IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 1, January 2025

DOI: 10.17148/IJARCCE.2025.14117

Cyber Victimization: A Study on Deepfake and Effects of Artificial Intelligence

Mohammed Marzuk.T.M[1], Vijayasarathy.R[1]

I Year Students, M.Sc. Forensic Science, Dr. M.G.R. Educational and Research Institute, Chennai, Tamil Nadu, India[1].

Abstract: For the welfare of society and many working sectors, people keep working on improving the scope and features of technology to make tasks easier. Many of these profound technology helps law enforcements and corporates to protect their data privacy but in contrast, those are also being used to steal sensitive data and do various kinds of cybercrime. Cybercrimes involves usage of both coding and software tools to find vulnerabilities to crack a system but with the creation and advancement of Artificial Intelligence, such tasks become so much easier. AI also paved the way to make new updates and features in the cyber space. Foundation of Artificial Intelligence was laid with research in fields of brain, computation and electrical networks which made scientists to work on creating a computer that is capable of thinking on its own[2]. Geoffrey Hinton, the godfather of AI himself has that use of AI should be tread carefully[14]. Social media acts as a medium of large amount of photographic, video and audio content. These data can be used to create, edit and morph images, videos and audios with minimal effort. Propagation of a websites that has AI features are being used to morph images of person to past it in a pornographic content. Deepart.io is one of the websites that got banned because it allowed creation of morphed pornographic content[1]. Regulations and restrictive guidelines on social media for posting images are weak in some popular applications like telegram and twitter. It allows such morphed pornographic content to propagate in cyber space easily. It's nearly impossible to find difference between a normal image and morphed image without use of technical softwares which is a primary cause for increasing victims of this cybercrime. Government organizations doesn't provide enough awareness on this topic among people either. The simply and proper way to provide awareness and avoid these crimes is within the creation of the problem itself, which is the use of Artificial Intelligence itself.

Keywords: Deepfake, Artificial Intelligence, Pornography, Cyber Laws, Cybercrime, Victimization, Morphing.

I) INTRODUCTION

Deepfakes can be an image, video or audio file that has been morphed realistically and superimposed with an image of another real person or non-existent person made with the help of artificial intelligence. As the algorithm has "learned" the face's features from various angles, and how it moves in different expressions, it able to replicate it in a way that follows the expressions. The research for deepfake was initially started for academical purposes in the 1990s and it was simple to find which of them was real content and which was morphed. But with the advancement in areas of study like neural networks and generative adversarial networks (GANs), it became a nightmare to distinguish between normal and morphed images[2]. In 2017, November 2nd, a reddit user created a reddit page with the name "Deepfake" which was the first time this term was ever used. The user and members of the reddit page used an open-source face swapping algorithm to morph images of celebrities and popular actresses in pornographic content[7]. Even though that community was banned for violation of guidelines by reddit in February 2018, about 90000 subscribers already downloaded the algorithm to create deep fakes and started spreading it[3]. Primary use of Deepfake was applied in field of art and acting, many companies started using deepfake for advertisements, movie scenes, voice manipulation. Digital clones of actors can be created and used even without them in time of need with the help of deepfake technology. Deepfake was used for de-aging character of actor Vijay in an Indian Tamil film "The Greatest of All Time" which was portrayed by Ayaz Khan[4]. Even though, there is a great potential in the field of deepfake, the creation and spread of pornographic deepfake hyped eventually. A Desktop application named "Fakeapp" was launched which allowed its users to edit images into pornographic content without need of any prior knowledge in coding or editing works[1]. The year 2019 became a year that dedicated itself to launch of many other applications like command line- based application Deepfacelab, open sourced Faceswap, Web based Deepfakesweb. A Japanese Artificial Intelligence Company, DataGrid launched an application that can create a person with deepfake from scratch[11]. World's first visual threat intelligence company, Sensity.AI evaluated the spread of deepfake in 2019 and concluded that it has 100% increase or more in successive years with about 52,000 deepfakes online in the year 2020[15] . In the year, 2020, came the advancement of deepfake in audio morphing which made creation of hyper-realistic audio and video content with as low as 5 seconds of clear audio as an input file[1]. In the same year, "Impressions", an application specifically made for mobile user was released which made propagation of pornographic deepfake to be increased drastically. Deepfakes are being used as a tool to manipulate and influence the thoughts of people in various matters like war, politics, entertainment industry and more. Sensity.AI made a report in 2024

DOI: 10.17148/IJARCCE.2025.14117

which revealed that some of the middle east countries like Saudi Arabia, Iran and so on, south east countries like Thailand, Malayasia and so on, and south Asian countries like India, Sri Lanka and so on[15]. The Anonymity, which cyber space provides makes people use it as a place to show their dark and intrusive thoughts which can't be shown in reality. Both excitement and a psychological high that comes from making pornographic contents of famous celebrities and actors paves a way for them to satisfy their wildest fantasies. Watching these morphed content offers them a sense of escape from reality to satisfy their need of accomplishment of achieving something which they couldn't do in real life. The more realistic the deepfake is, the more it satisfies the wildest dreams and fantasies of people which makes them create and share it in cyber space. The creation and distribution of deepfake increased the number of fake content and news in a wide scale, which made academics and scientists to work on way to counter it and to spread awareness regarding its risks among people. Microsoft started working on its very own Deepfake Detection tool in 2020[1]. Many websites and organizations started to work on creating and improving existing algorithms for deepfake detection. There are several extensions like Deepfakeproof, Google Deepfake detection, Deep Fake detector and Hiya Deepfake Voice Detector that can be added in web browser that can be used to detect deepfake content in websites, detect deepfake videos and audios in youtube[12]. Surf Security has Launched the beta version of its World's First AI Deepfake Detecting Browser for police, military and media organizations worldwide to detect deepfake with about 98% accuracy in real time while browsing[16]. It is said to be releases in the year 2025. Even though there are many free websites, the accuracy level of most of those websites is low and can't be detected in real time which requires high level proper algorithms in industrial quality. Government Actions are necessary to make such industry level detection software to be made public for people use and to provide awareness in these field of deepfakes, its risk and detection method.

II) MATERIALS

- Google form
- Cover letter
- Samples from the age 18 to 26
- Pie Charts were taken from Google form

III) METHODOLOGY

A. *SAMPLE*

Samples were taken from 150 respondents of age group between 18 – 26. All of the samples were taken from the Srinivasan College of Arts and Science, Perambalur, Tamil Nadu, India. The Pie chart data was taken from the Google form itself. The data was collected during the months of October to November.

B. *PRIMARY DATA*

A Questionnaire form was made to query about content associated with this topic and circulated to collect data among people.

The questions present in the questionnaire includes:

1. Have you come across of the term "deep fake" before?
2. Have you ever witnessed a deep fake content on social media?
3. How worried are you about the potential misuse of deep fake technology?
4. In your opinion, do deep fakes pose a threat to political elections and public figures?
5. Do you believe there should be stricter regulations on the creation and distribution of deep fake content?
6. In your opinion, how deep fake technology can be effectually combated or detected?
7. Would you stand by the use of AI-based tools to identify and mark out deep fake content?
8. In your opinion, do deep fakes have the possibilities to undermine trust in media and journalism?

DOI: 10.17148/IJARCCE.2025.14117

9. Do you verify the authenticity of the content you consume online regularly?

10. In your opinion, do spreading creating and spreading deepfakes is sexual offense?

11. Would you consider taking measures to educate yourself and others about the risks correlated with deep fakes?

12. Are you familiar with the procedures to be followed if you are subjected with deepfake?

13. Do you believe the government should initiate free websites to aid deepfake victims?

C. *SECONDARY DATA*

Secondary data was collected using Google Form (Digital media).

IV) RESULTS AND DISCUSSION

1. Have you come across of the term "deep fake" before?

Among the respondents of 150 who participated in our questionnaire, 26.7% have never even heard the term “DEEPFAKE” before.

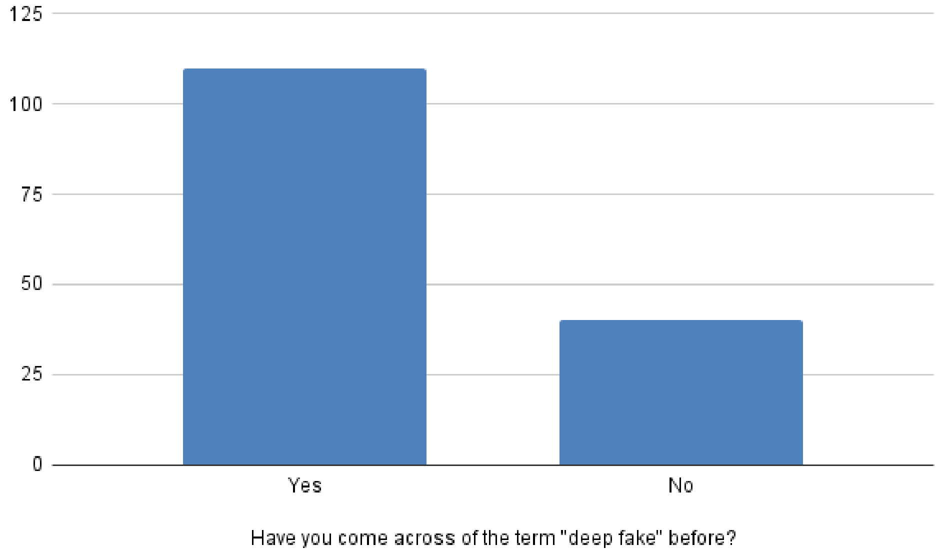

Fig I: come across of the term "deep fake"

DOI: 10.17148/IJARCCE.2025.14117

2. Have you ever witnessed a deep fake content on social media?
42% of the respondents has said that they have never seen a deepfake content.

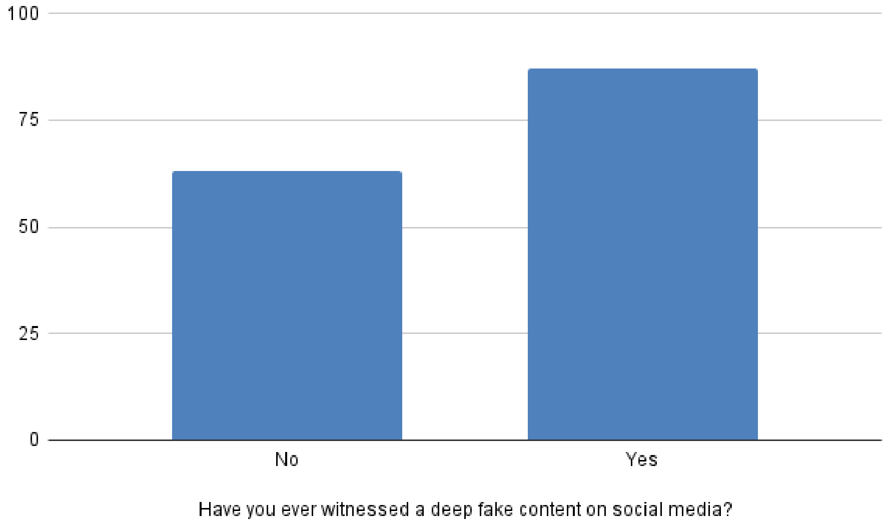

Fig II: witnessed a deep fake content on social media

3. How worried are you about the potential misuse of deep fake technology?

56.7% of the respondents are said to be deeply considered that deepfake could be misused.

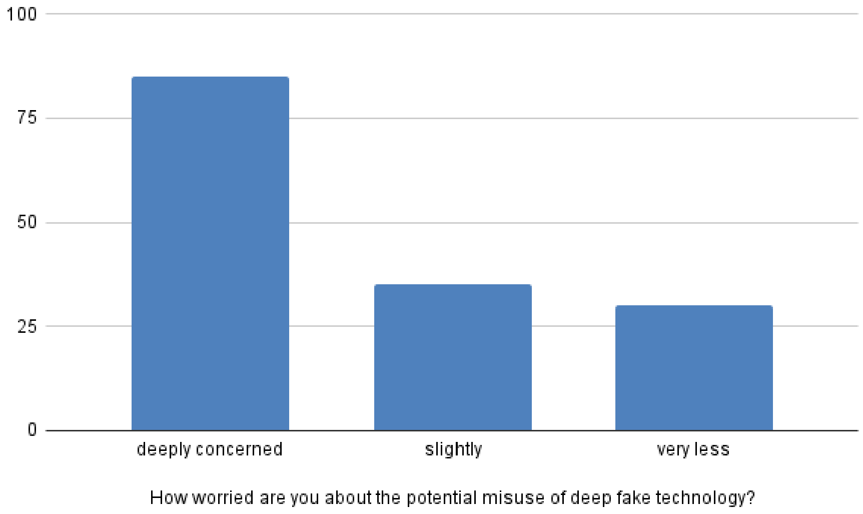

Fig III: worried about the potential misuse of deep fake technology

DOI: 10.17148/IJARCCE.2025.14117

4. In your opinion, do deep fakes pose a threat to political elections and public figures?
Among the respondents, 48% of them thinks that deepfake content has the ability to influence elections and pose as a threat

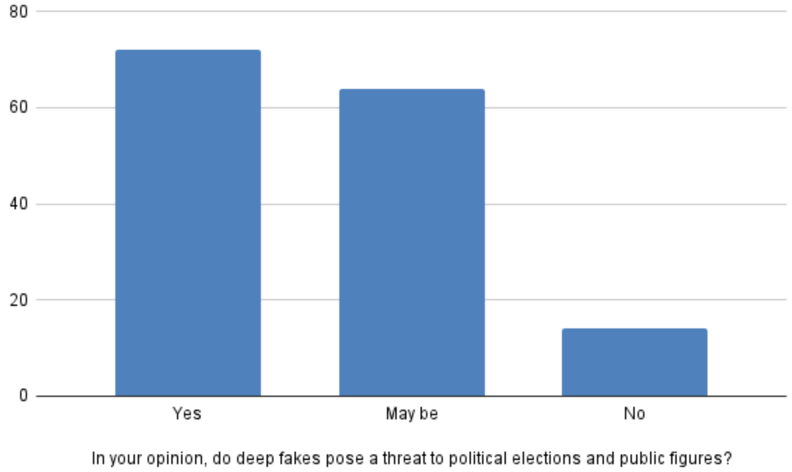

Fig IV: deep fakes pose a threat to political elections and public figures

5. Do you believe there should be stricter regulations on the creation and distribution of deep fake content?
76% of the respondents believes that there should be strict regulations on the creation and sharing of a deepfake content

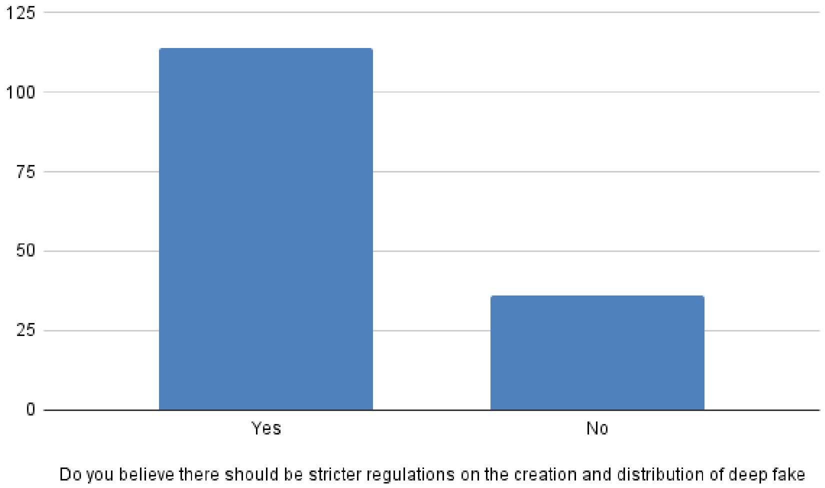

Fig V: stricter regulations on the creation and distribution of deep fake content

DOI: 10.17148/IJARCCE.2025.14117

6. In your opinion, how deep fake technology can be effectually combated or detected?
Among the respondents, 56% of them thinks deepfake can be easily countered if the social media is to make guidelines that can restrict illicit deepfakes and 33.3% of the population says that it's government's responsibility to spread awareness among the people regarding such problems.

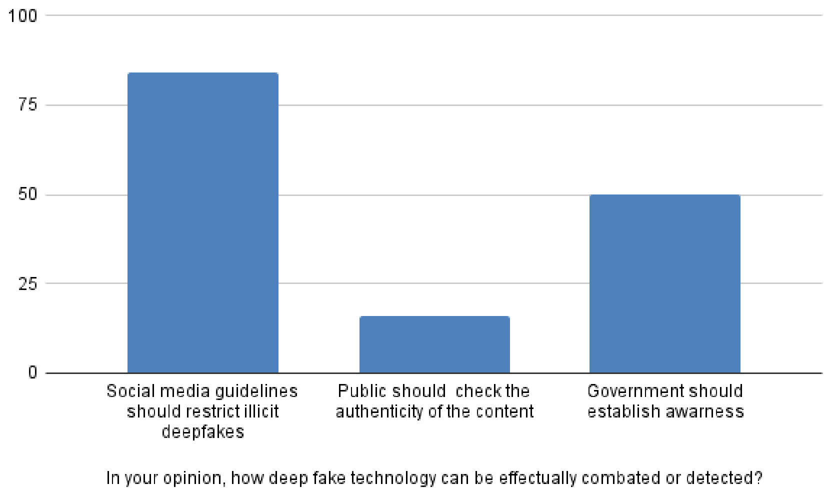

Fig VI: how deep fake technology can be effectually combated

7. Would you stand by the use of AI-based tools to identify and mark out deep fake content?
68% of the respondents are ready to support use of Artificial Intelligence to detect deepfake.

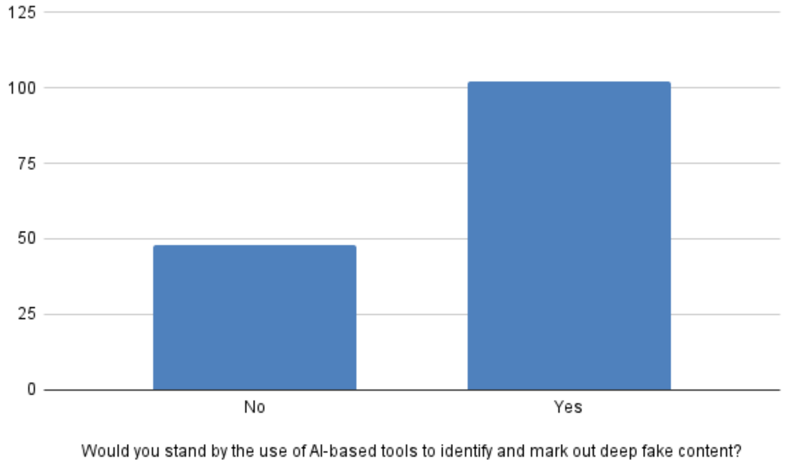

Fig VII: use of AI-based tools to identify and mark out deep fake

DOI: 10.17148/IJARCCE.2025.14117

8. In your opinion, do deep fakes have the possibilities to undermine trust in media and journalism?
47.3% of our study’s respondents thinks that deepfake can undermine the trust of media and journalism due to spreading of fake news.

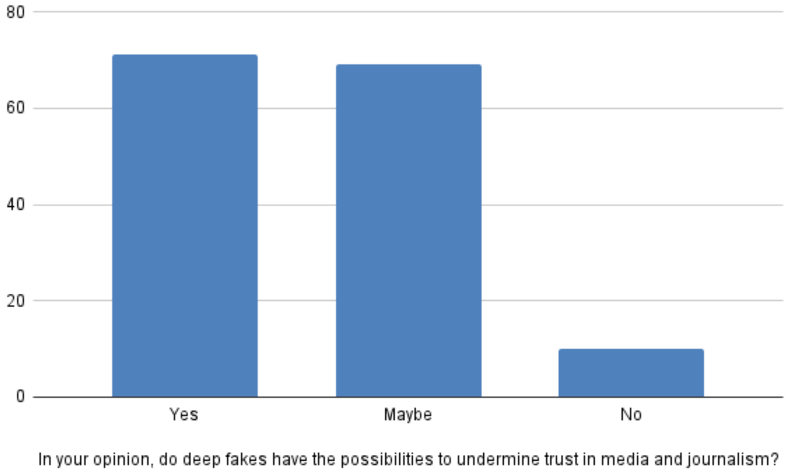

Fig VIII: possibilities to undermine trust in media and journalism

9. Do you verify the authenticity of the content you consume online regularly?
About 28% of the respondents doesn’t usually verify the online content they consume.

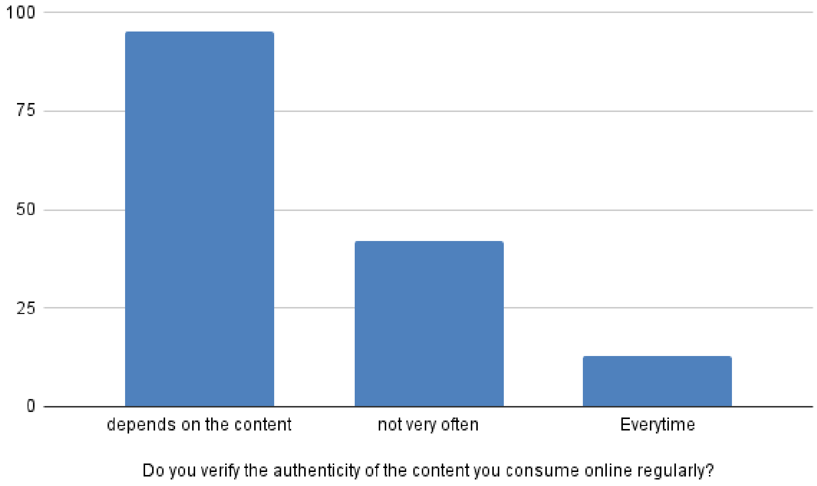

Fig IX: verify the authenticity of the content

DOI: 10.17148/IJARCCE.2025.14117

10. In your opinion, do spreading creating and spreading deepfakes is sexual offense?

About 56% of our respondents considers deepfake as a sexual offence.

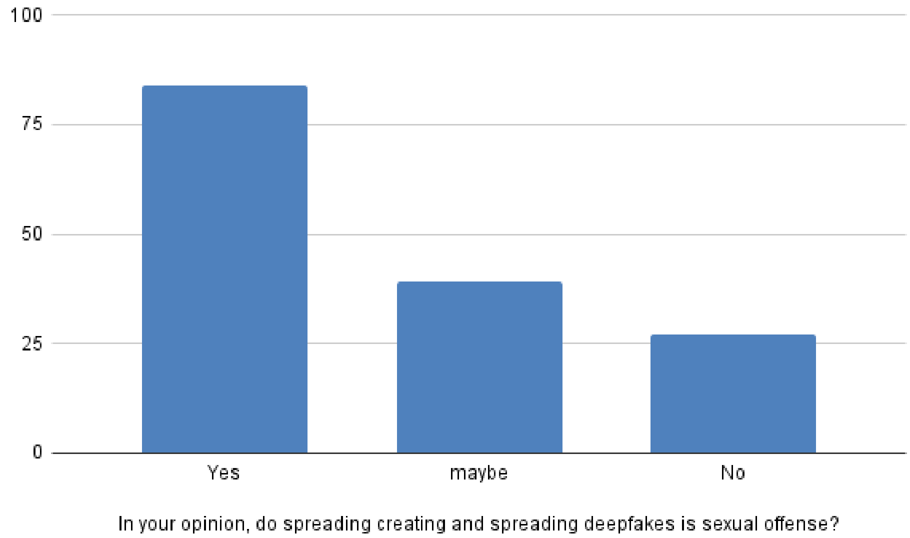

Fig X: spreading deepfakes is sexual offense

11. Would you consider taking measures to educate yourself and others about the risks correlated with deep fakes?

88.7% of the respondents are willing to learn and teach others regarding ill effects of deepfakes.

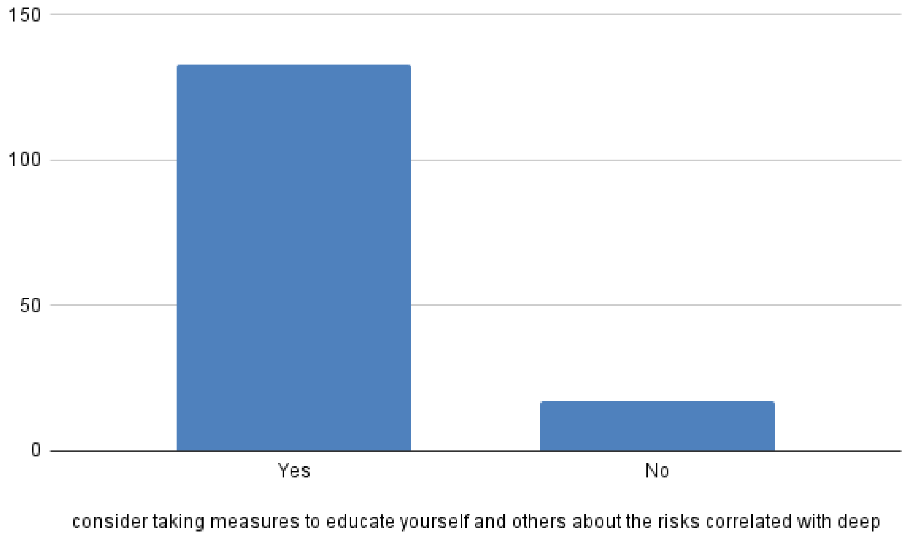

Fig XI: taking measures to educate yourself and others

DOI: 10.17148/IJARCCE.2025.14117

12. Are you familiar with the procedures to be followed if you are subjected with deepfake?
Among the respondents, 58% of them doesn't the procedures that are necessary to be followed if they are to become a victim.

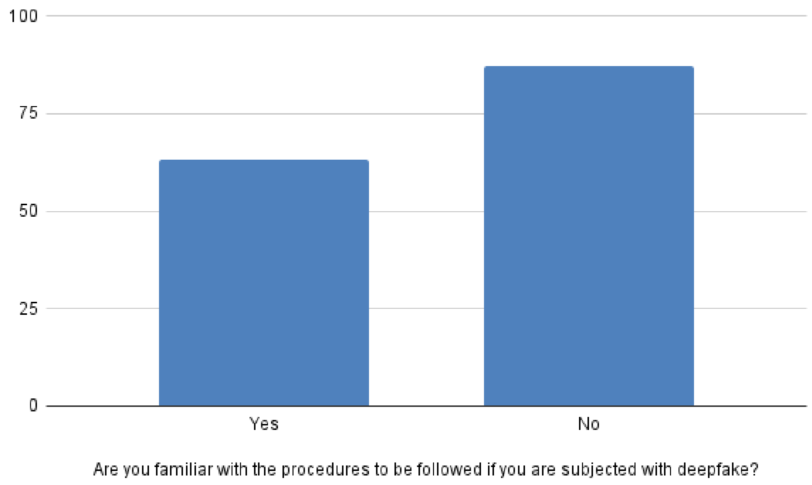

Fig XII: procedures to be followed if you are subjected with deepfake

13. Do you believe the government should initiate free websites to aid deepfake victims?

No matter how many solutions we try to muster up by ourselves, Government's help is necessary so 90.7% of the respondents says that government should come up with free websites to help deepfake victims.

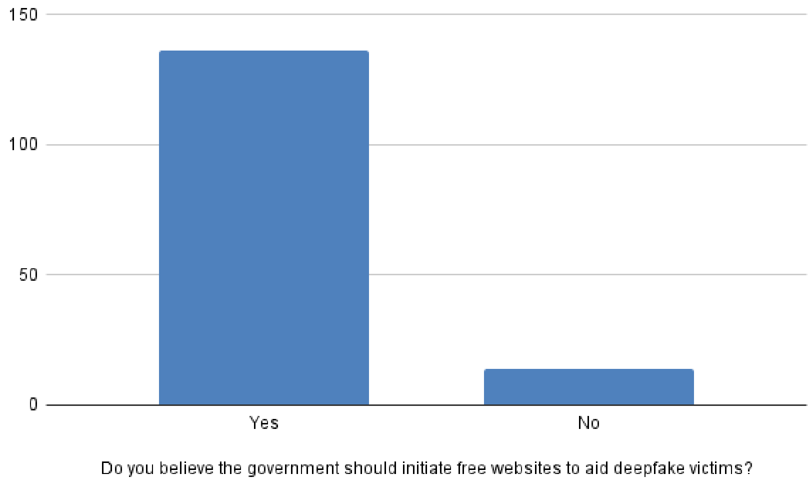

Fig XII: the government should initiate free websites to aid deepfake victim

V) CONCLUSION

Despite having a various benefit, deepfake is extensively used for malicious purpose. Advancement in opensource AI tools and bots, creating deepfakes became easier and it evolved as a threat to the society where social media is widely used providing bunch of input for creation without consent. Still prevention taken from government regarding the issues is very less despite the increase in deepfakes since late 2017. Lack of awareness about deepfakes among public facilitate the ease of spreading fake news and content using AI. A proper education regarding the contemporary crime and ways to counter to it in day-to-day usage would be helpful.

DOI: 10.17148/IJARCCE.2025.14117

As we discussed earlier the major cause for the development of deep fakes is AI but ironically with constructive use of the same AI we can prevent, identify and detect deepfake content. There are number of tools which can be used for the purpose using which we can verify the integrity of the content we consume.

A. *Ways counter deepfakes*

1. By looking for the minute facial reaction alterations such as lip sync error, facial type and hair mismatch, lack of face and neck alignment, influence of AI can be confirmed.
2. Government could launch opensource website focused on the deepfake crime for detection of AI (with advanced features) in a content and interface to register complaint regarding such crime.
3. Metadata tagging can be introduced, using which similar to normal metadata (MAC address) influence of AI in a content can also be tagged, so sharing of such content from the original source will always indicate the influence of AI in the content.
4. Different opensource websites like Faceforensic++ are available which can be used to check the integrity of the content.

REFERENCES

[1]. Finger, L. (2022, September 8). Overview of how to create deepfakes - it's scarily simple. Forbes. https://www.forbes.com

[2]. Mahmud, B. U., & Sharmin, A. (2021). Deep insights of deepfake technology: A review. *arXiv preprint arXiv:2105.00192*.

[3]. Chadha, A., Kumar, V., Kashyap, S., & Gupta, M. (2021). Deepfake: an overview. In *Proceedings of Second International Conference on Computing, Communications, and Cyber-Security: IC4S 2020* (pp. 557-566). Springer Singapore.

[4]. Wikipedia contributors. (2024, November 22). *Deepfake*. Wikipedia. https://en.wikipedia.org

[5]. Fido, D., Rao, J., & Harper, C. A. (2022). Celebrity status, sex, and variation in psychopathy predicts judgements of and proclivity to generate and distribute deepfake pornography. Computers in Human Behavior, 129, 107141.

[6]. Gosse, C., & Burkell, J. (2020). Politics and porn: how news media characterizes problems presented by deepfakes. *Critical Studies in Media Communication*, *37*(5), 497–511.

[7]. Ajder, H., Cavalli, F., Patrini, G., & Cullen, L. (2019). The State of Deepfakes: Landscape, Threats, and Impact. Deeptracelabs.

[8]. Hancock, J. T., & Bailenson, J. N. (2021). The social impact of deepfakes. Cyberpsychology, behavior, and social networking, 24(3), 149-152.

[9]. Karasavva, V., & Noorbhai, A. (2021). The real threat of deepfake pornography: A review of Canadian policy. *Cyberpsychology, Behavior, and Social Networking*, *24*(3), 203–209.

[10]. Jha, P., & Jain, S. (2021). Detecting and Regulating Deepfakes in India: A Legal and Technological Conundrum. *Available at SSRN 4411227*.

[11]. Kalmykov, M. (2023, November 28). Deepfake technology in video industry. (n.d.). https://www.dataart.com

[12]. Robuck, M. (2024, October 18). *Hiya launches Chrome tool to detect deepfake AI audio*. Mobile World Live. https://www.mobileworldlive.comKatarya, R., & Lal, A. (2020, October). A study on combating emerging threat of deepfake weaponization. In 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC) (pp. 485-490). IEEE.

[13]. Pelley, S. (2024, June 16). *Geoffrey Hinton on the promise, risks of artificial intelligence | 60 Minutes*. CBS News. https://www.cbsnews.com

[14]. Team, S. (2024b, October 21). *Sensity AI: Best All-In-One Deepfake Detection Software 2024*. Sensity. https://sensity.ai/

[15]. *SURF SECURITY LAUNCHES WORLD'S FIRST AI DEEPFAKE DETECTING BROWSER*. (2024, November 20). KRON4. https://www.kron4.com