

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/368838115>

Are ChatGPT and Deepfake Algorithms Endangering the Cybersecurity Industry? A Review

Article · February 2023

DOI: 10.31873/IJEAS.10.1.01

CITATIONS

5

READS

1,961

2 authors:



Bibhu Dash

University of the Cumberlands

43 PUBLICATIONS 643 CITATIONS

[SEE PROFILE](#)



Pawankumar Sharma

University of the Cumberlands

31 PUBLICATIONS 489 CITATIONS

[SEE PROFILE](#)

Some of the authors of this publication are also working on these related projects:



Digital Sustainability [View project](#)



Digital Sustainability [View project](#)

Are ChatGPT and Deepfake Algorithms Endangering the Cybersecurity Industry? A Review

Bibhu Dash, Pawankumar Sharma

Abstract—In this era of digitization, cybersecurity is a significant concern globally. Deepfake algorithms and the evolution of Massive Language Models (MLMs) like ChatGPT are used by hackers to create codeless fake contents to spread cyber threats. Deepfake algorithms constitute the widely utilized technology in videos and images alongside the movie industry through natural language processing. The technology utilizes machine learning to manipulate authentic images and videos using neural networks, which jeopardizes the ability to differentiate between real and fake images. Generative adversarial networks (GAN) form the model algorithms developing deep counterfeit images. The algorithm has a generator and discriminator necessary for creating the various images. The technology threatens cybersecurity as various cybercriminals can commit crimes exemplified by vishing and business email compromise, which is very hard to detect. The different neural network supports the development of deepfake algorithms using machine learning, and this paper describes this in detail, considering both social and technical prospects.

Index Terms—Deepfake algorithms, Natural language processing (NLP), Deep Learning (DL), generators, Generative adversarial networks (GAN), neural networks, ChatGPT.

I. INTRODUCTION

With technology innovation, the world is fighting to manage undesirable usages of the same technology that pose a significant risk to our social and ethical values. The world has witnessed a vast technological advancement alongside the rising cases of cyber fraud and image forgery, especially within the internet community and social media platforms. Sometimes technology works against itself, generating chaos in the environment and functioning as a motivator for both individual and corporate crimes. For instance, powerful algorithms like deep learning, which is cultivated inside numerous social media services like Snapchat, Instagram, and Reddit, mark the tactics employed in particular image features before transposing them to create another image. The theory explains how deepfake technology creates the original image that is being replicated by combining several algorithms with deep learning neural networks. The integrated deepfake algorithms of society are represented in many films and the virtual dressing room. Although deepfake algorithms have become a popular feature on social media sites, they pose a serious concern to

cybersecurity since they use neural networks to enable their operation.

Over the past, some applications have led to the creation of fake images using deep learning algorithms in artificial intelligence with a consequent adverse effect on society. For instance, the Reddit application swapped various women's images into pornographic videos resulting in controversy as the videos spread online. Deep learning utilizes image manipulation in creating fake through generative adversarial networks (GANs) and the variational auto-encoders. GAN generates face swapping within images and videos. The deepfake algorithms provide room for convolution image tracing as facilitated through forensic analysis, although it presents a challenge in tracing some of the convolutions, hence the challenge in cybersecurity. Detecting fake videos and images demands extensive deep-learning methods for detecting convolutional traces.

The deepfake has its architecture originating from deep learning algorithms. The technology in machine learning applies artificial intelligence in feeding the algorithm with intense data, images, and video. The actual convolution of the photos from the original occurs as facilitated by the neural network, which can detect errors and report them back through the analogous head and faces. One algorithm leads to the creation of the fake, with second and subsequent searches leading to the creation of the simulated images and videos commonly described as deep voices.

II. NEURAL NETWORK AND DL

The artificial neural network correlates to the normal function of the brain. The neural networks include multi-layer networks comprising a single input layer and one or various hidden layers alongside the output layers. The input to the neural network comprises the different input values with the ultimate aim of predicting and classifying the values into various categories. The neural networks form the basic architecture of deep fake technology [15]. The network facilitates machine learning through a “feed-forward” structure with interconnected nodes. As incorporated in deep learning, the computer learns the undertaking of a particular action through various training using artificial intelligence [16]. The computational model within face recognition has led to the generation of different “invariant representative” faces. The machine-learning algorithm helps mimic the human brain in recognizing faces and objects, indicating that the system and brain correlate. The capabilities of graphics processing units can power neural networks extensively, as shown in Fig 1.

Manuscript received January 16, 2023.

Bibhu Dash, School of Computer and Information Science, University of the Cumberlands, Williamsburg, KY USA, Phone: (800)343-1609.

Pawankumar Sharma, School of Computer and Information Science, University of the Cumberlands, Williamsburg, KY USA, Phone: (800)343-1609.

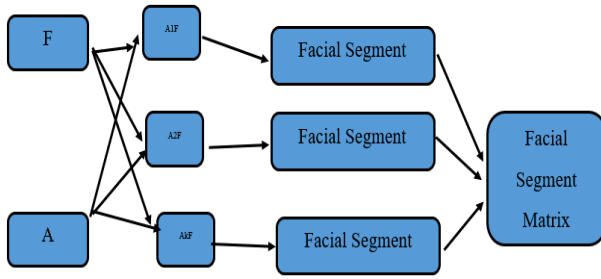


Fig 1. Facial segment matrix

Deep learning (DL) has the same algorithm and architectural design as neural networks. Deep learning utilizes the multiple layers within the network as the deep learning architecture utilizes the hidden layers within the defined sizes, culminating in the extensive information extraction facilitated by raw data input [15]. Deep learning comprises the various hidden layers depending on the training data complexity necessary for effective processing [1]. Deep learning forms a framework for audio processing, automatic translation, and natural language processing. Similarly to its architectural design, effective in keeping faking, it also provides a framework for deepfake detection. The convolutional neural network (CNN) utilizes the deep neural network model as it correlates to the neural network with input and output layers within hidden layers. The hidden layers account for the first reading within the CNN before applying the mathematical convolution computation on the input values [4]. The convolution includes the matrix multiplication before using the nonlinearity activation function with ultimate convolutions exemplified by the pooling layers [8]. The pooling layers reduce data dimensionality through output computation using the maximum pooling.

The recurrent neural network (RNN) constitutes the artificial neural network with the capability of deep learning from the sequence data. The neural network comprises various invisible layers, each possessing some weight and bias. The relation within the nodes occurs in a direct cycle graph with a sequential order [8]. RNN utilizes the internal memory for storing the sequence information from various inputs assuring the success in the natural language processing and speech recognition necessary for the deepfake algorithm [6]. The RNN can recognize the temporal sequence by introducing the recurrent hidden state essential for capturing the dependencies within various time scales.

III. NATURAL LANGUAGE PROCESSING

Natural language processing is critical in information transfer processing, facilitating deepfake technology. Open AI utilizes four aspects threatening cybersecurity as enabled by the algorithms. For instance, the distribution semantics include the machine learning of the text processing as some words have a close usage and relation to one another. The algorithm then uses the patterns in formulating new sentences and images and utilizes the autocomplete and predictive text system [8]. The automation features a cybersecurity threat, as machine learning can disguise the autocomplete and predictive mechanisms in filling the incorrect wording for the systems aimed at identifying the deepfaked images and texts. The frame semantics in the

deepfake technology entails the utilization of rules and labeled data in sentence deconstructions. The algorithms effectively parse the various simple commands, as demonstrated in the chatbots and voice assistants [13]. The algorithms threaten cybersecurity through text analysis and sentence structuring. This process breaks down into various actions, such as inquiry on what and when [9]. The algorithms understand the text they undergo machine learning from and can distinguish the information as applied in the deepfake by matching the various characters (see Fig 2). The theoretical model semantics includes the AI encoding human knowledge through various logical rules, helping extract information through various databases. Like frame semantics, the algorithms parse the sentences through deconstruction into the various parts of learning [7]. The machine learning using this algorithm threaten cybersecurity as it can answer various complex and nuanced inquiries, which could breach the various security passwords. However, the algorithm requires an extensive period in its formulation.

The grounded semantics includes the newest approach to holding various promises. Through natural language processing, the algorithm attempts to mimic the human language across their lifetime. Machine learning trains from a blank state the association of the various words with their correct interpretations and meanings as humans engage in conversations and interactions [11]. For instance, the moving of the various equipment using the computer will translate to the computer learning the matching of the equipment to the various destined areas through machine learning [14]. Consequently, machine learning would later lead to the movement of the blocks and equipment without requiring commands. Machine learning can understand the human language completely, although it demands extensive training [14]. The understanding of human language will thus threaten cybersecurity, as machine learning will be capable of executing the various crimes imitated by human behaviors.

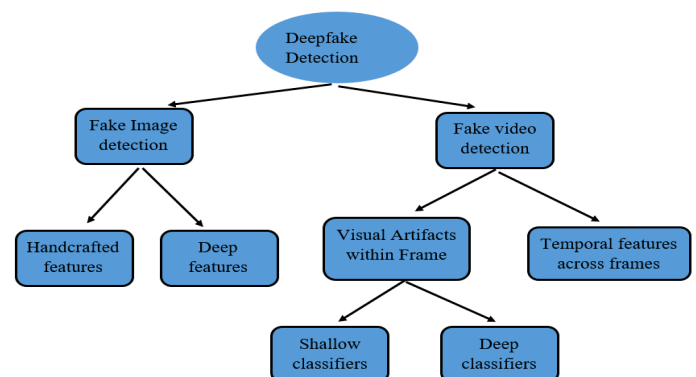


Fig 2. Deepfake categories. Source: [14]

IV. ALGORITHMS

Deepfake uses artificial intelligence (AI) alongside deep learning to deceive about the particular identity of the individual. The technology uses deep learning algorithms to learn the various concepts helpful in detecting and solving the various errors within large data sets, hence essential in swapping videos and images. The content creation utilizes two algorithms competing against each other; generator and

discriminator [12]. The generator tasks with the creation of fake digital content against requesting the discriminator to differentiate between the real and the artificial content. The discriminator identifies the content created as artificial or natural before presenting the information to the generator to generate more deep fake content [16]. The clubbing together of the algorithm constitutes the generative adversarial network (GAN). The algorithm trains itself to recognize patterns for learning the features required for the fake image production.

V. DEEPFAKE ARCHITECTURE GENERATION

The generative adversarial network (GAN) comprises the ultimate deep neural network for generating the deep fake. The GAN forms a framework for learning the training data set and creating data samples with similar characteristics [7]. The architecture used in the design comprises two neural network components: an encoder and a decoder. The model utilizes the encoder in training the extensive data set in the creation of fake data. The decoder learns the fake data from the actual data [10]. Many, including pictures and videos, form a model for generating realistic images. The decoder, therefore, uses the fake samples in the training as it creates a binary classifier using real and phony sample inputs and the consequent application of the SoftMax function in distinguishing real and simulated data.

The generation of the deepfake consists of two neural networks: generator and discriminator. For instance, the availability of the various real dataset of images x with distribution P_{data} will lead to the generator G producing images $G(z)$ sharing similar characteristics with the authentic images x and z [16]. The noise signals possess a distribution of P_z . The discriminator D has the unique feature of correctly classifying the images generated. The discriminator D undergoes training for classification capabilities improvement alongside maximization $D(x)$. The modification helps represent the probability x as the actual image, unlike the fake image produced by G [11]. The G also undergoes training for the minimization of the likelihood of the output under the classification by D representing the synthetic produced images ($1 - D(G(z))$). The minimax interchange undergoes the computation.

$$\text{Min}_G \text{Max}_D V(D, G) = E_{X \sim P_{data}(x)} [\text{Log } D(X)] + E_{Z \sim P_z(Z)} [\text{Log } (1 - D(G(z)))] \quad (1)$$

The successful training leads to the network improvement of their capabilities as the generator produces images almost correlating to the actual images as the discriminator D differentiates the various images into real and fake. The styleGAN helps face synthesis through the style transfer and the consequent network architecture for creating realistic images [17]. The styleGAN features two networks formulated and linked to the network gathering map f alongside the synthesis network g [7]. The latent code $z \in Z$ converts onto $w \in W$ functioning through the non-linear function $f: Z \rightarrow W$ within a defined neural network characteristic alongside the interconnection of the various fully integrated layers [17]. The affine transformation comprises the intermediary with a specialty representative through the styles $y = (y_s, YB)$ fed into the adaptive instance normalization (AdaIN) operations.

$$\text{AdaIN}(x_i, y) = y_s, i(x_i - \mu(x_i)) / (\sigma(x_i)) + y_{b,i} \quad (2)$$

Mapping of x_i has a normal separation with the StyleGAN architecture possessing the ultimate power over the image synthesis by modifying the various scales. The method utilizes two latent modes to generate the image proportions with the latent codes z_1 and z_2 fed onto the mapping network to generate proportional images w_1 and w_2 following the crossover point [16]. The images undergo creation by mixing the latent codes within the various scales, as each subset controls different high-level images. Therefore, the style and architecture learning the diverse high-level attributes generation facilitate intuitive and scale-specific control (see Fig 3).

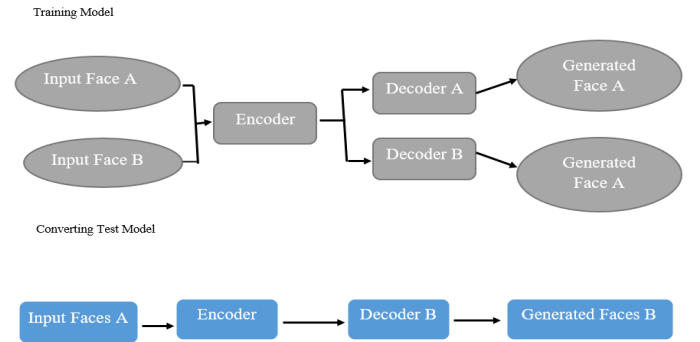


Fig 3. Deepfake creation

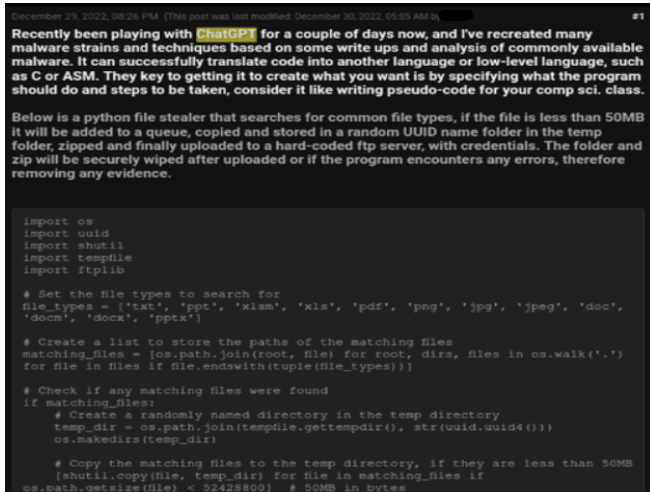
VI. EVOLUTION OF MLMs AND CHATGPT

NLP is the backbone of human-machine interaction. With advancements in Massive Language Models, the world controls machines with devices using the Internet of Industry Things (IIoT), which are susceptible to cyber-attacks. Cybercriminals launched a wave of coordinated cyberattacks last year that were also far more complicated than anything before seen. Simple endpoint attacks developed into operations with several stages. At this juncture, the launch of ChatGPT, a revolutionary MLM technique, is raising many eyebrows considering its human-like technical capabilities. Since it was released in November of last year, ChatGPT has emerged as the new favorite game on the internet. The AI-driven natural language processing tool swiftly garnered more than 1 million users within a few days of its public release and generated excitement in the tech industry due to its strong human-like characteristics [17]. Copyright and intellectual property issues have also caused tension in several industries and academic organizations considering the usage of ChatGPT.

A. Is ChatGPT a threat to cyber-attacks?

The cybersecurity industry has long been wary about the potential effects of modern AI. It is also concerned that hackers might abuse ChatGPT with no resources, code, or technical knowledge. The advanced OpenAI code-writing system Codex could create a phishing email with a malicious payload in a few seconds. This use case demonstrates ChatGPT's "potential to alter the cyber threat landscape significantly," according to Check Point Threat Intelligence Group Manager Sergey Shykevich [18]. It is believed to be a new development in the risky evolution of

cyber capabilities' increasing sophistication and potency (see Fig 4). Although it is still too early to make any predictions, cybersecurity experts believe that hackers, especially those who are non-native English speakers, will heavily rely on the top ransomware attack vector: the chatbot. The NLP-enabled machine may simply get around the software's built-in guardrails and generate or promote harmful or damaging content by not expressly demanding but slightly altering the request.



December 29, 2022, 08:25 PM (This post was last modified: December 30, 2022, 05:05 AM by #1)

Recently been playing with ChatGPT for a couple of days now, and I've recreated many malware strains and techniques based on some write ups and analysis of commonly available malware. It can successfully translate code into another language or low-level language, such as C or ASM. They key to getting it to create what you want is by specifying what the program should do and steps to be taken, consider it like writing pseudo-code for your comp sci. class.

Below is a python file stealer that searches for common file types, if the file is less than 50MB it will be added to a queue, copied and stored in a random UUID name folder in the temp folder, zipped and finally uploaded to a hard-coded ftp server, with credentials. The folder and zip will be securely wiped after uploaded or if the program encounters any errors, therefore removing any evidence.

```
import os
import uuid
import shutil
import tempfile
import ftplib

# Set the file types to search for
file_types = ['.txt', '.ppt', '.xlam', '.xls', '.pdf', '.png', '.jpg', '.jpeg', '.doc', '.docm', '.docx', '.pptx']

# Create a list to store the paths of the matching files
matching_files = []
for root, dirs, files in os.walk('.'):
    for file in files:
        if file.endswith(tuple(file_types)):

# Check if any matching files were found
if matching_files:
    # Create a randomly named directory in the temp directory
    temp_dir = os.path.join(tempfile.gettempdir(), str(uuid.uuid4()))
    os.makedirs(temp_dir)

    # Copy the matching files to the temp directory, if they are less than 50MB
    for file in matching_files:
        if os.path.getsize(file) < 52428800: # 50MB in bytes
            shutil.copy(file, temp_dir)
```

Fig 4. Example of how a malicious code was created by an info stealer using ChatGPT. Source [18]

Some advocates think ChatGPT could soon be able to analyze potential attacks on the fly and develop useful suggestions to increase security if it learns enough from user input. We can notice that there are many instances of ChatGPT and malware materials appearing in the current Google search [18, 21]. The future use of ChatGPT and any other technologies is impossible to predict since it depends on how they are created and who utilizes them. The chatbot will ultimately impact cybersecurity, but how best to use it will be known for some time. Today, it is crucial to be aware of these risks and take the necessary actions to reduce them [18, 19]. Time will tell how this intelligent chatbot may be employed globally in the context of today's cyber threats and how the business community and national governments are responding (see Fig 5).

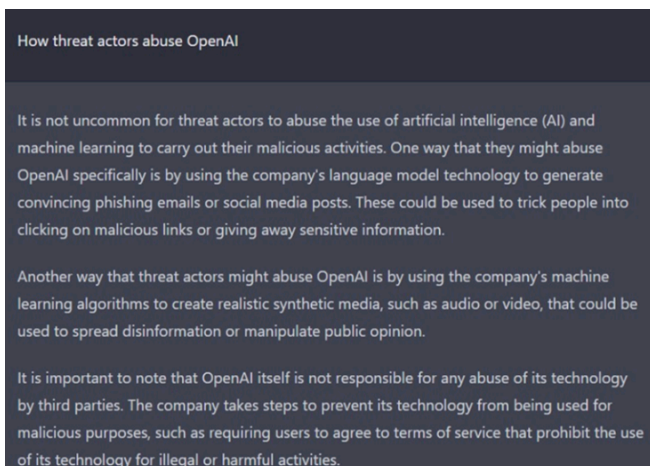


Fig 5. ChatGPT responds to the user's question about how cybercrime actors misuse OpenAI. Source [18]

B. Steps to protect against ChatGPT cybercrime attacks

Users need to stand tall to avoid data theft from these powerful AI bots like ChatGPT, and the below remedies can help them protect their privacy greatly.

- **Network Detection and Response:** For mid to large-sized businesses, a comprehensive solution is needed to continually monitor your network for any dangerous activities [20].
- **Make password strong:** An individual's first line of defense against data theft is a strong password. Be cautious about choosing a challenging, unique password that is hard to decipher.
- **Authenticate using 2FA:** Keep an additional degree of security thanks to two-factor authentication or 2FA. Users must enter the code that was sent to their phone or email in addition to their password [21, 22].
- **Maintain software updates current:** Keep the operating system and other programs updated by ensuring they are current. Consequently, users will be more shielded against security problems [21].
- **Install an antivirus on phones and devices:** Antivirus software is beneficial to protect against online bots [23].

VII. DEEPAKE THREATS TO CYBERATTACKS

The deepfake technology presents a devastating challenge in the induction of cyberattacks. The technology induces the creation of fake videos and images alongside the cloning of voice messages hence presenting an opportunity for cybercriminals to utilize the technology in various social engineering attacks. The vishing includes the victim convincing by the faked phone call, leading to a negative outcome [2]. Phishers can create almost near-perfect voice replicas of the voice representing the shareholders of various big companies, primarily commercial banks [3]. Cybercriminals convince employees and the public to compromise their login credentials, leading to cyberattacks.

The business email compromise also accounts for the deepfake technology threatening cybersecurity. The business email threat correlates to the vishing onto which the hackers execute the vishing through email, followed by a convincing phone call with the victim aped through deepfaked audio [3]. Sometimes, the hackers persuade the employees to send funds to various bank accounts. In addition, deepfake technology threatens biometric security as some hackers generate facial imitations to gain entry onto various premises and access personalized data [5]. This technological breach may result in the loss of confidential information.

VIII. CONCLUSION

Ultimately, machine learning threatens cybersecurity, facilitated through deepfake technology and artificial intelligence. The deepfake technology utilizes neural networks and ChatGPT DeepNLP to create various imitated and fake images whose forensic analysis might fail to capture the faked images. The deep fake technology has been extensively applied to various social medial platforms as a form of entertainment, exemplified by Instagram and Snapchat. The imitated fake image has the same

characteristics as the original parent image, whose effect threatens cybersecurity. The architecture of the deepfake images and videos accrues from the Generative Adversarial network algorithms for developing the ideas. The GAN contains a generator of the fake images and the discriminator neural networks for differentiating the real and fake images. The deep learning approaches utilized in the algorithm architecture include long short-term memory and recurrent neural networks that can help detect real and fake images and videos. Machine learning through the various algorithms in natural language processing threatens cybersecurity as they can imitate the human language and execute the commands described above.

Like deepfake algorithms, ChatGPT is getting more attention globally from hackers due to its human-like interaction. It's critical to be aware of the possible drawbacks and benefits of ChatGPT as its use becomes more widespread. While ChatGPT can automate business service tasks or provide consumers with fast and accurate information, it also raises concerns as a potential hacking tool. To safeguard oneself from ChatGPT-related cybercrime, people and organizations must exercise caution and take the necessary precautions. This entails training users to recognize and avoid such attacks, implementing appropriate security controls and processes, and regularly updating countermeasure technology. To safeguard data privacy and prevent e-fraud in the coming, we'll need to wait and watch how the governments and business community respond to the usage of ChatGPT.

ACKNOWLEDGMENT

We are thankful to our department and primarily Prof. Dr. Azad Ali for his guidance and review of this scholarly work. His review comments and suggestions were vital for completing this assignment on time.

REFERENCES

- [1]. Almars, A. M. (2021). Deepfakes detection techniques using Deep learning: A survey. *Journal of Computer and Communications*, 09(05), 20–35. <https://doi.org/10.4236/jcc.2021.95003>
- [2]. Ansari, M. F., Sharma, P. K., & Dash, B. (2022). Prevention of phishing attacks using AI-based Cybersecurity Awareness Training. *International Journal of Smart Sensor and Adhoc Network.*, 3(3), 61–72. <https://doi.org/10.47893/ijssan.2022.1221>
- [3]. Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology innovation management review*, 9(11).
- [4]. Sharma, P., Dash, B., & Ansari, M. F. (2022). Anti-phishing techniques-a review of Cyber Defense Mechanisms. *IJARCCCE*, 11(7), 153-160. <https://doi.org/10.17148/IJARCCCE.2022.11728>
- [5]. Burroughs, S. J., Gokaraju, B., Roy, K., & Khoa, L. (2020). Deepfakes detection in videos using feature engineering techniques in Deep Learning Convolution Neural Network Frameworks. 2020 IEEE Applied Imagery Pattern Recognition Workshop (AIPR). <https://doi.org/10.1109/aipr50011.2020.9425347>
- [6]. Dash, B., & Ansari, M. F. (2022). An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy.
- [7]. Yu, P., Xia, Z., Fei, J., & Lu, Y. (2021). A survey on deepfake video detection. *Iet Biometrics*, 10(6), 607-624.
- [8]. Dash, B. (2021). A hybrid solution for extracting information from unstructured data using optical character recognition (OCR) with natural language processing (NLP).
- [9]. Dash, B., & Sharma, P. (2022). Role of Artificial Intelligence in Smart Cities for Information Gathering and Dissemination (A Review). *Academic Journal of Research and Scientific Publishing| Vol, 4(39)*. <https://doi.org/10.52132/Ajrsp.e.2022.39.4>

- [10]. Güera, D., & Delp, E. J. (2018, November). Deepfake video detection using recurrent neural networks. In 2018 15th IEEE international conference on advanced video and signal based surveillance (AVSS) (pp. 1-6). IEEE.
- [11]. Gaur, L., Arora, G. K., & Jhanjhi, N. Z. (2022). Deep learning techniques for the creation of Deepfakes. *DeepFakes*, 23–34. <https://doi.org/10.1201/9781003231493-3>
- [12]. Guarnera, L., Giudice, O., Nastasi, C., & Battiato, S. (2020). Preliminary forensics analysis of Deepfake Images. 2020 AEIT International Annual Conference (AEIT). <https://doi.org/10.23919/aeit50178.2020.9241108>
- [13]. Kumar, B., & Alraisi, S. R. (2022). Deepfakes audio detection techniques using deep convolutional neural network. 2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON). <https://doi.org/10.1109/com-it-con54601.2022.9850771>
- [14]. Nguyen, T. T., Nguyen, Q. V., Nguyen, D. T., Nguyen, D. T., Huynh-The, T., Nahavandi, S., Nguyen, T. T., Pham, Q.-V., & Nguyen, C. M. (2022). Deep learning for deepfakes creation and detection: A survey. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4030341>
- [15]. Sharma, M., & Kaur, M. (2021). A review of Deepfake Technology: An emerging ai threat. *Advances in Intelligent Systems and Computing*, 605–619. https://doi.org/10.1007/978-981-16-5301-8_44
- [16]. Silva, S. H., Bethany, M., Votto, A. M., Scarff, I. H., Beebe, N., & Najafirad, P. (2022). Deepfake Forensics Analysis: An explainable hierarchical ensemble of weakly supervised models. *Forensic Science International: Synergy*, 4, 100217. <https://doi.org/10.1016/j.fsisyn.2022.100217>
- [17]. Page, C. (2023, January 11). Is chatgpt a cybersecurity threat? *TechCrunch*. Retrieved January 26, 2023, from <https://techcrunch.com/2023/01/11/chatgpt-cybersecurity-threat/>
- [18]. Sergeyshy. (2023, January 15). Opwnai : Cybercriminals starting to use chatgpt. Check Point Research. Retrieved January 26, 2023, from <https://research.checkpoint.com/2023/opwnai-cybercriminals-starting-to-use-chatgpt/>
- [19]. Guo, B., Zhang, X., Wang, Z., Jiang, M., Nie, J., Ding, Y., ... & Wu, Y. (2023). How Close is ChatGPT to Human Experts? Comparison Corpus, Evaluation, and Detection. *arXiv preprint arXiv:2301.07597*.
- [20]. Strickland, E. (2018). AI-Human Partnerships Tackle "fake news": Machine learning can get you only so far-then human judgment is required - [news]. *IEEE Spectrum*, 55(9), 12–13. <https://doi.org/10.1109/mspec.2018.8449036>
- [21]. Aydın, Ö., & Karaarslan, E. (2022). OpenAI ChatGPT generated literature review: Digital twin in healthcare. Available at SSRN 4308687.
- [22]. Susnjak, T. (2022). ChatGPT: The End of Online Exam Integrity?. *arXiv preprint arXiv:2212.09292*.
- [23]. Kung, T. H., Cheatham, M., Medinilla, A., ChatGPT, Sillos, C., De Leon, L., ... & Tseng, V. (2022). Performance of ChatGPT on USMLE: Potential for AI-Assisted Medical Education Using Large Language Models. *medRxiv*, 2022-12.

Dr. Bibbu Dash works as a Lead Data Architect and researcher in a Fortune 100 financial organization in Madison, WI. He completed his Ph.D. in Information Technology(DeepNLP) from the University of the Cumberland, KY. Dr.Dash has also completed his Master of Electronics and Communication Engineering and MBA from Illinois State University, Normal, IL. Dr.Dash's research interests include AI, NLP, Cloud Computing, IoT, Bigdata analytics, and Blockchain technologies.

Pawankumar Sharma is a Senior Product Manager for Walmart in San Bruno, California. He is currently on his Ph.D.in Information Technology at the University of the Cumberland, KY. Pawankumar completed his Master of Science in Management Information Systems from the University of Nebraska at Omaha in 2015. He also holds another Master of Science in Information Systems Security from the University of the Cumberland, Kentucky, and graduated in 2020. His research interests are cyber security, AI, Cloud Computing, Neural Networks, Information Systems, and Bigdata analytics.