International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Adversarial Attacks and Defenses in Deep Learning Models

Khaja Shahini Begum[1], Dr. Bathina Rajesh Kumar[2], Gundala Venkata Rama Lakshmi[3], R S S Raju Battula[4], Elangovan Muniyandy[5], Amit Verma[6], Dr. Ajmeera Kiran[7]

Submitted: 04/02/2024 **Revised**: 12/03/2024 **Accepted**: 18/03/2024

Abstract: This paper investigates the complex interactions that lead to adversarial weaknesses in deep learning systems. This analyses various adversarial attack strategies, including FGSM and PGD, to evaluate how well they may undermine model fidelity. These results highlight the ongoing cat-and-mouse game between deep-learning security attackers and defenders. Although much progress has been made in increasing model resilience, the lack of a globally defined strategy highlights the necessity for a diversified security policy. This study shows the need for continual innovation and the persistent difficulty of protecting deep learning models against hostile threats..

Keywords: *Deep Learning, Adversarial Attack, Agile Methodology, Cyber Attack*

1. Introduction

Deep Learning and Artificial Intelligence procedural techniques help most people ensure a better life in various aspects of life like marketing, selling, bank predictions, medical predictions, and many more. The more and more developed deep learning models give critical thought to ensuring the security vulnerability of deep learning models to adversarial samples that have been recognized widely [26]. The cause of people sabotaging the deep learning model causes them to make problems to generate wrong predictions and misbehaviour. The defined technique is very important to learn so the machine can remain healthy and not get disturbed by the people implementing the adversarial attacks.

1.1. Research aim and objectives

Aim: The research paper aims to analyse the adversarial attacks in the deep learning model and find out the defence mechanism to prevent these types of attacks for helping the deep learning models.

Objectives:

- To analyse the adversarial attacks within the deep learning model
- To predict the attacks that affect the machine deep learning and predict the type of box attack and study it
- To provide a defence mechanism against these attacks helps deep learning models not fail their predictions and helps people
- To support the deep learning companies by making a cure or a solution to prevent these types of attacks

1.2. Research Rationale

Advertisements can trick the deep learning model by disturbing the previous samples of deep learning. Disturbance causes the model to hesitate and tend to make wrong choices and predictions which is impossible for humans with problems with hearing and vision, believe the machine and make a confidently wrong prediction [34]. The three types of attack models are white box, grey box, and black box. The attacks from the adversaries assume having knowledge of the target model including architecture and parameters and attack by creating directly crafted adversaries' samples which are the features of white box attacks. Grey box uses the knowledge of the adversaries that is limited to the structure of the model target. Black box threat model the adversarial samples are created for the adversaries but they are in the process of query [35].

2. Literature Review

2.1. Types of adversarial attacks

There are more adversarial attacks and many are also used by people who also trying to improvise the attack models. An attack that is very different from the others that depends on the probability of space measures is called a distributional adversarial attack (DAA). PGD takes the

[1]*Research Scholar, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India Email:khajashahin@gmail.com*
[2]*Assistant Professor, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India Email: rajeshbathina@kluniversity.in*
[3]*Assistant Professor, CVR College of Engineering, Hyderabad, India Email: gvrlaksmi@cvr.ac.in*
[4]*Department of Computer Science and Engineering, Aditya Engineering College, Surampalem, Kakinada, Andhra Pradesh, India Email: raju.brss@gmail.com*
[5]*Department of Biosciences, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamil Nadu, India Email: muniyandy.e@gmail.com*
[6]*University Centre for Research and Development, Chandigarh University, Gharuan Mohali, Punjab, India Email: amit.e9679@cumail.in*
[7]*Assistant Professor, Department of Computer Science and Engineering, MLR Institute of Technology, Dundigal, Hyderabad, Telangana, 500043,India Email: kiranphd.jntuh@gmail.com*

adversarial samples generated independently for each sample and DAA features optimization and possibly adversarial products scattering out everywhere. The researcher has shown the attacks and raised the issue of whether there is a naturally sturdy algorithm that can fool the network of hard samples [20]. Iteratively updating the sturdiness using all target samples with each iteration of the hard-core samples cannot fool and optimize the model and for that additional perturbations are added to the recent perturbation. The perturbation gradually shows the friendliest samples to fool the network. Other attacks like an adversarial patch make the problem in recognizing the facial expression, and the glasses in the picture. The model only targets the physical target in the world. The people used adversarial glasses to recognize the attacks like a true VGG-Face CNN system [27]. The adversarial loss provides the optimization of the patch basis of the warm images, a transformation of the patches, and the location as well.

2.2. Adversarial defence and its significance

Adversarial defences are very important for the effectiveness of the attacks that are used for manipulating people and making up a fake classification to use. Adversarial training is a built-in defence method technique used to improve the robustness of a neural network system of machine learning by training the neural network with the samples of adversarial. Ensemble adversarial training is used to adversarial train a strong Image Net model by FGSM about random stats. A Black box however can make the training model vulnerable so a training methodology that incorporates the adversarial samples transferred from multiple pre-trained models is named ensemble adversarial training (EAT) [21].

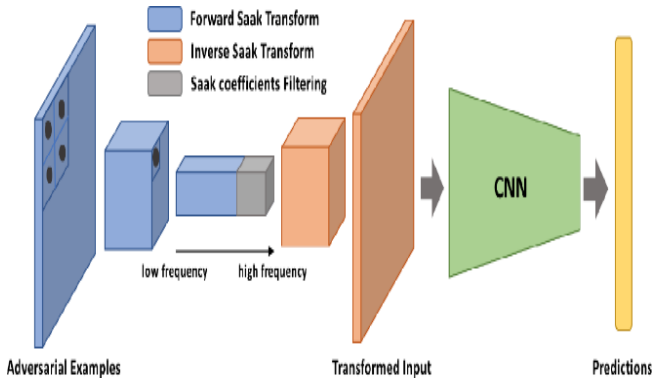

Fig 1. Process of Defense Adversarial Attacks

Research shows that the EAT models display sturdiness against adversarial samples created by many multi-step steps as well as single-step attacks on the other model. EAT is more successful than every other adversarial training and also better than PGD adversarial training. Adversarial logit pairing is used to check the stability training between the pairs of attacks and the defence mechanism [22]. The Generative adversarial method is used to work like a generator that takes the gradients of a trained classifier the respect of which is used to make out the samples. It generates a sturdier classifier than the FGSM with the help of training the classifier on both used and generated samples.

2.3. Collector Technologies and Design Considerations

No defence can achieve a balance between the period of efficiency and strength of effectiveness. The effectiveness of adversarial training gives the results of the best performance with a sustained reckoning cost of the product [23]. The configuration of the system is random and a demonising-based defence mechanism system which may take maybe one minute or maybe a few seconds.

2.4. Factors Affecting Adversarial Attacks in DL

Non-robust features give the information of the adversarial examples as an output perspective of data features. The features are split into robust and non-robust features. The features are being investigated by extracting the DNN from the perspective of the frequency spectrum of the image domain. The high frequency observed by researcher was almost unnoticeable. Vulnerabilities caused by adversarial are defined as a mystery caused by non-robust components [24]. High dimension which explores the connections of sturdiness and data dimension and created a metric to check the robustness of the classifiers. Another factor is the insufficient data that only watches to have connections with adversarial, they are not large enough to get the robust model. The use of pre-training on larger datasets through the classification is not enhanced [33].

2.5. Recent Technological Advances and Innovations

The deep learning and privacy are fragmented due to the difference in the threats and the objectives. Securing the deep learning models with more sturdiness that can preserve sensitive data and the user has to be involved in collaborative training. Different privacy techniques can reduce the success rate of the invasion although the cost of training the model of defence mechanism is immense [28]. The implicit possibilities of checking the attacks and studying the attacks are to explore the vulnerabilities so that the defenders can countermeasure from the previous data and train to make success. Monitoring methods can help to check any suspicious activity in the Deep Learning. Deep learning also uses long short-term memory to detect anomalies and log monitoring models that encourage exploration of what a model needs [25].

Fig 2. Adversarial Attacks ML Attack

The training of the target model is indeed necessary and use this strategy to achieve potential countermeasures to defend from the attacks that occur in the training phase and prevent the submission of the dangerous models.

2.6. Literature Gap

This research has discussed many types of models that can attack and defend as well. Previous research about the topic is also provided such as robustness certification, anti-crafting, post-crafting, detection of defence present in the deep learning model, and creation of a disease-specific application model. This research is past findings to find the unique properties of the deep learning models. The best strategy is always at the last moment to predict the problems predict the issues and generalize the solutions. Deep learning has made incredible strides in recent years, and it is now being used for everything from picture identification to the processing of natural language. The emergence of hostile assaults, however, poses a substantial challenge in addition to these accomplishments. The adversarial assaults and responses against deep learning models are explored in depth in this survey of the literature. Adversarial assaults are well-produced input perturbations meant to trick models into making incorrect predictions or conclusions [26]. Black-box assaults, physical-world attacks, and gradient-based approaches are just a few of the attack tactics that have been devised. On the other hand, researchers have attempted to strengthen models against such attacks via training methods that are adversarial, robust effectiveness, and detection approaches. This analysis emphasizes the continual game of cat and mouse game between attackers and defences as it critically evaluates the advantages and disadvantages of both offensive and defensive strategies. The development of safe and dependable deep learning systems needs to have a thorough grasp of this dynamic environment.

3. Methodology

3.1. Research Approach

The deductive research approach uses the current theory to find the new theory. This is used in this project that improves the accuracy of the project and helps to generate accurate outcomes in the research. Developing these theories helps in current theoretical models and earlier study findings [1].

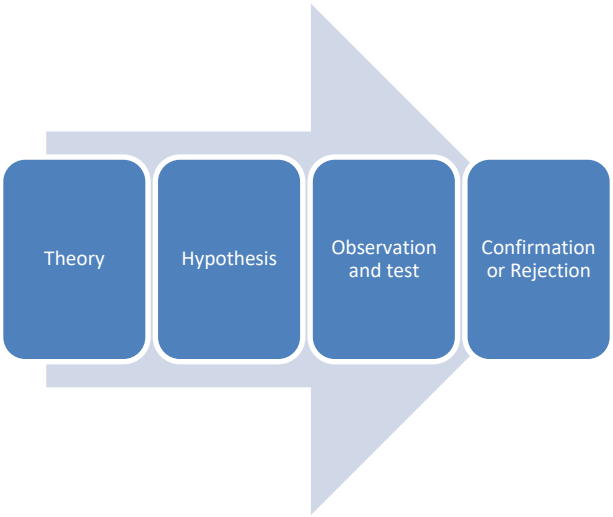

Fig. 3. Deductive research approach

The research tries to produce empirical evidence that either supports or contradicts these assumptions through systematic experimentation and data analysis. Establishing the project in existing knowledge, the deductive approach assures a structured and logical continuation of the research, increasing the project's validity and trustworthiness [29].

3.2. Research Design

The “experimental research design” used in this project enables controlled investigations to test hypotheses and demonstrate causal linkages. The effectiveness of various securities is strategies against adversarial attacks in deep learning models. Significant findings on the impact of defensive systems by carefully regulating experimental circumstances and using statistical analysis can be generated by using this approach [2].

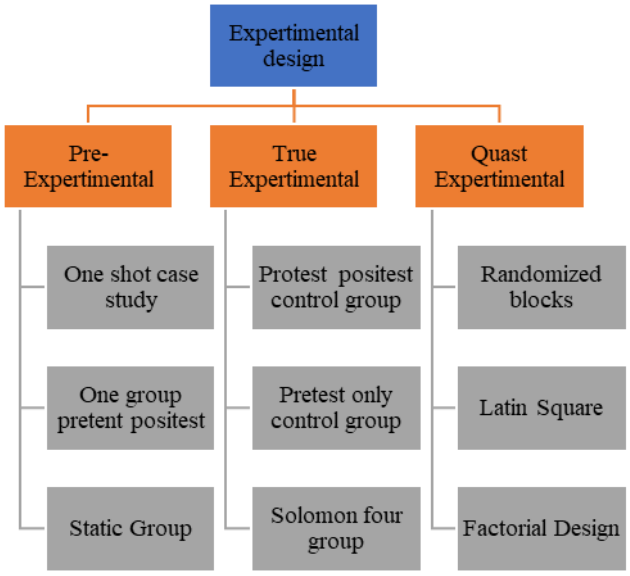

Fig. 4. Experimental research design

The experimental methodology offers a disciplined framework for accumulating empirical data, ensuring validity and generalizes ability of the research findings to the larger field of deep learning models that are beneficial for this project.

3.3. Project Management Approach

Agile development approaches place a strong emphasis on iterative cooperation and development, allowing for adjustments in response to new information and evolving conditions. This promotes consistent communication among team members and stakeholders, establishing an atmosphere for research that is dynamic and adaptable [3].

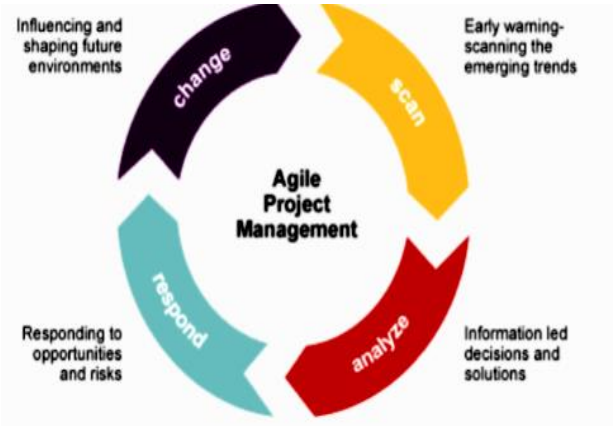

Fig. 5. Agile project management approach

The project can effectively address changing research issues, guarantee on-time completion, and preserve the applicability of its discoveries in the quickly developing field of deep learning and adversarial attacks by using an agile strategy [4].

3.4. Data Collection Method

Secondary data sources for the project "Adversarial Attacks and Defences in Deep Learning Models" include journal articles, reports, and datasets about adversarial attacks, defence tactics, and deep learning models. This corpus of pieces of information is reviewed and synthesized by researchers to guide their research designs, hypotheses, and experimental guidelines [5]. The use of secondary data gathering has several benefits, including affordability, accessibility to a wealth of resources, and the capacity to expand on prior studies. The integrity of the research is ensured by strict attention paid to ethical issues such as correct citation, plagiarism prevention, and the validity and quality of secondary data sources [6].

Ethical Considerations

This research prioritizes ethical issues, especially when it comes to AI and deep learning models. Researchers are required to adhere to research ethics standards throughout the project, such as informed consent, data privacy, and transparency. The initiative follows moral standards for ethical AI development and application [7]. Addressing difficulties with bias, fairness, and possible harm from adversarial attacks are all part of this. Fairness in experiment design should be given priority, and researchers should think about how their findings will affect society as a whole. To keep the project's credibility, the calibre and relevancy of secondary sources are analysed [8].

4. Results

Theme 1: Effectiveness of Adversarial Attacks in deep learning models

4.1. Attack strategies

Diverse assault tactics are what give hostile attacks their effectiveness. Notably, gradient-based assaults have become more popular because of how well they produce tiny perturbations that cause misclassification [30]. Transfer attacks, which make use of the ability of adversarial examples to transfer between several models, have also been discovered to be successful. The analysis of this theme shows that adversaries use a variety of tactics, including physical, black-box, and white-box attacks, to take advantage of model weaknesses in various ways [9].

4.2. Impact on models

An important component of this issue is how adversarial attacks affect deep learning models. The investigation shows that these attacks can seriously impair the accuracy and integrity of models. Deep learning models, which are frequently thought of as robust, are found to be susceptible to these expertly designed shocks [10]. As a result, the theme emphasizes that, especially in safety-critical systems, the effects of adversarial attacks go beyond simple model misinterpretation to include potentially disastrous results.

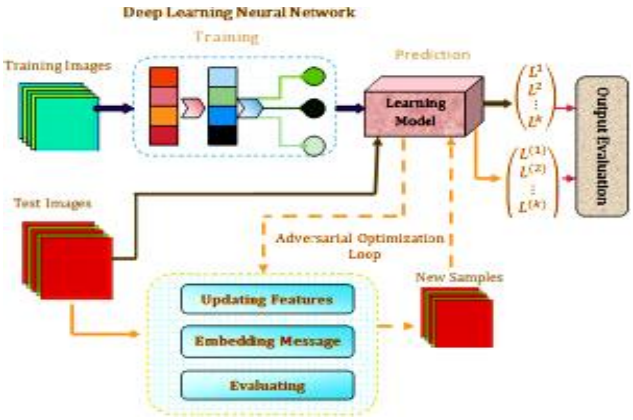

Fig. 6. Attack on deep learning model

4.3. Trends in effectiveness

This analysis reveals discernible trends in the efficacy of hostile attacks. A recurrent pattern appears across numerous domains and applications: adversarial attacks continue to be a serious concern. According to the findings, adversaries modify their techniques as deep learning models advance, making earlier protection systems less effective [11]. This analysis demonstrates the variety of assault tactics used by adversaries, the significant effect these attacks have on models, and the ongoing pattern of evolving threats. This investigation serves as a sobering reminder of the need for strong defence mechanisms and continual watchfulness in the deep learning community to reduce the hazards brought on by hostile attacks [12].

Theme 2: Efficacy of Defence Mechanisms

4.4. Adversarial training

Adversarial training, which entails putting models through training on both clean and hostile data, is a common defence strategy. According to the analysis, adversarial training shows promise for reducing adversarial attacks. Models trained using adversarial data generally perform better when exposed to adversarial inputs, reducing misclassification rates and raising overall accuracy, according to experiments and studies [13]. This is crucial to remember that adversarial training could call for extra time and computational resources for model convergence.

4.5. Model assembling

Model assembling, in which various models are merged to generate predictions collectively, is a different security strategy. Model assembling may improve defence against adversarial attacks, according to thematic analysis. The predictions of various models are combined, making it more difficult for opponents to create deceptive inputs that fool the entire ensemble [14]. This approach has shown promise in strengthening model robustness and minimizing vulnerabilities.

4.6. Interpretability and explainability

Techniques for interpretability and explainability are also crucial in defence mechanisms. The analysis shows how interpretable models, like decision trees or rule-based models, can be useful for locating adversarial examples and comprehending model behaviour [15].

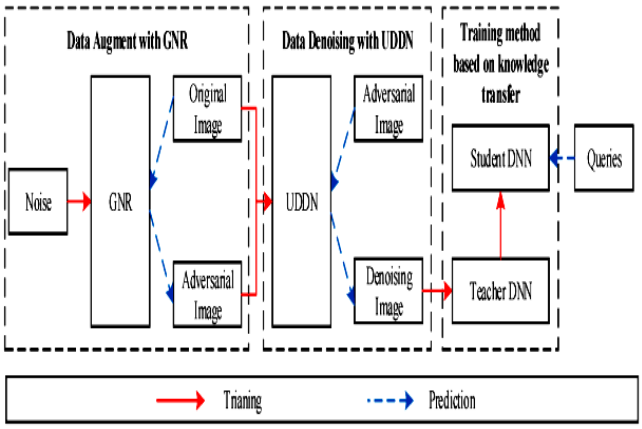

Fig. 7. Attack and defences

Explain ability techniques, such as feature attribution methods, provide insight into the decision-making processes of models, assisting in the identification and reduction of hostile inputs. A trade-off between resilience and accuracy is also necessary because some defence strategies may result in poorer model performance on clean data. This helps to create even more potent protection mechanisms in the context of deep learning models; however, further study and innovation are required due to the always-changing nature of adversarial attacks [16].

Theme 3: Ethical and Societal Implications

4.7. Privacy Concerns and Data Security

Adversarial attacks provide serious ethical problems for data security and privacy. These assaults have the potential to compromise private data, resulting in possible breaches and illegal access. Adversarial attacks might have disastrous effects on people and organizations in a variety of sectors, including healthcare and finance [17]. Defence systems are essential for reducing these hazards. The retention of confidence in AI systems is crucial to evaluate how well they protect data. Numerous examples from the real world show how adversarial attacks have resulted in privacy violations, highlighting how urgent it is to address this ethical issue.

4.8. Bias and Fairness Issues

Adversarial assaults can make AI models more biased, leading to unjust or discriminating outputs. Serious ethical questions are raised when minority populations or certain demographic groups are disproportionately vulnerable to antagonistic influence. Biased predictions can have serious repercussions in industries where AI models are crucial, such as the medical and legal domains. This is crucial to

assess the ethical ramifications of such biases [18]. The effectiveness of defence mechanisms in reducing bias and ensuring justice in AI systems needs to be evaluated. Recognizing these systems' shortcomings and difficulties is essential for dealing with bias effectively.

4.9. Regulatory and Legal Considerations

Discussions about legal and regulatory frameworks for AI security and accountability have been sparked by adversarial attacks. A closer look at the regulatory environment finds an increasing emphasis on AI ethics, accountability, and transparency [31]. These laws aim to define standards that companies, users, and creators of AI should adhere to this make the project more appropriate.

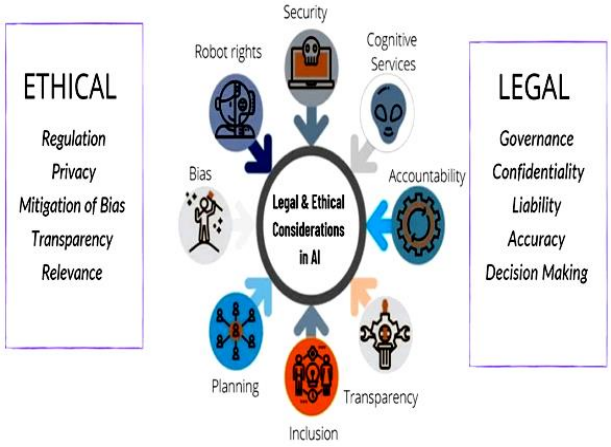

Fig. 8. Ethical consideration

Instances of harmful AI behaviour, such as adversarial attacks, raise questions of liability and accountability [19]. This is crucial to comprehend the obligations of all parties involved and the repercussions of non-compliance.

5. Evaluation and Conclusion

5.1. Conclusion

The effectiveness of defence mechanisms against adversarial attacks in deep learning models is analysed in this project. The objectives of the defensive strategies respect the different stages directly involved in the adversarial attack life cycle. The research has provided actual evidence to support the continuing conversation in the field of deep learning security through careful experimentation and data analysis. This makes it clear that using these models in security-critical applications presents considerable difficulties due to their susceptibility to adversarial assaults.

5.2. Research recommendation

The deep Learning Model has incredible performance in solving the objectives of people's daily lives, and the vast security, and provides a generative rise in concerns about the vulnerability of the models to adversarial samples to evaluate the security and sturdiness [24]. The few fundamental problems cause the adversarial system to create a sturdy border and no existing defence mechanism achieves efficiency and effectiveness against adversarial training which is very expensive many of the defences are said to be more vulnerable to discussed open challenges and the problems and help to boost the people and guide them to help in this critical area.

5.3. Future work

The continual weapons race between defenders and attackers, however, emphasizes the necessity of ongoing research in this area. Protecting deep learning models from adversarial attacks is still a difficult problem that is always changing and requiring new research and innovations [32]. The project's major focus remains on ethical issues, such as informed consent, data protection, fairness, and responsible AI research.

References

[1] Zhang, W.E., Sheng, Q.Z., Alhazmi, A. and Li, C., 2020. Adversarial attacks on deep-learning models in natural language processing: A survey. ACM Transactions on Intelligent Systems and Technology (TIST), 11(3), pp.1-41.

[2] Huang, T., Zhang, Q., Liu, J., Hou, R., Wang, X. and Li, Y., 2020. Adversarial attacks on deep-learning-based SAR image target recognition. Journal of Network and Computer Applications, 162, p.102632.

[3] Ibitoye, O., Abou-Khamis, R., Matrawy, A. and Shafiq, M.O., 2019. The Threat of Adversarial Attacks on Machine Learning in Network Security--A Survey. arXiv preprint arXiv:1911.02621.

[4] Anthi, E., Williams, L., Rhode, M., Burnap, P. and Wedgbury, A., 2021. Adversarial attacks on machine learning cybersecurity defences in industrial control systems. Journal of Information Security and Applications, 58, p.102717.

[5] Fawaz, H.I., Forestier, G., Weber, J., Idoumghar, L. and Muller, P.A., 2019, July. Adversarial attacks on deep neural networks for time series classification. In 2019 International Joint Conference on Neural Networks (IJCNN) (pp. 1-8). IEEE.

[6] Yuan, J., Zhou, S., Lin, L., Wang, F. and Cui, J., 2020. Black-box adversarial attacks against deep learning-based malware binaries detection with GAN. In ECAI 2020 (pp. 2536-2542). IOS Press.

[7] Rauber, J., Zimmermann, R., Bethge, M. and Brendel, W., 2020. Foolbox native: Fast adversarial attacks to benchmark the robustness of machine learning models in pytorch, tensorflow, and jax. Journal of Open Source Software, 5(53), p.2607.

[8] Han, X., Hu, Y., Foschini, L., Chinitz, L., Jankelson, L. and Ranganath, R., 2020. Deep learning models for electrocardiograms are susceptible to adversarial attack. Nature medicine, 26(3), pp.360-363.

[9] Zhang, C., Costa-Perez, X. and Patras, P., 2022. Adversarial attacks against deep learning-based network intrusion detection systems and defense mechanisms. IEEE/ACM Transactions on Networking, 30(3), pp.1294-1311.

[10] Newaz, A.I., Haque, N.I., Sikder, A.K., Rahman, M.A. and Uluagac, A.S., 2020, December. Adversarial attacks to machine learning-based smart healthcare systems. In GLOBECOM 2020-2020 IEEE Global Communications Conference (pp. 1-6). IEEE.

[11] Mani, N., Moh, M. and Moh, T.S., 2021. Defending deep learning models against adversarial attacks. International Journal of Software Science and Computational Intelligence (IJSSCI), 13(1), pp.72-89.

[12] Huang, T., Chen, Y., Yao, B., Yang, B., Wang, X. and Li, Y., 2020. Adversarial attacks on deep-learning-based radar range profile target recognition. Information Sciences, 531, pp.159-176.

[13] Ma, J., Zhang, J., Shen, G., Marshall, A. and Chang, C.H., 2023. White-Box Adversarial Attacks on Deep Learning-Based Radio Frequency Fingerprint Identification. arXiv preprint arXiv:2308.07433.

[14] Kim, B., Shi, Y., Sagduyu, Y.E., Erpek, T. and Ulukus, S., 2021, December. Adversarial attacks against deep learning based power control in wireless communications. In 2021 IEEE Globecom Workshops (GC Wkshps) (pp. 1-6). IEEE.

[15] Chen, C., Zhao, X. and Stamm, M.C., 2019. Generative adversarial attacks against deep-learning-based camera model identification. IEEE Transactions on Information Forensics and Security.

[16] Ren, Z., Baird, A., Han, J., Zhang, Z. and Schuller, B., 2020, May. Generating and protecting against adversarial attacks for deep speech-based emotion recognition models. In ICASSP 2020-2020 IEEE International conference on acoustics, speech and signal processing (ICASSP) (pp. 7184-7188). IEEE.

[17] Nowroozi, E., Mohammadi, M., Golmohammadi, P., Mekdad, Y., Conti, M. and Uluagac, S., 2022. Resisting deep learning models against adversarial attack transferability via feature randomization. arXiv preprint arXiv:2209.04930.

[18] Xu, Y., Du, B. and Zhang, L., 2021. Self-attention context network: Addressing the threat of adversarial attacks for hyperspectral image classification. IEEE Transactions on Image Processing, 30, pp.8671-8685.

[19] Ibitoye, O., Shafiq, O. and Matrawy, A., 2019, December. Analyzing adversarial attacks against deep learning for intrusion detection in IoT networks. In 2019 IEEE global communications conference (GLOBECOM) (pp. 1-6). IEEE.

[20] L. Yang and S. Liu, "Adversarial Attack and Defense in Breast Cancer Deep Learning Systems," Bioengineering, vol. 10, (8), pp. 973, 2023. Available: https://www.proquest.com/scholarly-journals/adversarial-attack-defense-breast-cancer-deep/docview/2856790190/se-2. DOI: https://doi.org/10.3390/bioengineering10080973.

[21] Y. Lee and J. Kim, "Robustness of Deep Learning Models for Vision Tasks," Applied Sciences, vol. 13, (7), pp. 4422, 2023. Available: https://www.proquest.com/scholarly-journals/robustness-deep-learning-models-vision-tasks/docview/2799587811/se-2. DOI: https://doi.org/10.3390/app13074422.

[22] R. L. Alaoui and H. N. El, "Generative Adversarial Network-based Approach for Automated Generation of Adversarial Attacks Against a Deep-Learning based XSS Attack Detection Model," International Journal of Advanced Computer Science and Applications, vol. 14, (7), 2023. DOI: https://doi.org/10.14569/IJACSA.2023.0140797.

[23] G. Zhang et al, "Visual privacy attacks and defenses in deep learning: a survey," The Artificial Intelligence Review, vol. 55, (6), pp. 4347-4401, 2022. DOI: https://doi.org/10.1007/s10462-021-10123-y.

[24] A. Albattah and M. A. Rassam, "Detection of Adversarial Attacks against the Hybrid Convolutional Long Short-Term Memory Deep Learning Technique for Healthcare Monitoring Applications," Applied Sciences, vol. 13, (11), pp. 6807, 2023. DOI: https://doi.org/10.3390/app13116807.

[25] A. Kazim et al, "Deep Image Restoration Model: A Defense Method Against Adversarial Attacks," Computers, Materials, & Continua, vol. 71, (2), pp. 2209-2224, 2022. DOI: https://doi.org/10.32604/cmc.2022.020111.

[26] Jati, A., Hsu, C.C., Pal, M., Peri, R., AbdAlmageed, W. and Narayanan, S., 2021. Adversarial attack and defense strategies for deep speaker recognition systems. Computer Speech & Language, 68, p.101199.

[27] Im Choi, J. and Tian, Q., 2022, June. Adversarial attack and defense of yolo detectors in autonomous driving scenarios. In 2022 IEEE Intelligent Vehicles Symposium (IV) (pp. 1011-1017). IEEE.

[28] Li, J., Liu, Y., Chen, T., Xiao, Z., Li, Z. and Wang, J., 2020. Adversarial attacks and defenses on cyber–physical systems: A survey. IEEE Internet of Things Journal, 7(6), pp.5103-5115.

[29] Wu, D., Xu, J., Fang, W., Zhang, Y., Yang, L., Xu, X., Luo, H. and Yu, X., 2021. Adversarial attacks and defenses in physiological computing: A systematic review. arXiv preprint arXiv:2102.02729.

[30] Wu, H., Wang, C., Tyshetskiy, Y., Docherty, A., Lu, K. and Zhu, L., 2019. Adversarial examples on graph data: Deep insights into attack and defense. arXiv preprint arXiv:1903.01610.

[31] Tian, J., Li, T., Shang, F., Cao, K., Li, J. and Ozay, M., 2019, October. Adaptive normalized attacks for learning adversarial attacks and defenses in power systems. In 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm) (pp. 1-6). IEEE.

[32] Fursov, I., Morozov, M., Kaploukhaya, N., Kovtun, E., Rivera-Castro, R., Gusev, G., Babaev, D., Kireev, I., Zaytsev, A. and Burnaev, E., 2021, August. Adversarial attacks on deep models for financial transaction records. In Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining (pp. 2868-2878).

[33] Kalita, K., Ramesh, J. V. N., Cepova, L., Pandya, S. B., Jangir, P., & Abualigah, L. (2024). Multi-objective exponential distribution optimizer (MOEDO): a novel math-inspired multi-objective algorithm for global optimization and real-world engineering design problems. Scientific reports, 14(1), 1816.

[34] S. P. Praveen, P. Chaitanya, A. Mohan, V. Shariff, J. V. N. Ramesh and J. Sunkavalli, "Big Mart Sales using Hybrid Learning Framework with Data Analysis," 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2023, pp. 471-477, doi: 10.1109/ICACRS58579.2023.10404941.

[35] P. Dedeepya, P. Chiranjeevi, V. Narasimha, V. Shariff, J. Ranjith and J. V. N. Ramesh, "Image Recognition and Similarity Retrieval with Convolutional Neural Networks," 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2023, pp. 709-716, doi: 10.1109/ICACRS58579.2023.10404664.

[36] D. Gupta et al., "Optimizing Cluster Head Selection for E-Commerce-Enabled Wireless Sensor Networks," in IEEE Transactions on Consumer Electronics, doi: 10.1109/TCE.2024.3360513.

[37] Singh, A., Rani, P., Ramesh, J. V. N., Athawale, S. V., Alkhayyat, A. H., Aledaily, A. N., ... & Sharma, R. (2024). Blockchain-Based Lightweight Authentication Protocol for Next-Generation Trustworthy Internet of Vehicles Communication. IEEE Transactions on Consumer Electronics.

[38] Babu, S.Z.D. et al. (2022). Analysation of Big Data in Smart Healthcare. In: Gupta, M., Ghatak, S., Gupta, A., Mukherjee, A.L. (eds) Artificial Intelligence on Medical Data. Lecture Notes in Computational Vision and Biomechanics, vol 37. Springer, Singapore. https://doi.org/10.1007/978-981-19-0151-5_21

[39] Bansal R., Gupta A., Singh R. and Nassa V. K., (2021). Role and Impact of Digital Technologies in E-Learning amidst COVID-19 Pandemic. 2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT), pp. 194-202.doi: 10.1109/CCICT53244.2021.00046.

[40] Dushyant, K., Muskan, G., Gupta, A. and Pramanik, S. (2022). Utilizing Machine Learning and Deep Learning in Cyber security: An Innovative Approach", in Cyber security and Digital Forensics, M. M. Ghonge, S. Pramanik, R. Mangrulkar,D. N. Le, Eds, Wiley, https://doi.org/10.1002/9781119795667.ch12

[41] Gupta A., Singh R., Nassa V. K., Bansal R., Sharma P. and Koti K., (2021) Investigating Application and Challenges of Big Data Analytics with Clustering. 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), pp. 1-6.doi: 10.1109/ICAECA52838.2021.9675483.

[42] M. Dhingra, D. Dhabliya, M. K. Dubey, A. Gupta and D. H. Reddy, "A Review on Comparison of Machine Learning Algorithms for Text Classification," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1818-1823, doi: 10.1109/IC3I56241.2022.10072502.

[43] D. Mandal, A. Shukla, A. Ghosh, A. Gupta and D. Dhabliya, "Molecular Dynamics Simulation for Serial and Parallel Computation Using Leaf Frog Algorithm," 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Himachal Pradesh, India, 2022, pp. 552-557, doi: 10.1109/PDGC56933.2022.10053161.

[44] P. R. Kshirsagar, D. H. Reddy, M. Dhingra, D. Dhabliya and A. Gupta, "A Review on Application of

Deep Learning in Natural Language Processing," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1834-1840, doi: 10.1109/IC3I56241.2022.10073309.