International Journal of Computer Applications Technology and Research
Volume 14–Issue 02, 293 – 305, 2025, ISSN:-2319–8656
DOI:10.7753/IJCATR1402.1021

Machine Learning-Based Detection and Mitigation of DDoS Attacks in Smart Grid Systems

*Nwaoha Stephen Ochiabuto
*Metallurgical Training Institute, PMB 1555
Onitsha Anambra State

#Okeke Ogochukwu C.
#Department of Computer Science,
Chukwuemeka Odumegwu Ojukwu University,
Uli AN, NG

Abstract: The increasing integration of advanced communication technologies in smart grid systems has significantly improved their efficiency and reliability. However, this interconnectedness also exposes the grid to cyber threats, particularly Distributed Denial-of-Service (DDoS) attacks, which can disrupt operations and compromise system security. This study presents the development of a machine learning-based framework for detecting and mitigating DDoS attacks in smart grid environments. The proposed model leverages advanced machine learning algorithms to analyze network traffic, identify abnormal patterns indicative of DDoS attacks, and implement real-time mitigation strategies. A hybrid approach combining supervised and unsupervised learning enhanced detection accuracy and adaptability to evolving attack patterns. The model was tested on simulated and real-world datasets, demonstrating high detection rates, low false-positive rates, and efficient response times. This research contributes to improving the resilience of smart grid systems by providing an intelligent, automated solution for DDoS attack management, ensuring the uninterrupted delivery of essential services.

Keywords: Machine Learning, DDoS Detection, Smart Grid Security, Cyber Threat Mitigation, Network Traffic Analysis, Resilient Smart Grids

INTRODUCTION

Distributed Denial of Service (DDoS), subclass of denial of service (DoS) attacks is a cyber threat on the Internet that has rapidly garnered the attention of the Industrial Internet of Things (IIoT) such as Smart Grid system (SGs) and research community. A smart grid also known as the intelligent grid is an advanced electrical grid that uses digital technology and relies heavily on network protocols and topology to improve the efficiency, reliability, and sustainability of electricity distribution. This dependence on communication technology makes it vulnerable to cyber threats such as Distributed DenialofService (DDoS), posing significant risks to the overall availability of the smart grid framework. This research investigates the impact of DDoS attack targeting Internet of Things (IoT) utilities in Smart Grid Systems (SGs) and propose an efficient machine-learning model to detect and mitigates DDOS flooding attacks.

Distributed Denial of Service (DDoS) attacks also known as a fraudulent resource consumption (FRC) attack is caused when an attacker uses multiple machines, called botnets, to flood the target host with overwhelming packets which results in denial of services(Yan, Yu, Gong & Li, 2020). It is a cybercrime in which aims to consume services, resources or cause starvation of resources to disrupt a network device (node) through establishing requests that leads to overloading the application servers or make them unavailable. As stated by Naveen and Manu (2019), DDoS attack involves multiple connected online devices, collectively known as a botnet, which are used to overwhelm a target website with fake traffic. Unlike other kinds of cyberattacks, DDoS assaults don't attempt to breach your security perimeter. Rather, it aims to make your website and servers unavailable to legitimate users. DDoS can also be used as a smokescreen for other malicious activities and to take down security appliances, breaching the target's security perimeter. The vulnerability of the internet, the distributed nature of cloud computing, various security issues related to cloud computing service models, and the cloud's main attributes contribute to its susceptibility to security threats associated with cloud service availability.

Akgun, et al., (2022) note that Distributed Denial of Service (DDoS) attacks represent one of the major sophisticated threats that are particularly difficult to counter due to their distributed nature, often leading to disruptions in cloud services. Though there are a number of intrusion detection solutions proposed by different researchers, and cloud service providers (CSP) that are currently using different detection solutions by promising that their product is well secured, there is no such a perfect solution that prevents the DDoS attack.

The characteristics of a DDoS attack, i.e., having different appearances with different scenarios, make it difficult to detect. According to Jazi et al. (2020), DDoS attacks are recognized for their disruptive nature and capacity to deplete the computing resources and bandwidth of their targets within just a few minutes. In spite of being trivial in execution, they are easily detectable mostly due to their dynamic and voluminous attack rates. The increasing availability of DDoS-for-hire services and the proliferation of billions of unsecured IoT devices and botnets contributed to a significant increase in DDoS attacks. These attacks continue to grow in magnitude, frequency, and sophistication (Prasad et al., 2019).

Ahmad and Zhang (2020) indicate that the electricity demand is rising daily, with forecasts suggesting an increase of 30% to 40% over the next 20 years. Current power grids are aging, increasingly overloaded, unreliable, and insufficient in electricity production. Consequently SG system brings renewable resources into the traditional grid and from the smart meter to the smart grid, which help to maintain a better relationship between demand and supply but SGs are vulnerable to cyber-attacks, posing significant risks to the Smart Grid's overall availability due to their reliance on communication technology. In their comprehensive review, Adi et al., (2020) state that the smart grid is evolving alongside advanced technologies, including renewable power generation (solar, wind, hydro), storage systems, distributed generation, and bi-directional communication, all of which are integral to the smart grid system. A smart grid has an analytical and well-organized approach to the management of energy supply and usage. The smart grid facilitates bidirectional contact between energy suppliers and their clients that is, it's a communication network embedded over the traditional electric grid to enable bidirectional communication and power flow between powerhouses and customers for reliable and efficient use of electricity. Therefore it requires reliable, stable, cost-effective, efficient, environmentally sustainable, and healthier facilities and the developmentof smart grids required the integration of diverse technologies and applications. Sensors, smart meters, gateway, cloud are some of the IoT components used to collect data from individual consumers. The main aim of a SG is to maintain equilibrium between demand and supply through predicting the electricity demand (Avancini et al., 2021).

The study conducted by Ghasempour (2019) found that the Smart Grid System (SGS) represents an enhancement of the 20th-century techniques used in electric power generation, transmission, and distribution. It enables easy monitoring and maintenance of power systems through a collection of communication networks, Internet of Things (IoT) devices, computer resources and software, hence it's also refers to as Electrical Grid or Intelligent Grid. The possibilities with IoT are enormous but the risks are there. The biggest draw back and challenge IoT faces is security and privacy. Mitigation of this draw back in IoT systems is a comprehensive task that requires a deep understanding of both cybersecurity and smart grid systems.

According to Adi et al., (2020), the applications of the Internet of Things (IoT) have surged dramatically, resulting in the generation of vast amounts of data that are necessary for effective intelligent data processing. However, the varying IoT infrastructures (i.e., cloud, edge, fog) and the limitations of the IoT application layer protocols in transmitting/receiving messages become the barriers in creating intelligent IoT applications. These barriers prevent current intelligent IoT applications to adaptively learn from other IoT applications. In their work, Adi et al. (2020) critically review the processing of IoT-generated data for machine learning analysis and highlight the current challenges in advancing intelligent solutions within the IoT environment. They noted that IoT devices are limited in computational and communication resources, which pose significant bottlenecks in developing adaptive, intelligent solutions that utilize machine learning techniques. The proposed framework opens up some new challenges for future work in machine-to-machine communications. In cybersecurity, research can include the study of influence of malicious machines on other devices that may lead to system compromise.

Comprehensive review by Moreno et al., (2021), suggest that the extensive integrated topology of smart grids (SGs) and their communication systems makes them particularly vulnerable to cyber threats. Cybercriminals have exploited these vulnerabilities to launch various cyber-physical attacks on SGs. As a result, there has been a notable increase in the prevalence of cyber threats targeting smart grids, particularly Distributed Denial-of-Service (DDoS) attacks. These threats negatively impact the efficiency and sustainability of SGs.

A Survey on Machine Learning Techniques for Cyber Security in the last decade by Shaukat et sal., (2020) reveal that pervasive growth and usage of the Internet and mobile applications have expanded cyberspace. The cyberspace has become more vulnerable to automated and prolonged cyberattacks. The previously used security systems are no longer sufficient because cybercriminals are smart enough to evade conventional security systems. Conventional security systems lack efficiency in detecting previously unseen and polymorphic security attacks.

In this work, the researcher is proposing the development of Real-Time Distributed Denial-of-Service (DDoS) Cyber-Incident Detection and Mitigation attacks targeting Smart Grid Systems (SGs) using Machine Learning Algorithm.

PROBLEM STATEMENT

i. Communication protocols of smart grid systems make them vulnerable to various cyber security risks, such as distributed denial of service (DDoS attacks which leads to disruption of critical energy services.
ii. The constantly evolving tactics of cyber attackers in industrial environments, such as smart grids, pose a significant challenge in developing adaptive method for effective detection and mitigation of cyber threats.
iii. The application layer Distributed Denial of Service (DDoS) attacks on the Internet do not manifest themselves at the network level, these types of attacks commonly avoid traditional network-layer-based detection mechanisms.
iv. Researchers calling for improving the accuracy of DDOS attack detection

International Journal of Computer Applications Technology and Research
Volume 14–Issue 02, 293 – 305, 2025, ISSN:-2319–8656
DOI:10.7753/IJCATR1402.1021

AIM AND OBJECTIVES OF THE STUDY

This work aims to develop a model for real-time Distributed Denial-of-Service (DDOS) cyber-incident detection and mitigation in smart grids using a machine learning algorithm with the following objectives.

i. To develop a model that can effectively detect Distributed Denial-of-Service (DDoS) attacks in real-time within a smart grid system.
ii. To develop a novel detection approach for DDoS attacks based on a hybridized algorithm that will provide better model accuracy.
iii. To use different types of classifiers to compare the model accuracy of detecting the DDoS attacks to determine the efficient model accuracy for the detection of DDoS attacks.

SIGNIFICANCE OF THE STUDY

The significance of the study are:

i. Smart Grid Operations: This research will improve the resilience of smart grids by optimizing power distribution and identifying anomalies or faults.
ii. Resource Management: Using machine learning (ML) algorithms for DDoS detection and mitigation enhances the efficiency of network resources during an attack, helping to lower operational costs and avoid unnecessary expenses.
iii. By sharing the research outcomes, findings, methodologies, and insights generated by this research, this work contributes to the broader body of knowledge in cybersecurity and smart grid technology. This work also enriches the understanding of DDoS threats in smart grid environments and provides valuable insights for future research and development efforts.

SUMMARY OF LITERATURE REVIEW

Distributed Denial of Service (DDoS) Attacks

DDoS attacks are a significant cybersecurity challenge, particularly within Smart Grid (SG) systems, due to their reliance on communication technologies. These attacks flood a target server or network with malicious traffic, rendering them unavailable for legitimate users. The proliferation of unsecured Internet of Things (IoT) devices has further exacerbated the frequency and sophistication of these attacks, as attackers leverage botnets to execute large-scale disruptions.

DDoS attacks are classified into three main categories:

1. **Volumetric Attacks**: Aim to exhaust bandwidth using techniques like flooding and amplification.
2. **Protocol Attacks**: Exploit weaknesses in network protocols, such as TCP SYN flooding.
3. **Application Layer Attacks**: Target vulnerabilities in application protocols, such as HTTP flooding.

Detection remains challenging due to the dynamic and stealthy nature of these attacks. Machine Learning (ML) offers promising solutions by analyzing traffic anomalies and identifying malicious patterns.

Smart Grid Systems

Smart Grids integrate traditional power grids with digital technologies, facilitating bidirectional communication and efficient energy management. While enabling real-time monitoring and renewable energy integration, these systems are highly susceptible to cyber threats, especially DDoS attacks. Key components of Smart Grids include smart meters, sensors, and advanced metering infrastructure (AMI), which enhance efficiency but also introduce vulnerabilities.

Machine Learning for Cybersecurity

ML algorithms have been increasingly applied to detect and mitigate DDoS attacks in Smart Grids. These algorithms learn traffic patterns to distinguish between legitimate and malicious traffic, adapting to new attack methods. Popular ML algorithms include:

- **Support Vector Machines (SVMs)**: Effective for binary classification tasks.
- **Random Forests (RFs)**: Useful for high-dimensional data.
- **Naïve Bayes Classifiers**: Probabilistic models ideal for large datasets.

Challenges in Smart Grid Security

1. **Vast Infrastructure**: Diverse network topologies and components complicate detection and mitigation.
2. **Data Scarcity**: Limited access to real-world datasets hampers model training.
3. **Real-Time Requirements**: ML models must detect and respond to threats in real time.
4. **Ethical Concerns**: Data privacy and security remain critical issues.

Table 1: Key Insights from Literature

Aspect	Details	References
DDoS Attack Types	Volumetric, Protocol, Application Layer Attacks	Sumathi et al., 2022
Challenges	Stealthy nature, dynamic attack patterns, lack of robust models	Vishwakarma et al., 2020
Smart Grid Features	Real-time monitoring, bidirectional communication, renewable integration	Singh et al., 2020
ML Algorithms	SVM, Random Forest, Naïve Bayes	Cervantes et al., 2020; Li et al., 2020
Limitations	Ethical issues, limited datasets, high computational demands	Naveen et al., 2019
Applications in SG	Enhancing grid security, anomaly detection, demand forecasting	Prasad et al., 2021

Table 2: Comparison of Smart Grid and Traditional Grid

Criterion	Traditional Grid	Smart Grid
Customer Interaction	Limited	Extensive
Metering	Electromechanical	Digital (real-time pricing, net metering)
Reliability	Reactive	Proactive and automated
Transmission Losses	~10%	~2%
Topology	Spiral	Networked
Energy Efficiency	Low	High
Communication Flow	One-way	Two-way
Environmental Impact	High pollution	Low pollution

The literature underscores the critical vulnerabilities of Smart Grids to DDoS attacks and the potential of ML algorithms for effective detection and mitigation. However, challenges such as data scarcity, ethical considerations, and real-time requirements must be addressed to fully harness the potential of ML in securing Smart Grids.

METHODOLOGY

In addressing Distributed Denial of Service (DDoS) protection for smart grids, a Risk-Based Framework combined with adaptive software development methodology is adopted. This approach focuses on identifying risks specific to smart grid infrastructure and implementing iterative improvements to enhance security.

Adaptive Software Development (ASD) as proposed by Jim Highsmith and Sam Bayeris a software development process which is considered as a direct advanced extension of an earlier agile framework Rapid Application Development (RAD). This methodology is designed to optimize the development process, ensuring that the final product meets user needs while adhering to project timelines.It is a cyclic process with the phase name reflects adaptability to changing demands, requirements, and market needs. It is used as an ideal technique for building complex software and systems. This methodology provides us with the ability to accommodate changes and adaptability in turbulent environments like detecting and mitigating cyber-attack in smart gride system with products evolving with little planning and learning.In Adaptive Software Development, no preplanned steps are followed or any traditional life cycle is followed rather it is based on constant change, re-evaluation, and evolving products with lightweight planning and continuous learning.Adaptive Software Development has a dynamic Speculate-Collaborate-Learn Lifecycle that focuses on results, not tasks, and the results are identified as application features.

The Adaptive Software Development practices are driven by a belief in continuous adaptation, with the lifecycle equipped to accepting continuous change as the norm. ASD “life cycle” incorporates three phases namely: Speculation, Collaboration and Learning.

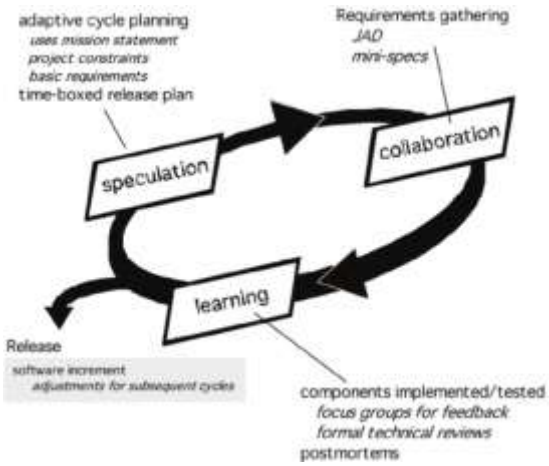


Figure 1: Adaptive development life cycle(Pressman (2021)

1. **Speculation:** During this phase project is initiated and planning is conducted. The project plan uses project initiation information like project requirements, user needs, customer mission statement, etc, to define set of release cycles that the project wants.
2. **Collaboration:** It is the difficult part of ASD as it needs the workers to be motivated. It collaborates communication and teamwork but emphasizes individualism as individual creativity plays a major role in creative thinking. People working together must trust each others to
3. **Learning:** The workers may have a overestimate of their own understanding of the technology which may not lead to the desired result. Learning helps the workers to increase their level of understanding over the project.

System Model

The objective of this research is to propose a machine-learning model, which detects abnormal network traffic packets quickly and accurately. For any scenario in which this tool might be used, we consider two main actors: operators and adversaries. During normal operation, industrial devices send data through the server back to the operators. If any action is required, the operators send instructions to the control center via the server. If the utility server is faced with a DDoS attack, the DDoS tool detects this and gives feedback to the operators. The operators then need to act, based on this information, to mitigate the attack. Figure 1 overviews the considered system model to show the flow of information between its different modules and demonstrates how this information influences the SG's operations.

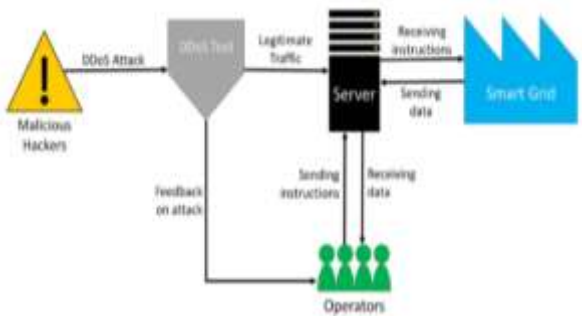


Figure 2 System model of the smart grid

When the tool is launched, the user must import the network data capture that they want to analyze. The tool then analyzes the data and detects whether any attacks have occurred.

If no attacks are detected, the tool goes on standby until the new data capture is inputted. If attacks are detected, the tool displays the logs, IOC, and recommended actions for each of the detected attacks. Finally, the generated logs and displayed indicators can help the operator take suitable measures to maintain the power system's secure and stable operation.

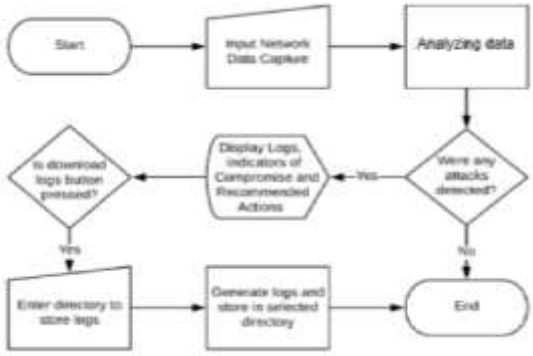


Figure 3: Information flow and overall process

PROPOSED SYSTEM AND IMPLEMENTATION

System Architecture

Figure 4.2 System Architecture

Program Module Specification.

Developing a real-time Distributed Denial-of-Service (DDoS) cyber-incident detection and mitigation system for smart grids using machine learning algorithms requires a systematic approach. The step-by-step approach to be adopted in the design and implementation of the project pipeline is as follows:

1. Importing libraries
2. Data Pre-processing
3. Data Exploration
4. Data Splitting
5. Model Training (SVM, KNN, NaivBaye)
6. Model Evaluation (Accuracy, F1 Score, Recall, Precision, Confusion Matrix)
7. Model Comparison..

International Journal of Computer Applications Technology and Research
Volume 14–Issue 02, 293 – 305, 2025, ISSN:-2319–8656
DOI:10.7753/IJCATR1402.1021

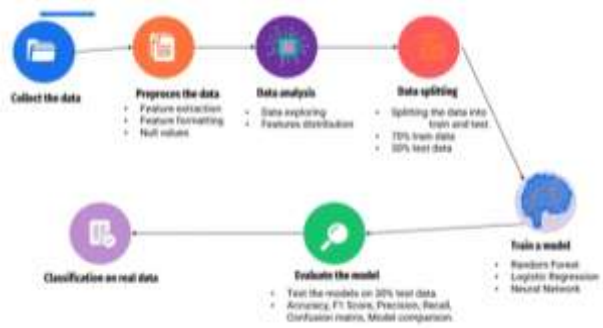


Figure 4.3 Program Module stages

i. **Project Planning and Requirements Analysis:** This involves Identification of the specific smart grid components and communication networks that need protection and determine the performance metrics for detection and mitigation (e.g., detection accuracy, response time. Deep understanding of smart grid architecture, components (sensors, devices), and communication network protocols and data centers is essential.

ii. **Data Collection and Preprocessing:** Here, real-time data from smart grid components, including data from sensors, IoT devices, and network traffic will be collected, the data will be preprocessed and cleaned by handling missing values, noise, and outliers etc.

iii. Data Cleaning for the Dataset: While preparing a dataset, it is common to encounter many data quality issues such as Nan values, outliers, and duplicates. Data cleaning is a crucial step in data preprocessing to alleviate the potential negative impact of such issues on the quality of the dataset. In this study, we dropped all samples that contained Nan, empty, or infinite values. In this study, after data cleaning, the sample count was reduced from 215,761 to 215,076, with 685 removed samples

iv. **Feature Engineering: The** features include network traffic patterns, packet statistics, system performance metrics, etc. and relevant features from the data will be extracted and used for DDoS detection.

v. Selection of appropriate machine learning algorithms/Model: Common choices for appropriate machine learning algorithms for DDoS detection and mitigation include supervised learning algorithms like Random Forest, Support Vector Machines (SVM), KNN and Naiv Bayer for network traffic analysis.

vi. **Training and Testing:** For efficient model training via these ML algorithms, the dataset will be spited into training and testing sets then the selected machine learning model(s) is trained on historical data while evaluation of the model(s) will be carried out using testing data to assess their performance.

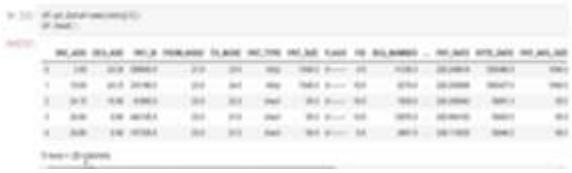
vii. **DDoS Detection:** A thresholds or anomaly detection mechanisms to identify abnormal network behavior indicative of a DDoS attack will be setup.

viii. **Testing and Validation: There will be**thorough testing of the system in any chosen controlled environment to ensure its effectiveness and reliability. Various DDoS attack scenarios will be validated to ascertain the system's performance

Result and Discussion

The machine learning algorithms are successfully trained with the training dataset of

CICDDoS2019 provided by the Kaggle as our experimental dataset. **It** contains benign and the most up-to-date common DDoS attacks, which resembles the true real-world data (PCAPs) as presented in Table 3.



The hybrid model is used for making analysis of the DDoSattaxk on the smart grid system environment and thereby calculating the performance and accuracy of the model

Evaluating the performance of machine learning models involves various metrics that help assess how well a model is performing. **The model metrics** evaluation **is done using Accuracy,** precision, ROC AUC (Receiver Operating Characteristic) curve, recall, and F1 score to ensure a comprehensive evaluation of model performance.

(A) Accuracy: Is the ratio of correctly predicted instances to the total instances.

$$\text{Accuracy}=\frac{TP+TN}{TP+TN+FP+FN}$$

Where

- **True Positive (TP):** The number of positive instances that were correctly predicted as positive by the model.

International Journal of Computer Applications Technology and Research
Volume 14–Issue 02, 293 – 305, 2025, ISSN:-2319–8656
DOI:10.7753/IJCATR1402.1021

- **True Negative (TN):** The number of negative instances that were correctly predicted as negative by the model.
- **False Positive (FP):** The number of negative instances that were incorrectly predicted as positive by the model. and
- **False Negative (FN):** he number of positive instances that were incorrectly predicted as negative by the model.

Table 6 indicates the first series testing of each model and calculating their respective accuracies

Model	Naïve Bayes NB	K-Nearest Neighbors (KNN)	Support Vector Machine (SVM)	Ensemble Model
Accuracies	0.60	1.00	0.99	0.95

1. **Naive Bayes (NB) Accuracy = 0.60.**

An accuracy of 60% indicates that the Naive Bayes model correctly predicts the class for 60% of the instances in the dataset. This suggests that the model may not be capturing the underlying patterns well.

2. **K-Nearest Neighbors (KNN) Accuracy = 1.00.**

A perfect accuracy score of 100% indicates that the KNN model correctly classifies every instance in the dataset

3. **Support Vector Machine (SVM) Accuracy = 0.99**

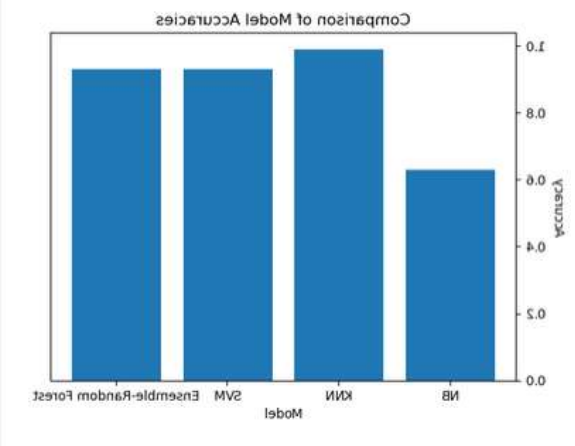
An accuracy of 99% suggests that the SVM model performs exceptionally well, misclassifying only a small fraction of instances. This indicates strong classification capability.

4. **Ensemble Model Accuracy = 0.95.**

An accuracy of 95% indicates that the ensemble model is highly effective, successfully classifying the majority of instances. This shows that it leverages the strengths of multiple models to achieve high performance.

Implication: The ensemble method is strong, and it tends to be more robust against overfitting compared to individual models, making it a reliable choice.

Model Accuracies Representation Using Bar Chart



Bar Chart visualize the performance metrics of different models to help us understand the distribution of predictions, assess model accuracy, identify potential issues and a way to compare their effectiveness visually

(B) Precision:

The ratio of correctly predicted positive observations to the total predicted positives. It measures the accuracy of positive predictions

Precision $=\frac{TP}{TP+FP}$

The model Precision Values

1. Naive Bayes: Precision = 1.00

This means that every positive prediction made by the Naive Bayes model is correct. There are no false positives.

2. KNN: Precision = 1.00

Naive Bayes, KNN also has perfect precision, indicating no false positives in its predictions.

3. SVM: Precision ≈ 0.98

This indicates that about 98% of the positive predictions are correct, with some false positives present.

4. Ensemble: Precision = 1.00

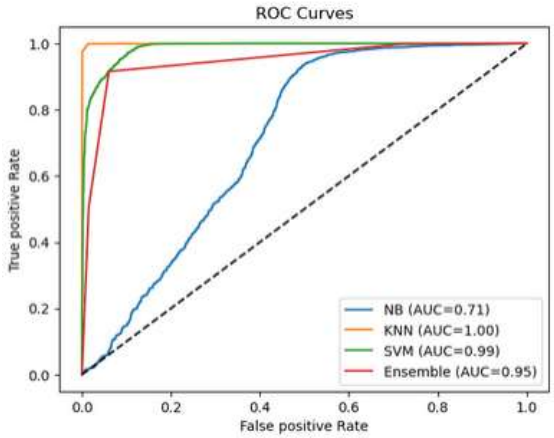
The ensemble model achieves perfect precision as well, indicating that all its positive predictions are correct.

All models except for SVM achieve perfect precision. This suggests that they are good at minimizing false positives.

International Journal of Computer Applications Technology and Research
Volume 14–Issue 02, 293 – 305, 2025, ISSN:-2319–8656
DOI:10.7753/IJCATR1402.1021

(C) ROC AUC (Receiver Operating Characteristic Area Under the Curve)

ROC (Receiver Operating Characteristic) curve**:** It is a graphical representation used to evaluate the performance of a binary classification model. It illustrates the trade-off between the true positive rate (sensitivity) and the false positive rate (1-specificity) at various threshold settings.



Interpreting the ROC curve results with the given AUC (Area Under the Curve) values provides insight into the performance of the models. Every positive instance is identified as positive, and every negative instance is identified as negative.

Results Overview

1. **Naive Bayes (NB) AUC = 0.70**

This indicates that the Naive Bayes model has a moderate ability to distinguish between positive and negative classes. An AUC of 0.70 suggests that the model is better than random guessing (0.50) but not particularly strong

2. **K-Nearest Neighbors (KNN) AUC = 1.0**

The KNN model achieves a perfect score, indicating that it can perfectly classify all instances without any errors. This means every positive instance is correctly identified, and no negative instances are misclassified as positive.

3. **Support Vector Machine (SVM) AUC = 0.99**

The SVM model also performs exceptionally well, with an AUC very close to 1.00. This suggests that it has a high true positive rate and very few false positives, making it highly effective for classification.

4. **Ensemble Model AUC = 0.95**

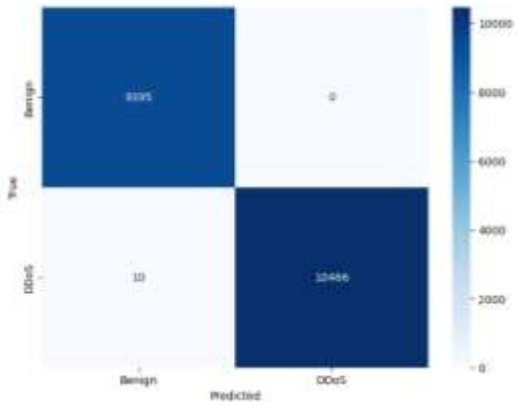
The ensemble model demonstrates strong performance, effectively combining predictions from multiple models to achieve an AUC of 0.95. This indicates that it can reliably distinguish between the classes, though it is not as strong as KNN or SVM in this case. The ensemble method is still very effective, and it can provide robustness against overfitting, especially in more complex datasets.

Note: Any model with an AUC of 0.50 does not provide any useful information and serves as a baseline for comparison.

Confusion Matrix

A confusion matrix is plotted which provides a visual representation of how well the model's predictions align with the actual labels in the dataset. It is a useful tool for evaluating the performance of a classification model.

Confusion Matrix



The confusion matrix is an essential tool for evaluating classification models, helping you understand not just the overall accuracy but also how the model is performing across different classes. It helps in diagnosing issues, improving the model, and understanding the trade-offs between different metrics, especially in contexts where false positives and false negatives carry different implications

CONCLUSION

This research paper discussed various machine learning algorithms employed to design the DDoS Detection System on smart grid. The machine learning based intrusion detection models were trained by CICDDoS2019 dataset provided by the Kaggle as our experimental dataset. Here, we have designed a hybrid algorithm which consists of a combination of three machine learning techniques to train a model which can be used to detect and classify the type of DDoS attack with greater accuracy than that of each individual machine learning techniques used in the hybrid model. The integration of these two algorithms may get the advantages of both algorithms, which leads to providing better results than the conventional algorithms. So, the hybrid combination of the SVM classifier algorithm with Naïve Baye and KNN models and the results obtained confirmed that the SVM based classifier model outperformed all other models with better intrusion detection

performance and a minimal number of feature subset as compared to other models.The hybrid model provide more level of accuracy prediction of the DDos attacks. Also, it is more effective than other models.

REFERENCES

Adi, E., Anwar, A., Baig, Z., &Zeadally, S. (2020). Machine learning and data analytics for the IoT. Neural computing and applications, 32, 16205-16233.

Abdullah, A. A., El-Den, B. M., Abo-Al-Ez, K. M., & Hassan, T. M. (2023). Security management for an advanced metering infrastructure (AMI) system of smart electrical grids. *Applied Sciences*, *13*(15), 8990.

Adi (2020) 'Machine learning and data analytics for the IoT', Neural Computing and Applications. Springer London,0123456789. doi: 10.1007/s00521-020-04874-y

Adi (2020) 'Machine learning and data analytics for the IoT', Neural Computing and Applications. Springer London,0123456789. doi: 10.1007/s00521-020-04874-y

Adi, E., Anwar, A., Baig, Z., &Zeadally, S. (2020). Machine learning and data analytics for the IoT. *Neural computing and applications*, *32*, 16205-16233.

Ahmad, T., & Zhang, D. (2020). A critical review of comparative global historical energy consumption and future demand: The story told so far. *Energy Reports*, *6*, 1973-1991.

Ahmed, Z., Afaqui, N., &Humayan, O. (2019). Detection and prevention of DDoS attacks on software defined networks controllers for smart grid. *International Journal of Computer Applications*, *975*, 8887.

Akgun, D., Hizal, S., &Cavusoglu, U. (2022). A new DDoS attacks intrusion detection model based on deep learning for cybersecurity. *Computers & Security*, *118*, 102748.

Alby, T. (2023). *Data Science in Practice*. CRC Press.

Alhaidari, F. A., &Alrehan, A. M. (2021). A simulation work for generating a novel dataset to detect distributed denial of service attacks on Vehicular Ad hoc NETwork systems.

International Journal of Distributed Sensor Networks, *17*(3), 15501477211000287.

Ali, S., & Li, Y. (2019). Learning multilevel auto-encoders for DDoS attack detection in smart grid network. *IEEE Access*, *7*, 108647-108659.

Alsaeedi, A., Bamasag, O., &Munshi, A. (2020, November). Real-Time DDoS flood Attack Monitoring and Detection (RT-AMD) Model for Cloud Computing. In *The 4th International Conference on Future Networks and Distributed Systems (ICFNDS)* (pp. 1-5).

Alsaeedi, A., Bamasag, O., &Munshi, A. (2020, November). Real-Time DDoS flood Attack Monitoring and Detection (RT-AMD) Model for Cloud Computing. In *The 4th International Conference on Future Networks and Distributed Systems (ICFNDS)* (pp. 1-5).

Alzahrani, R. J., &Alzahrani, A. (2021). Security analysis of ddos attacks using machine learning algorithms in networks traffic. *Electronics*, *10*(23), 2919.

Aronoff, K., Battistoni, A., Cohen, D. A., &Riofrancos, T. (2019). *A planet to win: why we need a Green New Deal*. Verso Books.

Avancini, D. B., Rodrigues, J. J., Rabêlo, R. A., Das, A. K., Kozlov, S., &Solic, P. (2021). A new IoT-based smart energy meter for smart grids. *International Journal of Energy Research*, *45*(1), 189-202.

Bhuiyan, M. R. A., Mamur, H., & Begum, J. (2021). A brief review on renewable and sustainable energy resources in Bangladesh. *Cleaner Engineering and Technology*, *4*, 100208.

Bilgin, Z., Tomur, E., Ersoy, M. A., &Soykan, E. U. (2019, September). Statistical appliance inference in the smart grid by machine learning. In *2019 IEEE 30th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC Workshops)* (pp. 1-7). IEEE.

Bilgin, Z., Tomur, E., Ersoy, M. A., &Soykan, E. U. (2019, September). Statistical appliance inference in the smart grid by machine learning. In *2019 IEEE 30th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC Workshops)* (pp. 1-7). IEEE.

Brajer, N., Cozzi, B., Gao, M., Nichols, M., Revoir, M., Balu, S., ...&Sendak, M. (2020). Prospective and external evaluation of a machine learning model to predict in-hospital mortality of adults at time of admission. *JAMA network open*, *3*(2), e1920733-e1920733.

Butun I, Osterberg P& Song H. (2019). *Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures.*

Butun I, Osterberg P& Song H. (2019). *Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures.IEEE Communications Surveys*

& Tutorials, 1–1. doi:10.1109/comst.2019.2953364.

Cervantes, J., Garcia-Lamont, F., Rodríguez-Mazahua, L., & Lopez, A. (2020). A comprehensive survey on support vector machine classification: Applications, challenges and trends. *Neurocomputing*, *408*, 189-215.

Chapman, A., Simperl, E., Koesten, L., Konstantinidis, G., Ibáñez, L. D., Kacprzak, E., &

Groth, P. (2020). Dataset search: a survey. *The VLDB Journal*, *29*(1), 251-272.

Chen, Z., Amani, A. M., Yu, X., &Jalili, M. (2023). Control and optimisation of power grids using smart meter data: A review. *Sensors*, *23*(4), 2118.

Diaba, S. Y., &Elmusrati, M. (2023). Proposed algorithm for smart grid DDoS detection based on deep learning. *Neural Networks*, *159*, 175-184.

Dileep, G. J. R. E. (2020). A survey on smart grid technologies and applications. *Renewable energy*, *146*, 2589-2625.

Dudnik, A., Kuzmych, L., Trush, O., Domkiv, T., Leshchenko, O., &Vyshnivskyi, V. (2020). Smart home technology network construction method and device interaction organization concept. In *2020 IEEE 2nd international conference on system analysis & intelligent computing (SAIC)* (pp. 1-6). IEEE.

Emmanuel, T., Maupong, T., Mpoeleng, D., Semong, T., Mphago, B., &Tabona, O. (2021). A survey on missing data in machine learning. *Journal of Big data*, *8*, 1-37.

Ghasempour, A. (2019) 'Internet of things in smart grid: Architecture, applications, services, key technologies, and challenges', Inventions, 4(1). doi: 10.3390/inventions4010022.

Gopal, S. B., Poongodi, C., Nanthiya, D., Priya, R. S., Saran, G., &Priya, M. S. (2021, February). Mitigating DoS attacks in IoT using Supervised and Unsupervised Algorithms–A Survey. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1055, No. 1, p. 012072). IOP Publishing.

Gopal, S. B., Poongodi, C., Nanthiya, D., Priya, R. S., Saran, G., &Priya, M. S. (2021, February). Mitigating DoS attacks in IoT using Supervised and Unsupervised Algorithms–A Survey. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1055, No. 1, p. 012072). IOP Publishing.

Grid, S. et al. (no date) 'NIST Special Publication 1108r3 NIST Framework and Roadmap for Smart Grid Interoperability NISTSpecial Publication 1108r3 NIST Framework and Roadmap for Smart Grid Interoperability'

Halladay, J., Cullen, D., Briner, N., Warren, J., Fye, K., Basnet, R., ...&Doleck, T. (2022). Detection and characterization of DDoS attacks using time-based features. *IEEE Access*, *10*, 49794-49807.

Hiran, K. K., Jain, R. K., Lakhwani, K., &Doshi, R. (2021). *Machine Learning: Master Supervised and Unsupervised Learning Algorithms with Real Examples (English Edition)*. BPB Publications.

Hossain, M. A., Pota, H. R., Hossain, M. J., &Blaabjerg, F. (2019). Evolution of microgrids with converter-interfaced generations: Challenges and opportunities. *International Journal of Electrical Power & Energy Systems*, *109*, 160-186.

https://www.javatpoint.com/machine-learning-algorithms Date Retrieved 4th February, 2024

https://www.projectpro.io/article/8-feature-engineering-techniques-for-machine-learning/423

IEEE Communications Surveys & Tutorials, 1–1. doi:10.1109/comst.2019.2953364.

Jaafar GA, Abdullah SM, Ismail S. 2019. Review of recent detection methods for HTTP DDoS attack. Journal of Computer Networks and Communications 2019(4):1–10DOI 10.1155/2019/1283472.

Jaafar GA, Abdullah SM, Ismail S. 2019. Review of recent detection methods for HTTP DDoSattack. Journal of Computer Networks and Communications 2019(4):1–10
DOI 10.1155/2019/1283472.

Jafari, H., Moghaddami, M., Olowu, T. O., Sarwat, A. I., &Mahmoudi, M. (2020). Virtual inertia-based multipower level controller for inductive electric vehicle charging systems. *IEEE Journal of Emerging and Selected Topics in Power Electronics*, *9*(6), 7369-7382.

Jazi, H. H., Gonzalez, H., Stakhanova, N., &Ghorbani, A. A. (2020). Detecting HTTP-based application layer DoS attacks on web servers in the presence of sampling. *Computer Networks*, *121*, 25-36.

Judge, M. A., Khan, A., Manzoor, A., &Khattak, H. A. (2022). Overview of smart grid implementation: Frameworks, impact, performance and challenges. *Journal of Energy Storage*, *49*, 104056.

Kabeyi, M. J. B., &Olanrewaju, O. A. (2023). Smart grid technologies and application in the sustainable

energy transition: a review. *International Journal of Sustainable Energy*, *42*(1), 685-758.

Khan, S., Kifayat, K., Kashif Bashir, A., Gurtov, A., & Hassan, M. (2020). *Intelligent intrusion detection system in smart grid using computational intelligence and machine learning. Transactions on Emerging Telecommunications Technologies.* doi:10.1002/ett.4062 10.1002/ett.4062 downloaded on **2020-08-08**

Khan, S., Kifayat, K., Kashif Bashir, A., Gurtov, A., & Hassan, M. (2020). *Intelligent intrusion detection system in smart grid using computational intelligence and machine learning. Transactions on Emerging Telecommunications Technologies.* doi:10.1002/ett.4062 10.1002/ett.4062 downloaded on **2020-08-08**

Khan, S., Kifayat, K., Kashif Bashir, A., Gurtov, A., & Hassan, M. (2021). Intelligent intrusion detection system in smart grid using computational intelligence and machine learning. *Transactions on Emerging Telecommunications Technologies*, *32*(6), e4062.

Kuralkar, S., Mulay, P., &Chaudhari, A. (2020). Smart energy meter: applications, bibliometric reviews and future research directions. *Science & Technology Libraries*, *39*(2), 165-188.

Li, Q. N., & Li, T. H. (2020). Research on the application of Naive Bayes and Support Vector Machine algorithm on exercises Classification. In *Journal of Physics: Conference Series* (Vol. 1437, No. 1, p. 012071). IOP Publishing

Liu, Z., Wang, Y., Feng, F., Liu, Y., Li, Z., & Shan, Y. (2023). A DDoS Detection Method Based on Feature Engineering and Machine Learning in Software-Defined Networks. *Sensors*, *23*(13), 6176.

Mahesh, B. (2020). Machine learning algorithms-a review. *International Journal of Science and Research (IJSR).[Internet]*, *9*(1), 381-386.

Mbungu, N. T., Naidoo, R. M., Bansal, R. C., Siti, M. W., &Tungadio, D. H. (2020). An overview of renewable energy resources and grid integration for commercial building applications. *Journal of Energy Storage*, *29*, 101385.

Mohanty, D., Sethi, K., Prasath, S., Rout, R. R., &Bera, P. (2021, June). Intelligent Intrusion Detection System for Smart Grid Applications. In *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (pp. 1-8). IEEE.

Mohanty, D., Sethi, K., Prasath, S., Rout, R. R., &Bera, P. (2021, June). Intelligent Intrusion Detection System for Smart Grid Applications. In *2021 International Conference on*

Cyber Situational Awareness, Data Analytics and Assessment (CyberSA) (pp. 1-8). IEEE.

Moreno Escobar, J. J., Morales Matamoros, O., Tejeida Padilla, R., Lina Reyes, I., & Quintana Espinosa, H. (2021). A comprehensive review on smart grids: Challenges and opportunities. *Sensors*, *21*(21), 6978.

Najafimehr, M., Zarifzadeh, S., &Mostafavi, S. (2023). DDoS attacks and machine-learning-based detection methods: A survey and taxonomy. *Engineering Reports*, *5*(12), e12697.

Naveen Bindra,& Manu Sood. (2019). Detecting DDoS Attacks Using Machine Learning Techniques and Contemporary Intrusion Detection Dataset. Automatic Control and Computer Sciences, 53(5), 419–428. doi:10.3103/s0146411619050043

Naveen Bindra,& Manu Sood. (2019). Detecting DDoS Attacks Using Machine Learning Techniques and Contemporary Intrusion Detection Dataset. Automatic Control and Computer Sciences, 53(5), 419–428. doi:10.3103/s0146411619050043

Panda, D. K., & Das, S. (2021). Smart grid architecture model for control, optimization and data analytics of future power networks with more renewable energy. *Journal of Cleaner Production*, *301*, 126877.

Paullada, A., Raji, I. D., Bender, E. M., Denton, E., & Hanna, A. (2021). Data and its (dis) contents: A survey of dataset development and use in machine learning research. *Patterns*, *2*(11).

Prasad, D., Singh, R. P., Mukherjee, S., Chattaraj, S., Sarkar, K., & Khan, M. I. (2021). Approaches to smart grid network communication and security. In *Advances in Smart Grid Power System* (pp. 103-158). Academic Press.

Rashid, M., Kamruzzaman, J., Imam, T., Wibowo, S., & Gordon, S. (2022). A tree-based stacking ensemble technique with feature selection for network intrusion detection. *Applied Intelligence*, *52*(9), 9768-9781.

Sagu, A., Gill, N. S., &Gulia, P. (2022). Hybrid deep neural network model for detection of security attacks in IoT enabled environment. *International Journal of Advanced Computer Science and Applications*, *13*(1).

Santos, R., Souza, D., Santo, W., Ribeiro, A., & Moreno, E. (2019). Machine learning algorithms to detect DDoS attacks in SDN. Concurrency and Computation: Practice and Experience, e5402. doi:10.1002/cpe.5402

Serrano, J. B., Wang, S., Chavez, K. M. G., Hourani, A., &Sithamparanathan, K. (2022). A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks. *Engineering Science and Technology, an International Journal*, *31*, 1-15.

Sharafaldin, I.; Lashkari, A.H.; Hakak, S.; Ghorbani, A.A. Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy. In Proceedings of the 2019 International Carnahan Conference on Security Technology (ICCST), Chennai, India, 1-3 October 2019; pp. 1-8.

Sharafaldin, I.; Lashkari, A.H.; Hakak, S.; Ghorbani, A.A. Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy. In Proceedings of the 2019 International Carnahan Conference on Security Technology (ICCST), Chennai, India, 1-3 October 2019; pp. 1-8.

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I.A., & Xu, M. (2020). A Survey on Machine Learning Techniques for Cyber Security in the Last Decade. IEEE Access, 8, 222310-222354.

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I.A., & Xu, M. (2020). A Survey on Machine Learning Techniques for Cyber Security in the Last Decade. IEEE Access, 8, 222310-222354.

Shukla, P., Krishna, C. R., &Patil, N. V. (2023). Iot traffic-based DDoS attacks detection mechanisms: A comprehensive review. *The Journal of Supercomputing*, 1-58.

Singh, G., &Khare, N. (2022). A survey of intrusion detection from the perspective of intrusion datasets and machine learning techniques. *International Journal of Computers and Applications*, *44*(7), 659-669.

Singh, G., &Khare, N. (2022). A survey of intrusion detection from the perspective of intrusion datasets and machine learning techniques. *International Journal of Computers and Applications*, *44*(7), 659-669.

Singh, R., & Gill, N. S. (2020). Use of IoT and Machine Learning for Efficient Power Management Through Smart Grid: A Review.

Tahsien S. M, Karimipour H,&Spachos P. (2020). Machine learning based solutions for security of Internet of Things(IoT): A survey. Journal of Network and Computer Applications, 102630. doi:10.1016/j.jnca.2020.102630

Tran, M. K., Panchal, S., Chauhan, V., Brahmbhatt, N., Mevawalla, A., Fraser, R., & Fowler, M. (2022).Python-based scikit-learn machine learning models for thermal and electrical performance prediction of high-capacity lithium-ion battery. *International Journal of Energy Research*, *46*(2), 786-794.

Transformation of DDoS attacks in Global warefare, 2019. https://qz.com/860630/ddos-attacks-have-gone from-a-minor-nuisance-to-a-possible-new-form-of-global-warfare/. Accessed January 1, 2019.

Tutorialspoint. (n.d.). Adaptive Software Development Lifecycle. Retrieved from https://www.tutorialspoint.com/adaptive_software_development/adaptive_software_development_lifecycle.htm

University of New Brunswick. (2019). *CICDDoS2019 dataset*. https://www.unb.ca/cic/datasets/ddos-2019.html

Vahidi, S., Ghafouri, M., Au, M., Kassouf, M., Mohammadi, A., &Debbabi, M. (2023). Security of wide-area monitoring, protection, and control (WAMPAC) systems of the smart grid: A survey on challenges and opportunities. *IEEE Communications Surveys & Tutorials*, *25*(2), 1294-1335.

Vercio, L. L., Amador, K., Bannister, J. J., Crites, S., Gutierrez, A., MacDonald, M. E., ...&

Forkert, N. D. (2020). Supervised machine learning tools: a tutorial for clinicians. *Journal of Neural Engineering*, *17*(6), 062001.

Verdonck, T., Baesens, B., Óskarsdóttir, M., &vandenBroucke, S. (2021). Special issue on feature engineering editorial. *Machine Learning*, 1-12.

Vishwakarma, R., & Jain, A. K. (2020). A survey of DDoS attacking techniques and defence mechanisms in the IoT network. *Telecommunication systems*, *73*(1), 3-25.

Yan, Q., Yu, F. R., Gong, Q., & Li, J. (2020). Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues,

and challenges. *IEEE communications surveys & tutorials*, *18*(1), 602-622.

Zhe, W., Wei, C., &Chunlin, L. (2020, July). DoS attack detection model of smart grid based on machine learning method. In *2020 ieee international conference on power, intelligent computing and systems (ICPICS)* (pp. 735-738). IEEE.

Zheng, J., Gao, D. W., & Lin, L. (2021, April). Smart meters in smart grid: An overview. In *2021 IEEE green technologies conference (GreenTech)* (pp. 57-64). IEEE.

Zhou, B., Sun, B., Zang, T., Cai, Y., Wu, J., & Luo, H. (2022). Security risk assessment approach for distribution network cyber physical systems considering cyber attack vulnerabilities. *Entropy*, *25*(1), 47.