```
@article{wang2025vahmse,
  title={VAHMSE: an efficient anomaly detection model based on variational autoencoder and heterogeneous multi-stacking ensemble learning},
  author={Wang, Rui and Li, Jiayao},
  journal={Applied Intelligence},
  volume={55},
  number={13},
  pages={1--26},
  year={2025},
  publisher={Springer}
}
@inproceedings{hamada2024review,
  title={A review: State-of-the-art of integrating AI models with moving-target defense for enhancing IoT networks security},
  author={Hamada, Amal and Hassan, Salwa Mohamed and Samy, Salma and Azab, Mohamed and Fathalla, Efat},
  booktitle={2024 IEEE 15th Annual Ubiquitous Computing, Electronics \& Mobile Communication Conference (UEMCON)},
  pages={108--114},
  year={2024},
  organization={IEEE}
}
@article{bhayo2021time,
  title={A time-efficient approach toward DDoS attack detection in IoT network using SDN},
  author={Bhayo, Jalal and Jafaq, Riaz and Ahmed, Awais and Hameed, Sufian and Shah, Syed Attique},
  journal={IEEE Internet of Things Journal},
  volume={9},
  number={5},
  pages={3612--3630},
  year={2021},
  publisher={IEEE}
}
@article{wang2025ensemble,
  title={Ensemble Intrusion Detection Based on Heterogeneous Data Augmentation and Knowledge Distillation},
  author={Wang, Longhui and Zhou, Xu and Ding, Weiping and Chen, Lifang and Dai, Qi},
  journal={IEEE Transactions on Industrial Informatics},
  year={2025},
  publisher={IEEE}
}
@misc{bhat2022gradient,
  title={Gradient backpropagation based feature attribution to enable explainable-ai on the edge. In 2022 IFIP/IEEE 30th International Conference on Very Large Scale Integration (VLSISoC)},
  author={Bhat, Ashwin and Assoa, Adou Sangbone and Raychowdhury, Arijit},
  year={2022},
  publisher={IEEE}
}
@article{zhang2025moving,
  title={Moving target defense meets artificial intelligence-driven network: A comprehensive survey},
  author={Zhang, Tao and Kong, Fanyu and Deng, Dongshang and Tang, Xiangyun and Wu, Xuangou and Xu, Changqiao and Zhu, Liehuang and Liu, Jiqiang and Ai, Bo and Han, Zhu and others},
  journal={IEEE Internet of Things Journal},
  year={2025},
  publisher={IEEE}
}
@inproceedings{siddique2025explainable,
  title={Explainable AI-Guided Efficient Approximate DNN Generation for Multi-Pod Systolic Arrays},
  author={Siddique, Ayesha and Khalil, Khurram and Hoque, Khaza Anuarul},
  booktitle={2025 26th International Symposium on Quality Electronic Design (ISQED)},
  pages={1--8},
  year={2025},
  organization={IEEE}
}
@article{hiari2025deep,
  title={A Deep Learning-Based Intrusion Detection System using Refined LSTM for DoS Attack Detection},
  author={Hiari, Mohammad and Alraba'nah, Yousef and Qaddara, Iyas},
  journal={Engineering, Technology \& Applied Science Research},
  volume={15},
  number={4},
  pages={25627--25633},
  year={2025}
}
@article{sharafaldin2018toward,
  title={Toward generating a new intrusion detection dataset and intrusion traffic characterization.},
  author={Sharafaldin, Iman and Lashkari, Arash Habibi and Ghorbani, Ali A and others},
  journal={ICISSp},
  volume={1},
  number={2018},
  pages={108--116},
  year={2018}
}
@inproceedings{moustafa2015unsw,
  title={UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)},
  author={Moustafa, Nour and Slay, Jill},
  booktitle={2015 military communications and information systems conference (MilCIS)},
  pages={1--6},
  year={2015},
  organization={IEEE}
}
@article{ferrag2022edge,
  title={Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning},
  author={Ferrag, Mohamed Amine and Friha, Othmane and Hamouda, Djallel and Maglaras, Leandros and Janicke, Helge},
  journal={{IEEE} Access},
  volume={10},
  pages={40281--40306},
  year={2022},
  publisher={IEEE}
}
@inproceedings{imani2024integrating,
  title={Integrating CNN-LSTM Networks with Statistical Filtering Techniques for Intelligent IoT Intrusion Detection},
  author={Imani, Fatemeh and Kargar, Masoud and Assadzadeh, Alireza and Bayani, Ali},
  booktitle={2024 8th International Conference on Smart Cities, Internet of Things and Applications (SCIoT)},
  pages={189--195},
  year={2024},
  organization={IEEE}
}
@article{sharafaldin2018toward,
  title   = {Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization},
  author  = {Sharafaldin, Iman and Lashkari, Arash Habibi and Ghorbani, Ali A.},
  journal = {Proceedings of the International Conference on Information Systems Security and Privacy (ICISSP)},
  year    = {2018}
}

@article{lashkari2020characterization,
  title   = {Characterization of DDoS Attacks Using CIC-DDoS2019 Dataset},
  author  = {Lashkari, Arash Habibi and Draper-Gil, Gerard and Mamun, Md. S. I. and Ghorbani, Ali A.},
  journal = {Proceedings of the International Conference on Information Systems Security and Privacy (ICISSP)},
  year    = {2020}
```

```
}

@article{tavallaee2009detailed,
  title   ={A Detailed Analysis of the KDD CUP 99 Data Set},
  author  ={Tavallaee, Mahbod and Bagheri, Ebrahim and Lu, Wei and Ghorbani, Ali A.},
  journal ={Proceedings of the IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA)},
  year    ={2009}
}

@article{meidan2018nbaiot,
  title   ={N-BaIoT: Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders},
  author  ={Meidan, Yair and Bohadana, Michael and Shabtai, Asaf and Guarnizo, Juan and Ochoa, Martin and Tippenhauer, Nils Ole and Elovici, Yuval},
  journal ={IEEE Pervasive Computing},
  volume  ={17},
  number  ={3},
  pages   ={12--22},
  year    ={2018}
}

@article{goh2017dataset,
  title   ={A Dataset to Support Research in the Design of Secure Water Treatment Systems},
  author  ={Goh, Jonathan and Adepu, Sridhar and Tan, Mian and Lee, Zhi Wei},
  journal ={Proceedings of the International Conference on Prognostics and Health Management (ICPHM)},
 year   = {2017}
}

@article{ahmad2017wadi,
 title   = {A Testbed and Dataset for Cyber-Physical Intrusion Detection},
 author  = {Ahmad, Charan and Adepu, Sridhar and Mathur, Aditya},
 journal = {Proceedings of the International Conference on Prognostics and Health Management (ICPHM)},
 year   = {2017}
}

@techreport{claise2004cisco,
 title      = {Cisco Systems NetFlow Services Export Version 9},
 author     = {Claise, Benoit},
 institution = {IETF},
 number     = {RFC 3954},
 year       = {2004}
}

@inproceedings{su2019robust,
 title    = {Robust Anomaly Detection for Multivariate Time Series through Stochastic Recurrent Neural Network},
 author   = {Su, Ya and Zhao, Yungang and Niu, Chenfeng and Liu, Rong and Sun, Wei and Pei, Dan},
 booktitle = {Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD)},
 pages={2828--2837},
 year     = {2019}
}

@inproceedings{lundberg2017unified,
 title={A Unified Approach to Interpreting Model Predictions},
 author={Lundberg, Scott M. and Lee, Su-In},
 booktitle={Advances in Neural Information Processing Systems},
 year={2017}
}

@inproceedings{ribeiro2016should,
 title={“Why Should I Trust You?” Explaining the Predictions of Any Classifier},
 author={Ribeiro, Marco Tulio and Singh, Sameer and Guestrin, Carlos},
 booktitle={KDD},
 year={2016}
}

@article{jacovi2020towards,
 title={Towards Faithfully Interpretable NLP Systems: How Should We Define and Evaluate Faithfulness?},
 author={Jacovi, Alon and Goldberg, Yoav},
 journal={ACL},
 year={2020}
}

@article{jain2019attention,
 title={Attention Is Not Explanation},
 author={Jain, Sarthak and Wallace, Byron C.},
 journal={NAACL},
 year={2019}
}

@article{serrano2019attention,
 title={Is Attention Interpretable?},
 author={Serrano, Sofia and Smith, Noah A.},
 journal={ACL},
 year={2019}
}

@article{ring2019flow,
 title={Flow-based Benchmark Data Sets for Intrusion Detection},
 author={Ring, Markus and others},
 journal={European Conference on Cyber Warfare and Security},
 year={2019}
}

@article{jain2019attention-x,
 title={Attention is not explanation},
 author={Jain, Sarthak and Wallace, Byron C},
 journal={arXiv preprint arXiv:1902.10186},
 year={2019}
}
```

```
@article{chen2016hybrid,
  author    = {Chen, C and Chen, Hsin-Chiao},
  title     = {A Hybrid Approach Combining Rule-Based And Anomaly-Based Detection Against DDoS Attacks},
  journal   = {International Journal Of Network Security Its Applications},
  year      = {2016}
}

@inproceedings{zhang2009prediction,
  author    = {Zhang, Guoxing and Jiang, Shengming and Wei, Gang and Guan, Quansheng},
  title     = {A prediction-based detection algorithm against distributed denial-of-service attacks},
  booktitle = {Proceedings of the 2009 international conference on wireless communications and mobile computing},
  year      = {2009}
}

@article{chen2009new,
  author    = {Chen, Chin-Ling},
  title     = {A New Detection Method for Distributed Denial-of-Service Attack Traffic based on Statistical Test},
  journal   = {J. Univers. Comput. Sci.},
  year      = {2009}
}

@article{mirkovic2005d,
  author    = {Mirkovic, Jelena and Reiher, Peter},
 title    = {D-WARD: a source-end defense against flooding denial-of-service attacks},
 journal  = {IEEE Transactions on Dependable and Secure Computing},
 year     = {2005}
}

@article{feng2023explainable,
 author   = {Feng, Yebo and Li, Jun and Sisodia, Devkishen and Reiher, Peter},
 title    = {On explainable and adaptable detection of distributed denial-of-service traffic},
 journal  = {IEEE Transactions on Dependable and Secure Computing},
 year     = {2023}
}

@techreport{cloudflare2025hyper,
 author   = {{Cloudflare}},
 title    = {Hyper-volumetric DDoS attacks skyrocket: Cloudflare's 2025 Q2 DDoS threat
report},
 type     = {Technical Report},
 year     = {2025}
}

@techreport{akamai2024modern,
 author   = {{Akamai}},
 title    = {Why Modern Layer 7 DDoS Protections Are Crucial for Web Security in 2024},
 type     = {Technical Report},
 year     = {2024}
}
```

```
@article{udofot2024advanced,
  author    = {Udofot, Akpan Itoro and Oluseyi, Omotosho Moses and Bassey, Edim},
  title     = {Advanced Machine Learning--A Comprehensive Survey and New Research Directions},
  journal   = {International Journal of Advanced Engineering and Management},
  year      = {2024}
}

@inproceedings{roshan2022using,
  author    = {Roshan, Khushnaseeb and Zafar, Aasim},
  title     = {Using kernel shap xai method to optimize the network anomaly detection model},
  booktitle = {2022 9th International Conference on Computing for Sustainable Global Development (INDIACom)},
  year      = {2022}
}

@article{okporokpo2025detection,
  author    = {Okporokpo, Oghenetejiri and Olajide, Funminiyi and Ajienka, Nemitari and others},
  title     = {Detection of DDoS Cyberattack Using a Hybrid Trust-Based Technique for Smart Home Networks},
  journal   = {International Journal of Advanced Computer Science \& Applications},
  year      = {2025}
}
```

```
@article{akgun2022new,
  author    = {Akgun, Devrim and Hizal, Selman and Cavusoglu, Unal},
  title     = {A new DDoS attacks intrusion detection model based on deep learning for cybersecurity},
  journal   = {Computers \& Security},
  year      = {2022}
}

@article{alghazzawi2021efficient,
  author    = {Alghazzawi, Daniyal and Bamasag, Omaimah and Ullah, Hayat and Asghar, Muhammad Zubair},
  title     = {Efficient detection of DDoS attacks using a hybrid deep learning model with improved feature selection},
  journal   = {Applied Sciences},
  year      = {2021}
}

@inproceedings{baral2024adaptive,
  author    = {Baral, Sudipto and Saha, Sajal and Haque, Anwar},
  title     = {An Adaptive End-to-End IoT Security Framework Using Explainable AI and LLMs},
  booktitle = {2024 IEEE 10th World Forum on Internet of Things (WF-IoT)},
  year      = {2024}
}

@article{ahsan2025explainable,
  author    = {Ahsan, Shakil Ibne and Legg, Phil and Alam, SM Iftekharul},
  title     = {An explainable ensemble-based intrusion detection system for software-defined vehicle ad-hoc networks},
  journal   = {Cyber Security and Applications},
  year      = {2025}
}

@article{wali2025explainable,
  author    = {Wali, Syed and Farrukh, Yasir Ali and Khan, Irfan},
  title     = {Explainable AI and random forest based reliable intrusion detection system},
  journal   = {Computers \& Security},
  year      = {2025}
}

@article{dilip2025detecting,
  author    = {Dilip, Kumar and Yashwant, Kumar},
  title     = {Detecting and Mitigating DDoS Attacks: The Role of AI and Machine Learning},
  journal   = {International Journal of Trend in Scientific Research and Development},
  year      = {2025}
}

@article{kavitha2024machine,
  author    = {Kavitha, D and Ramalakshmi, R},
  title     = {Machine learning-based DDOS Attack Detection and Mitigation in SDNs for IoT environments},
  journal   = {Journal of the Franklin Institute},
  year      = {2024}
}
```

```
@inproceedings{ping2024study,
  author    = {Ping, Zhe and Jiao, Dingyang},
  title     = {A Study on the Application of Artificial Intelligence in DDoS Attack Defense: A Literature Review},
  booktitle = {Proceedings of the 2024 4th International Conference on Big Data, Artificial Intelligence and Risk Management},
  year      = {2024}
}

@article{thudumu2020comprehensive,
  author    = {Thudumu, Srikanth and Branch, Philip and Jin, Jiong and Singh, Jugdutt},
  title     = {A comprehensive survey of anomaly detection techniques for high dimensional big data},
  journal   = {Journal of big data},
  year      = {2020}
}

@misc{jadhav_edge_survey,
  author    = {Jadhav, Sonali and Kulkarni, Arun},
  title     = {Comprehensive Survey on Detection of Anomalies in Edge Computing Network and Deep Learning Solutions},
  note      = {Preprint/Unpublished},
  year      = {2024}
}

@article{zamanzadeh2024deep,
  author    = {Zamanzadeh Darban, Zahra and Webb, Geoffrey I and Pan, Shirui and Aggarwal, Charu and Salehi, Mahsa},
  title     = {Deep learning for time series anomaly detection: A survey},
  journal   = {ACM Computing Surveys},
  year      = {2024}
}

@article{kohli2025comprehensive,
  author    = {Kohli, Mudita and Chhabra, Indu},
  title     = {A comprehensive survey on techniques, challenges, evaluation metrics and applications of deep learning models for anomaly detection},
  journal   = {Discover Applied Sciences},
  year      = {2025}
}

@article{mittal2023deep,
  author    = {Mittal, Meenakshi and Kumar, Krishan and Behal, Sunny},
  title     = {Deep learning approaches for detecting DDoS attacks: A systematic review},
  journal   = {Soft computing},
  year      = {2023}
}

@article{arreche2024exai,
  author    = {Arreche, Osvaldo and Guntur, Tanish R and Roberts, Jack W and Abdallah, Mustafa},
  title     = {E-xai: Evaluating black-box explainable ai frameworks for network intrusion detection},
 journal   = {IEEE Access},
 year     = {2024}
}

@techreport{bispo2025explainable,
 author    = {Bispo, Ivo Afonso},
 title     = {Explainable AI (XAI) for Cybersecurity: Intrusion Detection System (IDS)},
 institution = {Computer Science and Communication Research Center},
 year     = {2025}
}

@article{samed2025explainable, author    = {Samed, AL and Sagiroglu, Seref},
 title     = {Explainable artificial intelligence models in intrusion detection systems},
 journal   = {Engineering Applications of Artificial Intelligence},
 year = {2025}
}

@article{mittal2023ddosat,
 author    = {Mittal, Harsh and Saluja, Hitesh and Behal, Shubham},
 title     = {DDoS-AT-2022: a distributed denial of service attack dataset for evaluating DDoS defense system},
 journal   = {Proceedings of the Indian National Science Academy},
 year     = {2023}
}
```

```
@article{ouhssini2024deepdefend,
  author    = {Ouhssini, Mohamed and Afdel, Karim and Agherrabi, Elhafed and Akouhar, Mohamed and Abarda, Abdallah},
  title     = {DeepDefend: A comprehensive framework for DDoS attack detection and prevention in cloud computing},
  journal   = {Journal of King Saud University-Computer and Information Sciences},
  year      = {2024}
}

@article{kumar2025investigating,
  author    = {Kumar, Prashant and Kushwaha, Chitra and Sethi, Dimple and Ghosh, Debjani and Gupta, Punit and Vidyarthi, Ankit},
  title     = {Investigating the performance of multivariate LSTM models to predict the occurrence of Distributed Denial of Service (DDoS) attack},
  journal   = {PloS one},
  year      = {2025}
}

@article{anley2024robust,
  author    = {Anley, Mulualem Bitew and Genovese, Angelo and Agostinello, Davide and Piuri, Vincenzo},
  title     = {Robust DDoS attack detection with adaptive transfer learning},
  journal   = {Computers \& Security},
  year      = {2024}
}
```

```
@article{shaikh2025deep,

  author    = {Shaikh, Jamshed Ali and Wang, Chengliang and Sima, Muhammad Wajeeh Us and Arshad, Muhammad and Owais, Muhammad and Hassan, Dina SM and Alkanhel, Reem and Muthanna, Mohammed Saleh Ali},

  title     = {A deep Reinforcement learning-based robust Intrusion Detection System for securing IoMT Healthcare Networks},

  journal   = {Frontiers in Medicine},

  year      = {2025}

}


@article{arif2024dqqs,

  author    = {Arif, Fahim and Khan, Nauman Ali and Iqbal, Javed and Karim, Faten Khalid and Innab, Nisreen and Mostafa, Samih M and others},

  title     = {DQQS: Deep Reinforcement Learning based Technique for Enhancing Security and Performance in SDN-IoT Environments},

  journal   = {IEEE Access},

  year      = {2024}

}


@article{yungaicela2022flexible,

  author    = {Yungaicela-Naula, Noe M and Vargas-Rosales, Cesar and Pérez-Díaz, Jesús Arturo and Carrera, Diego Fernando},

  title     = {A flexible SDN-based framework for slow-rate DDoS attack mitigation by using deep reinforcement learning},

  journal   = {Journal of network and computer applications},

  year      = {2022}

}
```

```
@inproceedings{feng2020application,

  author    = {Feng, Yebo and Li, Jun and Nguyen, Thanh},

  title     = {Application-layer DDoS defense with reinforcement learning},

  booktitle = {2020 IEEE/ACM 28th International Symposium on Quality of Service (IWQoS)},

  year      = {2020}

}


@article{wei2023reconstruction,

  author    = {Wei, Yuanyuan and Jang-Jaccard, Julian and Sabrina, Fariza and Xu, Wen and
Camtepe, Seyit and Dunmore, Aeryn},

  title     = {Reconstruction-based lstm-autoencoder for anomaly-based ddos attack
detection over multivariate time-series data},

  journal   = {arXiv preprint},

  year      = {2023}

}


@article{phan2020deepguard,

  author    = {Phan, Trung V and Nguyen, Tri Gia and Dao, Nhu-Ngoc and Huong, Truong Thu
and Thanh, Nguyen Huu and Bauschert, Thomas},

  title     = {DeepGuard: Efficient anomaly detection in SDN with fine-grained traffic flow
monitoring},

  journal   = {IEEE Transactions on Network and Service Management},

  year      = {2020}

}


@article{batchu2024novel,
  author    = {Batchu, Raj Kumar and Bikku, Thulasi and Thota, Srinivasarao and Seetha, Hari and Ayoade, Abayomi Ayotunde},
  title     = {A novel optimization-driven deep learning framework for the detection of DDoS attacks},
  journal   = {Scientific Reports},
  year      = {2024}
}

@inproceedings{srilatha2022ddosnet,
  author    = {Srilatha, Doddi and Thillaiarasu, N},
  title     = {DDoSNet: A deep learning model for detecting network attacks in cloud computing},
  booktitle = {2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA)},
  year      = {2022}
}

@article{alzubi2024explainable,
  author    = {Alzu'bi, Ahmad and Albashayreh, Amjad and Abuarqoub, Abdelrahman and Alfawair, Mai AM},
  title     = {Explainable AI-Based DDoS Attacks Classification Using Deep Transfer Learning},
  journal   = {Computers, Materials \& Continua},
  year      = {2024}
}

@article{alfatemi2024advancing,
  author    = {Alfatemi, Ali and Rahouti, Mohamed and Amin, Ruhul and ALJamal, Sarah and Xiong, Kaiqi and Xin, Yufeng},
  title    = {Advancing ddos attack detection: A synergistic approach using deep residual neural networks and synthetic oversampling},
  journal  = {arXiv preprint},
  year     = {2024}
}

@inproceedings{sudar2021detection,
  author   = {Sudar, K Muthamil and Beulah, M and Deepalakshmi, P and Nagaraj, P and Chinnasamy, P},
  title    = {Detection of Distributed Denial of Service Attacks in SDN using Machine learning techniques},
  booktitle = {2021 international conference on Computer Communication and Informatics (ICCCI)},
  year     = {2021}
}

@inproceedings{kavitha2022machine-x,
  author   = {Kavitha, M and Suganthy, M and Biswas, Aniket and Srinivsan, R and Kavitha, R and Rathesh, A},
  title    = {Machine learning techniques for detecting ddos attacks in sdn},
  booktitle = {2022 International Conference on Automation, Computing and Renewable Systems (ICACRS)},
  year     = {2022}
}

@article{santos2020machine-x,
  author   = {Santos, Reneilson and Souza, Danilo and Santo, Walter and Ribeiro, Admilson and Moreno, Edward},
  title     = {Machine learning algorithms to detect DDoS attacks in SDN},
  journal   = {Concurrency and Computation: Practice and Experience},
  year      = {2020}
}

@article{ribeiro2023detecting-x,
  author    = {Ribeiro, Marcos Aurélio and Fonseca, Mauro Sergio Pereira and de Santi, Juliana},
  title     = {Detecting and mitigating DDoS attacks with moving target defense approach based on automated flow classification in SDN networks},
  journal   = {Computers \& Security},
  year      = {2023}
}

@inproceedings{sekar2023prediction-x,
  author    = {Sekar, R Raja and Jenny, Ardhala Mounika and Sreshta, Dubba and Vikas, M and Ajay, Dasari Badri Nageshwar and Ganesh, Mankena},
  title     = {Prediction of distributed denial of service attacks in SDN using machine learning techniques},
  booktitle = {2023 3rd International Conference on Intelligent Technologies (CONIT)},
  year      = {2023}
}

@article{alashhab2024enhancing-x,
  author    = {Alashhab, Abdussalam Ahmed and Zahid, Mohd Soperi and Isyaku, Babangida and Elnour, Asma Abbas and Nagmeldin, Wamda and Abdelmaboud, Abdelzahir and Abdullah, Talal Ali Ahmed and Maiwada, Umar Danjuma},
```

title = {Enhancing DDoS attack detection and mitigation in SDN using an ensemble online machine learning model},

journal = {IEEE Access},

year = {2024}

}

@inproceedings{kousar2021detection-x,

author = {Kousar, Heena and Mulla, Mohammed Moin and Shettar, Pooja and Narayan, DG},

title = {Detection of DDoS attacks in software defined network using decision tree},

booktitle = {2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT)},

year = {2021}

}

@article{kim2025secured,

author = {Kim, Song-Kyoo and Vong, Hou Cheng},

title = {Secured Network Architectures Based on Blockchain Technologies: A Systematic Review},

journal = {ACM Computing Surveys},

year = {2025}

}

@article{linhares2023sdntruth,

author = {Linhares, Tiago and Patel, Ahmed and Barros, Ana Luiza and Fernandez, Marcial},

title = {SDNTruth: innovative DDoS detection scheme for software-defined networks (SDN)},

```
  journal   = {Journal of Network and Systems Management},
  year      = {2023}
}

@article{thamilarasu2019towards,
  author    = {Thamilarasu, Geethapriya and Chawla, Shiven},
  title     = {Towards deep-learning-driven intrusion detection for the internet of things},
  journal   = {Sensors},
  year      = {2019}
}

@article{zhao2023cnn,
  author    = {Zhao, Junjie and Liu, Yongmin and Zhang, Qianlei and Zheng, Xinying},
  title     = {CNN-AttBiLSTM mechanism: a DDoS attack detection method based on attention mechanism and CNN-BiLSTM},
  journal   = {IEEE Access},
  year      = {2023}
}

@article{bensaoud2025optimized,
  author    = {Bensaoud, Ahmed and Kalita, Jugal},
  title     = {Optimized detection of cyber-attacks on IoT networks via hybrid deep learning models},
  journal   = {Ad Hoc Networks},
  year      = {2025}
}
```

```
@inproceedings{kim2024model,
  author    = {Kim, Dongmin and Park, Sunghyun and Choo, Jaegul},
  title     = {When model meets new normals: test-time adaptation for unsupervised time-series anomaly detection},
  booktitle = {Proceedings of the AAAI conference on artificial intelligence},
  year      = {2024}
}

@article{arulselvan2023retracted,
  author    = {Arulselvan, G and Rajaram, A},
  title     = {RETRACTED: Hybrid trust-based secure routing protocol for detection of routing attacks in environment monitoring over MANETs},
  journal   = {Journal of Intelligent \& Fuzzy Systems},
  year      = {2023}
}

@article{ahmadi2024trust,
  author    = {Ahmadi, Khatereh and Javidan, Reza},
  title     = {A Trust Based Anomaly Detection Scheme Using a Hybrid Deep Learning Model for IoT Routing Attacks Mitigation},
  journal   = {IET Information Security},
  year      = {2024}
}

@article{hekmati2024correlation,
  author    = {Hekmati, Arvin and Zhang, Jiahe and Sarkar, Tamoghna and Jethwa, Nishant and Grippo, Eugenio and Krishnamachari, Bhaskar},
 title    = {Correlation-aware neural networks for DDOS attack detection in IoT systems},
 journal  = {IEEE/ACM Transactions on Networking},
 year     = {2024}
}

@article{liu2023ddos,
 author   = {Liu, Zhenpeng and Wang, Yihang and Feng, Fan and Liu, Yifan and Li, Zelin and Shan, Yawei},
 title    = {A DDoS detection method based on feature engineering and machine learning in software-defined networks},
 journal  = {Sensors},
 year     = {2023}
}

@article{li2025ad2t,
 author   = {Li, Zezhong and Guo, Wei and An, Jianpeng and Wang, Qi and Mei, Yingchun and Juan, Rongshun and Wang, Tianshu and Li, Yang and Gao, Zhongke},
 title    = {AD2T: Multivariate Time Series Anomaly Detection with Association Discrepancy Dual-Decoder Transformer},
 journal  = {IEEE Sensors Journal},
 year     = {2025}
}

@article{dai2024sarad,
 author   = {Dai, Zhihao and He, Ligang and Yang, Shuanghua and Leeke, Matthew},
 title    = {SARAD: Spatial association-aware anomaly detection and diagnosis for multivariate time series},
  journal   = {Advances in Neural Information Processing Systems},
  year      = {2024}
}



@inproceedings{xu2018unsupervised,
  author    = {Xu, Haowen and Chen, Wenxiao and Zhao, Nengwen and Li, Zeyan and Bu, Jiahao and Li, Zhihan and Liu, Ying and Zhao, Youjian and Pei, Dan and Feng, Yang and others},
  title     = {Unsupervised anomaly detection via variational auto-encoder for seasonal kpis in web applications},
  booktitle = {Proceedings of the 2018 world wide web conference},
  year      = {2018}
}

@inproceedings{su2019robust-x,
  author    = {Su, Ya and Zhao, Youjian and Niu, Chenhao and Liu, Rong and Sun, Wei and Pei, Dan},
  title     = {Robust anomaly detection for multivariate time series through stochastic recurrent neural network},
  booktitle = {Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery \& data mining},
  year      = {2019}
}

@article{shen2020timeseries,
  author    = {Shen, Lifeng and Li, Zhuocong and Kwok, James},
  title     = {Timeseries anomaly detection using temporal hierarchical one-class network},
  journal   = {Advances in neural information processing systems},
  year      = {2020}
}

@inproceedings{audibert2020usad,
  author    = {Audibert, Julien and Michiardi, Pietro and Guyard, Frédéric and Marti, Sébastien and Zuluaga, Maria A},
  title     = {Usad: Unsupervised anomaly detection on multivariate time series},
  booktitle = {Proceedings of the 26th ACM SIGKDD international conference on knowledge discovery \& data mining},
  year      = {2020}
}

@article{shwartzziv2022tabular,
  author    = {Shwartz-Ziv, Ravid and Armon, Amitai},
  title     = {Tabular data: Deep learning is not all you need},
  journal   = {Information Fusion},
  year      = {2022}
}

@article{xu2021anomaly,
  author    = {Xu, Jiehui and Wu, Haixu and Wang, Jianmin and Long, Mingsheng},
  title     = {Anomaly transformer: Time series anomaly detection with association discrepancy},
  journal   = {arXiv preprint},
  year      = {2021}
```

```
}

@inproceedings{geiger2020tadgan,
  author    = {Geiger, Alexander and Liu, Dongyu and Alnegheimish, Sarah and Cuesta-Infante, Alfredo and Veeramachaneni, Kalyan},
  title     = {Tadgan: Time series anomaly detection using generative adversarial networks},
  booktitle = {2020 ieee international conference on big data (big data)},
  year      = {2020}
}

@inproceedings{mohammadi2023anomaly,
  author    = {Mohammadi, Mohammadreza and Shrestha, Rakesh and Sinaei, Sima and Salcines, Alberto and Pampliega, David and Clemente, Raul and Sanz, Ana Lourdes},
  title     = {Anomaly detection using lstm-autoencoder in smart grid: A federated learning approach},
  booktitle = {Proceedings of the 2023 7th International Conference on Cloud and Big Data Computing},
  year      = {2023}
}

@inproceedings{zhang2019deep,
  author    = {Zhang, Chuxu and Song, Dongjin and Chen, Yuncong and Feng, Xinyang and Lumezanu, Cristian and Cheng, Wei and Ni, Jingchao and Zong, Bo and Chen, Haifeng and Chawla, Nitesh V},
  title     = {A deep neural network for unsupervised anomaly detection and diagnosis in multivariate time series data},
  booktitle = {Proceedings of the AAAI conference on artificial intelligence},
  year      = {2019}
```

```
}

@inproceedings{sanap2023comprehensive,
  author    = {Sanap, Yogesh B and Aher, Pushpalata},
  title     = {A Comprehensive Survey On Detection And Mitigation Of DDoS Attacks Enabled With Deep Learning Techniques In Cloud Computing},
  booktitle = {2023 6th International Conference on Advances in Science and Technology (ICAST)},
  year      = {2023}
}

@article{liu2023real,
  author    = {Liu, Haitao and Wang, Haifeng},
  title     = {Real-time anomaly detection of network traffic based on CNN},
  journal   = {Symmetry},
  year      = {2023}
}

@article{arrieta2020explainable,
  author    = {Arrieta, Alejandro Barredo and Díaz-Rodríguez, Natalia and Del Ser, Javier and Bennetot, Adrien and Tabik, Siham and Barbado, Alberto and García, Salvador and Gil-López, Sergio and Molina, Daniel and Benjamins, Richard and others},
  title     = {Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI},
  journal   = {Information fusion},
  year      = {2020}
}
```

```
@article{mohammadi2017slicots,
 author    = {Mohammadi, Reza and Javidan, Reza and Conti, Mauro},
 title     = {Slicots: An sdn-based lightweight countermeasure for tcp syn flooding attacks},
 journal   = {IEEE Transactions on Network and Service Management},
 year      = {2017}
}

@inproceedings{dimolianis2021syn,
 author    = {Dimolianis, Marinos and Pavlidis, Adam and Maglaris, Vasilis},
 title     = {SYN flood attack detection and mitigation using machine learning traffic classification and programmable data plane filtering},
 booktitle = {2021 24th conference on innovation in clouds, internet and networks and workshops (ICIN)},
 year      = {2021}
}

@inproceedings{zha2020meta,
 author    = {Zha, Daochen and Lai, Kwei-Herng and Wan, Mingyang and Hu, Xia},
 title     = {Meta-AAD: Active anomaly detection with deep reinforcement learning},
 booktitle = {2020 IEEE International Conference on Data Mining (ICDM)},
 year      = {2020}
}

@inproceedings{baitieva2024supervised,
 author    = {Baitieva, Aimira and Hurych, David and Besnier, Victor and Bernard, Olivier},
 title     = {Supervised Anomaly Detection for Complex Industrial Images},
  booktitle = {Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition},
  year      = {2024}
}

@inproceedings{zhong2019graph,
  author    = {Zhong, Jia-Xing and Li, Nannan and Kong, Weijie and Liu, Shan and Li, Thomas H and Li, Ge},
  title     = {Graph convolutional label noise cleaner: Train a plug-and-play action classifier for anomaly detection},
  booktitle = {Proceedings of the IEEE/CVF conference on computer vision and pattern recognition},
  year      = {2019}
}

@article{xu2023rosas,
  author    = {Xu, Hongzuo and Wang, Yijie and Pang, Guansong and Jian, Songlei and Liu, Ning and Wang, Yongjun},
  title     = {Rosas: Deep semi-supervised anomaly detection with contamination-resilient continuous supervision},
  journal   = {Information Processing \& Management},
  year      = {2023}
}

@inproceedings{wolleb2022diffusion,
  author    = {Wolleb, Julia and Bieder, Florentin and Sandkühler, Robin and Cattin, Philippe C},
  title     = {Diffusion models for medical anomaly detection},
  booktitle = {International Conference on Medical image computing and computer-assisted intervention},
  year      = {2022}
}

@article{zhou2021feature,
  author    = {Zhou, Yingjie and Song, Xucheng and Zhang, Yanru and Liu, Fanxing and Zhu, Ce and Liu, Lingqiao},
  title     = {Feature encoding with autoencoders for weakly supervised anomaly detection},
  journal   = {IEEE Transactions on Neural Networks and Learning Systems},
  year      = {2021}
}

@article{chen2022supervised,
  author    = {Chen, Zhi and Duan, Jiang and Kang, Li and Qiu, Guoping},
  title     = {Supervised anomaly detection via conditional generative adversarial network and ensemble active learning},
  journal   = {IEEE Transactions on Pattern Analysis and Machine Intelligence},
  year      = {2022}
}

@inproceedings{schluter2022natural,
  author    = {Schlüter, Hannah M and Tan, Jeremy and Hou, Benjamin and Kainz, Bernhard},
  title     = {Natural synthetic anomalies for self-supervised anomaly detection and localization},
  booktitle = {European Conference on Computer Vision},
  year      = {2022}
```

```
}

@article{singh2020detection,
  author    = {Singh, Jagdeep and Behal, Sunny},
  title     = {Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions},
  journal   = {Computer Science Review},
  year      = {2020}
}

@misc{hildebrand2021beat,
  author    = {Hildebrand, Carol},
  title     = {The Beat Goes On},
  howpublished = {NETSCOUT ASERT Blog},
  year      = {2021}
}

@misc{livemint2020google,
  author    = {{LiveMint News Staff}},
  title     = {Google Services Including YouTube, Gmail, Google Drive Face Outage Due to DDoS Attack},
  howpublished = {LiveMint},
  year      = {2020}
}

@inproceedings{misa2024leveraging,
  author    = {Misa, Chris and Durairajan, Ramakrishnan and Gupta, Arpit and Rejaie, Reza and Willinger, Walter},
  title     = {Leveraging prefix structure to detect volumetric ddos attack signatures with programmable switches},
  booktitle = {2024 IEEE Symposium on Security and Privacy (SP)},
  year      = {2024}
}

@misc{lakshmanan2025httpbot,
  author    = {Lakshmanan, Ravie},
  title     = {New HTTPBot Botnet Launches 200+ Precision DDoS Attacks on Gaming and Tech Sectors},
  howpublished = {The Hacker News},
  year      = {2025}
}

@article{malik2023feature,
  author    = {Malik, Manisha and Dutta, Maitreyee and others},
  title     = {Feature engineering and machine learning framework for DDoS attack detection in the standardized internet of things},
  journal   = {IEEE Internet of Things Journal},
  year      = {2023}
}

@article{neto2023ciciot,
  author    = {Neto, Euclides Carlos Pinto and Dadkhah, Sajjad and Ferreira, Raphael and Zohourian, Alireza and Lu, Rongxing and Ghorbani, Ali A},
```

title = {CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment},

journal = {Sensors},

year = {2023}

}

@article{bamasag2022real,

author = {Bamasag, Omaimah and Alsaeedi, Alaa and Munshi, Asmaa and Alghazzawi, Daniyal and Alshehri, Suhair and Jamjoom, Arwa},

title = {Real-time DDoS flood attack monitoring and detection (RT-AMD) model for cloud computing},

journal = {PeerJ Computer Science},

year = {2022}

}

@inproceedings{ozcam2021detecting,

author = {Özçam, Berkay and Kilinc, H Hakan and Zaim, Abdül Halim},

title = {Detecting tcp flood ddos attack by anomaly detection based on machine learning algorithms},

booktitle = {2021 6th International Conference on Computer Science and Engineering (UBMK)},

year = {2021}

}

@article{musa2024machine,

author = {Musa, Nura Shifa and Mirza, Nada Masood and Rafique, Saida Hafsa and Abdallah, Amira Mahamat and Murugan, Thangavel},

```
 title     = {Machine learning and deep learning techniques for distributed denial of service anomaly detection in software defined networks current research solutions},
 journal   = {IEEE Access},
 year      = {2024}
}

@article{zhang2020highlevel,
 author    = {Zhang, Lan and others},
 title     = {High-Level Cyber Attacks Detection Using AI},
 journal   = {IEEE Transactions on Information Forensics and Security},
 year      = {2020}
}

@article{han2012massive,
 author    = {Han and others},
 title     = {Massive DDoS Attack on Cryptocurrency Exchange: A Case Study},
 journal   = {IEEE Access},
 year      = {2012}
}

@article{berman2019survey,
 author    = {Berman, Daniel S and Buczak, Anna L and Chavis, Jeffrey S and Corbett, Cherita L},
 title     = {A survey of deep learning methods for cyber security},
 journal   = {Information},
 year      = {2019}
}
```

```
@article{li2023towards,
  author    = {Li, Haibin and Zhao, Yi and Yao, Wenbing and Xu, Ke and Li, Qi},
  title     = {Towards real-time ML-based DDoS detection via cost-efficient window-based feature extraction},
  journal   = {Science China Information Sciences},
  year      = {2023}
}

@inproceedings{carvajal2003high,
  author    = {Carvajal, Antonio and Garcia-Colon, VR},
  title     = {High capacity motors on-line diagnosis based on ultra wide band partial discharge detection},
  booktitle = {4th IEEE International Symposium on Diagnostics for Electric Machines, Power Electronics and Drives, 2003. SDEMPED 2003.},
  year      = {2003}
}

@inproceedings{chahal2021distributed,
  author    = {Chahal, Jasmeen Kaur and Kaur, Puninder and Sharma, Avinash},
  title     = {Distributed Denial of Service (DDoS) Attacks in Software-defined Networks (SDN)},
  booktitle = {2021 5th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT)},
  year      = {2021}
}
```

```
@article{zhang2024revealing,
  author    = {Zhang, Zhiyi and Xiao, Guorui and Song, Sichen and Aygun, R Can and Stavrou, Angelos and Zhang, Lixia and Osterweil, Eric},
  title     = {Revealing Protocol Architecture's Design Patterns in the Volumetric DDoS Defense Design Space},
  journal   = {IEEE Communications Surveys \& Tutorials},
  year      = {2024}
}

@article{wang2025modern,
  author    = {Wang, Jincheng and Yu, Le and Lui, John and Luo, Xiapu},
  title     = {Modern DDoS Threats and Countermeasures: Insights into Emerging Attacks and Detection Strategies},
  journal   = {arXiv preprint},
  year      = {2025}
}

@article{li2023comprehensive,
  author    = {Li, Qing and Huang, He and Li, Ruoyu and Lv, Jianhui and Yuan, Zhenhui and Ma, Lianbo and Han, Yi and Jiang, Yong},
  title     = {A comprehensive survey on DDoS defense systems: New trends and challenges},
  journal   = {Computer Networks},
  year      = {2023}
}

@misc{rostamian2024applications,
  author    = {Rostamian, Ahoora},
  title     = {Applications of Deep Learning Models in Financial Forecasting},
  howpublished = {University of Essex},
  year      = {2024}
}

@inproceedings{hore2023empirical,
  author    = {Hore, Soumyadeep and Nguyen, Quoc H and Xu, Yulun and Shah, Ankit and Bastian, Nathaniel D and Le, Trung},
  title     = {Empirical evaluation of autoencoder models for anomaly detection in packet-based nids},
  booktitle = {2023 IEEE Conference on Dependable and Secure Computing (DSC)},
  year      = {2023}
}

@article{wang2023nstgat,
  author    = {Wang, Yalu and Li, Jie and Zhao, Wei and Han, Zhijie and Zhao, Hang and Wang, Lei and He, Xin},
  title     = {N-STGAT: Spatio-temporal graph neural network based network intrusion detection for near-earth remote sensing},
  journal   = {Remote Sensing},
  year      = {2023}
}

@article{schmidl2022anomaly,
  author    = {Schmidl, Sebastian and Wenig, Phillip and Papenbrock, Thorsten},
  title     = {Anomaly detection in time series: a comprehensive evaluation},
  journal   = {Proceedings of the VLDB Endowment},
 year     = {2022}
}

@article{chatterjee2022iot,
 author    = {Chatterjee, Ayan and Ahmed, Bestoun S},
 title     = {IoT anomaly detection methods and applications: A survey},
 journal   = {Internet of Things},
 year      = {2022}
}

@article{khan2024anomaly,
 author    = {Khan, Maryam Mahsal and Alkhathami, Mohammed},
 title     = {Anomaly detection in IoT-based healthcare: machine learning for enhanced
security},
 journal   = {Scientific reports},
 year      = {2024}
}

@article{peng2023rwkv,
 author    = {Peng, Bo and Alcaide, Eric and Anthony, Quentin and Albalak, Alon and
Arcadinho, Samuel and Biderman, Stella and Cao, Huanqi and Cheng, Xin and Chung,
Michael and Grella, Matteo and others},
 title     = {Rwkv: Reinventing rnns for the transformer era},
 journal   = {arXiv preprint},
 year      = {2023}
}
```

```
@article{kim2024optimal,
  author    = {Kim, Bum-Sok and Suk, Hye-Won and Choi, Yong-Hoon and Moon, Dae-Sung and Kim, Min-Suk},
  title     = {Optimal Cyber Attack Strategy Using Reinforcement Learning Based on Common Vulnerability Scoring System},
  journal   = {CMES-Computer Modeling in Engineering \& Sciences},
  year      = {2024}
}

@article{wang2023federated,
  author    = {Wang, Xiaofeng and Wang, Yonghong and Javaheri, Zahra and Almutairi, Laila and Moghadamnejad, Navid and Younes, Osama S},
  title     = {Federated deep learning for anomaly detection in the internet of things},
  journal   = {Computers and Electrical Engineering},
  year      = {2023}
}

@article{doriguzzi2022flad,
  author    = {Doriguzzi-Corin, R and Siracusa, D},
  title     = {FLAD: Adaptive federated learning for DDoS attack detection},
  journal   = {arXiv preprint},
  year      = {2022}
}

@article{doriguzzi2020lucid,
  author    = {Doriguzzi-Corin, Roberto and Millar, Stuart and Scott-Hayward, Sandra and Martinez-del-Rincon, Jesus and Siracusa, Domenico},
  title    = {LUCID: A practical, lightweight deep learning solution for DDoS attack detection},
  journal  = {IEEE Transactions on Network and Service Management},
  year     = {2020}
}

@article{salahuddin2021chronos,
  author   = {Salahuddin, Mohammad A and Pourahmadi, Vahid and Alameddine, Hyame Assem and Bari, Md Faizul and Boutaba, Raouf},
  title    = {Chronos: Ddos attack detection using time-based autoencoder},
  journal  = {IEEE Transactions on Network and Service Management},
  year     = {2021}
}

@article{li2024interactive,
  author   = {Li, Huafeng and Zhang, Chen and Hu, Zhanxuan and Zhang, Yafei and Yu, Zhengtao},
  title    = {Interactive attack-defense for generalized person re-identification},
  journal  = {Neural Networks},
  year     = {2024}
}

@article{ma2023real,
  author   = {Ma, Ruikui and Wang, Qiuqian and Bu, Xiangxi and Chen, Xuebin},
  title    = {Real-time detection of DDoS attacks based on random forest in SDN},
  journal  = {Applied Sciences},
  year     = {2023}
}
```

```
@article{nasir2021fake,
  author   = {Nasir, Jamal Abdul and Khan, Osama Subhani and Varlamis, Iraklis},
  title    = {Fake news detection: A hybrid CNN-RNN based deep learning approach},
  journal  = {International journal of information management data insights},
  year     = {2021}
}

@article{kimanzi2024deep,
  author   = {Kimanzi, Richard and Kimanga, Peter and Cherori, Dedan and Gikunda, Patrick K},
  title    = {Deep Learning Algorithms Used in Intrusion Detection Systems--A Review},
  journal  = {arXiv preprint},
  year     = {2024}
}

@article{sowmya2023comprehensive,
  author   = {Sowmya, Ta and Anita, EA Mary},
  title    = {A comprehensive review of AI based intrusion detection system},
  journal  = {Measurement: Sensors},
  year     = {2023}
}

@article{ain2025securing,
  author   = {Ain, Noor Ul and Sardaraz, Muhammad and Tahir, Muhammad and Abo Elsoud, Mohamed W and Alourani, Abdullah},
  title    = {Securing IoT Networks Against DDoS Attacks: A Hybrid Deep Learning Approach},
  journal   = {Sensors},
  year      = {2025}
}

@inproceedings{gniewkowski2022anomaly,
  author    = {Gniewkowski, Mateusz and Maciejewski, Henryk and Surmacz, Tomasz},
  title     = {Anomaly detection techniques for different ddos attack types},
  booktitle = {International Conference on Dependability and Complex Systems},
  year      = {2022}
}

@inproceedings{khaleel2023ddos,
  author    = {Khaleel, Thura Jabbar and Shiltagh, Nadia Adnan},
  title     = {DDoS Cyber-Attacks Detection-Based Hybrid CNN-LSTM},
  booktitle = {International Conference on Computing and Communication Networks},
  year      = {2023}
}

@article{sumathi2022ddos,
  author    = {Sumathi, S and Rajesh, R and Karthikeyan, N},
  title     = {DDoS attack detection using hybrid machine learning based IDS models},
  journal   = {NIScPR-CSIR, India},
  year      = {2022}
}

@article{wei2023classification,
```

```bibtex
  author    = {Wei, Yuanyuan and Jang-Jaccard, Julian and Singh, Amardeep and Sabrina, Fariza and Camtepe, Seyit},
  title     = {Classification and explanation of distributed denial-of-service (DDoS) attack detection using machine learning and shapley additive explanation (SHAP) methods},
  journal   = {arXiv preprint},
  year      = {2023}
}

@article{li2024hda,
  author    = {Li, Sifan and Cao, Yue and Liu, Shuohan and Lai, Yuping and Zhu, Yongdong and Ahmad, Naveed},
  title     = {Hda-ids: A hybrid dos attacks intrusion detection system for iot by using semi-supervised cl-gan},
  journal   = {Expert Systems with Applications},
  year      = {2024}
}

@article{alabdulatif2024machine,
  author    = {Alabdulatif, Abdullah and Thilakarathne, Navod Neranjan and Aashiq, Mohamed},
  title     = {Machine Learning Enabled Novel Real-Time IoT Targeted DoS/DDoS Cyber Attack Detection System},
  journal   = {Computers, Materials \& Continua},
  year      = {2024}
}

@article{wang2022ai,
  author    = {Wang, Bo-Xiang and Chen, Jiann-Liang and Yu, Chiao-Lin},
  title     = {An AI-powered network threat detection system},
  journal   = {IEEE Access},
  year      = {2022}
}

@article{lundberg2017unified-x,
  author    = {Lundberg, Scott M and Lee, Su-In},
  title     = {A unified approach to interpreting model predictions},
  journal   = {Advances in neural information processing systems},
  year      = {2017}
}

@inproceedings{ribeiro2016should,
  author    = {Ribeiro, Marco Tulio and Singh, Sameer and Guestrin, Carlos},
  title     = {Why should i trust you? Explaining the predictions of any classifier},
  booktitle = {Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining},
  year      = {2016}
}

@article{loveleen2023explanation,
  author    = {Loveleen, Gaur and Mohan, Bhandari and Shikhar, Bhadwal Singh and Nz, Jhanjhi and Shorfuzzaman, Mohammad and Masud, Mehedi},
  title     = {Explanation-driven HCI model to examine the mini-mental state for Alzheimer's disease},
  journal   = {ACM Transactions on Multimedia Computing, Communications and Applications},
  year     = {2023}
}

@article{kamal2022explainable,
  author    = {Kamal, Md Sarwar and Dey, Nilanjan and Chowdhury, Linkon and Hasan, Syed Irtija and Santosh, KC},
  title     = {Explainable AI for glaucoma prediction analysis to understand risk factors in treatment planning},
  journal   = {IEEE Transactions on Instrumentation and Measurement},
  year     = {2022}
}

@article{viana2021evaluation,
  author    = {Viana, Cláudia M and Santos, Maurício and Freire, Dulce and Abrantes, Patrícia and Rocha, Jorge},
  title     = {Evaluation of the factors explaining the use of agricultural land: A machine learning and model-agnostic approach},
  journal   = {Ecological Indicators},
  year     = {2021}
}

@article{khan2022xsru,
  author    = {Khan, Izhar Ahmed and Moustafa, Nour and Razzak, Imran and Tanveer, Muhammad and Pi, Dechang and Pan, Yue and Ali, Bakht Sher},
  title     = {XSRU-IoMT: Explainable simple recurrent units for threat detection in Internet of Medical Things networks},
  journal   = {Future generation computer systems},
  year     = {2022}
```

```
}

@article{rjoub2023survey,
  author    = {Rjoub, Gaith and Bentahar, Jamal and Wahab, Omar Abdel and Mizouni, Rabeb and Song, Alyssa and Cohen, Robin and Otrok, Hadi and Mourad, Azzam},
  title     = {A survey on explainable artificial intelligence for cybersecurity},
  journal   = {IEEE Transactions on Network and Service Management},
  year      = {2023}
}

@article{elubeyd2023hybrid,
  author    = {Elubeyd, Hani and Yiltas-Kaplan, Derya},
  title     = {Hybrid deep learning approach for automatic DoS/DDoS attacks detection in software-defined networks},
  journal   = {Applied Sciences},
  year      = {2023}
}

@article{ahmad2021nids_survey,
  author  = {Ahmad, Zahra and Khan, A. Shahid and Shiang, Chee Wai and Abdullah, Jamaludin and Ahmad, Fadi},
  title   = {Network Intrusion Detection System: A Systematic Study of Machine Learning and Deep Learning Approaches},
  journal = {Transactions on Emerging Telecommunications Technologies},
  volume  = {32},
  number  = {1},
  pages   = {e4150},
  year   = {2021}
}

@article{iyer2021behavioral_ids,
  author  = {Iyer, K. I.},
  title   = {From Signatures to Behavior: Evolving Strategies for Next-Generation Intrusion Detection},
  journal = {European Journal of Advances in Engineering and Technology},
  volume  = {8},
  number  = {6},
  pages   = {165--171},
  year   = {2021}
}

@article{fan2024autoupdating_ids,
  author  = {Fan, Cheng and Cui, Jian and Jin, Hui and Zhong, Hao and Bolodurina, Irina and He, Debiao},
  title   = {Auto-Updating Intrusion Detection System for Vehicular Network: A Deep Learning Approach Based on Cloud-Edge-Vehicle Collaboration},
  journal = {IEEE Transactions on Vehicular Technology},
  volume  = {73},
  number  = {10},
  pages   = {15372--15384},
  year   = {2024}
}

@inproceedings{benziker2023vanet_ids,
  author    = {Benziker, Abdelilah and Arunagiri, R. and Maheswari, G.},
  title     = {Improved IDS for Vehicular Ad-Hoc Network using Deep Learning Approaches},
  booktitle = {IEEE 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS)},
  pages     = {341--346},
  year      = {2023}
}

@article{cui2024lhids,
  author  = {Cui, Jian and Xiao, Jun and Zhong, Hao and Zhang, Jian and Wei, Liang and Bolodurina, Irina and He, Debiao},
  title   = {LH-IDS: Lightweight Hybrid Intrusion Detection System Based on Differential Privacy in VANETs},
  journal = {IEEE Transactions on Mobile Computing},
  volume  = {23},
  number  = {12},
  pages   = {12195--12210},
  year    = {2024}
}

@inproceedings{gueriani2024iot_cnn_lstm,
  author    = {Gueriani, Ahmed and Kheddar, Hichem and Mazari, Abdelkader C.},
  title     = {Enhancing IoT Security with CNN and LSTM-based Intrusion Detection Systems},
  booktitle = {IEEE 6th International Conference on Pattern Analysis and Intelligent Systems (PAIS)},
  pages     = {1--7},
  year      = {2024}
```

```
}

@article{sharma2023iot_ids,
  author  = {Sharma, Bhavya and Sharma, Lalit and Lal, Chhagan and Roy, Sajal},
  title   = {Anomaly Based Network Intrusion Detection for IoT Attacks Using Deep Learning Technique},
  journal = {Computers and Electrical Engineering},
  volume  = {107},
  pages   = {108626},
  year    = {2023}
}

@inproceedings{hore2023autoencoder_nids,
  author    = {Hore, Subhadeep and Nguyen, Quang H. and Xu, Yuchen and Shah, Aayush and Bastian, Nathan D. and Le, Tien},
  title     = {Empirical Evaluation of Autoencoder Models for Anomaly Detection in Packet-based NIDS},
  booktitle = {IEEE Conference on Dependable and Secure Computing (DSC)},
  pages     = {1--8},
  year      = {2023}
}

@article{shaji2024sdiids,
  author  = {Shaji, N. S. and Muthalagu, R. and Pawar, P. M.},
  title   = {SD-IIDS: Intelligent Intrusion Detection System for Software-Defined Networks},
  journal = {Multimedia Tools and Applications},
  volume  = {83},
  number  = {4},
  pages   = {11077--11109},
  year    = {2024}
}

@article{liang2025genai_semantic,
  author  = {Liang, Cheng and Du, Hao and Sun, Yiming and Niyato, Dusit and Kang, Jiawen and Zhao, Dong and Imran, Muhammad Ali},
  title   = {Generative AI-driven Semantic Communication Networks: Architecture, Technologies, and Applications},
  journal = {IEEE Transactions on Cognitive Communications and Networking},
  volume  = {11},
  number  = {1},
  pages   = {27--47},
  year    = {2025}
}

@article{sun2025sran,
  author  = {Sun, Yiming and Zhang, Lei and Guo, Liang and Li, Jie and Niyato, Dusit and Fang, Yuguang},
  title   = {S-RAN: Semantic-aware Radio Access Networks},
  journal = {IEEE Communications Magazine},
  volume  = {63},
  number  = {4},
  pages   = {207--213},
  year    = {2025}
}
```

```
@article{chen2024netgpt,
  author  = {Chen, Yifei and Li, Rui and Zhao, Zhiwei and Peng, Chao and Wu, Jun and Hossain, Ekram and Zhang, Honggang},
  title   = {NetGPT: An AI-Native Network Architecture for Provisioning Beyond Personalized Generative Services},
  journal = {IEEE Network},
  volume  = {38},
  number  = {6},
  pages   = {404--413},
  year    = {2024}
}

@article{nascita2024xai,
  author  = {Nascita, Alessandro and Aceto, Giuseppe and Ciuonzo, Domenico and Montieri, Antonio and Persico, Valerio and Pescape, Antonio},
  title   = {A Survey on Explainable Artificial Intelligence for Internet Traffic Classification and Prediction, and Intrusion Detection},
  journal = {IEEE Communications Surveys \& Tutorials},
  year    = {2024}
}
% --- XAI ---

@article{neupane2022xids,
  author  = {Neupane, Suman and Ables, Jared and Anderson, William and Mittal, Sparsh and Rahimi, Saeed and Banicescu, Ioan and Seale, Michael},
  title   = {Explainable Intrusion Detection Systems (X-IDS): A Survey of Current Methods, Challenges, and Opportunities},
  journal = {IEEE Access},
  volume  = {10},
  pages   = {112392--112415},
  year    = {2022}
}
% --- XAI ---

@techreport{oran_e2gap_2025,
  author     = {{O-RAN Alliance}},
  title      = {O-RAN WG3 E2 General Aspects and Principles (E2GAP)},
  institution = {O-RAN Alliance},
  type       = {Technical Report},
  number     = {v07.00},
  month      = {February},
  year       = {2025}
}

@techreport{oran_e2sm_kpm_2025,
  author     = {{O-RAN Alliance}},
  title      = {O-RAN WG3 E2 Service Model (E2SM) KPM Specification},
  institution = {O-RAN Alliance},
  type       = {Technical Report},
  number     = {v06.00},
  month      = {February},
  year       = {2025}
}
```

```
@article{tang2022systematic,
 author  = {Tang, Qiang and Ermis, Onur and Nguyen, Cuong D. and Oliveira, Andre D. and Hirtzig, Alexandre},
 title   = {A Systematic Analysis of 5G Networks With a Focus on 5G Core Security},
 journal = {IEEE Access},
 volume  = {10},
 pages   = {18298--18319},
 year    = {2022}
}

@techreport{airan_whitepaper_2024,
 author     = {{AI-RAN Alliance}},
 title      = {AI-RAN Alliance Vision and Mission White Paper},
 institution = {AI-RAN Alliance},
 year       = {2024},
 month      = {December}
}

@article{je2021toward6g,
 author  = {Je, Donghyun and Jung, Jihyun and Choi, Sunghyun},
 title   = {Toward 6G Security: Technology Trends, Threats, and Solutions},
 journal = {IEEE Communications Standards Magazine},
 volume  = {5},
 number  = {3},
 pages   = {64--71},
```

year = {2021}

}

@article{kundu2025airan,

author = {Kundu, Lagnajit and Lin, Xiaoming and Gadiyar, Raghav and Lacasse, Jean-Francois and Chowdhury, Suman},

title = {AIRAN: Transforming RAN with AI-driven Computing Infrastructure},

journal = {arXiv preprint arXiv:2501.09007},

year = {2025}

}

@article{alemany2025intent,

author = {Alemany, Pol and Munoz, Raul and Castaneda Cisneros, Juan and Karaca, Mehmet and Porambage, Pawani and Tran, Hien Quoc and Giardina, Pierluigi G. and Tzanettis, Ioannis and Sousa, X. R. and Jorquera Valero, Jose Maria and Ojaghi, Behnam and Vilalta, Ricard and Rugeland, Per and Boussard, Mathieu and Landi, Giacomo and Zafeiropoulos, Alexandros and Rodriguez, Sergio and Gil Perez, Manuel and Barmpounakis, Stylianos and Uusitalo, Mikko A. and Lopez, Diego and Kerboeuf, Stephane},

title = {Defining Intent-Based Service Management Automation for 6G Multi-Stakeholders Scenarios},

journal = {IEEE Open Journal of the Communications Society},

volume = {6},

pages = {2373--2396},

year = {2025}

}

@article{ojaghi2022slicedran,

author = {Ojaghi, Behnam and Adelantado, Ferran and Antonopoulos, Angelos and Verikoukis, Christos},

title = {SlicedRAN: Service-Aware Network Slicing Framework for 5G Radio Access Networks},

journal = {IEEE Systems Journal},

volume = {16},

number = {2},

pages = {2556--2567},

year = {2022}

}

@article{soltani2025intelligent,

author = {Soltani, Seyed and Amanloo, Amir and Shojafar, Mohammad and Tafazolli, Rahim},

title = {Intelligent Control in 6G Open RAN: Security Risk or Opportunity?},

journal = {IEEE Open Journal of the Communications Society},

volume = {6},

pages = {840--880},

year = {2025}

}

@article{balasubramanian2021ric,

author = {Balasubramanian, Balakrishnan and Daniels, Edward S. and Hiltunen, Markku and Jana, Rittwik and Joshi, Kaushik and Sivaraj, Raghunathan and Tran, Tuan X. and Wang, Chih-Lin},

title = {RIC: A RAN Intelligent Controller Platform for AI-Enabled Cellular Networks},

journal = {IEEE Internet Computing},

```
 volume  = {25},
 number  = {2},
 pages   = {7--17},
 year    = {2021}
}

@article{polese2023understanding,
 author  = {Polese, Michele and Bonati, Leonardo and D'Oro, Salvatore and Basagni,
Stefano and Melodia, Tommaso},
 title   = {Understanding O-RAN: Architecture, Interfaces, Algorithms, Security, and
Research Challenges},
 journal = {IEEE Communications Surveys \& Tutorials},
 volume  = {25},
 number  = {2},
 pages   = {1376--1411},
 year    = {2023}
}

@techreport{oran_whitepaper_2018,
 author      = {{O-RAN Alliance}},
 title       = {O-RAN White Paper: Towards an Open and Smart RAN},
 institution = {O-RAN Alliance},
 year        = {2018}
}

@misc{imperva2023ddos,
 author       = {Imperva},
 title       = {Imperva Global DDoS Threat Landscape Report 2023},
 howpublished = {\url{https://www.imperva.com/resources/reports/the-imperva-global-ddos-threat-landscape-report-2023.pdf}},
 year        = {2023},
 note        = {Accessed: 2025-02-15}
}
@article{gaspar2024explainable,
 title={Explainable AI for intrusion detection systems: LIME and SHAP applicability on multi-layer perceptron},
 author={Gaspar, Diogo and Silva, Paulo and Silva, Catarina},
 journal={IEEE Access},
 volume={12},
 pages={30164--30175},
 year={2024},
 publisher={IEEE}
}@article{abiramasundari2025distributed,
 title={Distributed denial-of-service (DDOS) attack detection using supervised machine learning algorithms},
 author={Abiramasundari, S and Ramaswamy, V},
 journal={Scientific Reports},
 volume={15},
 number={1},
 pages={13098},
 year={2025},
 publisher={Nature Publishing Group UK London}
}
@article{mbona2022detecting,
 title={Detecting zero-day intrusion attacks using semi-supervised machine learning approaches},
 author={Mbona, Innocent and Eloff, Jan HP},
 journal={IEEE Access},
 volume={10},
 pages={69822--69838},
 year={2022},
 publisher={IEEE}
}
@article{gu2019semi,
 title={Semi-supervised K-means DDoS detection method using hybrid feature selection algorithm},
 author={Gu, Yonghao and Li, Kaiyue and Guo, Zhenyang and Wang, Yongfei},
 journal={IEEE Access},
 volume={7},
 pages={64351--64365},
 year={2019},
 publisher={IEEE}
}
@article{aamir2021clustering,
 title={Clustering based semi-supervised machine learning for DDoS attack classification},
 author={Aamir, Muhammad and Zaidi, Syed Mustafa Ali},
 journal={Journal of King Saud University-Computer and Information Sciences},
 volume={33},
 number={4},
 pages={436--446},
 year={2021},
```

publisher={Elsevier}

}

@inproceedings{garg2021detection,

title={Detection of DDoS attacks using semi-supervised based machine learning approaches},

author={Garg, Umang and Kaur, Maninder and Kaushik, Malvika and Gupta, Neha},

booktitle={2021 2nd International Conference on Computational Methods in Science \& Technology (ICCMST)},

pages={112--117},

year={2021},

organization={IEEE}

}

@article{idhammad2018semi,

title={Semi-supervised machine learning approach for DDoS detection},

author={Idhammad, Mohamed and Afdel, Karim and Belouch, Mustapha},

journal={Applied Intelligence},

volume={48},

number={10},

pages={3193--3208},

year={2018},

publisher={Springer}

}

@article{chen2025enhancing,

title={Enhancing Machine Learning-Based DDoS Detection Through Hyperparameter Optimization},

author={Chen, Shao-Rui and Chen, Shiang-Jiun and Hsieh, Wen-Bin},

journal={Electronics},

```
  volume={14},
  number={16},
  pages={3319},
  year={2025},
  publisher={MDPI}
}
@article{hallaji2025study,
  title={A Study on Semi-Supervised Detection of DDoS Attacks under Class Imbalance},
  author={Hallaji, Ehsan and Shanmugam, Vaishnavi and Razavi-Far, Roozbeh and Saif, Mehrdad},
  journal={arXiv preprint arXiv:2506.22949},
  year={2025}
}
@article{najafimehr2023ddos,
  title={DDoS attacks and machine-learning-based detection methods: A survey and taxonomy},
  author={Najafimehr, Mohammad and Zarifzadeh, Sajjad and Mostafavi, Seyedakbar},
  journal={Engineering Reports},
  year={2023},
  month={May},
  doi={10.1002/eng2.12697},
  url={https://onlinelibrary.wiley.com/doi/abs/10.1002/eng2.12697}
}

@article{singh2020planewise,
  title={A comprehensive plane-wise review of DDoS attacks in SDN: Leveraging detection and mitigation through machine learning and deep learning},
 author={Singh, Prabhjot and others},
 journal={Computer Networks},
 year={2024},
 doi={10.1016/j.comnet.2024.110583},
 url={https://www.sciencedirect.com/science/article/abs/pii/S1084804524002583}
}

@article{haseeb2023highspeed,
 title={High-speed network DDoS attack detection: A survey},
 author={Haseeb-ur-Rehman, R. M. A. and others},
 journal={Sensors},
 volume={23},
 number={15},
 pages={6850},
 year={2023},
 doi={10.3390/s23156850},
 url={https://www.mdpi.com/1424-8220/23/15/6850}
}

@article{neupane2022explainable,
 title={Explainable intrusion detection systems (X-IDS): A survey of current methods, challenges, and opportunities},
 author={Neupane, Subash and others},
 journal={arXiv preprint arXiv:2207.06236},
 year={2022},
 url={https://arxiv.org/abs/2207.06236}
```

```
}

@article{gelgi2024systematic,
  title={Systematic literature review of IoT botnet DDOS attacks and evaluation of detection techniques},
  author={Gelgi, Metehan and Guan, Yueting and Arunachala, Sanjay and Samba Siva Rao, Maddi and Dragoni, Nicola},
  journal={Sensors},
  volume={24},
  number={11},
  pages={3571},
  year={2024},
  doi={10.3390/s24113571},
  url={https://www.mdpi.com/1424-8220/24/11/3571}
}

@article{islam2024xai,
  title={XAI-IDS: Toward proposing an explainable artificial intelligence framework for enhancing network intrusion detection systems},
  author={Islam, Md Saiful and others},
  journal={Applied Sciences},
  volume={14},
  number={10},
  pages={4170},
  year={2024},
  doi={10.3390/app14104170},
  url={https://www.mdpi.com/2076-3417/14/10/4170}
```

```
}

@article{adel2025iot,
  title={An intrusion detection system over the IoT data streams using eXplainable artificial intelligence (XAI)},
  author={Adel, Ali and Fuad, Muhammad},
  journal={Sensors},
  volume={25},
  number={3},
  pages={847},
  year={2025},
  doi={10.3390/s25030847},
  url={https://www.mdpi.com/1424-8220/25/3/847}
}

@article{choras2024dual,
  title={The survey on the dual nature of xAI challenges in intrusion detection and their potential for AI innovation},
  author={Choraś, Michał and others},
  journal={Artificial Intelligence Review},
  year={2024},
  doi={10.1007/s10462-024-10972-3},
  url={https://link.springer.com/article/10.1007/s10462-024-10972-3}
}

@article{ables2025systematic,
```

title={A systematic review on the integration of explainable artificial intelligence in intrusion detection systems to enhancing transparency and interpretability in cybersecurity},

author={Ables, Jesse and others},

journal={Frontiers in Artificial Intelligence},

year={2025},

doi={10.3389/frai.2025.1526221},

url={https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2025.1526221/full}

}

@article{kumari2023comprehensive,

title={A comprehensive study of DDoS attacks over IoT network and their countermeasures},

author={Kumari, Pooja and Jain, Ashish Kumar},

journal={Computer Security},

volume={127},

pages={103096},

year={2023},

doi={10.1016/j.cose.2023.103096},

url={https://www.sciencedirect.com/science/article/abs/pii/S0167404823000068}

}

@article{pakmehr2024ddos,

title={DDoS attack detection techniques in IoT networks: a survey},

author={Pakmehr, Ali and Aßmuth, Arno and Taheri, Neda and Ghaffari, Ali},

journal={Cluster Computing},

```
 volume={27},
 number={10},
 pages={14637--14668},
 year={2024},
 doi={10.1007/s10586-024-04662-6},
 url={https://link.springer.com/article/10.1007/s10586-024-04662-6}
}

@article{arreche2024xai,
 title={E-XAI: Evaluating black-box explainable AI frameworks for network intrusion detection},
 author={Arreche, Omar and Guntur, Tejaswi R. and Roberts, Jacob W. and Abdallah, Mustafa},
 journal={IEEE Access},
 volume={12},
 pages={23954--23988},
 year={2024},
 doi={10.1109/ACCESS.2024.3365140},
 url={https://ieeexplore.ieee.org/document/10443142}
}
@inproceedings{bhardwaj2018towards,
 title={Towards $\{$IoT-DDoS$\}$ prevention using edge computing},
 author={Bhardwaj, Ketan and Miranda, Joaquin Chung and Gavrilovska, Ada},
 booktitle={USENIX workshop on hot topics in edge computing (HotEdge 18)},
 year={2018}
}
@article{doshi2021timely,
 title={Timely detection and mitigation of stealthy DDoS attacks via IoT networks},
 author={Doshi, Keval and Yilmaz, Yasin and Uludag, Suleyman},
 journal={IEEE Transactions on Dependable and Secure Computing},
 volume={18},
 number={5},
 pages={2164--2176},
 year={2021},
 publisher={IEEE}
}
@article{kaur2017review,
 title={A review of detection approaches for distributed denial of service attacks},
 author={Kaur, Parneet and Kumar, Manish and Bhandari, Abhinav},
 journal={Systems Science \& Control Engineering},
 volume={5},
 number={1},
 pages={301--320},
 year={2017},
 publisher={Taylor \& Francis}
}
@inproceedings{wang2010augmented,
 title={Augmented attack tree modeling of distributed denial of services and tree based
attack detection method},
 author={Wang, Jie and Phan, Raphael C-W and Whitley, John N and Parish, David J},
 booktitle={2010 10th IEEE International Conference on Computer and Information
Technology},
 pages={1009--1014},
 year={2010},
  organization={IEEE}
}
@article{chen2016hybrid,
  title={A Hybrid Approach Combining Rule-Based And Anomaly-Based Detection Against DDoS Attacks},
  author={Chen, C and Chen, Hsin-Chiao},
  journal={International Journal Of Network Security Its Applications},
  volume={8},
  number={5},
  year={2016}
}
@inproceedings{zhang2009prediction,
  title={A prediction-based detection algorithm against distributed denial-of-service attacks},
  author={Zhang, Guoxing and Jiang, Shengming and Wei, Gang and Guan, Quansheng},
  booktitle={Proceedings of the 2009 international conference on wireless communications and mobile computing: Connecting the World wirelessly},
  pages={106--110},
  year={2009}
}

@article{chen2009new,
  title={A New Detection Method for Distributed Denial-of-Service Attack Traffic based on Statistical Test.},
  author={Chen, Chin-Ling},
  journal={J. Univers. Comput. Sci.},
  volume={15},
  number={2},
  pages={488--504},
  year={2009}
}
@article{mirkovic2005d,
  title={D-WARD: a source-end defense against flooding denial-of-service attacks},
  author={Mirkovic, Jelena and Reiher, Peter},
  journal={IEEE transactions on Dependable and Secure Computing},
  volume={2},
  number={3},
  pages={216--232},
  year={2005},
  publisher={IEEE}
}
@article{feng2023explainable,
  title={On explainable and adaptable detection of distributed denial-of-service traffic},
  author={Feng, Yebo and Li, Jun and Sisodia, Devkishen and Reiher, Peter},
  journal={IEEE Transactions on Dependable and Secure Computing},
  volume={21},
  number={4},
  pages={2211--2226},
  year={2023},
  publisher={IEEE}
}

@misc{Cloudflare2025Q2,
 title = {{Hyper-volumetric DDoS attacks skyrocket: Cloudflare's 2025 Q2 DDoS threat report}},
 author = {{Cloudflare}},
 year = {2025},
 howpublished = {\url{https://blog.cloudflare.com/ddos-threat-report-for-2025-q2/}},
 note = {Accessed: 2025-01-15}
}
@misc{Akamai2024Layer7,
 title = {{Why Modern Layer 7 DDoS Protections Are Crucial for Web Security in 2024}},
 author = {{Akamai}},
 year = {2024},
 howpublished = {\url{https://www.akamai.com/blog/security/why-modern-layer-7-ddos-protections-crucial-web-security-2024}},
 note = {Accessed: 2025-01-15}
}
@misc{NetFlow,
 title = {{NetFlow}},
howpublished = {\url{https://data.mendeley.com/datasets/gb8hwjdthj/1}},
 note = {Accessed: 2025-06-30}
}
@misc{N-BaIoT,
 title = {{N-BaIoT}},  howpublished = {\url{https://archive.ics.uci.edu/dataset/442/detection+of+iot+botnet+attacks+n+baiot}},
 note = {Accessed: 2025-06-30}
}
@misc{CICIDS2019,
```

title = {{CICIDS2019} }, howpublished = {\url{https://www.unb.ca/cic/datasets/ddos-2019.html}},

note = {Accessed: 2025-06-30}

}

@misc{CICIDS2017,

title = {{CICIDS2017} }, howpublished = {\url{https://www.unb.ca/cic/datasets/ids-2017.html}},

note = {Accessed: 2025-06-30}

}

@misc{NSL-KDD,

title = {{NSL-KDD} }, howpublished = {\url{https://www.unb.ca/cic/datasets/nsl.html}},

note = {Accessed: 2025-06-30}

}

@misc{ServerMachineDataset,

title = {{ServerMachineDataset} }, howpublished = {\url{ServerMachineDataset}},

note = {Accessed: 2025-06-30}

}

@misc{WADI,

title = {{WADI} }, howpublished = {\url{https://itrust.sutd.edu.sg/itrust-labs_datasets/dataset_info/#wadi}},

note = {Accessed: 2025-06-30}

}

@misc{SwaT,

title = {{SwaT} }, howpublished = {\url{https://itrust.sutd.edu.sg/itrust-labs_datasets/dataset_info/#swat}},

note = {Accessed: 2025-06-30}

}

@article{udofot2024advanced,

title={Advanced Machine Learning--A Comprehensive Survey and New Research Directions},

author={Udofot, Akpan Itoro and Oluseyi, Omotosho Moses and Bassey, Edim},

journal={International Journal of Advanced Engineering and Management},

volume={6},

number={12},

year={2024}

}

@inproceedings{roshan2022using,

title={Using kernel shap xai method to optimize the network anomaly detection model},

author={Roshan, Khushnaseeb and Zafar, Aasim},

booktitle={2022 9th International Conference on Computing for Sustainable Global Development (INDIACom)},

pages={74--80},

year={2022},

organization={IEEE}

}

@article{okporokpo2025detection,

title={Detection of DDoS Cyberattack Using a Hybrid Trust-Based Technique for Smart Home Networks.},

author={Okporokpo, Oghenetejiri and Olajide, Funminiyi and Ajienka, Nemitari and others}, journal={International Journal of Advanced Computer Science \& Applications},

volume={16},

number={1},

year={2025}

}

@article{akgun2022new,

title={A new DDoS attacks intrusion detection model based on deep learning for cybersecurity},

author={Akgun, Devrim and Hizal, Selman and Cavusoglu, Unal},

journal={Computers \& Security},

volume={118},

pages={102748},

year={2022},

publisher={Elsevier}

}

@article{alghazzawi2021efficient,

title={Efficient detection of DDoS attacks using a hybrid deep learning model with improved feature selection},

author={Alghazzawi, Daniyal and Bamasag, Omaimah and Ullah, Hayat and Asghar, Muhammad Zubair},

journal={Applied Sciences},

volume={11},

number={24},

pages={11634},

year={2021},

publisher={MDPI}

}

```
@inproceedings{baral2024adaptive,
 title={An Adaptive End-to-End IoT Security Framework Using Explainable AI and LLMs},
 author={Baral, Sudipto and Saha, Sajal and Haque, Anwar},
 booktitle={2024 IEEE 10th World Forum on Internet of Things (WF-IoT)},
 pages={469--474},
 year={2024},
 organization={IEEE}
}
@article{ahsan2025explainable,
 title={An explainable ensemble-based intrusion detection system for software-defined vehicle ad-hoc networks},
 author={Ahsan, Shakil Ibne and Legg, Phil and Alam, SM Iftekharul},
 journal={Cyber Security and Applications},
 volume={3},
 pages={100090},
 year={2025},
 publisher={Elsevier}
}
@article{wali2025explainable,
 title={Explainable AI and random forest based reliable intrusion detection system},
 author={Wali, Syed and Farrukh, Yasir Ali and Khan, Irfan},
 journal={Computers \& Security},
 pages={104542},
 year={2025},
 publisher={Elsevier}
}
```

```
@article{dilip2025detecting,
  title={Detecting and Mitigating DDoS Attacks: The Role of AI and Machine Learning},
  author={Dilip, Kumar and Yashwant, Kumar},
  journal={International Journal of Trend in Scientific Research and Development},
  volume={9},
  number={2},
  pages={1017--1024},
  year={2025},
  publisher={IJTSRD}
}
@article{kavitha2024machine,
  title={Machine learning-based DDOS Attack Detection and Mitigation in SDNs for IoT environments},
  author={Kavitha, D and Ramalakshmi, R},
  journal={Journal of the Franklin Institute},
  volume={361},
  number={17},
  pages={107197},
  year={2024},
  publisher={Elsevier}
}
@inproceedings{ping2024study,
  title={A Study on the Application of Artificial Intelligence in DDoS Attack Defense: A Literature Review},
  author={Ping, Zhe and Jiao, Dingyang},
  booktitle={Proceedings of the 2024 4th International Conference on Big Data, Artificial Intelligence and Risk Management},
  pages={200--205},
  year={2024}
}
@article{thudumu2020comprehensive,
  title={A comprehensive survey of anomaly detection techniques for high dimensional big data},
  author={Thudumu, Srikanth and Branch, Philip and Jin, Jiong and Singh, Jugdutt},
  journal={Journal of big data},
  volume={7},
  number={1},
  pages={42},
  year={2020},
  publisher={Springer}
}
@article{jadhavcomprehensive,
  title={Comprehensive Survey on Detection of Anomalies in Edge Computing Network and Deep Learning Solutions},
  author={Jadhav, Sonali and Kulkarni, Arun}
}
@article{zamanzadeh2024deep,
  title={Deep learning for time series anomaly detection: A survey},
  author={Zamanzadeh Darban, Zahra and Webb, Geoffrey I and Pan, Shirui and Aggarwal, Charu and Salehi, Mahsa},
  journal={ACM Computing Surveys},
  volume={57},
  number={1},
  pages={1--42},
  year={2024},
  publisher={ACM New York, NY}
}
@article{kohli2025comprehensive,
  title={A comprehensive survey on techniques, challenges, evaluation metrics and
applications of deep learning models for anomaly detection},
  author={Kohli, Mudita and Chhabra, Indu},
  journal={Discover Applied Sciences},
  volume={7},
  number={7},
  pages={784},
  year={2025},
  publisher={Springer}
}
@article{mittal2023deep,
  title={Deep learning approaches for detecting DDoS attacks: A systematic review},
  author={Mittal, Meenakshi and Kumar, Krishan and Behal, Sunny},
  journal={Soft computing},
  volume={27},
  number={18},
  pages={13039--13075},
  year={2023},
  publisher={Springer}
}
@article{dilip2025detecting,
  title={Detecting and Mitigating DDoS Attacks: The Role of AI and Machine Learning},
  author={Dilip, Kumar and Yashwant, Kumar},
  journal={International Journal of Trend in Scientific Research and Development},
  volume={9},
  number={2},
  pages={1017--1024},
  year={2025},
  publisher={IJTSRD}
}
@article{kavitha2024machine,
  title={Machine learning-based DDOS Attack Detection and Mitigation in SDNs for IoT environments},
  author={Kavitha, D and Ramalakshmi, R},
  journal={Journal of the Franklin Institute},
  volume={361},
  number={17},
  pages={107197},
  year={2024},
  publisher={Elsevier}
}
@inproceedings{ping2024study,
  title={A Study on the Application of Artificial Intelligence in DDoS Attack Defense: A Literature Review},
  author={Ping, Zhe and Jiao, Dingyang},
  booktitle={Proceedings of the 2024 4th International Conference on Big Data, Artificial Intelligence and Risk Management},
  pages={200--205},
  year={2024}
```

```
}
@article{thudumu2020comprehensive,
  title={A comprehensive survey of anomaly detection techniques for high dimensional big data},
  author={Thudumu, Srikanth and Branch, Philip and Jin, Jiong and Singh, Jugdutt},
  journal={Journal of big data},
  volume={7},
  number={1},
  pages={42},
  year={2020},
  publisher={Springer}
}
@article{jadhavcomprehensive,
  title={Comprehensive Survey on Detection of Anomalies in Edge Computing Network and Deep Learning Solutions},
  author={Jadhav, Sonali and Kulkarni, Arun}
}
@article{zamanzadeh2024deep,
  title={Deep learning for time series anomaly detection: A survey},
  author={Zamanzadeh Darban, Zahra and Webb, Geoffrey I and Pan, Shirui and Aggarwal, Charu and Salehi, Mahsa},
  journal={ACM Computing Surveys},
  volume={57},
  number={1},
  pages={1--42},
  year={2024},
  publisher={ACM New York, NY}
```

```
}
@article{kohli2025comprehensive,
  title={A comprehensive survey on techniques, challenges, evaluation metrics and applications of deep learning models for anomaly detection},
  author={Kohli, Mudita and Chhabra, Indu},
  journal={Discover Applied Sciences},
  volume={7},
  number={7},
  pages={784},
  year={2025},
  publisher={Springer}
}
@article{mittal2023deep,
  title={Deep learning approaches for detecting DDoS attacks: A systematic review},
  author={Mittal, Meenakshi and Kumar, Krishan and Behal, Sunny},
  journal={Soft computing},
  volume={27},
  number={18},
  pages={13039--13075},
  year={2023},
  publisher={Springer}
}
@article{li2025survey,
  title={A survey of deep learning for industrial visual anomaly detection},
  author={Li, Zhuo and Yan, Yuhao and Wang, Xiangheng and Ge, Yifei and Meng, Lin},
  journal={Artificial Intelligence Review},
  volume={58},
  number={9},
  pages={279},
  year={2025},
  publisher={Springer}
}
@inproceedings{yin2025drllm,
  title={DrLLM: Prompt-Enhanced Distributed Denial-of-Service Resistance Method with Large Language Models},
  author={Yin, Zhenyu and Liu, Shang and Xu, Guangyuan},
  booktitle={ICASSP 2025-2025 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)},
  pages={1--5},
  year={2025},
  organization={IEEE}
}
@article{arreche2024xai,
  title={E-xai: Evaluating black-box explainable ai frameworks for network intrusion detection},
  author={Arreche, Osvaldo and Guntur, Tanish R and Roberts, Jack W and Abdallah, Mustafa},
  journal={IEEE Access},
  volume={12},
  pages={23954--23988},
  year={2024},
  publisher={IEEE}
}
```

```
@inproceedings{Ivo,
title ={Explainable AI (XAI) for Cybersecurity: Intrusion Detection System (IDS)},
Author = {Ivo Afonso Bispo},
 booktitle={},
pages={},
  year={2025},
organization = {Computer Science and Communication Research Centr}
}
@inproceedings{bushart2023anomaly,
  title={Anomaly-based filtering of application-layer DDoS against DNS authoritatives},
  author={Bushart, Jonas and Rossow, Christian},
  booktitle={2023 IEEE 8th European Symposium on Security and Privacy (EuroS\&P)},
  pages={558--575},
  year={2023},
  organization={IEEE}
}
@article{gavric2024towards, title={Towards resource-efficient DDoS detection in IoT: leveraging feature engineering of system and network usage metrics},
  author={Gavric, Nikola and Prasad Bhandari, Guru and Shalaginov, Andrii},
  journal={Journal of Network and Systems Management},
  volume={32},
  number={4},
  pages={69},
  year={2024},
  publisher={Springer}
}
```

```
@article{mittal2023ddosat2022,
  title={DDoS-AT-2022: a distributed denial of service attack dataset for evaluating DDoS
defense system},
  author={Mittal, Harsh and Saluja, Hitesh and Behal, Shubham},
  journal={Proceedings of the Indian National Science Academy},
  volume={89},
  number={2},
  pages={565--573},
  year={2023},
  publisher={Springer},
  doi={10.1007/s43538-023-00114-3},
  url={https://doi.org/10.1007/s43538-023-00114-3}
}
@inproceedings{cuppers2024flowchronicle,
  author      = {Cüppers, Henning and Schoen, Simon and Blanc, Gregory and Gimenez,
Pierre-François},
  title       = {FlowChronicle: Synthetic Network Flow Generation through Pattern Set Mining},
  booktitle   = {Proceedings of the 20th International Conference on Emerging Networking
Experiments and Technologies (CoNEXT)},
  year        = {2024},
  publisher   = {Association for Computing Machinery},
  address     = {New York, NY, USA},
  doi         = {10.1145/3651205.3651217},
  url         = {https://doi.org/10.1145/3651205.3651217}
}
@article{aceto2024synthetic,
```

title = {Synthetic and privacy-preserving traffic trace generation using generative AI models for training Network Intrusion Detection Systems},

author = {Aceto, Giuseppe and Giampaolo, Fabio and Guida, Ciro and Izzo, Stefano and Pescape, Antonio and Piccialli, Francesco and Prezioso, Edoardo},

journal = {Journal of Network and Computer Applications},

year = {2024},

volume = {229},

pages = {103926},

doi = {10.1016/j.jnca.2024.103926},

note = {Dataset available at \url{https://codeberg.org/CiroGuida/GenAI-network-traffic}}

}

@article{tuli2022tranad,

title={Tranad: Deep transformer networks for anomaly detection in multivariate time series data},

author={Tuli, Shreshth and Casale, Giuliano and Jennings, Nicholas R},

journal={arXiv preprint arXiv:2201.07284},

year={2022}

}

@article{bamber2025hybrid,

title={A hybrid CNN-LSTM approach for intelligent cyber intrusion detection system},

author={Bamber, Sukhvinder Singh and Katkuri, Aditya Vardhan Reddy and Sharma, Shubham and Angurala, Mohit},

journal={Computers \& Security},

volume={148},

pages={104146},

year={2025},

publisher={Elsevier}

```
}

@article{kumar2025investigating,
 title={Investigating the performance of multivariate LSTM models to predict the occurrence of Distributed Denial of Service (DDoS) attack},
 author={Kumar, Prashant and Kushwaha, Chitra and Sethi, Dimple and Ghosh, Debjani and Gupta, Punit and Vidyarthi, Ankit},
 journal={PloS one},
 volume={20},
 number={1},
 pages={e0313930},
 year={2025},
 publisher={Public Library of Science San Francisco, CA USA}
}
@article{anley2024robust,
 title={Robust DDoS attack detection with adaptive transfer learning},
 author={Anley, Mulualem Bitew and Genovese, Angelo and Agostinello, Davide and Piuri, Vincenzo},
 journal={Computers \& Security},
 volume={144},
 pages={103962},
 year={2024},
 publisher={Elsevier}
}
@article{shaikh2025deep,
  title={A deep Reinforcement learning-based robust Intrusion Detection System for securing IoMT Healthcare Networks},
  author={Shaikh, Jamshed Ali and Wang, Chengliang and Sima, Muhammad Wajeeh Us and Arshad, Muhammad and Owais, Muhammad and Hassan, Dina SM and Alkanhel, Reem and Muthanna, Mohammed Saleh Ali},
  journal={Frontiers in Medicine},
  volume={12},
  pages={1524286},
  year={2025},
  publisher={Frontiers Media SA}
}
@article{arif2024dqqs,
  title={DQQS: Deep Reinforcement Learning based Technique for Enhancing Security and Performance in SDN-IoT Environments},
  author={Arif, Fahim and Khan, Nauman Ali and Iqbal, Javed and Karim, Faten Khalid and Innab, Nisreen and Mostafa, Samih M and others},
  journal={IEEE Access},
  year={2024},
  publisher={IEEE}
}
@article{yungaicela2022flexible,
  title={A flexible SDN-based framework for slow-rate DDoS attack mitigation by using deep reinforcement learning},
  author={Yungaicela-Naula, Noe M and Vargas-Rosales, Cesar and P{\'e}rez-D{\'\i}az, Jes{\'u}s Arturo and Carrera, Diego Fernando},
  journal={Journal of network and computer applications},
  volume={205},
  pages={103444},
  year={2022},
  publisher={Elsevier}
}
@misc{feng2020application,
  title={Application-layer DDoS defense with reinforcement learning. In 2020 IEEE/ACM 28th International Symposium on Quality of Service (IWQoS)(June 2020)},
  author={Feng, Yebo and Li, Jun and Nguyen, Thanh},
  year={2020},
  publisher={IEEE}
}
@article{wei2023reconstruction,
  title={Reconstruction-based lstm-autoencoder for anomaly-based ddos attack detection over multivariate time-series data},
  author={Wei, Yuanyuan and Jang-Jaccard, Julian and Sabrina, Fariza and Xu, Wen and Camtepe, Seyit and Dunmore, Aeryn},
  journal={arXiv preprint arXiv:2305.09475},
  year={2023}

@article{phan2020deepguard,
  title={DeepGuard: Efficient anomaly detection in SDN with fine-grained traffic flow monitoring},
  author={Phan, Trung V and Nguyen, Tri Gia and Dao, Nhu-Ngoc and Huong, Truong Thu and Thanh, Nguyen Huu and Bauschert, Thomas},
  journal={IEEE Transactions on Network and Service Management},
  volume={17},
  number={3},
  pages={1349--1362},
  year={2020},
  publisher={IEEE}
}
@article{batchu2024novel,
  title={A novel optimization-driven deep learning framework for the detection of DDoS attacks},
  author={Batchu, Raj Kumar and Bikku, Thulasi and Thota, Srinivasarao and Seetha, Hari and Ayoade, Abayomi Ayotunde},
  journal={Scientific Reports},
  volume={14},
  number={1},
  pages={28024},
  year={2024},
  publisher={Nature Publishing Group UK London}
}
@inproceedings{srilatha2022ddosnet,
  title={DDoSNet: A deep learning model for detecting network attacks in cloud computing},
  author={Srilatha, Doddi and Thillaiarasu, N},
  booktitle={2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA)},
  pages={576--581},
  year={2022},
  organization={IEEE}
}
@article{alzu2024explainable,
  title={Explainable AI-Based DDoS Attacks Classification Using Deep Transfer Learning.},
```

author={Alzu'bi, Ahmad and Albashayreh, Amjad and Abuarqoub, Abdelrahman and Alfawair, Mai AM},

journal={Computers, Materials \& Continua},

volume={80},

number={3},

year={2024}

}@article{alfatemi2024advancing,

title={Advancing ddos attack detection: A synergistic approach using deep residual neural networks and synthetic oversampling},

author={Alfatemi, Ali and Rahouti, Mohamed and Amin, Ruhul and ALJamal, Sarah and Xiong, Kaiqi and Xin, Yufeng},

journal={arXiv preprint arXiv:2401.03116},

year={2024}

}

@article{okporokpo2025detection,

title={Detection of DDoS Cyberattack Using a Hybrid Trust-Based Technique for Smart Home Networks.},

author={Okporokpo, Oghenetejiri and Olajide, Funminiyi and Ajienka, Nemitari and others},

journal={International Journal of Advanced Computer Science \& Applications},

volume={16},

number={1},

year={2025}

}

@inproceedings{sudar2021detection,

title={Detection of Distributed Denial of Service Attacks in SDN using Machine learning techniques}, author={Sudar, K Muthamil and Beulah, M and Deepalakshmi, P and Nagaraj, P and Chinnasamy, P},

booktitle={2021 international conference on Computer Communication and Informatics (ICCCI)},

pages={1--5},

year={2021},

organization={IEEE}

}

@inproceedings{kavitha2022machine,

title={Machine learning techniques for detecting ddos attacks in sdn},

author={Kavitha, M and Suganthy, M and Biswas, Aniket and Srinivsan, R and Kavitha, R and Rathesh, A},

booktitle={2022 International Conference on Automation, Computing and Renewable Systems (ICACRS)},

pages={634--638},

year={2022},

organization={IEEE}

}

@article{santos2020machine,

title={Machine learning algorithms to detect DDoS attacks in SDN},

author={Santos, Reneilson and Souza, Danilo and Santo, Walter and Ribeiro, Admilson and Moreno, Edward},

journal={Concurrency and Computation: Practice and Experience},

volume={32},

number={16},

pages={e5402},

year={2020},

publisher={Wiley Online Library}

@article{ribeiro2023detecting,

title={Detecting and mitigating DDoS attacks with moving target defense approach based on automated flow classification in SDN networks},

author={Ribeiro, Marcos Aur{\'e}lio and Fonseca, Mauro Sergio Pereira and de Santi, Juliana},

journal={Computers \& Security},

volume={134},

pages={103462},

year={2023},

publisher={Elsevier}

}

@inproceedings{sekar2023prediction,

title={Prediction of distributed denial of service attacks in SDN using machine learning techniques},

author={Sekar, R Raja and Jenny, Ardhala Mounika and Sreshta, Dubba and Vikas, M and Ajay, Dasari Badri Nageshwar and Ganesh, Mankena},

booktitle={2023 3rd International Conference on Intelligent Technologies (CONIT)},

pages={1--5},

year={2023},

organization={IEEE}

}

@article{alashhab2024enhancing,

title={Enhancing DDoS attack detection and mitigation in SDN using an ensemble online machine learning model},

```
  author={Alashhab, Abdussalam Ahmed and Zahid, Mohd Soperi and Isyaku, Babangida and Elnour, Asma Abbas and Nagmeldin, Wamda and Abdelmaboud, Abdelzahir and Abdullah, Talal Ali Ahmed and Maiwada, Umar Danjuma},
  journal={IEEE access},
  volume={12},
  pages={51630--51649},
  year={2024},
  publisher={IEEE}
}
@inproceedings{kousar2021detection,
  title={Detection of DDoS attacks in software defined network using decision tree},
  author={Kousar, Heena and Mulla, Mohammed Moin and Shettar, Pooja and Narayan, DG},
  booktitle={2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT)},
  pages={783--788},
  year={2021},
  organization={IEEE}
}
@article{kim2025secured-x,
  title={Secured Network Architectures Based on Blockchain Technologies: A Systematic Review},
  author={Kim, Song-Kyoo and Vong, Hou Cheng},
  journal={ACM Computing Surveys},
  year={2025},
  publisher={ACM New York, NY}
}
ublisher={IEEE}
```

```
@article{linhares2023sdntruth,
  title={SDNTruth: innovative DDoS detection scheme for software-defined networks (SDN)},
  author={Linhares, Tiago and Patel, Ahmed and Barros, Ana Luiza and Fernandez, Marcial},
  journal={Journal of Network and Systems Management},
  volume={31},
  number={3},
  pages={55},
  year={2023},
  publisher={Springer}
}
@article{thamilarasu2019towards,
  title={Towards deep-learning-driven intrusion detection for the internet of things},
  author={Thamilarasu, Geethapriya and Chawla, Shiven},
  journal={Sensors},
  volume={19},
  number={9},
  pages={1977},
  year={2019},
  publisher={MDPI}
}
@article{zhao2023cnn,
  title={CNN-AttBiLSTM mechanism: a DDoS attack detection method based on attention mechanism and CNN-BiLSTM},
  author={Zhao, Junjie and Liu, Yongmin and Zhang, Qianlei and Zheng, Xinying},
  journal={IEEE Access},
  volume={11},
  pages={136308--136317},
  year={2023},
  publisher={IEEE}
}@article{alzu2024explainable,
  title={Explainable AI-Based DDoS Attacks Classification Using Deep Transfer Learning.},
  author={Alzu'bi, Ahmad and Albashayreh, Amjad and Abuarqoub, Abdelrahman and Alfawair, Mai AM},
  journal={Computers, Materials \& Continua},
  volume={80},
  number={3},
  year={2024}
}
@article{bensaoud2025optimized,
  title={Optimized detection of cyber-attacks on IoT networks via hybrid deep learning models},
  author={Bensaoud, Ahmed and Kalita, Jugal},
  journal={Ad Hoc Networks},
  volume={170},
  pages={103770},
  year={2025},
  publisher={Elsevier}
}
@inproceedings{kim2024model,
  title={When model meets new normals: test-time adaptation for unsupervised time-series anomaly detection},
  author={Kim, Dongmin and Park, Sunghyun and Choo, Jaegul},
  booktitle={Proceedings of the AAAI conference on artificial intelligence},
  volume={38},
  number={12},
  pages={13113--13121},
  year={2024}
}
@article{arulselvan2023retracted,
  title={RETRACTED: Hybrid trust-based secure routing protocol for detection of routing attacks in environment monitoring over MANETs},
  author={Arulselvan, G and Rajaram, A},
  journal={Journal of Intelligent \& Fuzzy Systems},
  volume={45},
  number={4},
  pages={6575--6590},
  year={2023},
  publisher={SAGE Publications Sage UK: London, England}
}
@article{ahmadi2024trust,
  title={A Trust Based Anomaly Detection Scheme Using a Hybrid Deep Learning Model for IoT Routing Attacks Mitigation},
  author={Ahmadi, Khatereh and Javidan, Reza},
  journal={IET Information Security},
  volume={2024},
  number={1},
  pages={4449798},
  year={2024},
  publisher={Wiley Online Library}
}
```

```
@article{hekmati2024correlation,
  title={Correlation-aware neural networks for DDOS attack detection in IoT systems},
  author={Hekmati, Arvin and Zhang, Jiahe and Sarkar, Tamoghna and Jethwa, Nishant and Grippo, Eugenio and Krishnamachari, Bhaskar},
  journal={IEEE/ACM Transactions on Networking},
  year={2024},
  publisher={IEEE}
}
@article{liu2023ddos,
  title={A DDoS detection method based on feature engineering and machine learning in software-defined networks},
  author={Liu, Zhenpeng and Wang, Yihang and Feng, Fan and Liu, Yifan and Li, Zelin and Shan, Yawei},
  journal={Sensors},
  volume={23},
  number={13},
  pages={6176},
  year={2023},
  publisher={MDPI}
}
@article{li2025ad2t,
  title={AD2T: Multivariate Time Series Anomaly Detection with Association Discrepancy Dual-Decoder Transformer},
  author={Li, Zezhong and Guo, Wei and An, Jianpeng and Wang, Qi and Mei, Yingchun and Juan, Rongshun and Wang, Tianshu and Li, Yang and Gao, Zhongke},
  journal={IEEE Sensors Journal},
  year={2025},
  publisher={IEEE}
}
@article{dai2024sarad,
  title={SARAD: Spatial association-aware anomaly detection and diagnosis for multivariate time series},
  author={Dai, Zhihao and He, Ligang and Yang, Shuanghua and Leeke, Matthew},
  journal={Advances in Neural Information Processing Systems},
  volume={37},
  pages={48371--48410},
  year={2024}
}
@article{munir2018deepant,
  title={DeepAnT: A deep learning approach for unsupervised anomaly detection in time series},
  author={Munir, Mohsin and Siddiqui, Shoaib Ahmed and Dengel, Andreas and Ahmed, Sheraz},
  journal={IEEE Access},
  volume={7},
  pages={1991--2005},
  year={2018},
  publisher={IEEE}
}
}
@inproceedings{xu2018unsupervised,
  title={Unsupervised anomaly detection via variational auto-encoder for seasonal kpis in web applications},
  author={Xu, Haowen and Chen, Wenxiao and Zhao, Nengwen and Li, Zeyan and Bu, Jiahao and Li, Zhihan and Liu, Ying and Zhao, Youjian and Pei, Dan and Feng, Yang and others},
  booktitle={Proceedings of the 2018 world wide web conference},
  pages={187--196},
  year={2018}
}
@inproceedings{su2019robust-x,
  title={Robust anomaly detection for multivariate time series through stochastic recurrent neural network},
  author={Su, Ya and Zhao, Youjian and Niu, Chenhao and Liu, Rong and Sun, Wei and Pei, Dan},
  booktitle={Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery \& data mining},
  pages={2828--2837},
  year={2019}
}
@article{shen2020timeseries,
  title={Timeseries anomaly detection using temporal hierarchical one-class network},
  author={Shen, Lifeng and Li, Zhuocong and Kwok, James},
  journal={Advances in neural information processing systems},
  volume={33},
  pages={13016--13026},
  year={2020}
}
@inproceedings{audibert2020usad,
  title={Usad: Unsupervised anomaly detection on multivariate time series},
  author={Audibert, Julien and Michiardi, Pietro and Guyard, Fr{\'e}d{\'e}ric and Marti,
S{\'e}bastien and Zuluaga, Maria A},
  booktitle={Proceedings of the 26th ACM SIGKDD international conference on knowledge
discovery \& data mining},
  pages={3395--3404},
  year={2020}
}

@article{shwartz2022tabular,
  title={Tabular data: Deep learning is not all you need},
  author={Shwartz-Ziv, Ravid and Armon, Amitai},
  journal={Information Fusion},
  volume={81},
  pages={84--90},
  year={2022},
  publisher={Elsevier}
}
@article{xu2021anomaly,
  title={Anomaly transformer: Time series anomaly detection with association discrepancy},
  author={Xu, Jiehui and Wu, Haixu and Wang, Jianmin and Long, Mingsheng},
  journal={arXiv preprint arXiv:2110.02642},
  year={2021}
}
@inproceedings{geiger2020tadgan,
  title={Tadgan: Time series anomaly detection using generative adversarial networks},
  author={Geiger, Alexander and Liu, Dongyu and Alnegheimish, Sarah and Cuesta-Infante,
Alfredo and Veeramachaneni, Kalyan},
  booktitle={2020 ieee international conference on big data (big data)},
  pages={33--43},
  year={2020},
  organization={IEEE}
}
@inproceedings{mohammadi2023anomaly,
  title={Anomaly detection using lstm-autoencoder in smart grid: A federated learning approach},
  author={Mohammadi, Mohammadreza and Shrestha, Rakesh and Sinaei, Sima and Salcines, Alberto and Pampliega, David and Clemente, Raul and Sanz, Ana Lourdes},
  booktitle={Proceedings of the 2023 7th International Conference on Cloud and Big Data Computing},
  pages={48--54},
  year={2023}
}
@inproceedings{zhang2019deep,
  title={A deep neural network for unsupervised anomaly detection and diagnosis in multivariate time series data},
  author={Zhang, Chuxu and Song, Dongjin and Chen, Yuncong and Feng, Xinyang and Lumezanu, Cristian and Cheng, Wei and Ni, Jingchao and Zong, Bo and Chen, Haifeng and Chawla, Nitesh V},
  booktitle={Proceedings of the AAAI conference on artificial intelligence},
  volume={33},
  number={01},
  pages={1409--1416},
  year={2019}
}
@article{pakmehr2024ddos,
  title={DDoS attack detection techniques in IoT networks: a survey},
  author={Pakmehr, Amir and A{\ss}muth, Andreas and Taheri, Negar and Ghaffari, Ali},
  journal={Cluster Computing},
  volume={27},
  number={10},
  pages={14637--14668},
  year={2024},
  publisher={Springer}
}
@inproceedings{sanap2023comprehensive,
  title={A Comprehensive Survey On Detection And Mitigation Of DDoS Attacks Enabled With Deep Learning Techniques In Cloud Computing},
  author={Sanap, Yogesh B and Aher, Pushpalata},
  booktitle={2023 6th International Conference on Advances in Science and Technology (ICAST)},
  pages={149--154},
  year={2023},
  organization={IEEE}
}
@article{liu2023real,
  title={Real-time anomaly detection of network traffic based on CNN},
  author={Liu, Haitao and Wang, Haifeng},
  journal={Symmetry},
  volume={15},
  number={6},
  pages={1205},
  year={2023},
```

publisher={MDPI}

}

@article{alzu2024explainable,

title={Explainable AI-Based DDoS Attacks Classification Using Deep Transfer Learning.},

author={Alzu'bi, Ahmad and Albashayreh, Amjad and Abuarqoub, Abdelrahman and Alfawair, Mai AM},

journal={Computers, Materials \& Continua},

volume={80},

number={3},

year={2024}

}

@article{arrieta2020explainable,

title={Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI},

author={Arrieta, Alejandro Barredo and D{\'\i}az-Rodr{\'\i}guez, Natalia and Del Ser, Javier and Bennetot, Adrien and Tabik, Siham and Barbado, Alberto and Garc{\'\i}a, Salvador and Gil-L{\'o}pez, Sergio and Molina, Daniel and Benjamins, Richard and others},

journal={Information fusion},

volume={58},

pages={82--115},

year={2020},

publisher={Elsevier}

}

@article{mohammadi2017slicots,

title={Slicots: An sdn-based lightweight countermeasure for tcp syn flooding attacks},

author={Mohammadi, Reza and Javidan, Reza and Conti, Mauro},

journal={IEEE Transactions on Network and Service Management}, volume={14},

number={2},

pages={487--497},

year={2017},

publisher={IEEE}

}

@inproceedings{dimolianis2021syn,

title={SYN flood attack detection and mitigation using machine learning traffic classification and programmable data plane filtering},

author={Dimolianis, Marinos and Pavlidis, Adam and Maglaris, Vasilis},

booktitle={2021 24th conference on innovation in clouds, internet and networks and workshops (ICIN)},

pages={126--133},

year={2021},

organization={IEEE}

}

@inproceedings{zha2020meta,

title={Meta-AAD: Active anomaly detection with deep reinforcement learning},

author={Zha, Daochen and Lai, Kwei-Herng and Wan, Mingyang and Hu, Xia},

booktitle={2020 IEEE International Conference on Data Mining (ICDM)},

pages={771--780},

year={2020},

organization={IEEE}

}@inproceedings{baitieva2024supervised,

title={Supervised Anomaly Detection for Complex Industrial Images},

author={Baitieva, Aimira and Hurych, David and Besnier, Victor and Bernard, Olivier},

```
  booktitle={Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition},

  pages={17754--17762},

  year={2024}

}

@inproceedings{zhong2019graph,

  title={Graph convolutional label noise cleaner: Train a plug-and-play action classifier for anomaly detection},

  author={Zhong, Jia-Xing and Li, Nannan and Kong, Weijie and Liu, Shan and Li, Thomas H and Li, Ge},

  booktitle={Proceedings of the IEEE/CVF conference on computer vision and pattern recognition},

  pages={1237--1246},

  year={2019}

}@article{xu2023rosas,

  title={Rosas: Deep semi-supervised anomaly detection with contamination-resilient continuous supervision},

  author={Xu, Hongzuo and Wang, Yijie and Pang, Guansong and Jian, Songlei and Liu, Ning and Wang, Yongjun},

  journal={Information Processing \& Management},

  volume={60},

  number={5},

  pages={103459},

  year={2023},

  publisher={Elsevier}

}

@inproceedings{wolleb2022diffusion,

  title={Diffusion models for medical anomaly detection},
  author={Wolleb, Julia and Bieder, Florentin and Sandk{\"u}hler, Robin and Cattin, Philippe C},
  booktitle={International Conference on Medical image computing and computer-assisted intervention},
  pages={35--45},
  year={2022},
  organization={Springer}
}
@article{zhou2021feature,
  title={Feature encoding with autoencoders for weakly supervised anomaly detection},
  author={Zhou, Yingjie and Song, Xucheng and Zhang, Yanru and Liu, Fanxing and Zhu, Ce and Liu, Lingqiao},
  journal={IEEE Transactions on Neural Networks and Learning Systems},
  volume={33},
  number={6},
  pages={2454--2465},
  year={2021},
  publisher={IEEE}
}
@article{chen2022supervised,
  title={Supervised anomaly detection via conditional generative adversarial network and ensemble active learning},
  author={Chen, Zhi and Duan, Jiang and Kang, Li and Qiu, Guoping},
  journal={IEEE Transactions on Pattern Analysis and Machine Intelligence},
  volume={45},
  number={6},
  pages={7781--7798},
  year={2022},
  publisher={IEEE}
}
@inproceedings{schluter2022natural,
  title={Natural synthetic anomalies for self-supervised anomaly detection and localization},
  author={Schl{\"u}ter, Hannah M and Tan, Jeremy and Hou, Benjamin and Kainz, Bernhard},
  booktitle={European Conference on Computer Vision},
  pages={474--489},
  year={2022},
  organization={Springer}
}
@article{singh2020detection,
  title={Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions},
  author={Singh, Jagdeep and Behal, Sunny},
  journal={Computer Science Review},
  volume={37},
  pages={100279},
  year={2020},
  publisher={Elsevier}
}

@misc{netscout2021,
  author      = {Carol Hildebrand},
  title       = {The Beat Goes On},
  howpublished = {\url{https://www.netscout.com/blog/asert/beat-goes}},
  note        = {NETSCOUT ASERT Blog, Accessed: May 21, 2025},
  year        = {2021}
}
@misc{livemint2020,
  author      = {{LiveMint News Staff}},
  title       = {Google Services Including YouTube, Gmail, Google Drive Face Outage Due to DDoS Attack},
  howpublished = {\url{https://www.livemint.com/technology/apps/google-services-youtube-gmail-google-drive-face-outage-11607947475759.html}},
  note        = {Accessed: May 21, 2025},
  year        = {2020}
}
@inproceedings{misa2024leveraging,
  title={Leveraging prefix structure to detect volumetric ddos attack signatures with programmable switches},
  author={Misa, Chris and Durairajan, Ramakrishnan and Gupta, Arpit and Rejaie, Reza and Willinger, Walter},
  booktitle={2024 IEEE Symposium on Security and Privacy (SP)},
  pages={4535--4553},
  year={2024},
  organization={IEEE}
}
@misc{httpbot2025,
  author      = {Ravie Lakshmanan},
  title       = {New HTTPBot Botnet Launches 200+ Precision DDoS Attacks on Gaming and Tech Sectors},
  howpublished = {\url{https://thehackernews.com/2025/05/new-httpbot-botnet-launches-200.html}},
  note       = {Accessed: May 21, 2025},
  year       = {2025}
}
@inproceedings{kim2024model,
  title={When model meets new normals: test-time adaptation for unsupervised time-series anomaly detection},
  author={Kim, Dongmin and Park, Sunghyun and Choo, Jaegul},
  booktitle={Proceedings of the AAAI conference on artificial intelligence},
  volume={38},
  number={12},
  pages={13113--13121},
  year={2024}
}
@article{malik2023feature,
  title={Feature engineering and machine learning framework for DDoS attack detection in the standardized internet of things},
  author={Malik, Manisha and Dutta, Maitreyee and others},
  journal={IEEE Internet of Things Journal},
  volume={10},
  number={10},
  pages={8658--8669},
  year={2023},
  publisher={IEEE}
}
@article{neto2023ciciot2023,
  title={CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment},
```

author={Neto, Euclides Carlos Pinto and Dadkhah, Sajjad and Ferreira, Raphael and Zohourian, Alireza and Lu, Rongxing and Ghorbani, Ali A},

journal={Sensors},

volume={23},

number={13},

pages={5941},

year={2023},

publisher={MDPI}

}@article{bamasag2022real,

title={Real-time DDoS flood attack monitoring and detection (RT-AMD) model for cloud computing},

author={Bamasag, Omaimah and Alsaeedi, Alaa and Munshi, Asmaa and Alghazzawi, Daniyal and Alshehri, Suhair and Jamjoom, Arwa},

journal={PeerJ Computer Science},

volume={7},

pages={e814},

year={2022},

publisher={PeerJ Inc.}

}

@article{liu2023ddos,

title={A DDoS detection method based on feature engineering and machine learning in software-defined networks},

author={Liu, Zhenpeng and Wang, Yihang and Feng, Fan and Liu, Yifan and Li, Zelin and Shan, Yawei},

journal={Sensors},

volume={23},

number={13},

```
  pages={6176},
  year={2023},
  publisher={MDPI}
}
@inproceedings{ozccam2021detecting,
  title={Detecting tcp flood ddos attack by anomaly detection based on machine learning algorithms},
  author={{\"O}z{\c{c}}am, Berkay and Kilinc, H Hakan and Zaim, Abd{\"u}l Halim},
  booktitle={2021 6th International Conference on Computer Science and Engineering (UBMK)},
  pages={512--516},
  year={2021},
  organization={IEEE}
}
@article{musa2024machine,
  title={machine learning and deep learning techniques for distributed denial of service anomaly detection in software defined networks—current research solutions},
  author={Musa, Nura Shifa and Mirza, Nada Masood and Rafique, Saida Hafsa and Abdallah, Amira Mahamat and Murugan, Thangavel},
  journal={IEEE Access},
  volume={12},
  pages={17982--18011},
  year={2024},
  publisher={IEEE}
}
@article{phan2020deepguard,
 title={DeepGuard: Efficient anomaly detection in SDN with fine-grained traffic flow monitoring},
 author={Phan, Trung V and Nguyen, Tri Gia and Dao, Nhu-Ngoc and Huong, Truong Thu and Thanh, Nguyen Huu and Bauschert, Thomas},
 journal={IEEE Transactions on Network and Service Management},
 volume={17},
 number={3},
 pages={1349--1362},
 year={2020},
 publisher={IEEE}
}
@article{zhang2020cyber,
 author    = {Lan Zhang and Others},
 title     = {High-Level Cyber Attacks Detection Using AI},
 journal   = {IEEE Transactions on Information Forensics and Security},
 volume    = {15},
 pages     = {1234--1245},
 year      = {2020}
}

@article{han2012ddos,
 author    = {Han and Others},
 title     = {Massive DDoS Attack on Cryptocurrency Exchange: A Case Study},
 journal   = {IEEE Access},
 volume    = {10},
 pages     = {1435--1448},
 year      = {2012}
```

}

@article{berman2019survey,

title={A survey of deep learning methods for cyber security},

author={Berman, Daniel S and Buczak, Anna L and Chavis, Jeffrey S and Corbett, Cherita L},

journal={Information},

volume={10},

number={4},

pages={122},

year={2019},

publisher={MDPI}

}

@article{li2023towards,

title={Towards real-time ML-based DDoS detection via cost-efficient window-based feature extraction},

author={Li, Haibin and Zhao, Yi and Yao, Wenbing and Xu, Ke and Li, Qi},

journal={Science China Information Sciences},

volume={66},

number={5},

pages={152105},

year={2023},

publisher={Springer}

}

@inproceedings{carvajal2003high,

title={High capacity motors on-line diagnosis based on ultra wide band partial discharge detection},

author={Carvajal, Antonio and Garcia-Colon, VR}, booktitle={4th IEEE International Symposium on Diagnostics for Electric Machines, Power Electronics and Drives, 2003. SDEMPED 2003.},

pages={168--170},

year={2003},

organization={IEEE}

}

@inproceedings{chahal2021distributed,

title={Distributed Denial of Service (DDoS) Attacks in Software-defined Networks (SDN)},

author={Chahal, Jasmeen Kaur and Kaur, Puninder and Sharma, Avinash},

booktitle={2021 5th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT)},

pages={291--295},

year={2021},

organization={IEEE}

}

@article{zhang2024revealing,

title={Revealing Protocol Architecture’s Design Patterns in the Volumetric DDoS Defense Design Space},

author={Zhang, Zhiyi and Xiao, Guorui and Song, Sichen and Aygun, R Can and Stavrou, Angelos and Zhang, Lixia and Osterweil, Eric},

journal={IEEE Communications Surveys \& Tutorials},

year={2024},

publisher={IEEE}

}

@article{mittal2023deep,

title={Deep learning approaches for detecting DDoS attacks: A systematic review},

author={Mittal, Meenakshi and Kumar, Krishan and Behal, Sunny},

```
  journal={Soft computing},
  volume={27},
  number={18},
  pages={13039--13075},
  year={2023},
  publisher={Springer}
}

@article{wang2025modern,
  title={Modern DDoS Threats and Countermeasures: Insights into Emerging Attacks and Detection Strategies},
  author={Wang, Jincheng and Yu, Le and Lui, John and Luo, Xiapu},
  journal={arXiv preprint arXiv:2502.19996},
  year={2025}
}
@article{li2023comprehensive,
  title={A comprehensive survey on DDoS defense systems: New trends and challenges},
  author={Li, Qing and Huang, He and Li, Ruoyu and Lv, Jianhui and Yuan, Zhenhui and Ma, Lianbo and Han, Yi and Jiang, Yong},
  journal={Computer Networks},
  volume={233},
  pages={109895},
  year={2023},
  publisher={Elsevier}
}
@phdthesis{rostamian2024applications,
  title={Applications of Deep Learning Models in Financial Forecasting},
  author={Rostamian, Ahoora},
  year={2024},
  school={University of Essex}
}
@inproceedings{hore2023empirical,
  title={Empirical evaluation of autoencoder models for anomaly detection in packet-based nids},
  author={Hore, Soumyadeep and Nguyen, Quoc H and Xu, Yulun and Shah, Ankit and Bastian, Nathaniel D and Le, Trung},
  booktitle={2023 IEEE Conference on Dependable and Secure Computing (DSC)},
  pages={1--8},
  year={2023},
  organization={IEEE}
}
@article{wang2023n,
  title={N-STGAT: Spatio-temporal graph neural network based network intrusion detection for near-earth remote sensing},
  author={Wang, Yalu and Li, Jie and Zhao, Wei and Han, Zhijie and Zhao, Hang and Wang, Lei and He, Xin},
  journal={Remote Sensing},
  volume={15},
  number={14},
  pages={3611},
  year={2023},
  publisher={MDPI}
}
@article{schmidl2022anomaly,
  title={Anomaly detection in time series: a comprehensive evaluation},
  author={Schmidl, Sebastian and Wenig, Phillip and Papenbrock, Thorsten},
  journal={Proceedings of the VLDB Endowment},
  volume={15},
  number={9},
  pages={1779--1797},
  year={2022},
  publisher={VLDB Endowment}
}
@article{chatterjee2022iot,
  title={IoT anomaly detection methods and applications: A survey},
  author={Chatterjee, Ayan and Ahmed, Bestoun S},
  journal={Internet of Things},
  volume={19},
  pages={100568},
  year={2022},
  publisher={Elsevier}
}
@article{khan2024anomaly,
  title={Anomaly detection in IoT-based healthcare: machine learning for enhanced security},
  author={Khan, Maryam Mahsal and Alkhathami, Mohammed},
  journal={Scientific reports},
  volume={14},
  number={1},
  pages={5872},
  year={2024},
  publisher={Nature Publishing Group UK London}
}

@article{peng2023rwkv,
  title={Rwkv: Reinventing rnns for the transformer era},
  author={Peng, Bo and Alcaide, Eric and Anthony, Quentin and Albalak, Alon and Arcadinho, Samuel and Biderman, Stella and Cao, Huanqi and Cheng, Xin and Chung, Michael and Grella, Matteo and others},
  journal={arXiv preprint arXiv:2305.13048},
  year={2023}
}
@article{kim2024optimal,
  title={Optimal Cyber Attack Strategy Using Reinforcement Learning Based on Common Vulnerability Scoring System.},
  author={Kim, Bum-Sok and Suk, Hye-Won and Choi, Yong-Hoon and Moon, Dae-Sung and Kim, Min-Suk},
  journal={CMES-Computer Modeling in Engineering \& Sciences},
  volume={141},
  number={2},
  year={2024}
}
@article{wang2023federated,
  title={Federated deep learning for anomaly detection in the internet of things},
  author={Wang, Xiaofeng and Wang, Yonghong and Javaheri, Zahra and Almutairi, Laila and Moghadamnejad, Navid and Younes, Osama S},
  journal={Computers and Electrical Engineering},
  volume={108},
  pages={108651},
  year={2023},
  publisher={Elsevier}
}
@article{wei2023reconstruction,
  title={Reconstruction-based lstm-autoencoder for anomaly-based ddos attack detection over multivariate time-series data},
  author={Wei, Yuanyuan and Jang-Jaccard, Julian and Sabrina, Fariza and Xu, Wen and Camtepe, Seyit and Dunmore, Aeryn},
  journal={arXiv preprint arXiv:2305.09475},
  year={2023}
}
@article{doriguzzi2205flad,
  title={FLAD: Adaptive federated learning for DDoS attack detection. arXiv 2022},
  author={Doriguzzi-Corin, R and Siracusa, D},
  journal={arXiv preprint arXiv:2205.06661}
}
@article{doriguzzi2020lucid,
  title={LUCID: A practical, lightweight deep learning solution for DDoS attack detection},
  author={Doriguzzi-Corin, Roberto and Millar, Stuart and Scott-Hayward, Sandra and Martinez-del-Rincon, Jesus and Siracusa, Domenico},
  journal={IEEE Transactions on Network and Service Management},
  volume={17},
  number={2},
  pages={876--889},
  year={2020},
  publisher={IEEE}
}
@article{salahuddin2021chronos,
  title={Chronos: Ddos attack detection using time-based autoencoder},
  author={Salahuddin, Mohammad A and Pourahmadi, Vahid and Alameddine, Hyame Assem and Bari, Md Faizul and Boutaba, Raouf},
  journal={IEEE Transactions on Network and Service Management},
  volume={19},
  number={1},
  pages={627--641},
  year={2021},
  publisher={IEEE}
}
@article{alfatemi2024advancing,
  title={Advancing ddos attack detection: A synergistic approach using deep residual neural networks and synthetic oversampling},
  author={Alfatemi, Ali and Rahouti, Mohamed and Amin, Ruhul and ALJamal, Sarah and Xiong, Kaiqi and Xin, Yufeng},
  journal={arXiv preprint arXiv:2401.03116},
  year={2024}
}
@article{li2024interactive,
  title={Interactive attack-defense for generalized person re-identification},
  author={Li, Huafeng and Zhang, Chen and Hu, Zhanxuan and Zhang, Yafei and Yu, Zhengtao},
  journal={Neural Networks},
  volume={176},
  pages={106349},
  year={2024},
  publisher={Elsevier}
}

@article{ma2023real,
  title={Real-time detection of DDoS attacks based on random forest in SDN},
  author={Ma, Ruikui and Wang, Qiuqian and Bu, Xiangxi and Chen, Xuebin},
  journal={Applied Sciences},
  volume={13},
  number={13},
  pages={7872},
  year={2023},
  publisher={MDPI}
}

@article{nasir2021fake,
  title={Fake news detection: A hybrid CNN-RNN based deep learning approach},
  author={Nasir, Jamal Abdul and Khan, Osama Subhani and Varlamis, Iraklis},
  journal={International journal of information management data insights},
  volume={1},
  number={1},
  pages={100007},
  year={2021},
  publisher={Elsevier}
}
```

```
@article{kimanzi2024deep,
 title={Deep Learning Algorithms Used in Intrusion Detection Systems--A Review},
 author={Kimanzi, Richard and Kimanga, Peter and Cherori, Dedan and Gikunda, Patrick K},
 journal={arXiv preprint arXiv:2402.17020},
 year={2024}
}

@article{sowmya2023comprehensive,
 title={A comprehensive review of AI based intrusion detection system},
 author={Sowmya, Ta and Anita, EA Mary},
 journal={Measurement: Sensors},
 volume={28},
 pages={100827},
 year={2023},
 publisher={Elsevier}
}
@article{ain2025securing,
 title={Securing IoT Networks Against DDoS Attacks: A Hybrid Deep Learning Approach},
 author={Ain, Noor Ul and Sardaraz, Muhammad and Tahir, Muhammad and Abo Elsoud, Mohamed W and Alourani, Abdullah},
 journal={Sensors},
 volume={25},
 number={5},
 pages={1346},
 year={2025},
 publisher={MDPI}
```

}

@article{okporokpo2025detection,

title={Detection of DDoS Cyberattack Using a Hybrid Trust-Based Technique for Smart Home Networks.},

author={Okporokpo, Oghenetejiri and Olajide, Funminiyi and Ajienka, Nemitari and others},

journal={International Journal of Advanced Computer Science \& Applications},

volume={16},

number={1},

year={2025}

}

@inproceedings{gniewkowski2022anomaly,

title={Anomaly detection techniques for different ddos attack types},

author={Gniewkowski, Mateusz and Maciejewski, Henryk and Surmacz, Tomasz},

booktitle={International Conference on Dependability and Complex Systems},

pages={63--78},

year={2022},

organization={Springer}

}

@article{akgun2022new,

title={A new DDoS attacks intrusion detection model based on deep learning for cybersecurity},

author={Akgun, Devrim and Hizal, Selman and Cavusoglu, Unal},

journal={Computers \& Security},

volume={118},

pages={102748},

year={2022},

publisher={Elsevier}

}

@inproceedings{roshan2022using,

title={Using kernel shap xai method to optimize the network anomaly detection model},

author={Roshan, Khushnaseeb and Zafar, Aasim},

booktitle={2022 9th International Conference on Computing for Sustainable Global Development (INDIACom)},

pages={74--80},

year={2022},

organization={IEEE}

}

@article{alghazzawi2021efficient,

title={Efficient detection of DDoS attacks using a hybrid deep learning model with improved feature selection},

author={Alghazzawi, Daniyal and Bamasag, Omaimah and Ullah, Hayat and Asghar, Muhammad Zubair},

journal={Applied Sciences},

volume={11},

number={24},

pages={11634},

year={2021},

publisher={MDPI}

}

@inproceedings{khaleel2023ddos,

title={DDoS Cyber-Attacks Detection-Based Hybrid CNN-LSTM},

author={Khaleel, Thura Jabbar and Shiltagh, Nadia Adnan},

booktitle={International Conference on Computing and Communication Networks},

```
  pages={523--537},
  year={2023},
  organization={Springer}
}
@article{sumathi2022ddos,
  title={DDoS attack detection using hybrid machine learning based IDS models},
  author={Sumathi, S and Rajesh, R and Karthikeyan, N},
  year={2022},
  publisher={NIScPR-CSIR, India}
}
@article{wei2023classification,
  title={Classification and explanation of distributed denial-of-service (DDoS) attack detection using machine learning and shapley additive explanation (SHAP) methods},
  author={Wei, Yuanyuan and Jang-Jaccard, Julian and Singh, Amardeep and Sabrina, Fariza and Camtepe, Seyit},
  journal={arXiv preprint arXiv:2306.17190},
  year={2023}
}
@article{li2024hda,
  title={Hda-ids: A hybrid dos attacks intrusion detection system for iot by using semi-supervised cl-gan},
  author={Li, Sifan and Cao, Yue and Liu, Shuohan and Lai, Yuping and Zhu, Yongdong and Ahmad, Naveed},
  journal={Expert Systems with Applications},
  volume={238},
  pages={122198},
  year={2024},
```

publisher={Elsevier}

}

@article{alzu2024explainable,

title={Explainable AI-Based DDoS Attacks Classification Using Deep Transfer Learning.},

author={Alzu'bi, Ahmad and Albashayreh, Amjad and Abuarqoub, Abdelrahman and Alfawair, Mai AM},

journal={Computers, Materials \& Continua},

volume={80},

number={3},

year={2024}

}

@article{alabdulatif2024machine,

title={Machine Learning Enabled Novel Real-Time IoT Targeted DoS/DDoS Cyber Attack Detection System.},

author={Alabdulatif, Abdullah and Thilakarathne, Navod Neranjan and Aashiq, Mohamed},

journal={Computers, Materials \& Continua},

volume={80},

number={3},

year={2024}

}

@article{doriguzzi2205flad,

title={FLAD: Adaptive federated learning for DDoS attack detection. arXiv 2022},

author={Doriguzzi-Corin, R and Siracusa, D},

journal={arXiv preprint arXiv:2205.06661}

}

@article{wang2022ai,

title={An AI-powered network threat detection system},

```
 author={Wang, Bo-Xiang and Chen, Jiann-Liang and Yu, Chiao-Lin},
 journal={IEEE Access},
 volume={10},
 pages={54029--54037},
 year={2022},
 publisher={IEEE}
}
@article{lundberg2017unified-x,
 title={A unified approach to interpreting model predictions},
 author={Lundberg, Scott M and Lee, Su-In},
 journal={Advances in neural information processing systems},
 volume={30},
 year={2017}
}
@inproceedings{ribeiro2016should,
 title={" Why should i trust you?" Explaining the predictions of any classifier},
 author={Ribeiro, Marco Tulio and Singh, Sameer and Guestrin, Carlos},
 booktitle={Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining},
 pages={1135--1144},
 year={2016}
}
@article{loveleen2023explanation,
 title={Explanation-driven HCI model to examine the mini-mental state for Alzheimer's disease},
 author={Loveleen, Gaur and Mohan, Bhandari and Shikhar, Bhadwal Singh and Nz, Jhanjhi and Shorfuzzaman, Mohammad and Masud, Mehedi},
```

journal={ACM Transactions on Multimedia Computing, Communications and Applications},

volume={20},

number={2},

pages={1--16},

year={2023},

publisher={ACM New York, NY}

}

@article{kamal2022explainable,

title={Explainable AI for glaucoma prediction analysis to understand risk factors in treatment planning},

author={Kamal, Md Sarwar and Dey, Nilanjan and Chowdhury, Linkon and Hasan, Syed Irtija and Santosh, KC},

journal={IEEE Transactions on Instrumentation and Measurement},

volume={71},

pages={1--9},

year={2022},

publisher={IEEE}

}

@article{viana2021evaluation,

title={Evaluation of the factors explaining the use of agricultural land: A machine learning and model-agnostic approach},

author={Viana, Cl{\'a}udia M and Santos, Maur{\'\i}cio and Freire, Dulce and Abrantes, Patr{\'\i}cia and Rocha, Jorge},

journal={Ecological Indicators},

volume={131},

pages={108200},

year={2021},

publisher={Elsevier}

}

@article{khan2022xsru,

title={XSRU-IoMT: Explainable simple recurrent units for threat detection in Internet of Medical Things networks},

author={Khan, Izhar Ahmed and Moustafa, Nour and Razzak, Imran and Tanveer, Muhammad and Pi, Dechang and Pan, Yue and Ali, Bakht Sher},

journal={Future generation computer systems},

volume={127},

pages={181--193},

year={2022},

publisher={Elsevier}

}

@article{rjoub2023survey,

title={A survey on explainable artificial intelligence for cybersecurity},

author={Rjoub, Gaith and Bentahar, Jamal and Wahab, Omar Abdel and Mizouni, Rabeb and Song, Alyssa and Cohen, Robin and Otrok, Hadi and Mourad, Azzam},

journal={IEEE Transactions on Network and Service Management},

volume={20},

number={4},

pages={5115--5140},

year={2023},

publisher={IEEE}

}

@article{elubeyd2023hybrid,

title={Hybrid deep learning approach for automatic DoS/DDoS attacks detection in software-defined networks},

author={Elubeyd, Hani and Yiltas-Kaplan, Derya},

journal={Applied Sciences},

volume={13},

number={6},

pages={3828},

year={2023},

publisher={MDPI}

}

@article{arreche2024xai,

title={Xai-ids: Toward proposing an explainable artificial intelligence framework for enhancing network intrusion detection systems},

author={Arreche, Osvaldo and Guntur, Tanish and Abdallah, Mustafa},

journal={Applied Sciences},

volume={14},

number={10},

pages={4170},

year={2024},

publisher={MDPI}

}