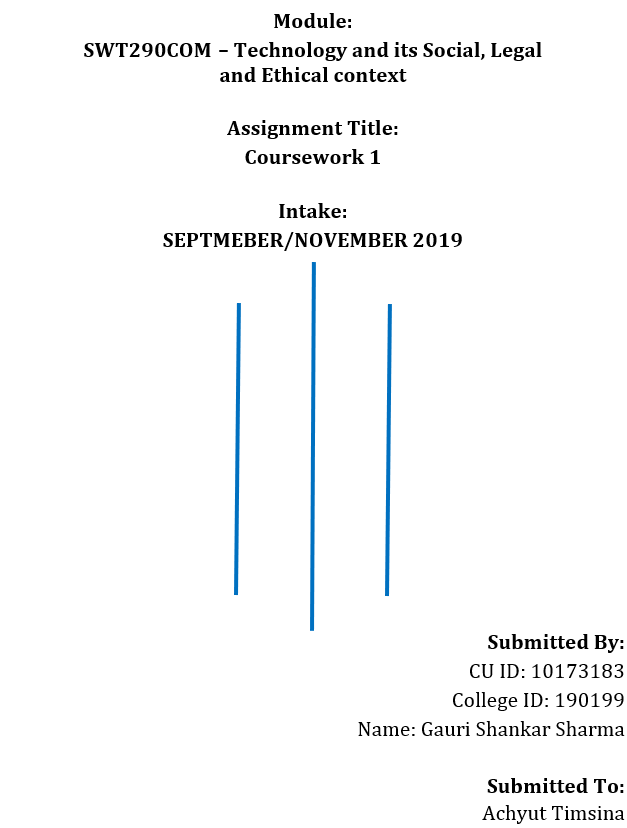
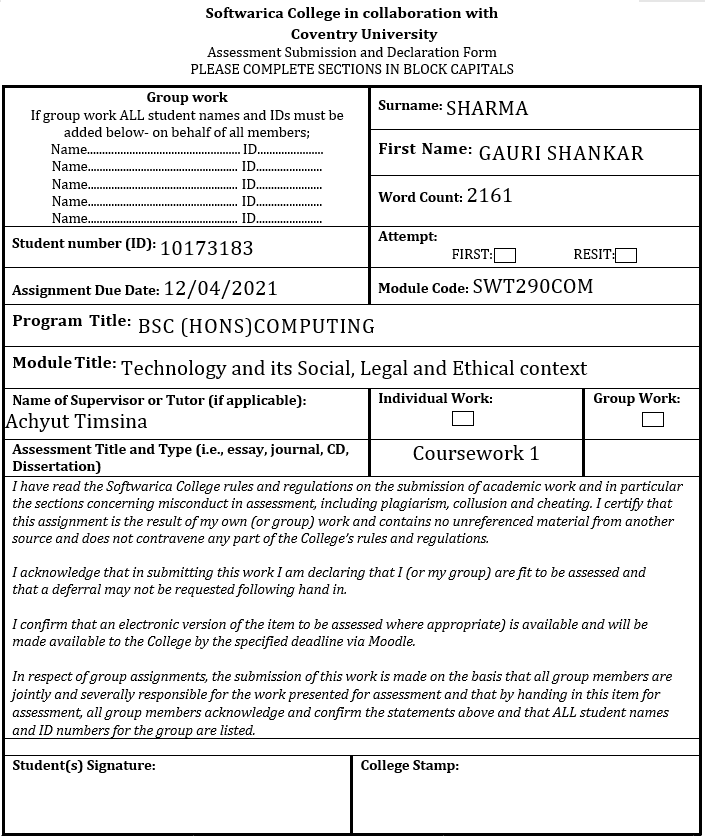
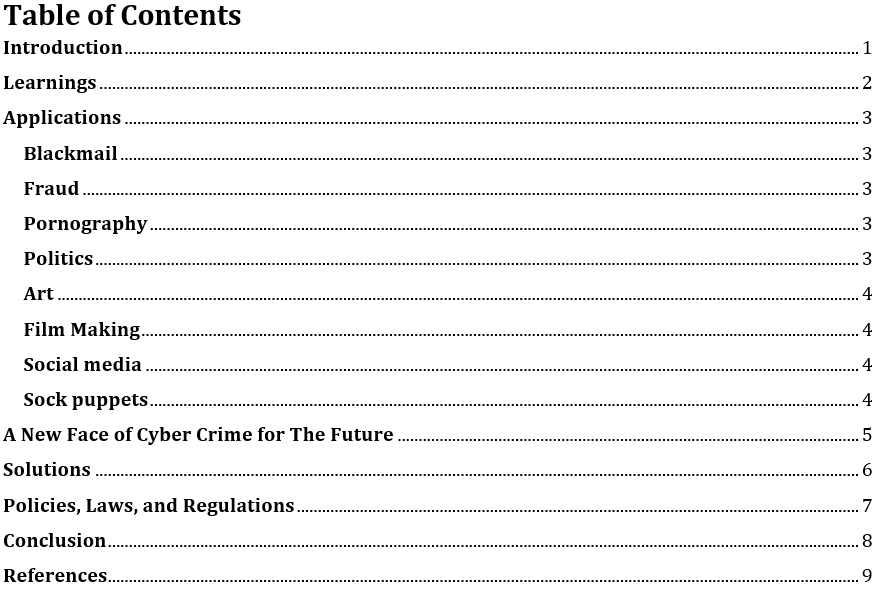
****

****

# **Abstract**

Deepfake is the main concern of this report. This report includes both positive and malicious use of deepfake and its impact, solutions for it, ethical implications for the future, laws, and policies related to it, and global awareness. It is used in video artworks, film industries to improve cinema content, to revive the dead ones, also to fraud people, generate porn of female celebrities, misrepresent politicians, blackmail people. It can be a new face of cybercrime in the future. Deepfake detecting technology should be developed and deepfake content should be removed from the social platform. People should be educated about deepfake. It lacks good laws and policies. Perfect laws and policies should be made and implemented.

****

# **Introduction**

This report gives a brief overview of the legal and ethical policies, current issues and solutions, current laws, and laws for the future related to Deep Fake. It is a newly immerged technology and it has a wide range of use and impact. It is a deep machine learning technology used by AI which enables to switch the likeness of a person in an existing image or video by someone else. It is mainly used to provide fake information in which the main content of the original image or video is altered by self-created false content. It all started from the beginning of the 1990s by researchers but the term “Deep Fake” started from a Reddit user at the end of 2017 (Cole, 2018). It is being used as a weapon against high-profile politicians, celebrities which can lead the current world to the wrong path and the rate of deep faking is increasing.



Figure 1: Deepfake Example (Wikipedia, 2021).

# **Learnings**

There is always a limitation on the use of computer technology since its invention and creation because computer technology can be used not only to achieve desired output without affecting or damaging others but also as a tool to do crimes or to damage, and affect others. Therefore, there are many rules and regulations, laws and policies on the use of computer technology and every single person needs to be aware of those laws and policies and have to use the available technology by staying within a certain boundary in the context of today’s computer world otherwise people could be trapped in very serious problems even if the intension is not to do crimes or to harm others.

Through this course, I knew about computer ethics, and laws like Privacy and Data Protection, Freedom of expression, Freedom of information, Intellectual Property, Computer Cybercrimes, and Digital Investigation. The data and information that a person shares with the internet should be private and in his control. It is unethical to access other’s private data and illegal to alter or damage them. Everyone has the right to protect their data and information. It’s unethical and illegal to share or support information that provides false information or damages the reputation of an organization or a person. It’s legal to get personal and economic benefit by sharing our ideas and self-created content on the internet but it will be illegal if the ideas or the content is stolen from others. People should always read the terms and conditions, policies before agreeing with online content or with mobile and computer applications. People should use technology only if they have full trust in it. All the technology that is available in today’s context is not trustable, people should trust only those technologies that are secure, protected, and authorized. People always should be aware of the new upcoming technology to stay updated and to get rid of being a victim of some kind of crime.

# **Applications**

## **Blackmail**

It can be used to blackmail people with the help of blackmail material produced from it. For example, a porn video in which the face of the actor in the video is replaced by the face of the victim can be used to black the victim to gain personal and economic benefit. Or it can be used to incriminate the victim.

## **Fraud**

Deepfake have made it very easy to fool people. It can be used to scam people making think them that they are receiving commands from a trusted person. Image or Video or Audio deepfake can be used as a tool. The CEO of a UK-based energy firm was scammed by the AI-generated voice of the chief executive of the firm’s parent German company in 2019. He was ordered to transfer €220, 000 into a Hungarian bank account (Damiani, 2019).

## **Pornography**

Almost all of the deepfake videos on the internet are pornography of people. Female celebrities are often targeted in those videos without their consent. A report published by the Dutch cybersecurity in October 2019 says 96% of the deepfake videos are porn videos of British, American, South Korean, and other celebrities (Wikipedia, 2021). The first pornographic deepfake video uses the likeness of an English actress Daisy Ridley (Roettgers, 2018). Deepfake technology can damage anyone’s reputation with these kinds of pornographic videos.

A Windows and Linux downloadable application called “DeepNude” was launched in the June of 2019. This app used neural networks to remove the clothes from the image of a women’s body. It has both free and paid versions but later on 27 June, it was removed and refunded to the consumers (deepnudeaap, 2019).

## **Politics**

The deepfake videos are used to misrepresent well-known politicians. This can damage the politician’s reputation and career in the political field. Deepfake videos are mostly famous for politician’s fake videos than porn videos. Politicians can use deepfake videos of the opponent to make the opponent down during election time. This could arise a very serious problem. A deepfake video of [Barack Obama](https://en.wikipedia.org/wiki/Barack_Obama) with Peele's voice was generated in April 2018 (Romano, 2018). It was produced by Buzzfeed by collaborating with Jordan Peele. It was used as a [public service](https://en.wikipedia.org/wiki/Public_service_announcement) to make awareness of the increase of deepfakes. Deepfakes of other politicians like Donald Trump, Mauricio Macri, Vladimir Putin are also available on the internet.

Deepfake has also positively helped the Politicians. The Delhi Bharatiya Janata Party used deepfake to distribute an English-language campaign advertisement of its leader. From it, they approach the target audience even if it did not speak the language of the voters (Christopher, 2020).

## **Art**

Deepfake can be used to create AI-generated actors, swap faces and bodies in video artworks. An artist named Joseph Ayerle published a video artwork “The Italian Game” in March 2018. The video artwork used deepfake technology to create an AI actress in which the actress has Al calculated face of movie star Ornella Multi and the body of Model Kendall Jenner traveling in time from 1978 to 2018 to explore generational reflections (Katerina Cizek, 2019).

## **Film Making**

Digitally altered or constructed actors have been already used in films before. Deepfake can contribute to new developments in film industries and it has. In Solo: A Star Wars Story movie, deepfake is used to insert the young face of Harrison Ford onto Han Solo’s face and similarly, deepfakes were used in Rogue One for the acting of Princess Leia (Radulovic, 2018) (Winick, 20198).

It can revive dead characters and actors with a simple and quick face swap for the fans to enjoy. Disney improved their visual effects with the help of high-resolution deepfake swapping technology. This helped to generate AI media at a 1024 x 1024 resolution which is better than the previous resolution of 256 x 256 (Naruniec, 2020).

## **Social media**

Deepfake is being famous in the social media mostly because of the apps which use deepfake technology and becomes available in social platform. The Internet meme also started utilizing deepfake technology.

## **Sock puppets**

Deepfake can be used to generate non-existent people or to create suck puppets who are active in both traditional and online media. This can help terrorism or do crimes by hiding personal details and information. Oliver Tayler is a non-existent person who was described as a student of a university in the UK but the person was involved in attacking a British legal academic and his wife (Satter, 2020).

# **A New Face of Cyber Crime for The Future**

Deepfake has an enormous number of ethical implications because it lacks rules and regulations, laws and policies and it can be misused by anyone, anytime, anywhere targeting anything or anyone. Even though it can be used positively for positive purposes, it is mostly being weaponized for malicious purposes. It can fool, mislead and generate debate among people or even can turn people from positive to negative side by providing false information which is very hard to distinguish from the original one. As a result, it can damage individuals, society, democracy, businesses, and even can make an untrusted truth fake news. It can break the connection of trust among people in the coming days because of these types of repeating false deepfake content.

What if a video of a politician is released a few days before the election showing the politician using hate speech, talking false information about others that undercut their image? It can make the politician lose the election or even can destroy the political career. What if a porn video of a female celebrity is released on social media? It will completely harm her reputation, break her relationship, destroy her high-profile celebrity career. What if a fake video of the CEO of a company is released talking about their project plan and details? This can make an economic loss to the company. What if a terrorist organization produces a video of a targeted country’s soldier dishonoring a religious place or a political activist calling for violence or shouting anti-religious slurs? This can create a big war and generate conflict between different countries (Jaiman, 2020).

# **Solutions**

Deepfake is an open-source technology and it has no limit and control on its use. To solve the problems created by deepfake, first of all, the video should be distinguished as a fake video. For this, a similar type of AI technology that was used to make it should be used to detect fake videos. Even if the video is detected as a fake, what then? Therefore, there is another solution for it which is improving media literacy. Online social platforms have policies for malicious synthetic media and disinformation. These platforms should filter the fake content by limiting sharing or removing the false informative content from their network. This will stop the spreading of fake content. Educating people about deepfake and making them aware of it also will be a better way of reducing the impact created by the deepfake contents. People will not trust any new type of false and confusion-creating video available on the internet. The misuse of deepfake technology can be reduced by making powerful laws, rules, and regulations. For example, deepfake technology should be developed and implemented under the control and vision of the government. Deepfake content creators should be punished as badly as its impact. Deepfake technology should be only used by professionals and authorized ones.

# **Policies, Laws, and Regulations**

Deepfake lacks good policies, laws, and regulations that can prevent it from being weaponized for malicious purposes. Even the developed countries like America, United Kingdom, Russia, etc. are suffering from deepfake content. In the context of Nepal, deepfake has not been weaponized yet. Some edited pictures or videos of politicians can be found on the internet but that did not use deepfake technology. Therefore, there is no specific law made for deepfake in Nepal. Anyhow if there exists a deepfake content that creates problems, The Cybercrime Act, xx (2018) can prevent the creating and spreading of deepfake content. This is the current legal framework on electronic evidence and cybercrime in Nepal through its Banking Offence and Punishment Act 2064 and Electronic Transactions Act, 2063. Illegal Devices (s10), Electronic Fraud (s12), Pornography (s14), Identity-Related Crime (s15) are the laws specified in The Cybercrime Act which can help the victim of deepfake content (Government, 2021).

The National Defense Authorization Act was the first bill that became law and provided sections relating to deepfakes. This was signed by President Trump on December 20, 2019, for the Fiscal Year 2020 (NDAA) (Hale, 2019).

# **Conclusion**

Deepfake has made it easy to falsify media, frequently without letting know about it. It has caused psychological harm, disruption in business, and instability in politics. Deepfake weaponization provides an enormous impact on personal freedom, national security, and the economy. But deepfake has been also used positively and some of them are explained above. Still, its malicious uses are more and increasing. Therefore, the world should be notified and made aware of deepfake and its impact that the future can face. Perfect laws, policies, rules, and regulations regarding deepfake should be made and strictly implemented all around the world. Deepfake technology creators should be under the vision of the government. Deepfake content should be detected and removed from social media platforms. Deepfake should be used for help and support not for weaponization that can cause serious problems in the incoming days.

# **References**

Christopher, N., 2020. *Vice.com.* [Online]   
Available at: https://www.vice.com/en/article/jgedjb/the-first-use-of-deepfakes-in-indian-election-by-bjp  
[Accessed 1 April 2021].

Cole, S., 2018. *Vice.com.* [Online]   
Available at: https://www.vice.com/en/article/bjye8a/reddit-fake-porn-app-daisy-ridley  
[Accessed 13 March 2020].

Damiani, J., 2019. *Forbes.* [Online]   
Available at: https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/?sh=2d38aa9a2241  
[Accessed 1 April 2021].

deepnudeaap, 2019. *Twitter.* [Online]   
Available at: https://twitter.com/deepnudeapp/status/1144307316231200768  
[Accessed 1 April 2021].

Government, N., 2021. *Octopus Cybercrime Community.* [Online]   
Available at: https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset\_publisher/CmDb7M4RGb4Z/content/nepal/pop\_up?\_101\_INSTANCE\_CmDb7M4RGb4Z\_viewMode=print&\_101\_INSTANCE\_CmDb7M4RGb4Z\_languageId=en\_GB#:~:text=State%20of%20cybercrime%20legislation&text=The%20current%2  
[Accessed 5 April 2021].

Hale, W., 2019. *JD Supra.* [Online]   
Available at: https://www.jdsupra.com/legalnews/first-federal-legislation-on-deepfakes-42346/  
[Accessed 5 April 2021].

Jaiman, A., 2020. *ORF.* [Online]   
Available at: https://www.orfonline.org/expert-speak/debating-the-ethics-of-deepfakes/  
[Accessed 5 April 2021].

Katerina Cizek, W. U. a. S. W., 2019. *Works In Progress.* [Online]   
Available at: https://wip.mitpress.mit.edu/pub/collective-wisdom-part-6/release/1  
[Accessed 2 April 2021].

Naruniec, J., 2020. *Studios.disneyresearch.com.* [Online]   
Available at: https://studios.disneyresearch.com/2020/06/29/high-resolution-neural-face-swapping-for-visual-effects/  
[Accessed 2 April 2021].

Radulovic, P., 2018. *Polygon.* [Online]   
Available at: https://www.polygon.com/2018/10/17/17989214/harrison-ford-solo-movie-deepfake-technology  
[Accessed 2 April 2021].

Roettgers, J., 2018. *Variety.com.* [Online]   
Available at: https://variety.com/2018/digital/news/deepfakes-porn-adult-industry-1202705749/  
[Accessed 1 April 2021].

Romano, A., 2018. *Vox.* [Online]   
Available at: https://www.vox.com/2018/4/18/17252410/jordan-peele-obama-deepfake-buzzfeed  
[Accessed 1 April 2021].

Satter, R., 2020. *U.S.* [Online]   
Available at: https://www.reuters.com/article/us-cyber-deepfake-activist-idUSKCN24G15E  
[Accessed 2 April 2021].

Wikipedia, 2021. *Wikipedia.* [Online]   
Available at: https://en.wikipedia.org/wiki/Deepfake  
[Accessed 1 April 2021].

Winick, E., 20198. *MIT Technology Review.* [Online]   
Available at: https://www.technologyreview.com/2018/10/16/139739/how-acting-as-carrie-fishers-puppet-made-a-career-for-rogue-ones-princess-leia/  
[Accessed 2 April 2021].