International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 1 (2026)



ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 1, 2026
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research

Hybrid Predictive Model-Integrated Advanced Cyber Security Threat Intelligence

A RAVI KIRAN 1, VARANASI SRIKARI2, GANGA SRIPAD PANCHAKRLA3, VALLBHANENI THANUSH4

#1 Assistant professor , Information Technology,,NRI Institute of Technology,Agiripalli

#2#3#4 B.Tech with Specialization of Information Technology in NRI Institute Of Technology,Agiripalli

Abstract: Using a hybrid stacking model that combines Random Forest (RF), K-Nearest Neighbor (KNN), and Multilayer Perceptron (MLP) classifiers, this expanded study offers an improved cyber-attack detection framework. To achieve high resilience and accuracy across a variety of benchmark datasets, such as NSL-KDD, CICIDS2017, CICDDOS2019, and X-IIOTID, the stacked ensemble leverages the advantages of these basic models. A Flask-based web interface is used to install the system, allowing users to interact with uploaded test datasets and forecast cyberattacks in real time. By emphasizing important feature contributions, Explainable AI (XAI) approaches promote interpretability and transparent, well-informed decision-making. Results from experiments show that the hybrid stacking framework is an effective scalable and intelligent solution for proactive cybersecurity defense, with up to 100% accuracy.

Index terms *- — Cyber-attack prediction, machine learning, deep learning, hybrid stacked model, NSL-KDD, CICIDS2017, DNN, explainable AI*

Received: 31-01-2026 Accepted: 05-03-2026 Published: 12-03-2026

1. INTRODUCTION

To identify malicious activity, cybersecurity systems frequently use deep learning and standard machine learning models such as SVM, KNN, Random Forest, Naïve Bayes, and Multilayer Perceptron (MLP). These methods classify network traffic and identify issues by examining historical data. They are able to see risks that they are previously aware of, but they find it difficult to handle zero-day assaults, high-dimensional data, and rapidly emerging cyberattack patterns. Security professionals find it difficult to comprehend how AI models operate and react to emerging risks as many of them are "black boxes."

Many machine learning and deep learning models are used to provide a comprehensive and adaptable cyber-attack prediction framework in order to overcome these issues. The system uses standard datasets such as NSL-KDD, CICIDS2017, CICDDOS2019, and X-IIOTID and applies techniques including Random Forest, SVM, KNN, MLP, Logistic Regression, Naïve Bayes, and DNN. The system is equitable for learning and generalization because of preprocessing, standardization, and data balance. Explainable AI (XAI) solutions clarify and open up feature importance, which helps analysts better comprehend and trust model results.

This study expands on the concept of a hybrid stacking model that uses Random Forest, KNN, and MLP classifiers to increase the accuracy and resilience of cyberattack datasets to various assaults. An ensemble approach makes it simpler to identify and categorize challenging assault scenarios by utilizing predictions from several models. Users may interact with and make predictions about the datasets in real time using the Flask-based web interface. By highlighting crucial facts and displaying decision patterns, explainable AI simplifies complex concepts. With this unique innovation, cyberattacks in modern digital infrastructures may now be detected in a high-performance, scalable, and intelligible manner.

2. LITERATURE SURVEY

a) Critical Role of Cyber Security in Global Economy

In many regions, the advancements in information technology have increased the threat to national security. Throughout military history, there has always been a significant power differential between opposing forces. It's always been this way. Changes in the economy, new technology, or just the number of parties engaged can all contribute to the uneven distribution of resources. The importance of information operations on contemporary battlefields is growing. The same weapons are used by all of the warriors in this arena: computers.

Despite the widespread presence of computers and network connections, cyberspace remains a battlefield for ongoing wars. The laws governing this dispute are still being developed and are being determined by international law. Protecting critical institutions and infrastructures that are critical to the economy and national security is equally as crucial as acquiring or maintaining sensitive information. The stakes are really high. Today's presentations will contextualize the importance of cyber security in safeguarding critical infrastructure and its impact on economic security. This relates to today's scheduled presentations.

b) From information security to cyber security

Information security and cyber security are frequently confused. Despite their overlap, this study argues that information security and cyber security are separate concepts. According to the report, cyber security safeguards persons as well as other objects and information resources. Human factors in information security primarily relate to the roles that individuals play in protecting data. Cybersecurity is much more crucial since individuals may become the targets of cyberattacks or unintentionally assist with them. Since it is our responsibility to protect vulnerable populations, like children, this new facet has ethical ramifications for society.

c) Solar Winds Hack: In-Depth Analysis and Countermeasures

Today's organizations are particularly susceptible to cyberattacks because of their heavy reliance on technology. Since technology became widely utilized, cyberattacks have increased in frequency and posed greater risks. The subject of this tale is SolarWinds, which was recently the target of one of the largest cyberattacks. In addition, this article discusses supply chains in general, how hackers can attack them, and the consequences for those impacted. The article concludes with a set of recommendations for preventing such attacks in the future. We conducted extensive online research to obtain the facts. We've seen that supply chain hackers usually look for minor flaws in the system or even make their own holes to enter and target every supplier in the chain. To protect sensitive or confidential data, all firms must have a very strong security system.

d) Analyzing WannaCry Ransomware Considering the Weapons and Exploits

As ransomware grows in popularity, its creators are exploiting our anxieties. The sharp increase in ransomware assaults indicates that hacking tools are being merged and that ransomware-as-a-service (RaaS) is becoming more widespread. The study of the notorious WannaCry ransomware, one of the most widespread and destructive viruses of 2017, is discussed in this article. To understand WannaCry's multi-phased execution, including deployment, installation, destruction, and command-and-control, the anatomy of ransomware assaults is examined. Many hacking weapon components are used in the WannaCry execution chain. WannaCry incorporates a robust encryption method and a key structure in addition to embedding the binary in the resource area for multi-phased execution. A network analysis of WannaCry's exploits and a reverse engineering analysis of each component provide light on the program's internal architecture. The research's conclusions improve current security measures and guide future defensive strategies.

e) Grand Challenge: Applying Artificial Intelligence and Machine Learning to Cybersecurity

Because of the increasing number of attacks, cybersecurity is a major concern for all organizations. Threats to cybersecurity are becoming more serious and endangering our lives. Artificial intelligence (AI) and machine learning (ML) can help cyber analysts identify threats and offer guidance. Governments, corporations, and educational institutions worldwide must collaborate to encourage the use of AI and machine learning in cybersecurity.

3. METHODOLOGY

i) Proposed Work:

Systems that anticipate cyberattacks are improved by using a hybrid stacked ensemble model that integrates MLP, KNN, and RF classifiers. Both attack and traffic data are provided via benchmark cybersecurity datasets such NSL-KDD, CICIDS2017, CICDDOS2019, and X-IIOTID, which are used to train the models separately. By stacking the predictions of several underlying models, a meta-classifier can determine which conclusion is most correct for each scenario. As a result, the findings are more precise and relevant to a larger variety of attack scenarios.

Normalization, encoding, and shuffling are used to remove bias and ensure data consistency during training. To evaluate model predictions and identify the most important attack detection features, we utilize Explainable AI (XAI). People are more forthcoming and self-assured when automated cybersecurity decisions are simple to comprehend.

The system is based on a web application that makes use of Flask, allowing users to input test datasets and immediately view the results of their predictions. The framework's growth and practical applications are demonstrated via a web-based version. A strong, adaptable, and transparent framework for detecting cyberattacks with nearly perfect accuracy and proactive cybersecurity defensive systems is made possible by the hybrid layered model, explainability, and real-time deployment.

ii) System Architecture:

The proposed cyber-attack prediction approach is a multi-stage pipeline that combines explainable AI, deep learning, and machine learning. The foundation is provided by benchmark cyber-attack datasets NSL-KDD, CICIDS2017, CICDDOS2019, and X-IIOTID. Label encoding, normalization, and data shuffling are examples of data preparation techniques used to preserve consistency and get rid of bias before to training. To identify and predict likely attack types on processed data, ML/DL techniques such as Random Forest, KNN, SVM, MLP, Logistic Regression, Naïve Bayes, and DNN were employed. The predictions are improved for increased accuracy and durability using a hybrid stacking model that combines MLP, KNN, and Random Forest. Cybersecurity experts may use a Flask-based web interface to enter test data and view the results. Incorporating SHAP (SHapley Additive exPlanations) for explainability facilitates transparent, data-driven security decisions and offers insights on feature relevance.

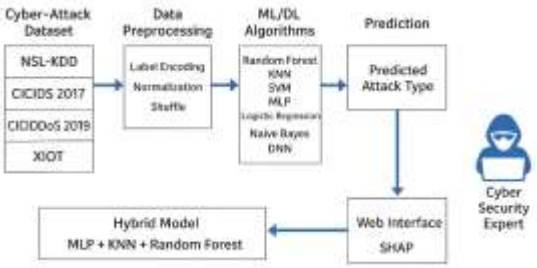


Fig 1: proposed architecture

iii) Modules:

a) Data Collection Module

- Gathers attack and normal traffic statistics from NSL-KDD, CICIDS2017, CICDDOS2019, and X-IIOTID benchmark datasets.
- Diversifies data to increase model generalization and resilience.

b) Data Preprocessing Module

- Label encoding, normalization, and data shuffling clean and normalize incoming data.
- Removes discrepancies and optimizes training and testing datasets.

c) Model Training Module

- ML/DL algorithms like Random Forest, KNN, SVM, MLP, Logistic Regression, Naïve Bayes, and DNN are trained on preprocessed data.
- Finds strong cyber-attack predictors by evaluating model performance.

d) Hybrid Stacked Model Module

- Stacks MLP, KNN, and Random Forest classifiers.
- Combines the basic model predictions to improve accuracy and eliminate false positives.

e) Explainable AI (XAI) Module

- Interprets model predictions using SHAP.
- Provides transparency and decision-making comprehension with feature significance analysis.

f) Web Interface Module

- Users or cybersecurity professionals may input test datasets and view real-time forecasts using a Flask interface.
- Displays attack categories and explanations for proactive security.

iv) Algorithms:

1. Random Forest (RF):

This ensemble learning technique builds many decision trees during training and aggregates their predictions to improve stability and accuracy. It can handle high-dimensional network data because it minimizes overfitting by averaging the results of separate trees. Random Forest predicts cyberattacks by accurately identifying different attack types and classifying intricate traffic patterns.

2. K-Nearest Neighbor (KNN):

KNN is a straightforward yet effective classification technique that determines a sample's label by looking at the majority class of its closest neighbors. It calculates the similarity between data points using distance metrics like the Manhattan or Euclidean distance. By comparing fresh samples to existing examples of network activity, KNN aids in the detection of abnormalities and the identification of assaults in cybersecurity.

3. Support Vector Machine (SVM):

SVM is a technique for supervised learning that uses an ideal hyperplane to divide data points into groups. Using kernel functions, it performs well in both linear and non-linear classification. SVM is particularly good at differentiating between malicious and legitimate traffic in cyberattack detection, particularly when the data has distinct boundaries.

4. Multilayer Perceptron (MLP):

A feedforward neural network with several layers of linked nodes is called a multilayer perceptron (MLP). In order to enable the model to learn intricate, non-linear correlations, each layer uses activation functions to alter the input data. By extracting deep feature representations from network data, MLP effectively detects complex attack patterns for cyberattack detection.

5. Logistic Regression (LR):

The statistical model known as logistic regression (LR) is employed for both binary and multi-class classification. It uses a sigmoid activation function to forecast the likelihood of an event (such as an assault or a typical occurrence). In this paradigm, LR provides quick and comprehensible predictions for fundamental intrusion detection, acting as a baseline model for comparing more complex algorithms.

6. Naïve Bayes (NB):

Predicated on the Bayes theorem, Naïve Bayes is a probabilistic classifier that presumes feature independence. Despite its simplicity, it is quite effective for real-time detection and works well on huge datasets. By calculating the probability of various attack types using past data, cyber-attack prediction rapidly classifies traffic.

7. Deep Neural Network (DNN):

This deep learning model can automatically extract high-level characteristics from unprocessed input data since it is made up of several hidden layers. It can identify complex and changing cyberthreats because it can learn complicated patterns and correlations. DNN helps this system achieve excellent accuracy and flexibility across a variety of datasets.

8. Hybrid Stacked Model (MLP + KNN + RF):

By using a stacking process, the Hybrid Stacked Model combines the advantages of Random Forest, KNN, and MLP. A meta-classifier integrates the predictions made by each base model to create the final result. This ensemble methodology is the most dependable method for predicting cyberattacks in real time since it improves resilience, reduces false detections, and achieves near-perfect accuracy.

4. EXPERIMENTAL RESULTS

NSL-KDD, CICIDS2017, CICDDOS2019, and X-IIOTID are four benchmark datasets that we utilized to evaluate the efficacy of several machine learning and deep learning algorithms for cyberattack prediction. Each dataset underwent preprocessing steps like as label encoding, normalization, and shuffling to ensure that the training was equitable and balanced. We trained and assessed the accuracy, precision, and dependability of the different models, including SVM, KNN, Random Forest, MLP, Logistic Regression, Naïve Bayes, and DNN. Out of all the models, the hybrid stacked model (MLP + KNN + Random Forest) performed the best. It achieved 100% accuracy on the CICIDS2017, CICDDOS2019, and X-IIOTID datasets and 99.90% accuracy on the NSL-KDD dataset. By highlighting the variables that had the most impact on predictions, Explainable AI (SHAP) greatly simplified the model. These findings demonstrate that the proposed hybrid model performs better at providing a robust, precise,

International Journal of Engineering Research and Science & Technology

and understandable cyberattack detection system that can operate in various and dynamic network environments.

Accuracy: The ability of a test to differentiate between healthy and sick instances is a measure of its accuracy. Find the proportion of analysed cases with true positives and true negatives to get a sense of the test's accuracy. Based on the calculations:

Accuracy = TP + TN /(TP + TN + FP + FN)

$$Accuracy = \frac{(TN + TP)}{T}$$

Precision: The accuracy rate of a classification or number of positive cases is known as precision. Accuracy is determined by applying the following formula:

Precision = True positives/ (True positives + False positives) = TP/(TP + FP)

$$\Pr e\,cision = \frac{TP}{(TP + FP)}$$

Recall: The recall of a model is a measure of its capacity to identify all occurrences of a relevant machine learning class. A model's ability to detect class instances is shown by the ratio of correctly predicted positive observations to the total number of positives.

$$Recall = \frac{TP}{(FN + TP)}$$

mAP: One ranking quality statistic is Mean Average Precision (MAP). It takes into account the quantity of pertinent suggestions and where they are on the list. The arithmetic mean of the Average Precision (AP) at K for each user or query is used to compute MAP at K.

$$mAP = \frac{1}{n}\sum_{k=1}^{k=n} AP_k$$

$$AP_k = \text{the AP of class } k$$

$$n = \text{the number of classes}$$

F1-Score: A high F1 score indicates that a machine learning model is accurate. Improving model accuracy by integrating recall and precision. How often a model gets a dataset prediction right is measured by the accuracy statistic..

$$F1 = 2 \cdot \frac{(Recall \cdot \Pr e\,cision)}{(Recall + \Pr e\,cision)}$$

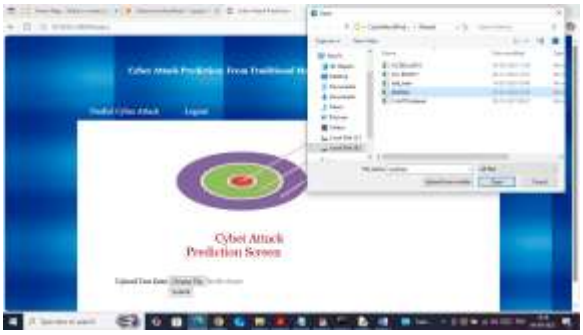


Fig 2 uploading test data file



Fig 3 results

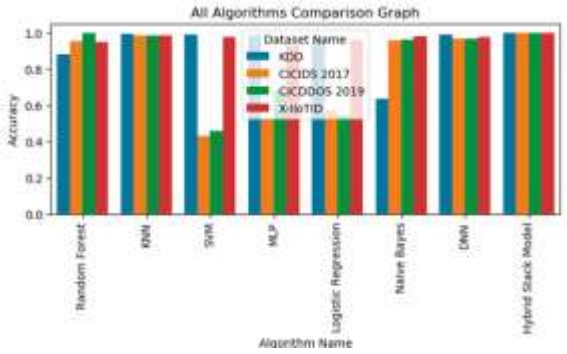


Fig 4 Accuracy graph

	Dataset Name	Algorithm Name	Accuracy
0	KDD	Random Forest	0.880250
1	CICIDS 2017	Random Forest	0.954596
2	CICDDOS 2019	Random Forest	1.000000
3	X-IIoTID	Random Forest	0.950000
4	KDD	KNN	0.993250
5	CICIDS 2017	KNN	0.983389
6	CICDDOS 2019	KNN	0.984981
7	X-IIoTID	KNN	0.984000
8	KDD	SVM	0.988250
9	CICIDS 2017	SVM	0.429679
10	CICDDOS 2019	SVM	0.458073
11	X-IIoTID	SVM	0.973500
12	KDD	MLP	0.986250
13	CICIDS 2017	MLP	0.521595

Table 1 all algorithms accuracy on each dataset

5. CONCLUSION

Because cyberattacks target digital infrastructures and are becoming more complex and diversified, they are still exceedingly difficult to detect. The evaluation of a number of deep learning and machine learning algorithms on the NSL-KDD, CICIDS2017, CICDDOS2019, and X-IIOTID benchmark datasets showed significant performance variability, highlighting the need for robust prediction models. Of the techniques examined, the hybrid stacking model—which combines MLP, KNN, and Random Forest classifiers—was the most accurate. It received 100% on the CICIDS2017, CICDDOS2019, and X-IIOTID datasets and 99.90% on the NSL-KDD dataset. This demonstrates that employing ensemble methods to identify various patterns in non-uniform datasets is effective. Additionally, by employing Explainable AI techniques, we were able to comprehend the contributions of various aspects, which clarified and simplified the situation. Making informed judgments in cybersecurity requires this. The results show that hybrid models, which include several learning paradigms, outperform standalone algorithms and offer almost perfect detection skills in a variety of cyberattack scenarios. These findings emphasize the necessity of combining machine learning, deep learning, and generative AI to improve prediction accuracy and strengthen systems against emerging cyberthreats. They also provide a reliable benchmark for selecting high-performance detection methods. The study shows a trend toward cyberattack prediction systems that are more adaptable and understandable.

6. FUTURE SCOPE

Real-time streaming data from live networks may be added to this architecture for forecasting cyberattacks in the future. This would enable prompt identification and response to current threats. By re-creating attack patterns that have never been seen before or that occur on the same day as the attack for model retraining, integrating Generative AI (GenAI) can further improve flexibility. Federated learning will enable several companies to train their models in a distributed, secure manner without jeopardizing data privacy. Additionally, the system will become more scalable and effective with the use of cloud deployment and automated incident response tools. The gadget may potentially develop into an intelligent cyber defense assistant that provides security professionals with concise justifications and recommendations on how to thwart attacks before they materialize.

REFERENCES

[1] G. S. Emile and M. Kala, ‘‘Critical role of cyber security in global economy,’’ Open J. Saf. Sci. Technol., vol. 13, no. 4, pp. 231–248, 2023, doi: 10.4236/ojsst.2023.134012.

[2] R. von Solms and J. van Niekerk, ‘‘From information security to cyber security,’’ Comput. Secur., vol. 38, pp. 97–102, Oct. 2013.

[3] J.W.GoodellandS.Corbet,‘‘Commoditymarketexposuretoenergyfirm distress: Evidence from the colonial pipeline ransomware Atta,’’ Finance Res. Lett., vol. 51, Jan. 2023, Art. no. 103329.

[4] R. Alkhadra, J. Abuzaid, M. AlShammari, and N. Mohammad, ‘‘Solar winds hack: In-depth analysis and countermeasures,’’ in Proc. 12th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT), Jul. 2021, pp. 1–7.

[5] Cobalt. (Jun. 20, 2024). 11 Biggest Cybersecurity Attacks in History. [Online]. Available: https://www.cobalt.io/blog/biggest-cybersecurity attacks-in-history

[6] D.-Y. Kao, S.-C. Hsiao, and R. Tso, ‘‘Analyzing WannaCry ransomware considering the weapons and exploits,’’ in Proc. 21st Int. Conf. Adv. Commun. Technol. (ICACT), Feb. 2019, pp. 1098–1107.

[7] K. Bresniker, A. Gavrilovska, J. Holt, D. Milojicic, and T. Tran, ‘‘Grand challenge: Applying artificial intelligence and machine learning to cybersecurity,’’ Computer, vol. 52, no. 12, pp. 45–52, Dec. 2019, doi: 10.1109/MC.2019.2942584.

[8] M. Husák, J. Komárková, E. Bou-Harb, and P. Celeda, ‘‘Survey of attack projection, prediction, and forecasting in cyber security,’’ IEEE Commun. Surveys Tuts., vol. 21, no. 1, pp. 640–660, 1st Quart., 2019.

[9] N. Mohamed, ‘‘Current trends in AI and ML for cybersecurity: A state of-the-art survey,’’ Cogent Eng., vol. 10, no. 2, pp. 1–11, Dec. 2023, doi: 10.1080/23311916.2023.2272358.

[10] L. Chan, I. Morgan, H. Simon, F. Alshabanat, D. Ober, J. Gentry, D. Min, and R. Cao, ‘‘Survey of AI in cybersecurity for information technology management,’’ in Proc. IEEE Technol. Eng. Manage. Conf. (TEMSCON), Jun. 2019, pp. 1–8.

[11] G. Disterer, ‘‘ISO/IEC 27000, 27001 and 27002 for information security management,’’ J. Inf. Secur., vol. 4, no. 2, pp. 92–100, 2013.
[12] J. H. Li, ‘‘Cyber security meets artificial intelligence: A survey,’’ Fron tiers Inf. Technol. Electron. Eng., vol. 19, no. 12, pp. 1462–1474, 2018, doi: 10.1631/FITEE.1800573.
[13] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, ‘‘Cybersecurity data science: An overview from machine learning perspective,’’ J. Big Data., vol. 7, pp. 1–29, May 2020, doi: 10.1186/s40537-020-00318-5.
[14] D.Aggarwal,D.Sharma,andA.B.Saxena,‘‘RoleofAIincybersecurity through anomaly detection and predictive analysis,’’ J. Informat. Educ. Res., vol. 3, no. 2, pp. 1–12, 2023.
[15] G. Srivastava, R. H. Jhaveri, S. Bhattacharya, S. Pandya, Rajeswari, P. K. R. Maddikunta, G. Yenduri, J. G. Hall, M. Alazab, and T. R. Gadekallu, ‘‘XAI for cybersecurity: State of the art, challenges, open issues and future directions,’’ 2022, arXiv:2206.03585.
[16] I. H. Sarker, M. H. Furhad, and R. Nowrozy, ‘‘AI-driven cybersecurity: An overview, security intelligence modeling and research directions,’’ Social Netw. Comput. Sci., vol. 2, no. 3, pp. 1–18, May 2021.
[17] D. Ucci, L. Aniello, and R. Baldoni, ‘‘Survey of machine learning tech niques for malware analysis,’’ Comput. Secur., vol. 81, pp. 123–147, Mar. 2019.
[18] D. Kwon, H. Kim, J. Kim, S. C. Suh, I. Kim, and K. J. Kim, ‘‘A survey of deep learning-based network anomaly detection,’’ Cluster Comput., vol. 22, no. S1, pp. 949–961, Jan. 2019.
[19] R. A. Nafea and M. A. Almaiah, ‘‘Cyber security threats in cloud: Literature review,’’ in Proc. Int. Conf. Inf. Technol. (ICIT), Jul. 2021, pp. 779–786.
[20] A.KuppaandN.-A.Le-Khac,‘‘Blackboxattacksonexplainableartificial intelligence(XAI) methods in cyber security,’’ in Proc. Int. Joint Conf. Neural Netw. (IJCNN), Jul. 2020, pp. 1–8.
[21] K. D. Ahmed and S. Askar, ‘‘Deep learning models for cyber security in IoT networks: A review,’’ Int. J. Sci. Bus., vol. 5, no. 3, pp. 61–70, Jan. 2021.
[22] J. Gerlings, A. Shollo, and I. Constantiou, ‘‘Reviewing the need for explainable artificial intelligence (xAI),’’ 2020, arXiv:2012.01007.
[23] G. Jaswal, V. Kanhangad, and R. Ramachandra, AI and Deep Learning in Biometric Security: Trends Potential and Challenges. Boca Raton, FL, USA: CRCPress, 2021.
[24] C. Rudin, ‘‘Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead,’’ 2018, arXiv:1811.10154.
[25] Marella, V. C., Veluru, S. R., & Erukude, S. T. (2025, September). FedOnco-Bench: A Reproducible Benchmark for Privacy-Aware Federated Tumor Segmentation with Synthetic CT Data. In 2025 4th International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) (pp. 870-876). IEEE..
[26] A.Bandi, P. V. S. R. Adapa, and Y. E. V. P. K. Kuchi, ‘‘The power of gen erative AI: A review of requirements, models, input–output formats, eval uation metrics, and challenges,’’ Future Internet, vol. 15, no. 8, Jul. 2023. [Online]. Available: https://www.mdpi.com/1999-5903/15/8/260
[27] J. Babcock and R. Bali, Generative AI With Python and Tensorflow 2: Create Images, Text, and Music With VAEs, GANs, LSTMs, Transformer Models. Birmingham, U.K.: Packt, 2021.
[28] ChatGPT. Accessed: Jun. 22, 2023. [Online]. Available: https://chat.openai.com/
[29] Dall·eNowAvailableWithoutWaitlist. Accessed:Jun. 22,2023.[Online]. Available: https://openai.com/blog/dall-e-now-available-without-waitlist
[30] B. Hitaj, P. Gasti, G. Ateniese, and F. Perez-Cruz, ‘‘PassGAN: A deep learning approach for password guessing,’’ 2017, arXiv:1709.00440.