



# ETHICAL HACKING IN AI-BASED CYBER WARFARE

MADE BY:- GAURAV NAIK , RISHIKESH SAGARE , SHRAWAN PARAB

---

# Abstract

shutterstock.com • 1210718851

## PROBLEM STATEMENT

- Imagine a hacker using AI to create a fake email that tricks a bank employee into giving away sensitive data. Now imagine the bank using AI to spot that attack before it happens. This is the reality of AI in cyber warfare; it's a powerful tool for both attackers and defenders. However, AI systems can also be hacked, creating new risks. For example, in 2020, hackers used AI to mimic a CEO's voice, stealing \$243,000 from a company. These challenges show why we need ethical hacking, where experts try to break into systems (with permission) to find and fix weaknesses before bad actors exploit them.

# OBJECTIVE

- The problem is that AI-driven cyber warfare is fast, complex, and hard to defend against with old methods. Ethical hacking needs to evolve to keep up. This research aims to:
- Understand how AI is used in cyber attacks and defenses.
- Explore how ethical hacking can use AI to protect systems.
- Discuss the ethical risks of AI hacking tools.
- Highlight the job and business opportunities in this field.
- Suggest future research to make ethical hacking better. This study will help students and professors understand how ethical hacking can make AI-based systems safer.

## LITERATURE REVIEW

- AI in Cyber Warfare: The Good and the Bad
- Ethical Hacking: Old and New Ways
- Case Study: AI Hacking in Healthcare
- Gaps in Current Defenses

# RESEARCH METHODOLOGY

This research uses a qualitative approach, meaning we studied existing information rather than collecting new data with experiments. We did a literature review, which is like reading a lot of books and articles to understand a topic. Here's how we did it:

- Finding Sources: We searched for articles using keywords like AI in cyber warfare, ethical hacking, and AI cybersecurity on Google Scholar and university databases.
- Choosing Sources: We picked only trustworthy sources, like peer-reviewed journals and reports from organizations like the Atlantic Council.
- Reading and Summarizing: We read about AI's role in attacks and defenses, how ethical hacking works, and its ethical and market impacts.
- Organizing Information: We grouped our findings into themes, like AI's benefits, risks, and future possibilities.

This method helped us understand the big picture of ethical hacking in AI-based cyber warfare without needing complex tools or experiments. It's perfect for an undergraduate project because it's clear and manageable.

## ETHICAL IMPACT

### ■ Ethical Concerns: Can AI Be Too Dangerous?

Using AI for hacking is like giving someone a powerful tool it can build or destroy. Ethical hackers use AI to protect systems, but the same AI could help criminals. For example, AI that generates fake emails for testing defenses could be used to scam people. Another worry is that AI might make decisions without human oversight. Imagine an AI wrongly flagging a hospital's system as safe, leaving it open to attack. To avoid this, ethical hackers need clear rules, like always having a human check AI's work.



# MARKET RELEVANCE

## ■ Market Relevance: Big Opportunities

AI in cybersecurity is a hot field. Companies and governments are spending billions to protect their systems. By 2026, the AI cybersecurity market could be worth \$40.8 billion . Ethical hackers with AI skills are in high demand. For example, companies like Microsoft hire them to test cloud systems. Militaries, like the U.S.Army, use AI to defend against cyber attacks from other countries .This means lots of jobs and innovation for students studying cybersecurity.



# FUTURE SCOPE

The future of ethical hacking in AI-based cyber warfare is full of possibilities. Here are some ideas for further research:

- Smart Threat Prediction: Create AI that guesses where hackers will attack next, like a weather forecast for cyberthreats.
- Rules: Develop guidelines to ensure AI is used safely in hacking, preventing misuse.
- Training: Teach more students and professionals how to use AI for ethical hacking.
- AI : Find ways to stop hackers from tricking AI systems with bad data.
- Teamwork: Encourage countries to share ideas for fighting AI-based cyber threats.

These ideas can make the internet safer and create exciting opportunities for researchers and cybersecurity experts.



THANK YOU