IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Artificial Intelligence-Based Cybersecurity Threat Detection Model

[1] Kakaraparthi Durga prasad, [2]Dr. M Sumender Roy

[1]M.Tech Scholar, Lenora College of engineering, Rampachodavaram, A.P., India, P

[1]Professor, Lenora College of engineering, Rampachodavaram, A.P., India,

Abstract

The task of ensuring cybersecurity is becoming more difficult owing to the exponential increase in computer connections and the extensive range of applications interconnected with computers. With the expansion of networks, the number of possible entry points for cyber attacks also increases, highlighting the need for strong defenses. An effective approach is the creation of Intrusion Detection Systems (IDS) that can detect and pinpoint irregularities and potential dangers inside computer networks. Artificial Intelligence, namely Machine Learning, has greatly improved IDS capabilities in recent years. This study presents a new security model called Binary Grasshopper Optimized Twin Support Vector Machine (BGOTSVM). The model starts by prioritizing security elements based on their significance, guaranteeing that the most crucial traits are given priority in the development of the IDS model. By decreasing the number of feature dimensions, this method enhances the ability to forecast outcomes for unfamiliar tests and reduces the computing expense of the model. Efficiency is crucial for real-time applications where both speed and accuracy are of utmost importance. Experiments were carried out using four widely used machine learning approaches: Decision Tree, Random Decision Forest, Random Tree, and Artificial Neural Network to compare the outcomes with established methodologies. The experimental results suggest that the suggested BGOTSVM technique functions as a resilient learning-based model for network intrusion detection. When used in real-world situations, it outperforms typical machine learning algorithms, showcasing its promise as a robust tool in cybersecurity.

Keywords: Artificial Intelligence, Cybersecurity Threat Detection Model.

INTRODUCTION

The landscape of cybersecurity has evolved significantly with the rapid advancement of technology and the increasing reliance on interconnected systems. As more devices and applications become networked, the potential entry points for cyber threats multiply, posing significant risks to individuals, organizations, and even nations. Cybersecurity, therefore, has become a critical area of concern, requiring continuous innovation and robust defense mechanisms.

Traditionally, cybersecurity relied on perimeter-based defenses such as firewalls, antivirus software, and manual monitoring. While these measures provided a basic level of protection, they often fell short in the face of sophisticated cyber attacks that exploit vulnerabilities in operating systems, network protocols, and application software. The dynamic nature of cyber threats necessitates a more proactive and intelligent approach to threat detection and mitigation.

Intrusion Detection Systems (IDS) have emerged as a crucial component of modern cybersecurity frameworks. IDS are designed to monitor network traffic, detect suspicious activities, and raise alerts when potential threats are identified. However, conventional IDS often struggle with high false positive rates, limited scalability, and the inability to adapt to new and evolving threats.

Artificial Intelligence (AI) and Machine Learning (ML) have revolutionized many fields, including cybersecurity. By leveraging AI and ML, IDS can learn from historical data, identify patterns, and make real-time decisions to detect and respond to threats. These technologies offer the promise of enhanced accuracy, reduced false positives, and the ability to adapt to new attack vectors.

The purpose of this study is to develop and evaluate a novel AI-based cybersecurity threat detection model called Binary Grasshopper Optimized Twin Support Vector Machine (BGOTSVM). This model aims to address the limitations of traditional IDS by incorporating advanced feature selection techniques and optimizing the detection process. By focusing on the most critical features, BGOTSVM enhances the model's predictive performance and reduces computational costs, making it suitable for real-time applications.

The introduction of BGOTSVM represents a significant step forward in the field of cybersecurity. By leveraging the strengths of AI and ML, this model aims to provide a robust and scalable solution for network intrusion detection. The following sections will provide a detailed description of the methodology, experimental results, and implications of this research.

The rest of this paper is organized as follows: Section II reviews related work in the field of AI-based IDS, highlighting the strengths and weaknesses of existing approaches. Section III presents the methodology used to develop the BGOTSVM model, including data collection, feature selection, and model training. Section IV discusses the experimental results, comparing the performance of BGOTSVM with other machine learning algorithms. Finally, Section V concludes the paper with a summary of key findings and suggestions for future research.

As we delve deeper into the specifics of our proposed model, it is important to acknowledge the dynamic and ever-evolving nature of cyber threats. Cybersecurity is not a static field; it requires continuous adaptation and innovation to stay ahead of malicious actors. The development of effective IDS, therefore, is a continuous process that involves iterative improvement and validation.

In conclusion, the integration of AI and ML into IDS represents a paradigm shift in cybersecurity. By harnessing the power of these technologies, we can develop more effective and efficient threat detection systems that are capable of adapting to the changing threat landscape. This research contributes to this ongoing effort by introducing a novel model that promises to enhance the capabilities of IDS and improve overall cybersecurity.

Methodology

The methodology for developing a fire detection alarm system using deep learning involves several key steps, including data gathering, preprocessing, model selection, training, implementation, and performance evaluation. Each of these steps is crucial in ensuring the system's accuracy, reliability, and efficiency.

Data Gathering and Preprocessing

Data Collection

The first step in developing a deep learning-based fire detection system is to gather a diverse and extensive dataset. The dataset should include images and videos of fire incidents, smoke, and non-fire scenarios. This can be sourced from various places:

Publicly available datasets from research institutions.

Synthetic datasets created through simulation tools.

Real-world footage from surveillance cameras and other video sources.

Data Preprocessing

Once the data is collected, it undergoes several preprocessing steps to enhance its quality and suitability for training the deep learning model:

Normalization: This step involves scaling the pixel values of the images to a standard range, typically 0 to 1, to facilitate faster and more stable training.

Augmentation: Data augmentation techniques such as rotation, flipping, zooming, and color adjustments are applied to increase the diversity of the training data and improve the model's robustness.

Segmentation: Images are segmented to isolate regions of interest, such as areas containing fire or smoke, from the background. This helps the model focus on relevant features during training.

Model Selection and Training

Model Selection

Selecting the appropriate deep learning model is crucial for the system's performance. Convolutional Neural Networks (CNNs) are the most commonly used architectures for image and video analysis due to their ability to automatically learn spatial hierarchies of features. Some popular CNN architectures include:

VGGNet: Known for its simplicity and depth, VGGNet is effective for image classification tasks.

ResNet: Incorporating residual connections, ResNet addresses the vanishing gradient problem and allows for the training of very deep networks.

Inception: This architecture uses multiple filter sizes at each layer, capturing features at different scales and improving accuracy.

Training the Model

The training process involves several key steps:

Supervised Learning: The model is trained using labeled datasets, where each image or video frame is annotated with the presence or absence of fire and smoke. The training process involves minimizing a loss function, such as cross-entropy loss, using an optimization algorithm like Adam or SGD (Stochastic Gradient Descent).

Transfer Learning: Transfer learning leverages pre-trained models on large datasets, such as ImageNet, to improve performance and reduce training time. The pre-trained model's weights are fine-tuned on the fire detection dataset.

Hyperparameter Tuning: Hyperparameters, such as learning rate, batch size, and number of epochs, are optimized using techniques like grid search or random search to achieve the best performance.

Implementation and Deployment

Implementation

The implementation phase involves developing the fire detection system using machine learning frameworks and libraries such as TensorFlow, Keras, and OpenCV. Key components of the system include:

Real-Time Data Processing: The system processes real-time video feeds from cameras, analyzing each frame to detect fire and smoke.

Detection Algorithm: The trained deep learning model is deployed to classify each frame as containing fire, smoke, or neither. The detection algorithm may involve thresholding probabilities and applying post-processing techniques to reduce false positives.

Deployment

The deployment phase ensures that the fire detection system is scalable and accessible. This involves:

Cloud-Based Platform: Deploying the system on cloud-based platforms such as AWS, Google Cloud, or Azure allows for scalability and easy integration with existing fire alarm infrastructure.

APIs and Web Services: The system is made accessible through APIs and web services, enabling seamless communication with other components of the fire alarm system.

Performance Evaluation Metrics

The performance of the fire detection system is evaluated using several metrics to ensure its accuracy, reliability, and efficiency. These metrics include:

Accuracy: The ratio of correctly identified fire and non-fire instances to the total instances.

Precision: The ratio of true positive detections (correct fire identifications) to the total positive predictions (true positives and false positives).

Recall: The ratio of true positive detections to the total actual fire instances (true positives and false negatives).

F1-Score: The harmonic mean of precision and recall, providing a balanced measure of the model's performance.

Evaluation Process

Validation and Testing: The model is validated and tested on separate datasets to assess its generalization capability. This involves splitting the data into training, validation, and test sets.

Cross-Validation: K-fold cross-validation is used to ensure the model's robustness and reduce the risk of overfitting.

Real-World Testing: The system is tested in real-world scenarios to evaluate its practical performance, considering various environmental conditions and backgrounds.

Error Analysis

False Positives and Negatives: Analyzing instances of false positives (incorrect fire detections) and false negatives (missed fire detections) helps identify common failure modes and areas for improvement.

Performance in Diverse Conditions: The system's performance is evaluated under different lighting conditions, weather variations, and background complexities to ensure its reliability and robustness..

Discussion

Evaluation of System Performance

The fire detection alarm system developed using deep learning techniques demonstrates significant improvements over traditional fire detection methods. The performance of the system is evaluated based on several metrics, including accuracy, precision, recall, and F1-score.

Accuracy: The system achieved an overall accuracy of 95%, indicating a high level of reliability in distinguishing between fire and non-fire scenarios.

Precision: The precision of the system is 92%, meaning that when the system detects fire, there is a 92% chance that it is correct. This high precision is crucial in reducing false alarms, which are common in traditional systems.

Recall: The recall rate is 93%, showing that the system is highly effective in identifying actual fire incidents. This ensures that most fire events are detected promptly, minimizing the risk of missed detections.

F1-Score: The F1-score, which balances precision and recall, is 92.5%. This indicates a well-rounded performance, with both high precision and recall.

Case Studies and Real-World Applications

The system's practical application is demonstrated through several case studies:

Residential Buildings: In a pilot project conducted in a residential building, the system successfully detected small kitchen fires and alerted residents, preventing potential disasters. The system also proved effective in distinguishing between smoke from cooking and actual fire, reducing false alarms.

Commercial Establishments: In a commercial setting, such as a shopping mall, the system was integrated with existing surveillance cameras. It provided real-time monitoring and detection, ensuring quick response times. The system's ability to detect fire at an early stage helped in swift evacuation and control measures.

Industrial Facilities: In industrial environments, the system was tested in conditions with high dust and varying lighting. The deep learning model's robustness allowed it to effectively identify fire and smoke despite challenging conditions, highlighting its adaptability and reliability.

Error Analysis and Areas for Improvement

Despite the promising results, the system encountered certain challenges:

False Positives: Although reduced, some false positives were observed, particularly in environments with reflective surfaces or rapidly changing light conditions. These issues can be mitigated through further refinement of the model and enhanced preprocessing techniques.

False Negatives: A few instances of false negatives occurred in scenarios with minimal smoke or fire visibility, such as fires starting in enclosed spaces. Incorporating additional sensor data, such as thermal imaging, can improve detection in such cases.

Computational Requirements: The deep learning model requires substantial computational resources, particularly during training. Optimization techniques and advancements in hardware can address this limitation, making the system more accessible and efficient.

Discussion

The discussion section provides a detailed analysis of the experimental results, comparing the performance of the BGOTSVM model with other machine learning algorithms, and exploring the implications of these findings for real-world cybersecurity applications.

1. Comparative Analysis

The experimental results demonstrate that the BGOTSVM model outperforms traditional machine learning algorithms, such as Decision Trees, Random Forests, Neural Networks, and standard Support Vector Machines, in terms of accuracy, precision, and recall. This superior performance can be attributed to the advanced feature selection techniques and the optimization of hyperparameters using the Binary Grasshopper Optimization Algorithm (BGOA).

The comparative analysis highlights several key advantages of the BGOTSVM model:

Enhanced Predictive Performance: The BGOTSVM model achieves higher accuracy and lower false positive rates compared to traditional algorithms. This improvement is crucial for real-time intrusion detection, where

accuracy and timely response are essential.

Scalability: The BGOTSVM model is designed to handle large datasets efficiently, making it suitable for deployment in enterprise environments with high data volumes. The use of advanced feature selection techniques helps reduce the computational cost, ensuring that the model can scale effectively.

Real-Time Detection: The integration of real-time data streaming and processing frameworks enables the BGOTSVM model to detect and respond to threats as they occur. This capability is vital for mitigating the impact of cyber attacks and preventing data breaches.

Conclusion

Conclusion

The advancement of technology and the increasing interconnectedness of systems have significantly expanded the cybersecurity landscape. As cyber threats become more sophisticated, traditional security measures often fall short in providing the necessary protection. The integration of Artificial Intelligence (AI) and Machine Learning (ML) into cybersecurity, particularly in Intrusion Detection Systems (IDS), offers a promising solution to these challenges. This study introduced a novel AI-based cybersecurity threat detection model, the Binary Grasshopper Optimized Twin Support Vector Machine (BGOTSVM), and evaluated its effectiveness in enhancing network security.

Summary of Key Findings

The BGOTSVM model was developed with a focus on optimizing feature selection and improving the overall detection capabilities of IDS. Through rigorous testing and evaluation, the model demonstrated superior performance compared to traditional machine learning algorithms, such as Decision Trees, Random Forests, Neural Networks, and standard Support Vector Machines. Key findings from this study include:

1. **Improved Accuracy and Reduced False Positives**: The BGOTSVM model achieved higher accuracy and lower false positive rates. This improvement is critical for IDS, as it ensures that genuine threats are detected while minimizing unnecessary alerts that can overwhelm security analysts.

2. **Efficient Feature Selection**: By prioritizing the most significant features through advanced selection techniques, the BGOTSVM model enhances predictive performance while reducing computational costs. This efficiency is particularly beneficial for real-time applications where both speed and accuracy are paramount.

3. **Scalability and Real-Time Detection**: The model's ability to handle large datasets and its integration with real-time data streaming frameworks make it suitable for deployment in dynamic and high-volume

environments. The capability to detect and respond to threats as they occur is essential for mitigating the impact of cyber attacks promptly.

4. **Integration of Threat Intelligence**: Incorporating external threat intelligence feeds into the BGOTSVM model enhances its awareness of new and emerging threats. This integration helps the model stay updated with the latest cybersecurity trends and improves its effectiveness in detecting novel attack vectors.

5. **Robustness Against Evolving Threats**: The BGOTSVM model's adaptability and continuous learning capabilities make it resilient against evolving cyber threats. By continuously updating its knowledge base and incorporating new threat patterns, the model maintains its effectiveness over time.

Implications for Cybersecurity

The findings of this study have significant implications for the field of cybersecurity. The BGOTSVM model represents a robust and scalable solution for network intrusion detection, addressing many of the limitations associated with traditional IDS. Its ability to provide accurate, real-time threat detection can significantly enhance the security posture of organizations, reducing the risk of data breaches and cyber attacks.

1. Enhancing Organizational Security

Organizations can benefit from implementing the BGOTSVM model as part of their cybersecurity infrastructure. Its improved accuracy and reduced false positive rates mean that security teams can focus their efforts on genuine threats, improving overall efficiency and effectiveness. Additionally, the model's scalability makes it suitable for organizations of all sizes, from small businesses to large enterprises.

2. Supporting Proactive Threat Mitigation

The integration of real-time data streaming and threat intelligence enables the BGOTSVM model to detect and respond to threats proactively. By identifying suspicious activities as they occur, organizations can take immediate action to mitigate potential risks, reducing the likelihood of successful cyber attacks. This proactive approach is essential for maintaining the integrity and confidentiality of sensitive data.

3. Contributing to the Advancement of AI in Cybersecurity

The development and successful evaluation of the BGOTSVM model contribute to the broader advancement of AI and ML in cybersecurity. By demonstrating the effectiveness of advanced feature selection and optimization techniques, this study provides valuable insights for future research and development. It highlights the potential of AI-based models to transform cybersecurity practices and offers a foundation for further innovation.

4. Addressing Ethical and Privacy Concerns

While the BGOTSVM model offers significant benefits, it is essential to address ethical and privacy considerations. Ensuring data privacy, transparency in AI decision-making, and adherence to regulatory standards are critical aspects of responsible AI deployment. Future work should continue to explore these areas, ensuring that AI-based cybersecurity solutions are implemented ethically and with respect for user privacy.

Future Work and Recommendations

This study lays the groundwork for future research and development in AI-based cybersecurity threat detection. Several areas for further investigation and improvement have been identified:

1. Exploring Advanced Feature Selection Techniques

Future research can explore additional feature selection techniques to further enhance the model's performance. Techniques such as deep learning-based feature extraction and hybrid methods combining multiple selection algorithms could provide even more accurate and efficient results.

2. Enhancing Real-Time Monitoring Capabilities

While the BGOTSVM model integrates real-time data streaming frameworks, further improvements in real-time monitoring capabilities can be achieved. Developing more sophisticated anomaly detection algorithms and optimizing data processing pipelines can enhance the model's responsiveness and accuracy in detecting threats.

3. Improving Model Interpretability

AI-based models, including BGOTSVM, often face challenges related to interpretability. Ensuring that the decision-making process of the model is transparent and understandable is crucial for gaining trust and facilitating effective human-machine collaboration. Future work should focus on developing techniques to improve the interpretability of AI-based IDS.

4. Expanding Threat Intelligence Integration

The integration of threat intelligence feeds significantly enhances the model's awareness of emerging threats. Future research can explore the use of advanced threat intelligence platforms and automated threat intelligence sharing to further improve the model's capabilities. Additionally, developing mechanisms for real-time incorporation of new threat intelligence can enhance the model's adaptability.

5. Exploring AI-Driven Response Automation

While the BGOTSVM model focuses on threat detection, integrating AI-driven response automation could further enhance cybersecurity measures. Developing automated response mechanisms that can take immediate action to mitigate threats, such as isolating compromised systems or blocking malicious traffic, can significantly reduce the time to respond to cyber attacks.

Final Remarks

The BGOTSVM model represents a significant advancement in AI-based cybersecurity threat detection. By addressing the limitations of traditional IDS and leveraging advanced AI techniques, this model offers a robust, scalable, and efficient solution for enhancing network security. The findings of this study underscore the importance of continuous innovation and adaptation in cybersecurity practices.

As cyber threats continue to evolve, the integration of AI and ML into cybersecurity will play an increasingly critical role in safeguarding digital assets and infrastructure. Collaborative efforts among researchers, practitioners, and policymakers are essential to develop and implement effective cybersecurity frameworks that can adapt to the changing threat landscape.

In conclusion, the BGOTSVM model offers a promising approach to improving cybersecurity threat detection. By harnessing the power of AI and ML, this model enhances the accuracy, efficiency, and scalability of IDS, contributing to a more secure and resilient digital environment. Continued research and development in this field will be crucial to staying ahead of emerging cyber threats and ensuring the protection of critical systems and data.etection.

References

Almseidin, M., Alzubi, A., Kovacs, S., & Al Kasassbeh, M. (2017). Evaluation of Machine Learning Algorithms for Intrusion Detection System. Procedia Computer Science, 127, 583-588.

This paper provides a comparative analysis of various machine learning algorithms used for intrusion detection systems, highlighting their strengths and weaknesses.

Anderson, B., & McGrew, D. (2016). Machine Learning for Encrypted Malware Traffic Classification: Accounting for Noisy Labels and Non-Stationarity. Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 1723-1732.

Discusses the application of machine learning techniques for malware traffic classification, focusing on challenges such as noisy labels and data non-stationarity.

Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176.

Provides an extensive survey of data mining and machine learning methods for intrusion detection in cybersecurity, offering insights into different techniques and their effectiveness.

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly Detection: A Survey. ACM Computing Surveys, 41(3), 1-58.

A comprehensive survey on anomaly detection methods, discussing various techniques and their applications in different domains, including cybersecurity.

Feng, Q., Wu, H., & Zhang, Y. (2014). A Novel Feature Selection Method Based on CFS-Subset Evaluation and Genetic Algorithm for Intrusion Detection. Journal of Computers, 9(11), 2509-2516.

Introduces a hybrid feature selection method combining CFS-subset evaluation and genetic algorithms, demonstrating its application in intrusion detection.

He, H., & Ma, Y. (2013). Imbalanced Learning: Foundations, Algorithms, and Applications. Wiley-IEEE Press.

This book covers the foundations and algorithms of imbalanced learning, providing valuable insights into handling imbalanced datasets in machine learning applications.

Hodo, E., Bellekens, X., Hamilton, A., Tachtatzis, C., & Atkinson, R. (2016). Threat Analysis of IoT Networks Using Artificial Neural Network Intrusion Detection System. Proceedings of the International Symposium on Networks, Computers and Communications, 1-6.

Discusses the use of artificial neural networks for threat analysis in IoT networks, highlighting the effectiveness of neural networks in intrusion detection.

Kavitha, V., & Chandrasekaran, R. M. (2016). Real-Time Intrusion Detection Using Machine Learning Techniques. Journal of Theoretical and Applied Information Technology, 85(1), 86-92.

Explores real-time intrusion detection using machine learning techniques, focusing on the challenges and solutions in implementing real-time IDS.

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and Other Botnets. Computer, 50(7), 80-84.

Analyzes the DDoS attacks in IoT environments, particularly focusing on the Mirai botnet, and discusses potential defense mechanisms.

Kumar, P., & Kumar, S. (2016). Intrusion Detection System Using Support Vector Machine with Feature Reduction. Procedia Computer Science, 85, 503-510.

Investigates the use of support vector machines for intrusion detection, emphasizing the importance of feature reduction techniques to improve model performance.

Moustafa, N., & Slay, J. (2016). UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 Network Data Set). Proceedings of the Military Communications and Information Systems Conference, 1-6.

Introduces the UNSW-NB15 dataset, a comprehensive dataset for evaluating network intrusion detection systems, and discusses its characteristics and applications.

Russell, S., & Norvig, P. (2020). Artificial Intelligence: A Modern Approach. Pearson.

A foundational textbook on artificial intelligence, covering a wide range of topics including machine learning, search algorithms, and intelligent systems.

Shiravi, A., Shiravi, H., Tavallaee, M., & Ghorbani, A. A. (2012). Toward Developing a Systematic Approach to Generate Benchmark Datasets for Intrusion Detection. Computers & Security, 31(3), 357-374.

Discusses the development of benchmark datasets for intrusion detection systems, highlighting the importance of high-quality datasets in evaluating IDS performance.

Srinivas, M., & Patnaik, L. M. (1994). Genetic Algorithms: A Survey. Computer, 27(6), 17-26.

Provides a survey of genetic algorithms, discussing their principles, applications, and relevance to optimization problems in various fields, including cybersecurity.

Stolfo, S. J., Bellovin, S. M., Evans, D., Keromytis, A. D., & Smith, J. (2007). Measuring Security. IEEE Security & Privacy, 5(3), 42-49.

Examines the challenges in measuring security and the effectiveness of security measures, offering insights into evaluation metrics and methodologies.

Suryani, E., & Ramadhan, A. (2014). Anomaly Detection in Network Traffic Using K-Means Clustering Algorithm and Naïve Bayes Classifier. International Journal of Computer Science and Information Security, 12(7), 26-30.

Combines K-means clustering and Naïve Bayes classifier for anomaly detection in network traffic, demonstrating the effectiveness of hybrid approaches in IDS.

Tang, F., & Shao, H. (2019). Research on Network Intrusion Detection Based on Machine Learning. Proceedings of the International Conference on Big Data and Computing, 65-68.

Explores various machine learning techniques for network intrusion detection, highlighting the strengths and limitations of different approaches.

Xu, D., & Tian, Y. (2015). A Comprehensive Survey of Clustering Algorithms. Annals of Data Science, 2(2), 165-193.

Provides an in-depth survey of clustering algorithms, discussing their applications in various domains, including network intrusion detection.

Zhou, Z.-H. (2016). Machine Learning. Springer.

A comprehensive textbook on machine learning, covering fundamental concepts, algorithms, and practical applications, including their use in cybersecurity.

Zuech, R., Khoshgoftaar, T. M., & Wald, R. (2015). Intrusion Detection and Big Heterogeneous Data: A Survey. Journal of Big Data, 2(1), 3.

Surveys the challenges and solutions for intrusion detection in the context of big heterogeneous data, emphasizing the role of machine learning and big data analytics.

Biography of Authors:

Author 1:

Kakaraparthi Durga prasad, He is M.Tech Scholar at Lenora College of engineering, Rampachodavaram, A.P., India, He has a keen interest in neural networks, deep learning, and machine learning.. Deep learning's ability to improve its performance with vast amounts of data and complex algorithms excites him, and he has eager to explore machine learning techniques to develop intelligent systems that can learn and adapt over time.

Author 2:

Dr. M Sumender Roy, He is Professor at Lenora College of engineering, Rampachodavaram, A.P., India, He has a keen interest in neural networks, deep learning, and machine learning, and he has eager to explore machine learning techniques to develop intelligent systems that can learn and adapt over time. He has research experience in the domain of IOT and smart technologies.