New Cybersecurity Threats That Can Emerge Due to The Development of AI In The Next Decade

Pravit Gupta

Abstract - This project examines how Artificial Intelligence (AI) may give rise to new cyber threats in the future. Some AI tools, such as FraudGPT and WormGPT, are already being used by criminals to create fake emails, develop viruses, and identify vulnerabilities in systems. There have also been real cases where AI was used to make fake videos and voices to trick people and steal money. The study uses ideas from other research to show that AI can be used for both good and bad purposes. To understand what people think, a survey was done with 83 people. Most people knew about AI and believed that AI-based cyber threats would increase in the next 10 years. But many also said they don't feel ready to deal with them. This shows we need better rules, more education, and teamwork between governments, companies.

Keywords – AI, Cybersecurity, Threat, GPT.

I. Introduction

In the past, there have been instances where AI has been used for malicious purposes. Tools popularly known as FraudGPT and WormGPT have been leveraged to commit cybercrimes. FraudGPT is a tool marketed on dark web platforms, offering capabilities such as crafting spear-phishing emails, generating malware, and identifying system vulnerabilities. It has been promoted as a subscription-based tool that provides a range of utilities for fraudulent activities [1].

WormGPT is another AI tool often used in cybercrime. It enables users to generate content for illegal purposes, such as phishing emails, malicious code, and other cyberattack vectors[2].

In early 2022, Thai criminals used deepfakes to impersonate police officers in extortion video calls. More recently, in February 2024, a Hong Kong officer of a multinational company was scammed out of $25.6 million after deepfake AI was used to impersonate a senior official in a conference call [3].

There have also been numerous cases of sex offenders using deepfake AI to create harmful content involving minors. In one case, a South Korean court sentenced a man for generating realistic, sexually abusive deepfake content involving children [3].

Generative AI has additionally been employed in phishing attacks. In a notable case, criminals used AI to replicate a CEO's voice, tricking an employee into transferring $230,000 to a fake supplier [3].

Research has also demonstrated that popular tools like Copilot can be exploited to create highly convincing spear-phishing emails. With access to someone's email account, these tools can mimic the person's tone and language, raising significant concerns [2].

"An alarming rise in AI-powered voice cloning scams shows how easily even a few seconds of audio can be used to create convincing impersonations" — notably, a Florida woman lost $15,000 after scammers cloned her daughter's voice to extort money over a fabricated accident [3].

Experts warn that deepfakes are reshaping corporate risk—"once easy to detect, deepfakes…have become incredibly sophisticated and accessible," generating an estimated **500,000 fakes in 2023 and projected to reach 8 million by 2025" [4]

Hackers used AI to create fake job ads and websites to steal people's data and spread malware [5].

In Kozhikode, India, a man received a WhatsApp video call from someone impersonating a former colleague. The deepfake face asked for ₹40,000, which the victim transferred before realizing it was a scam [6].

A 79-year-old woman in Bengaluru was tricked by a Facebook ad that showed a deepfake image of NR Narayana Murthy endorsing an AI trading platform. She lost over ₹34.6 lakh after investing and making fake "fees" [7].

Cybercriminals cloned the voice of a top railway official, asking for emergency funds via a WhatsApp call. The victim, a friend, transferred ₹2,00,000 before realizing it was a scam [8].

II. Literature Review

Recent studies have explored the dual role of AI in cybersecurity. On one hand, AI enhances defence mechanisms through improved threat detection and response. On the other hand, AI introduces vulnerabilities.

DOI : 10.35291/2454-9150.2025.0130

Generative AI models like FraudGPT and WormGPT have been used to initiate phishing campaigns and malware. Comprehensive reviews highlight the application of Large Language Models (LLMs) in tasks like vulnerability detection and malware analysis, while also pointing out limitations such as small datasets and the need for explainable models. The potential misuse of AI in creating things like deep fakes and manipulating public opinion highlights the need for robust ethical guidelines and regulatory frameworks.

Research Questions:

1. What are the new trends in cybersecurity threats expected in the future, especially those driven by more advanced attacker strategies?
2. How will advancements in technology cause the emergence of new cybersecurity threats, and what attack vectors will they introduce?
3. How can cybersecurity strategies evolve to counter future threats effectively, including the development of more advanced threats due to AI, adaptive security architectures, and enhanced digital forensics?
4. What role will international policies and rules play in mitigating cybersecurity risks, and how can global cooperation be strengthened to address transnational cyber threats?
5. How will the development of advanced hacking tools and knowledge impact the development of future threats?
6. What are the ethical implications of emerging cybersecurity technologies and strategies, and how can responsible innovation be ensured?

Objectives:

This study aims to look deeper into the emerging cybersecurity threats that will arise due to the development of Artificial Intelligence. It also aims to explore how new hacking tools may arise due to the development of Artificial Intelligence. It also looks deep into how cybercrime could further evolve with the evolution of AI systems. It will look into how cybersecurity systems can be enhanced to mitigate cybersecurity risks. It will assess the effectiveness of the current cybersecurity systems to defend against these emerging threats.

III. Overview of Existing Research

The integration of Artificial Intelligence (AI) into cybersecurity has caused both development and challenges. While AI enhances threat detection, it also makes advancements in cyberattacks.

Recent developments have used AI to craft dangerous cyberattacks. Tools like FraudGPT and WormGPT have been used to generate phishing emails, create malware, and identify a system's vulnerabilities. These AI-driven tools increase cybercrimes, enabling more targeted and effective attacks.

The rise of deepfake technology further increases cybercrime possibilities. Deep Fakes utilize AI to produce realistic audio and video content. Such technology has been exploited in various cybercrimes, including impersonating people in fraudulent communications and creating explicit content.

Theoretical framework

The Dual-Use Theory shows the capacity of technologies to have both beneficial and harmful purposes. In the case of AI, this theory shows how tools designed for enhancing cybersecurity can also be used for cybercrime. For example, generative AI models like FraudGPT and WormGPT have been used to launch phishing attacks and develop malware, which shows the dual-use property inherent in AI technologies. Ulrich Beck's Risk Society Theory tells us that modern technological advancements introduce new, often unpredictable risks. Applied to AI in cybersecurity, this theory says that the rapid development of AI systems can lead to security challenges that are difficult to predict. The global nature of AI-related risks, such as the proliferation of deepfakes and AI-driven misinformation campaigns, exemplifies the kind of systemic threats Beck described.

Identification of gaps in the literature

Many research studies have been conducted on what cybercrimes have currently been done using different AI tools; however, none so far focus on how cybercrime could grow and progress with the development of AI. There are also gaps in the study on how to defend against this if it occurs. Currently, various AI models can be manipulated through malicious inputs and further used for unethical purposes. This paper tries to fill these gaps and further suggest security measures to defend against emerging threats.

Relevance of the current study

The current study has explored in detail the cybercrimes that have happened in the past and how different AI tools have been used to conduct cybercrimes. They have also talked about how new AI tools have been created that have been used for cybercrime.

1. Research Design

This project used a survey to study how people think and feel about AI being used in cybercrime. Because AI is still growing and changing, a survey helped collect clear and organized answers from many different people. This kind of study is good when we want to see patterns, test ideas, and learn general facts. The goal was not only to see what people think now, but also to guess what they might worry about in the future. Since there is not much research on how AI might affect cybercrime and how people will deal with it, this project tries to explore new ideas using numbers and facts. The survey helped find out how aware people are, how much

DOI : 10.35291/2454-9150.2025.0130

they trust current security systems, and how ready they feel for future AI threats. It mainly focused on what is happening now instead of why it is happening. Using an online form made it easy to send to many people quickly.

2. Data Collection Methods

To collect the data, I made a Google Form that had simple questions people could answer easily. Google Forms was chosen due to its accessibility, built-in charts and automatic data collection into Google Sheets which making it convenient to use. The questions were multiple-choice and rating-type. They were made to check how much people know about AI, what they think about dangers like phishing and deepfakes, and how AI might change cybersecurity in the future. To improve reliability the questions were pilot-tested with 5 respondents and feedback was used to rephrase unclear options. I asked these questions after reading about current trends.

Before sharing, I tested the form with a few friends to check if the questions were easy to understand. After that, I sent the form on WhatsApp, email, and social media to reach more people. Everyone who filled it out did so by choice, and I added a short note at the beginning explaining what the survey was about and asking for their permission. All the questions were optional, so people could skip anything they didn't want to answer. The answers were saved directly in a spreadsheet, which made it easy to organize and study them.

3. Sampling Techniques

I used convenience sampling to find people for the survey. This means I asked people who were easy for me to reach, like friends and classmates. I shared the form on WhatsApp groups, Instagram stories, and Discord. This method may not give a perfect mix of all types of people, but it was useful and simple for this kind of project. It helped me get answers from different age groups and education levels. Most of the people were students and young people, who often know about tech and AI. Even though there can be some bias since the sample was self-chosen, the results still gave useful ideas about how people feel. The final number of people who answered was 83. I also included some questions to know their age, gender, and background. Age range was from 15–50+ which consisted of students and working professionals. This method worked well because the topic is new, and this project aims to learn more for future studies.

4. Data Analysis Procedures

I used simple math to look at the data. Google Sheets and Microsoft Excel were used to organize and visualize data. For questions with fixed answers, I used percentages to see what most people said. I also looked at averages to know how much people agreed or disagreed with different statements. I compared answers from different age groups, genders, or fields of study to see if there were any patterns. Cross-tabulation was used to compare responses across age and profession. Bar charts and pie charts were made to show the results in a clear way. For questions where people wrote their thoughts, I read the answers and picked out common ideas. This way, both numbers and opinions were included in the results. Even though this project did not use very complex tools like regression, it still gave good insights.

5. Ethical Considerations

I made sure the project followed all the rules of good research. At the beginning of the Google Form, I told people what the survey was about, that answering was their choice, and how the data would be used. People had to agree before they could take the survey. I didn't ask for names, emails, phone numbers, or anything personal, so everyone stayed anonymous. People could stop filling the form at any time if they didn't feel comfortable. The data was saved safely in my Google Drive with a password. I also made sure not to collect answers from anyone under 16 without permission from a guardian. Since the questions were simple and not personal, the study was safe and low-risk. Still, I followed all the basic research rules to keep everything honest and respectful.

IV. RESULTS

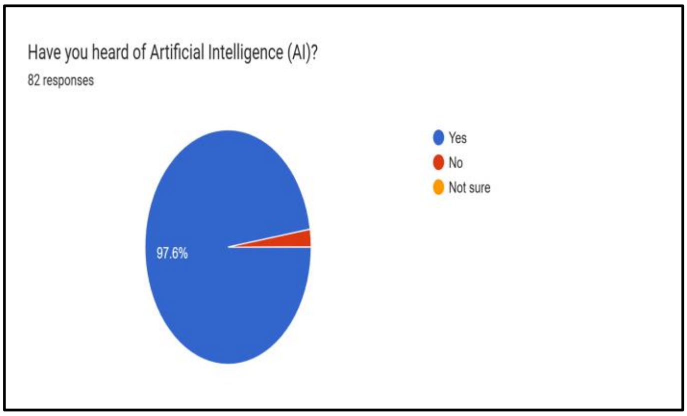
This report talks about the results from a survey we conducted about AI and cybersecurity. A total of 82 people filled out the form. We asked them about what they know, how they feel, and what they're worried about when it comes to AI being used in cybercrime.

Presentation of Data

We collected answers to 10 main questions. The questions covered things like awareness of AI, the risk of AI in cybercrime, who should be responsible for stopping it, and whether people would support new laws for it.

Tables and Figures

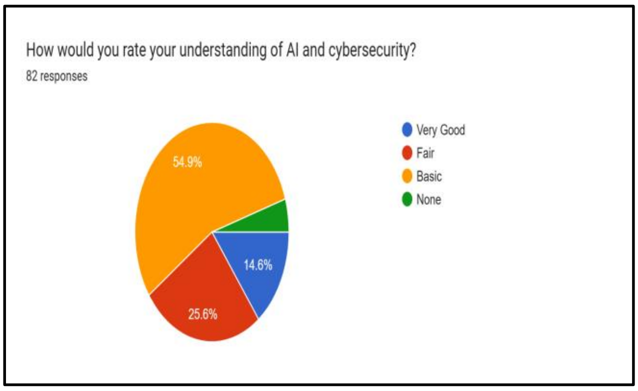
1. Have you heard of AI?



Almost everyone (97.6%) has heard about AI, showing high awareness among the people surveyed.

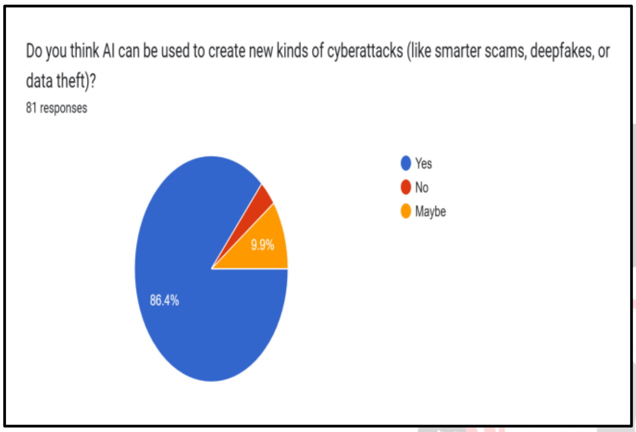
2. Understanding of AI and Cybersecurity

DOI : 10.35291/2454-9150.2025.0130



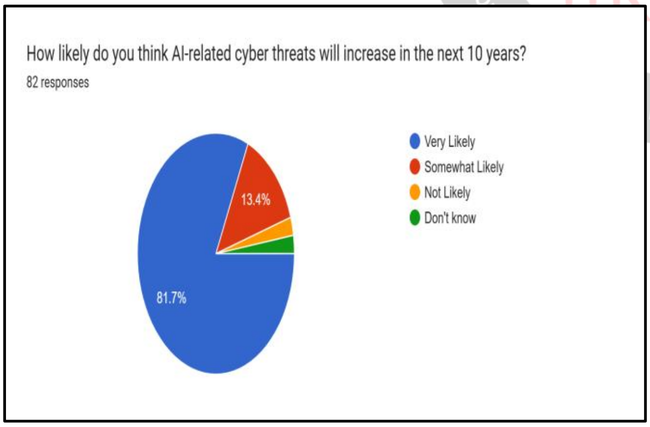
A very small percentage of people say they have no understanding, while only 14.6% feel they know AI and cybersecurity very well, others seem to have a basic understanding of it.

3. Can AI be used to create cyberattacks?



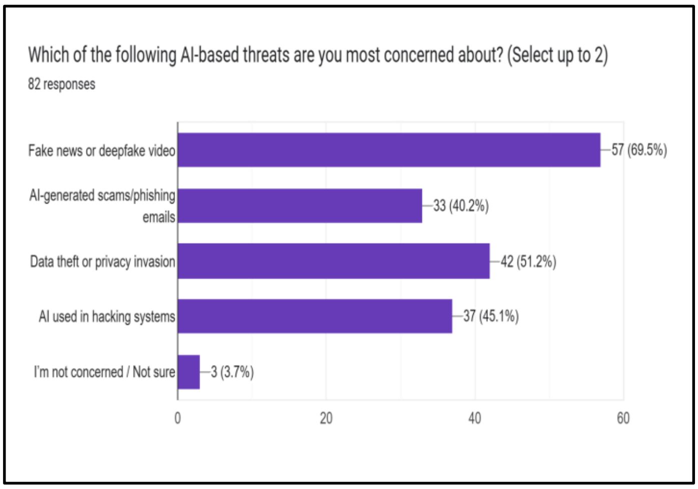
Most people (86.4%) believe AI can be used for dangerous attacks like deepfakes or scams.

4. Do you think AI threats will increase in the next 10 years?



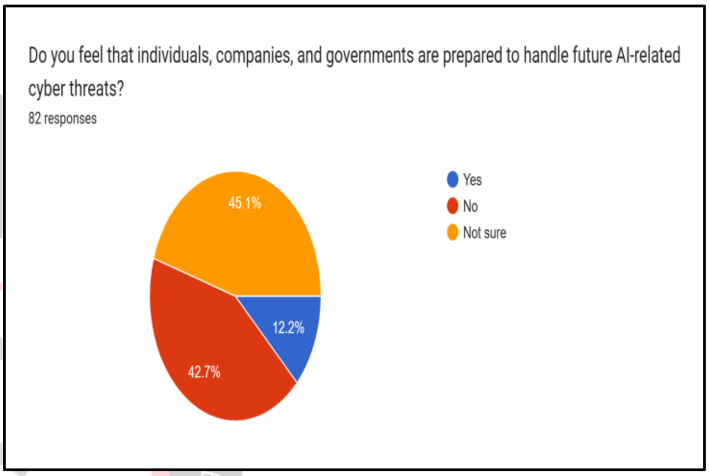
A large number (81.7%) think these threats will become more common in the future.

5. Most concerning AI-based threats:



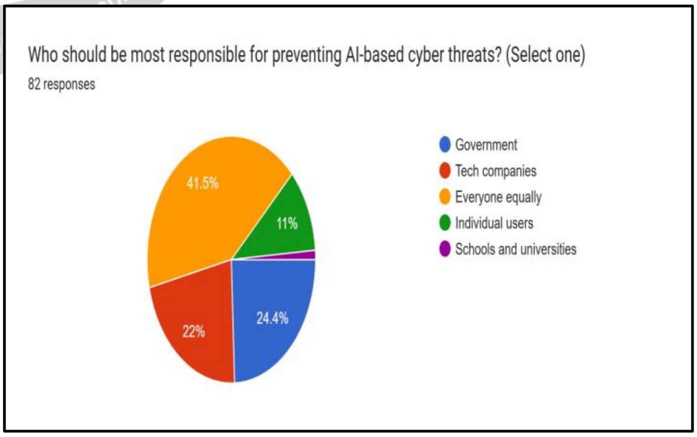
People are most worried about fake videos (69.5%) and data theft (51.2%).

6. Are we ready for future AI threats?



Only 12.2% feel confident that people, companies, and governments are prepared for future AI threats.

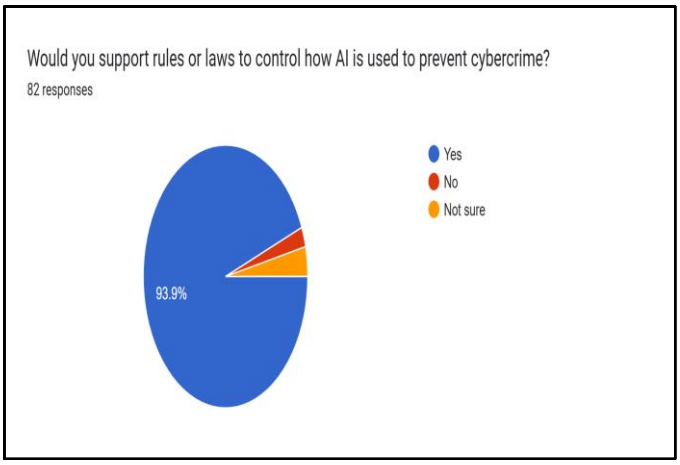
7. Who should stop AI-based cyber threats?



1. Most think everyone—governments, tech companies and users should share the responsibility (41.5%).

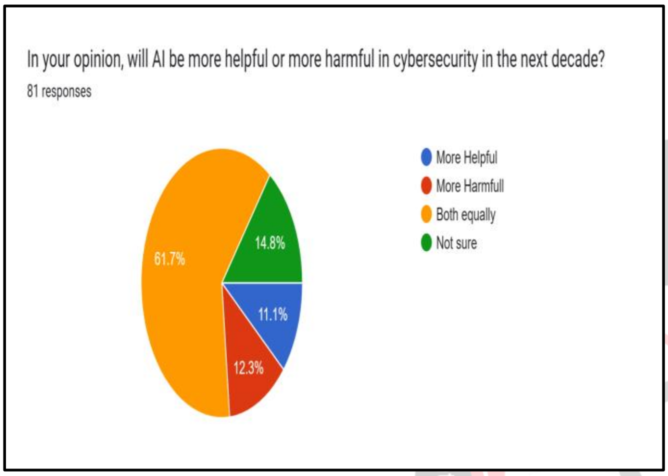
8. Do you support rules/laws to stop AI cybercrime

DOI : 10.35291/2454-9150.2025.0130



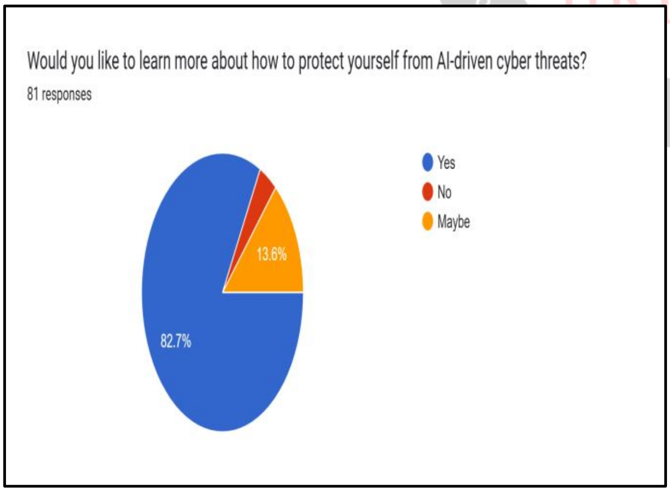
Most people (93.9%) support making rules to enforce the use of AI in the future to support cybercrime.

9. Will AI help or hurt cybersecurity in the future?



Many people (61.7%) feel that AI will be used in both cybersecurity and be harmful.

10. Want to learn more about AI safety?



Most people (82.7%) would like to learn more about how they can protect themselves in the future from AI based cyber threats.

Descriptive Statistics

- Most people (about 94%) have heard of AI. When it comes to understanding it, almost half say they have a "basic" idea. A big majority, 70 out of 81, think AI can be used for cyberattacks like scams and deepfakes. Also, 67 people think AI threats are "very likely" to grow in the next 10 years.

- These days, almost everyone has heard of AI. People use it for fun or work, but many are worried about it. They think AI might become dangerous if it's not controlled. It could affect jobs, privacy, or even safety in the future.

- Many people are worried because AI is being used to make fake news and scams and sometimes it's really hard to tell what is real and what is fake. AI can create fake videos, voices and messages that look and sound real and this can easily trick people. Scammers use AI to send fake emails or messages that try to steal someone's money or personal information. Because of this, people feel like they can't always trust what they see or hear online.

- Lots of people think that stopping bad things caused by AI shouldn't just be the job of one group and instead it should be done by everyone working together. The government should make rules, tech companies should make sure their AI tools are safe and regular people should learn how to stay careful online. If only one group tries to fix it, it won't be enough and the problem will keep growing. So it's important that everyone plays a part in keeping AI safe and useful.

- Most people think we need new rules to stop bad uses of AI. These rules can stop hackers and scammers from hurting others. If there are no rules, AI might be used in the wrong way. Rules will help keep people safe and still allow good use of AI.

- While many are not sure about how helpful or harmful AI will be, most want to learn more about how to protect themselves.

V. DISCUSSION

Interpretation of Results

From the results, we can say that most people know what AI is, but only a few have a strong understanding of how it is related to cybersecurity. Many people believe that AI can be used in dangerous ways, like making fake videos or stealing data. This shows that people are becoming more aware of how AI could be misused.

Also, most people think that AI-based threats will increase in the next 10 years. Only a small number of people said "no" or "don't know." This tells us that people expect AI to be a big part of future problems online. At the same time, they don't feel fully prepared. A lot of people answered "not sure" or "no" when asked if we are ready for these threats. This means we need to do more to educate and prepare everyone.

Many people said they are worried about how AI can be used in bad ways, like making deepfakes or stealing personal information. They also said that AI can be helpful and harmful, and that we need better laws to control it. Most people in our survey also agreed that we need rules and more knowledge to stay safe. This shows that people want to learn

DOI : 10.35291/2454-9150.2025.0130

and be more prepared. In the end, this study shows that even though people are aware of AI, they still need more help and support to fully understand and deal with its risks, especially in cybersecurity.

VI. Comparison with Existing Literature

In studies done before, researchers said that AI is both a tool and a threat in cybersecurity. Some reports from companies like IBM and research groups say AI helps stop threats faster, but also makes it easier to create scams or deepfakes. Our survey shows that many people agree with this idea. Most answers say AI will be both helpful and harmful. So what we found matches what experts are saying.

Also, other research has said that laws and rules about AI are needed. In our survey, almost everyone supported having rules to stop AI cybercrime. This again matches with what experts have already talked about in news articles and research papers.

Implications of the Findings

Our results show that people want to learn more about AI and how to stay safe online. Since many said they want more knowledge, schools and governments should try to give that info. We also saw that people think everyone has a role to play—government, companies, and even normal users.

This means that AI in cybersecurity isn't just a tech issue. It's something that needs teamwork from lots of different people. If we don't teach students or create rules early, then these problems could get worse over time.

Limitations of the Study

Even though the survey had 85 responses, it might not represent everyone. Most people in the survey already knew what AI was, so the results might be different if we asked a group that was not as familiar with technology.

Also, some questions allowed multiple answers, so it's hard to know which threat people fear the most. And because people answered online, they might have just guessed or clicked quickly without thinking deeply.

Still, the survey helps us understand what people are thinking, but more research with different types of people would help give a fuller picture.

VII. Citations

[1] Ironscales. (2023). Generative AI Fraud: FraudGPT, WormGPT, and Beyond. Retrieved from https://ironscales.com/blog/generative-ai-fraud-fraudgpt-wormgpt-and-beyond

[2] Global Initiative Against Transnational Organized Crime. (2024). AI, Deepfakes and Cyber Scams in South East Asia. Retrieved from https://globalinitiative.net/analysis/deepfakes-ai-cyber-scam-south-east-asia-organized-crime/

[3] People Staff. (2023, July 26). Woman conned out of $15K after AI cloned her daughter's voice in terrifying scam: 'I broke down'. People. https://people.com/woman-conned-out-of-usd15k-after-ai-cloned-daughters-voice-terrifying-scam-11775622

[4] Page, C. (2024, May 23). Inside the deepfake threat that's reshaping corporate risk. TechRadarPro. https://www.techradar.com/pro/inside-the-deepfake-threat-thats-reshaping-corporate-risk

[5] Khandelwal, S. (2023, August 17). *AI-generated job scams are on the rise*. The Hacker News. https://thehackernews.com/2024/11/north-korean-hackers-steal-10m-with-ai.html

[6] Chaturvedi, A. (2023, July 18). Kerala man loses Rs 40,000 to AI-based deepfake scam: Here's what it is. NDTV. https://www.ndtv.com/india-news/kerala-man-loses-rs-40-000-to-ai-based-deepfake-scam-heres-what-it-is

[7] The Times of India. (2025, June). *Cybercrooks dupe 79-year-old Bengaluru woman of Rs 35 lakh in AI trading scam*. https://timesofindia.indiatimes.com/city/bengaluru/cybercrooks-dupe-79-year-old-bengaluru-woman-of-rs-35-lakh-in-ai-trading-scam/articleshow/122097772.cms

[8] Times of India. (2024, December 27). AI voice cloning scam: Railway DG's friend loses ₹2 lakh to cybercriminals. https://timesofindia.indiatimes.com/city/ranchi/ai-voice-cloning-scam-railway-dgs-friend-loses-rs-2-lakh-to-cybercriminals/articleshow/116661144.cms

DOI : 10.35291/2454-9150.2025.0130