into GRC, with a strong focus on ransomware mitigation.

However, deeper analysis of ethical/legal issues and broader data inclusion (e.g., sensitive policies) could enhance its impact. The recommendations are practical, making the paper a useful reference for researchers and practitioners.

Article link :

<https://www.sce.carleton.ca/faculty/wainer/papers/1-s2.0-S0268401222000548-main.pdf>