Delta University for Science and Technology
Faculty of Artificial Intelligence
Cyber Security Department

AstraGuard AI (A Comprehensive Network Security System Powered by AI To Analysis and Block Real_time Attacks).

Esraa Salama Mohammed 4221177, Menna Essam Abd-Elhamid 4221272, Malak Ali Eldawansy 4221187,Naniss El-Sayed Yahia4221415,Fathy Abdelhamed Fathy 4221246, Mohamed Hisham Salah El-din 4221340

Abstract:

This project proposal outlines a plan to develop AstraGuard AI, an AI-powered Intrusion Detection System (IDS) designed to detect and mitigate cyber-attacks on networks. The primary aim of AstraGuard AI is to enhance defense mechanisms against diverse network attacks, including Port Scanning, Distributed Denial of Service (DDoS), and other intrusion types. Leveraging machine learning algorithms, the system will identify attack patterns in real-time, enabling automated responses to prevent further damage. Initially, AstraGuard AI will focus on selecting optimal features from network traffic data and training a predictive model capable of accurate attack classification. As a final step, specific post-detection measures will be designed to address each attack type. This project is intended to contribute to existing IDS capabilities by increasing detection speed, accuracy, and resource efficiency through an AI-driven approach.

Keywords: Cybersecurity, Networks, Sklearn, PortScan, Botnet, DDoS, SVM, CICIDS2017

1.Introduction:

In today’s digital landscape, cyber threats have evolved in complexity, targeting vulnerabilities within networks to cause disruptions, steal data, and compromise security. Common attacks such as Distributed Denial of Service (DDoS) and Port Scanning represent significant threats to organizations, often resulting in service outages and data breaches. To counter these challenges, advanced Intrusion Detection Systems (IDS) that leverage artificial intelligence and machine learning are emerging as powerful tools.

This project proposes the development of AstraGuard AI, an AI-driven IDS designed to detect and mitigate a variety of network attacks. AstraGuard AI will employ machine learning algorithms to recognize attack patterns in real-time, providing an automated and dynamic approach to intrusion detection. Unlike traditional IDS, which often rely on predefined rules and require constant manual updating, AstraGuard AI aims to learn from evolving attack data, enabling it to adapt to new and sophisticated cyber threats.

The initial stages of the project will focus on data preprocessing and feature selection to optimize model performance, followed by training a predictive model capable of classifying attack types with high accuracy. Upon detecting an attack, AstraGuard AI will initiate specific response measures tailored to the type of threat, thereby reducing the potential impact on network resources and enhancing overall security.

By implementing AstraGuard AI, this project aims to push the boundaries of IDS capabilities, providing a proactive defense mechanism that aligns with the increasing demands for speed, accuracy, and adaptability in cybersecurity. This solution is expected to set a foundation for future innovations in network defense, where AI-based systems can keep pace with the rapidly changing threat landscape.

2.Objectives:

The primary objective of the AstraGuard AI project is to create an advanced Intrusion Detection System (IDS) that leverages artificial intelligence to enhance network security. AstraGuard AI aims to identify and mitigate different types of network attacks through automated processes, ultimately improving detection accuracy, response speed, and adaptability to emerging threats.

The main objectives of this project are as follows:

- **Analyze Network Attack Types and Detection Methods:**

Conduct a detailed analysis of common network attack types, such as Port Scanning and Distributed Denial of Service (DDoS), to understand their characteristics and identify patterns that can be used for detection.

- **Develop a Machine Learning-Based Detection Model:**

Train a machine learning model capable of recognizing various attack patterns in network traffic. This model will be trained on a dataset containing labeled instances of both benign and malicious traffic, enabling it to distinguish different types of attacks.

- **Implement Post-Detection Mitigation Techniques:**

Create custom post-detection procedures for each attack type identified by the system, enabling AstraGuard AI to respond dynamically and limit the impact of each attack.

- **Evaluate and Refine the Model's Performance:**

Test and evaluate the model to determine its effectiveness in real-time network environments. Assess the model's accuracy, detection speed, and resource efficiency to ensure it meets security standards.

3. Methodology:

The methodology of the AstraGuard AI project will follow a systematic approach to develop an effective Intrusion Detection System (IDS) using machine learning. The methodology is organized into specific steps that will guide the model development from data preparation through to testing and evaluation. The main steps include:

3.1 Data Collection and Preprocessing:

Dataset Selection: We will choose a publicly available dataset, such as CICIDS2017, which includes labeled instances of normal and malicious network traffic. This dataset provides a mix of benign data and various attack types, including DDoS and Port Scanning.

3.2 Data Cleaning:

The data will be cleaned to remove any incomplete or irrelevant records. Columns with missing values will be handled appropriately, either by filling in with averages or removing them if they are unimportant.
Feature Engineering and Selection: We will analyze the dataset to select the most relevant features for detecting attack patterns, thus improving the model's accuracy and reducing computational load.

3.3 Model Training and Validation:

Algorithm Selection: We will experiment with several machine learning algorithms, including Random Forest, Support Vector Machine (SVM), Decision Tree, and AdaBoost, to identify the one that best suits our needs for accuracy, speed, and resource efficiency.

3.4 Model Training:

Each selected model will be trained on the preprocessed dataset, and we will optimize hyperparameters for each model to enhance its performance.

3.5 Validation and Testing:

A portion of the dataset will be reserved for testing to validate the model’s effectiveness in accurately identifying both benign and malicious traffic. Metrics such as accuracy, precision, recall, and F1-score will be used to evaluate each model's performance.

3.6 Post-Detection Response Mechanism:

Developing Response Rules: For each attack type, specific response mechanisms will be implemented. For instance, during a DDoS attack, the system could initiate IP filtering, while a Port Scanning attack may prompt blocking the source IP to reduce system load.

3.7 Integration with IDS System:

These response mechanisms will be incorporated into the model so that AstraGuard AI can not only detect but also take action against identified threats automatically.

3.8 Performance Evaluation:

The model will be tested under different simulated network attack scenarios to measure its accuracy, detection speed, and computational resource usage. This stage will also help identify any weaknesses or areas for improvement.

4.Conclusion:

The **AstraGuard AI** project aims to develop an advanced, AI-driven Intrusion Detection System that can effectively detect and respond to cyber-attacks on networks. By leveraging machine learning, **AstraGuard AI** is expected to provide high accuracy and adaptability in identifying and mitigating attack types such as **DDoS** and **Port Scanning**.

Through this project, we hope to achieve the following:

- **Enhanced Detection Accuracy and Speed**: By applying feature selection and using optimized algorithms, **AstraGuard AI** aims to outperform traditional IDS tools in terms of speed and accuracy.

- **Automated, Intelligent Response**: With tailored response mechanisms for each type of attack, **AstraGuard AI** will provide a proactive approach to cybersecurity, reducing reliance on manual intervention.
- **Scalability and Future Improvements**: The modular design of **AstraGuard AI** will allow for future updates, enabling it to adapt to new attack patterns and incorporate advanced machine learning techniques.

References:

1. Chicago Style (17th Edition, Author-Date): Kamar, Fady R. A., Nabil A. B. Yehia, and Mohamed A. Essam. 2021. "Artificial Intelligence in Structural Engineering: A State-of-the-Art Review." Sustainability 13 (19): 10743. https://doi.org/10.3390/su131910743

2. Ahmed, S., Lee, Y., Hyun, S.-H., & Koo, I. (2019). Unsupervised Machine Learning-Based Detection of Covert Data Integrity Assault in Smart Grid Networks Utilizing Isolation Forest. IEEE Transactions on Information Forensics and Security, 14(10), 2765-2777. https://doi.org/10.1109/tifs.2019.2902822

3. Diovu, R.C.; Agee, J.T. Quantitative analysis of firewall security under DDoS attacks in smart grid AMI networks. In Proceedings of the IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON), Owerri, Nigeria, 7–10 November 2017; pp. 696–701.

4. NGFWEnterprise Firewall. Forcepoint. 2021. Available online: https://www.forcepoint.com/product/ngfw-next-generation firewall (accessed on 26 December 2021).

5. Hussain, Y.S. Network Intrusion Detection for Distributed Denial-of-Service (DDoS) Attacks Using Machine Learning Classifica tion Techniques. Master's Thesis, University of Victoria, Victoria, BC, Canada, 2020. Available online: https://dspace.library.uvic.ca/handle/1828/11679 (accessed on 26 December 2021).

6. Kim, T. T., & Poor, H. V. (2011). Strategic Protection Against Data Injection Attacks on Power Grids. IEEE Transactions on Smart Grid, 2(2), 326-333. https://doi.org/10.1109/tsg.2011.2119336

7. Samuel, O., Al-Zahrani, F. A., Khan, R. J. u. H., Farooq, H., Shafiq, M., Afzal, M. K., & Javaid, N. (2020). Towards Modified Entropy Mutual Information Feature Selection to Forecast Medium-Term Load Using a Deep Learning Model in Smart Homes. Entropy (Basel, Switzerland), 22(1), 68-NA. https://doi.org/10.3390/e22010068

8. Sargolzaei, A., Yazdani, K., Abbaspour, A., Crane, C. D., & Dixon, W. E. (2020). Detection and Mitigation of False Data Injection Attacks in Networked Control Systems. IEEE Transactions on Industrial Informatics, 16(6), 4281-4292. https://doi.org/10.1109/tii.2019.2952067

9. Schmidt, D., Radke, K., Camtepe, S., Foo, E., & Ren, M. (2016). A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures. ACM Computing Surveys, https://doi.org/10.1145/2897166

10. Jamdagni, A., He, X., & Nanda, P. (2010). Network Intrusion Detection based on LDA for payload feature selection. 2010 IEEE Globecom Workshops, NA(NA), 1545-1549. https://doi.org/10.1109/glocomw.2010.5700198

11. Tufail, S., Parvez, I., Batool, S., & Sarwat, A. I. (2021). A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid. Energies, 14(18), 5894-NA. https://doi.org/10.3390/en14185894

12. Usman, M., Jan, M. A., He, X., & Chen, J. (2019). P2DCA: A Privacy-Preserving-Based Data Collection and Analysis Framework for IoMT Applications. IEEE Journal on Selected Areas in Communications, 37(6), 1222-1230. https://doi.org/10.1109/jsac.2019.2904349

13. Zhang, F., Kodituwakku, H. A. D. E., Hines, J. W., & Coble, J. B. (2019). Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data. IEEE Transactions on Industrial Informatics, 15(7), 4362 4369. https://doi.org/10.1109/tii.2019.2891261

14. Zhang, H., Liu, B., & Wu, H. (2021). Smart Grid Cyber Physical Attack and Defense: A Review. IEEE Access, 9(NA), 29641-29659. https://doi.org/10.1109/access.2021.3058628

15. Zhang, Y., Wang, L., Sun, W., Green, R. C., & Alam, M. (2011). Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids. IEEE Transactions on Smart Grid, 2(4), 796-808. https://doi.org/10.1109/tsg.2011.2159818

16. Zhou, X., Hu, Y., Liang, W., Ma, J., & Jin, Q. (2021). Variational LSTM Enhanced Anomaly Detection for Industrial Big Data. IEEE Transactions on Industrial Informatics, 17(5), 3469-3477. https://doi.org/10.1109/tii.2020.3022432

17. Appasani, B., & Mohanta, D. K. (2018). A review on synchrophasor communication system: communication technologies, standards and applications. Protection and Control of Modern Power Systems, 3(1), https://doi.org/10.1186/s41601-018-0110-4

18. Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network Intrusion Detection for IoT Security Based on Learning Techniques. IEEE Communications Surveys & Tutorials, 21(3), 2671 2701. https://doi.org/10.1109/comst.2019.2896380

19. Chen, C., Zhang, K., Yuan, K., Zhu, L., & Qian, M. (2018). Novel Detection Scheme Design Considering Cyber Attacks on Load Frequency Control. IEEE Transactions on Industrial Informatics, 14(5), 1932 1941. https://doi.org/10.1109/tii.2017.2765313

20. Chen, P.-Y., Yang, S., McCann, J. A., Lin, J., & Yang, X. (2015). Detection of false data injection attacks in smart-grid systems. Magazine, IEEE Communications 53(2), 206-213. https://doi.org/10.1109/mcom.2015.7045410