International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

ENHANCING INTRUSION DETECTION SYSTEMS THROUGH DEEP LEARNING AND AUTOENCODERS: A COMPREHENSIVE STUDY

Priya Bhashini Koyyagura, Dr. V V S S S BALARAM

Research Scholar,Anurag University,

priyabhashinikoyyagura@gmail.com.

Professor,Anurag University

drvbalaramcse@anurag.edu.in

Abstract. The rapid increase in sophisticated cyber threats necessitates the evolution of Intrusion Detection Systems (IDS) to ensure robust network security. Traditional IDS often struggle with high false positive and negative rates, and fail to detect complex intrusion patterns. This study investigates the integration of deep learning algorithms with autoencoders to address these challenges, proposing a novel approach to IDS enhancement. Deep learning algorithms are implemented and optimized to improve detection accuracy and reduce false alerts. Additionally, autoencoders are utilized for feature extraction and dimensionality reduction, enhancing the IDS's ability to identify subtle and intricate anomalies. The study evaluates the impact of autoencoder based preprocessing on the performance of deep learning models, hypothesizing that this integration significantly boosts detection rates and efficiency. A comprehensive comparative analysis is conducted, assessing the performance of traditional deep learning algorithms with and without autoencoder integration. Various performance metrics, including accuracy, precision, recall, F1 score, and computational efficiency, are employed to evaluate the models. The study explores the benefits and trade-offs of incorporating autoencoders, particularly in terms of detection accuracy, false positive/negative rates, and real-time applicability. This research provides valuable insights into the deployment of advanced IDS in real world scenarios, highlighting the most effective approaches for leveraging deep learning and autoencoder techniques. The findings aim to contribute significantly to the field of network security, offering enhanced reliability and robustness in intrusion detection.

Keywords: Intrusion Detection System, Deep Learning, Autoencoders, Anomaly Detection, Network Security, Feature Extraction, False Positives, False Negatives.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

1 INTRODUCTION

1.1 1.1 Background of Intrusion Detection Systems

Intrusion Detection Systems (IDS) are essential components of modern network security infrastructure[1]. They monitor network traffic for suspicious activity and potential threats, providing alerts when anomalies are detected. The primary goal of an IDS is to identify and mitigate security breaches, ensuring the integrity[2], confidentiality, and availability of network resources. Over the years, IDS technologies have evolved from simple signature-based systems, which detect known threats, to more sophisticated approaches like anomaly based and hybrid systems, which aim to identify both known and unknown threats. The continuous advancement in IDS technologies reflects the growing complexity and frequency of cyber threats in today's digital landscape[3].

1.2 Importance of Network Security

Let it be computer systems in a business organization, or telecommunication systems in a nation, network security is imperative with regard to confidentiality, integrity, and availability. The consequences of cyber-attacks include major monetary implications, brand demeanour, and interferences with activities. Therefore, effective security measure in the network such as IDS are crucial in order to curb unauthorized access and other malicious activities[4]. Network security also benefits the world’s organizations and the entire digital environment by safeguarding each network. Thus, more advanced and persistent being cyber threats, it is critical to implement comprehensive security measures, including the best IDS.

1.3 Challenges in Current IDS

Despite the advancements in IDS technologies, several challenges[4] persist. Traditional IDS often suffer from high false positive and false negative rates, leading to either unnecessary alerts or missed threats. The increasing volume and complexity of network traffic further complicate the task of accurately identifying malicious activities[4]. Additionally, attackers constantly develop new techniques to evade detection, rendering some IDS approaches less effective over time. Resource constraints, such as computational power[4] and storage capacity, also pose significant challenges[4], particularly in real time detection scenarios. These issues highlight the need for innovative approach-

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

es and continuous improvements in IDS technologies to effectively counter emerging threats.

2 LITERATURE REVIEW

2.1 Traditional Intrusion Detection Systems

Traditional Intrusion Detection Systems (IDS) have been the backbone of network security for many years[5]. These systems primarily rely on signature based and anomaly-based detection methods. Signature based IDS detect known threats by comparing network traffic against a database of known attack patterns, while anomaly-based IDS identify deviations from normal network behaviour. Notable traditional IDS include Snort and Bro (now Zeek), which have been widely deployed in various network environments[5]. The effectiveness of these systems largely depends on the quality and comprehensiveness of their rule sets and anomaly detection capabilities.

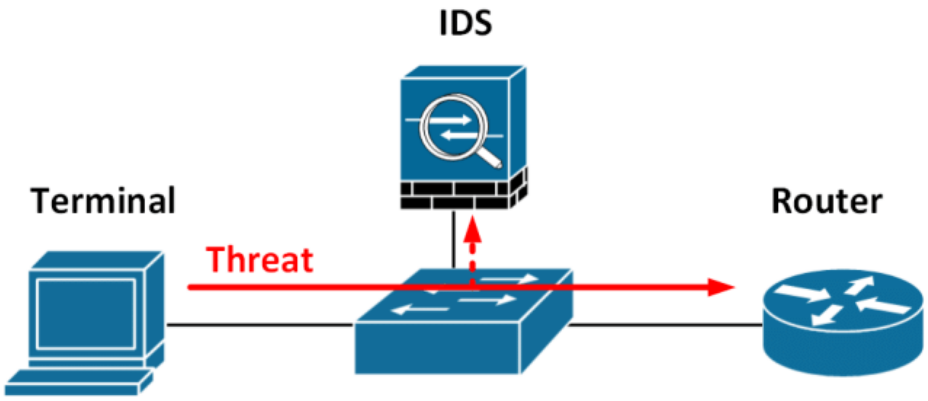

Fig. 1. Traditional Intrusion Detection System

2.2 Challenges in Traditional IDS

Despite their widespread use, traditional IDS face several significant challenges[6]. One major issue is their inability to detect novel or zero-day attacks[6], as signature-based systems can only recognize known threats[6]. Anomaly based IDS, on the other hand, often suffer from high false positive rates, as normal network behaviour can vary widely. Additionally, traditional IDS can struggle with scalability, especially in large, highspeed networks where they may become overwhelmed by the volume of traffic. These limitations necessitate the exploration of more advanced techniques to improve the effectiveness and efficiency of intrusion detection.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

2.3 Advancements in Deep Learning for IDS

Deep learning has shown many innovations that has helped the intrusion detection systems[7]. Some of the deep learning that have been used include convolutional neural networks CNN's, recurrent neural networks RNN's, and deep belief networks DBN's because they help in finding the complex pattern in the network traffic. These models can learn from the large datasets and generalize to analyse new attacks which was not trained from the dataset. Previous research has shown that IDS which is based on deep learning can detect more incidents and produce few false alarms of deep learning methods[7]. Another strength of these models is that they can to some extent perform feature extract-ion from raw data on their own

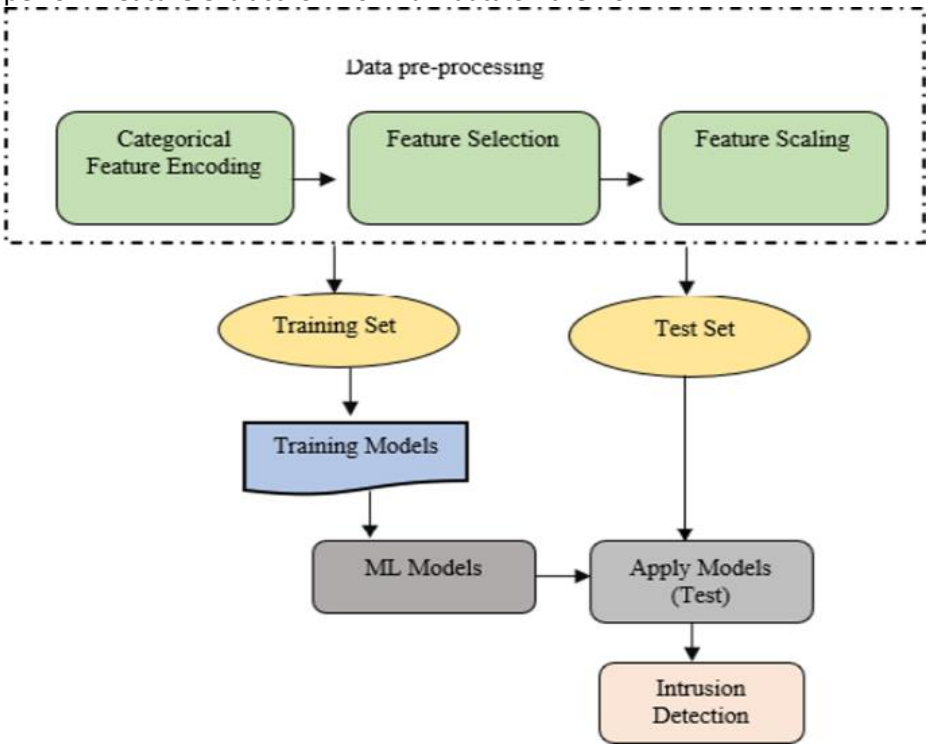

Fig. 2. Deep learning-based IDS

2.4 Current Challenges in Deep Learning based IDS

Thus, there are some issues that are associated with the use of deep learning-based IDS[8] . This is mainly due to the fact that large labelled data sets which are necessary for training are hard to come by specifically in the context of cybersecurity. Moreover, deep learning models are normally computa-

tionally expensive and take a lot of time for processing and memory hence presenting a challenge to real time implementation[8]. The limitation also includes the model interpretation, as deep learning models are regarded to be the “black boxes,” it is still very challenging to comprehend and trust the model’s decision-making. Solving these issues is vital for the practical application of deep learning-based IDS[8].

2.5 Role of Autoencoders in Enhancing Anomaly Detection

Autoencoders are a type of neural network commonly used in unsupervised learning, and are proving their effectiveness in IDS anomaly detection[9]. They are trained to perform feature extraction and feature quantization on input data while learning the features. Intrusion may, there for, be identified by using the amount of reconstruction errors, the higher they are the more probable that there has been an intranet. They are very efficient in drilling down into the details of the problem, and looking at the attacks in a different manner compared to the traditional methods[10]. They also come in handy when it comes into feature extraction as well as dimensionality reduction aiding in enhancing the efficiency of IDS[11].

2.6 Comparative Studies on IDS Techniques

Some researchers have done comparison of IDS techniques with a view of determining their effectiveness[12]. Such works tend to present a comparison between the conventional signature based and anomaly-based IDS with the latest deep learning IDS. Thus, some effective measures that can be used for the comparison are detection accuracy[12], the number of false positives, precision, recall, and the time needed for the computations. The results suggest that in general the IDS with the use of deep learning proves to be more efficient in comparison to the traditional systems in regards to the detection rate and false alarms. However, the studies also bring out the requirement of the further investigation of computational and interpretability of issues[12] that arise from deep learning models. New approaches to IDS have been proposed with the help of autoencoders integration, which has revealed the increased potential for anomaly detection – the major focus of IDS systems.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

3 3. PROPOSED METHODOLOGY

3.1 Overview of Deep Learning Algorithms for IDS

Deep learning techniques have paved way for enhancing Intrusion Detection Systems (IDS) because of the new abilities of detecting intricate and complex attacks inherent in the flow of traffic. Key algorithms include:

- Convolutional Neural Networks (CNNs)[13]: CNNs are particularly effective in processing and analyzing spatial data. In IDS, they can be used to identify patterns and anomalies in network traffic data by treating it as a multidimensional grid. CNNs excel in capturing hierarchical features, making them suitable for detecting intricate attack signatures.
- Recurrent Neural Networks (RNNs)[14]: RNNs are designed to handle sequential data and can maintain information over time, which is crucial for analysing network traffic that has temporal dependencies. Variants like Long Short-term Memory (LSTM) networks are often used to model complex sequences and detect anomalies that occur over time.
- Autoencoders[15]: Although primarily used for unsupervised learning, autoencoders can be adapted for anomaly detection in IDS by learning to reconstruct normal network traffic patterns and flagging deviations as potential threats.

All these algorithms offer different factors that make a positive contribution to the increased capabilities of IDS and the choice of the particular algorithm depends on the general requirements and opportunities of the network.

3.2 Incorporation of Autoencoders in IDS

Autoencoders are a class of neural networks designed to learn efficient representations of data, often used for feature extraction and dimensionality reduction. In the context of IDS, autoencoders are employed to enhance anomaly detection in several ways:

- Feature Extraction[16]: Autoencoders can automatically extract and compress features from raw network traffic data, reducing the dimensionality of the input while preserving important information. This helps in focusing on relevant features and improving the performance of subsequent detection models.
- Dimensionality Reduction[17]: By reducing the number of features, autoencoders simplify the data and make it easier for other models to process. This can lead to more efficient training and better detection accuracy.
- Anomaly Detection[18]: Autoencoders can be trained to reconstruct normal network traffic patterns. Deviations from this reconstructed pattern, as indicated by high reconstruction errors, can be flagged as anomalies. This approach helps in de-

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

tecting subtle and complex attack patterns that may be missed by traditional methods.

3.3 Integration of Deep Learning and Autoencoders

It has been established that the use of deep learning algorithms and autoencoders can sufficiently improve IDS[19]. This integration involves:

Preprocessing with Autoencoders: Applying autoencoders as the initial step in processing the net-work trafficking data in order to extract features and do feature space reduction. This step is helpful in reducing the generality of the data by limbering deeper learnt models on refined data with emphasis on prior crucial data.

- Deep Learning for Classification: Applying deep learning models, such as CNNs, RNNs, or DBNs, on the pre-processed data to detect and classify intrusions. The deep learning models can benefit from the reduced dimensionality and improved feature representation provided by autoencoders.
- Hybrid Approaches: Combining autoencoders with other deep learning techniques in a hybrid model to leverage the strengths of both. For example, using autoencoders for feature extraction and a CNN for classification can enhance detection performance and robustness.

This integrated solution postulates that the proposed solution of deep learning and autoencoders is more optimal and efficient to use in IDS.

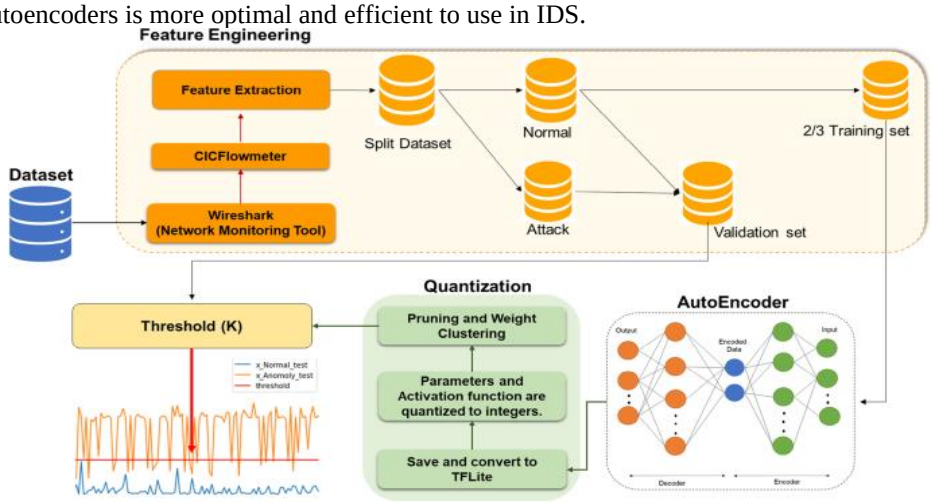

Fig. 3. Anomaly detection using DL & Autoencoders

3.4 Evaluation Metrics and Criteria

To assess the performance of IDS models, various evaluation metrics and criteria are used:

- Accuracy[20]: Measures the overall correctness of the model in identifying both normal and anomalous network traffic. It is calculated as the ratio of correctly classified instances to the total instances.
- Precision and Recall[20]: Precision indicates the proportion of true positives among all positive identifications, while recall measures the proportion of true positives among all actual positives. These metrics help in understanding the model's ability to correctly identify true intrusions and avoid false positives.
- F1 Score[20]: The F1 score is the harmonic mean of precision and recall, providing a balanced measure of model performance, especially in cases with imbalanced datasets.
- False Positive and False Negative Rates[20]: These rates indicate the number of normal traffic instances incorrectly classified as anomalies (false positives) and the number of actual intrusions missed by the model (false negatives).
- Computational Efficiency[20]: Assesses the model's performance in terms of processing time and resource usage. Efficient models are crucial for real time applications and largescale deployments.

By evaluating IDS models using these metrics, researchers can determine their effectiveness and identify areas for improvement, ensuring that the models are both accurate and practical for real world deployment.

4 Analysis and Discussion

4.1 4.1 Literature Based Performance Comparison of Models

The performance of intrusion detection systems (IDS) has been extensively studied in the literature, with various models being compared based on their effectiveness in detecting intrusions[21]. Traditional IDS techniques, such as signature based and anomaly-based methods, have been evaluated for their ability to identify known and novel threats. However, recent studies have shown that deep learning-based models, including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Deep Belief Networks (DBNs), generally outperform traditional methods in terms of detection accuracy and sensitivity to complex attack patterns.

Research indicates that deep learning models can achieve higher detection rates[21] and lower false positive rates compared to conventional IDS techniques. This improvement is attributed to their ability to learn and generalize from large datasets, enabling them to detect previously unseen attacks. Comparative studies in the literature often highlight the superior performance of deep learning approaches in various network environments, demonstrating their potential for more effective and comprehensive intrusion detection.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

4.2 Impact of Autoencoder Integration Based on Existing Studies

Autoencoders have been incorporated into IDS to enhance anomaly detection by leveraging their capabilities in feature extraction and dimensionality reduction. Existing studies suggest that autoencoders can significantly improve the performance of IDS by providing more accurate representations of normal network traffic and detecting subtle anomalies that may be missed by other methods[22].

The integration of autoencoders with traditional and deep learning-based IDS models has been shown to reduce false positive rates and improve overall detection accuracy. Autoencoders help in focusing on relevant features and reducing the noise in the data, which enhances the performance of the subsequent classification models[22]. Literature indicates that this integration can lead to more robust and reliable IDS, particularly in complex and dynamic network environments.

4.3 Analysis of Detection Accuracy, Precision, Recall, F1 Score, and Computational Efficiency from Literature

In analyzing IDS performance, various metrics such as detection accuracy, precision, recall, F1 score, and computational efficiency are commonly used

- Detection Accuracy: Studies show that deep learning-based IDS models generally achieve higher detection accuracy compared to traditional methods. The ability of these models to learn from extensive datasets contributes to their superior performance in identifying both known and novel attacks.
- Precision and Recall: Deep learning models often demonstrate improved precision and recall rates. High precision indicates fewer false positives, while high recall reflects the model's effectiveness in identifying true intrusions. Research highlights that integrating autoencoders can further enhance these metrics by improving feature representation and reducing false alarms.
- F1 Score: The F1 score, which balances precision and recall, is frequently used to evaluate the overall performance of IDS models. Literature suggests that deep learning models, especially those incorporating autoencoders, achieve higher F1 scores, reflecting a well-rounded performance in detecting intrusions.
- Computational Efficiency: Computational efficiency remains a critical factor for deploying IDS in real time scenarios. While deep learning models can be computationally intensive, advances in hardware and optimization techniques have made them more feasible for practical use. Studies indicate that although deep learning models require more computational resources, their performance gains often outweigh the associated costs.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

4.4 Discussion on False Positives and False Negatives in Literature

Both, false positives and false negative highly influence the IDS performance[23]. For example, the absence of an alert when an intrusion actually occurred is what is referred to as a false negative while an alert generated when no intrusion was actually taking place is referred to as a false positive[23].

The literature in this area further shows that conventional IDS techniques, specifically, signature-based IDSs, are inclined to produce more False Positives' as a result of their reliance on specifically defined attacks. However, deep learning models and in particular models using autoencoders normally receive lower numbers of False Positives due to the received models' abilities to learn more accurate patterns of normal and abnormal behaviour. Still, it is suggested that these models might miss some attacks, especially in new and more complex ones.

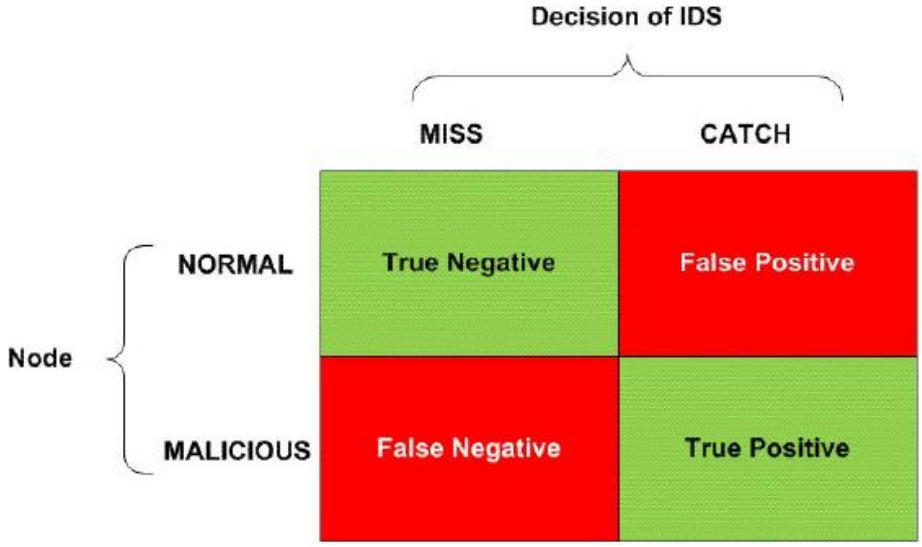

Fig. 4. False Negative and true Positive

4.5 Realtime Applicability of the Proposed Methods Based on Literature

The real time applicability of IDS methods is crucial for practical deployment, especially in dynamic network environments where timely detection of intrusions is essential. Literature suggests that while traditional IDS methods may struggle with scalability and real time processing, deep learning-based models, though computationally demanding, are increasingly being optimized for

real time use. Advancements in hardware, such as GPUs and TPUs, along with algorithmic improvements, have enhanced the feasibility of deploying deep learning models in real time scenarios. The integration of autoencoders further contributes to the efficiency of IDS by streamlining data processing and feature extraction. Studies indicate that, with appropriate optimization and resource management, deep learning models and autoencoders can be effectively applied in real time intrusion detection systems, offering improved accuracy and reduced latency in identifying threats.

5 Benefits and Trade offs

5.1 Advantages of Using Deep Learning and Autoencoders in IDS from Literature

Deep learning and autoencoders offer several significant advantages in enhancing Intrusion Detection Systems (IDS):

- Enhanced Detection Accuracy: According to recent studies, deep learning algorithms, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), can achieve higher detection accuracy compared to traditional IDS methods. Their ability to learn complex patterns from large datasets enables them to identify a wider range of attack vectors, including those that are previously unknown or sophisticated.
- Improved Anomaly Detection: Autoencoders excel in identifying anomalies by learning the normal patterns of network traffic and flagging deviations as potential intrusions. This capability is particularly valuable for detecting subtle and complex attack patterns that may be missed by conventional methods.
- Automated Feature Extraction: Deep learning models and autoencoders reduce the need for manual feature engineering by automatically learning and extracting relevant features from raw data. This not only streamlines the detection process but also enhances the model's ability to adapt to new and evolving threats.
- Scalability: Research indicates that deep learning models can be scaled to handle large volumes of network traffic, making them suitable for deployment in high-speed and high-volume network environments. The integration of autoencoders can further optimize data processing and improve the efficiency of these models.
- Reduced False Positives: Deep learning-based IDS, when combined with autoencoders, often exhibit lower false positive rates. Autoencoders help in finetuning the detection process by focusing on the most relevant features and reducing noise, leading to more accurate and reliable intrusion detection.

5.2 Trade-offs and Considerations for Practical Deployment Based on Existing Research

While deep learning and autoencoders offer numerous benefits, there are also several trade-offs and considerations for their practical deployment:

- Computational Resources: Deep learning models and autoencoders can be computationally intensive, requiring significant processing power and memory. Research highlights that while advances in hardware (e.g., GPUs and TPUs) have mitigated some of these challenges, the resource requirements can still be a barrier for real time applications, especially in resource constrained environments.
- Data Requirements: Deep learning models require large labelled datasets for training, which can be challenging to obtain in the field of cybersecurity. Autoencoders, though useful for unsupervised learning, also depend on substantial amounts of data to learn effective representations of normal behaviour. This data requirement can limit the applicability of these models in scenarios where data is scarce.
- Model Interpretability: One of the significant challenges associated with deep learning models is their "black box" nature, making it difficult to interpret and understand their decision-making processes. This lack of transparency can be a concern for security professionals who need to validate and trust the system's outputs.
- False Negatives: Despite their advantages, deep learning models and autoencoders are not immune to false negatives. While these models can reduce false positive rates, they may still miss certain types of attacks, particularly those that are novel or highly sophisticated. Balancing detection accuracy with the risk of false negatives remains a critical consideration.
- Integration and Maintenance: Implementing and maintaining deep learning-based IDS can be complex and resource intensive. The integration of autoencoders into existing systems requires careful tuning and ongoing maintenance to ensure that the models remain effective as network environments and attack vectors evolve.

Overall, while deep learning and autoencoders present powerful tools for enhancing IDS, careful consideration of these trade-offs is necessary to ensure that the benefits outweigh the challenges in practical deployment scenarios.

6 Conclusion

6.1 Summary of Findings from Literature

Thus, the literature points to those traditional IDS methods, although fundamental, lack effectiveness in identifying new and sophisticated threats. Autoencoder is an added feature that makes deep learning models more efficient in the detection of equations, anomalies, and features. Most of these improvements solve the issues arising from the traditional methods but at the

same time introduce the following challenges Facing computational and model interpretability.

6.2 Contributions to the Field of Network Security from Literature

As highlighted in this review, deep learning especially the autoencoders have revolutionized the IDS solutions. Thus, these methods bring more detection capabilities and enhance the abilities of anomaly detection, which adds to the strengthening and making of the network security more efficient. Therefore, the global understanding of deep learning integrated with autoencoders revolves around future innovations and enhancing IDS.

6.3 Final Thoughts and Implications Derived from Literature

The continued evolution of IDS technologies is essential for addressing the growing complexity of cyber threats. While deep learning and autoencoders offer promising advancements, ongoing research and practical considerations are crucial for optimizing these solutions. The implications of these findings highlight the need for a balanced approach, integrating advanced techniques with practical deployment strategies to achieve effective and reliable network security.

7 REFERENCES

1. Kumar, S., Gupta, S., & Arora, S. (2021). Research trends in network-based intrusion detection systems: A review. *Ieee Access*, *9*, 157761-157779.
2. Sun, C. C., Cardenas, D. J. S., Hahn, A., & Liu, C. C. (2020). Intrusion detection for cybersecurity of smart meters. *IEEE Transactions on Smart Grid*, *12*(1), 612-622.
3. Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *Artificial Intelligence Review*, *54*(5), 3849-3886.
4. Islabudeen, M., & Kavitha Devi, M. K. (2020). A smart approach for intrusion detection and prevention system in mobile ad hoc networks against security attacks. *Wireless Personal Communications*, *112*(1), 193-224.
5. Thakkar, A., & Lohiya, R. (2022). A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions. *Artificial Intelligence Review*, *55*(1), 453-563.
6. Lee, S. W., Mohammadi, M., Rashidi, S., Rahmani, A. M., Masdari, M., & Hosseinzadeh, M. (2021). Towards secure intrusion detection systems using deep learning techniques: Comprehensive analysis and review. *Journal of Network and Computer Applications*, *187*, 103111.
7. Sicato, J. C. S., Singh, S. K., Rathore, S., & Park, J. H. (2020). A comprehensive analyses of intrusion detection system for IoT environment. *Journal of Information Processing Systems*, *16*(4), 975-990.

8. Sohi, S. M., Seifert, J. P., & Ganji, F. (2021). RNNIDS: Enhancing network intrusion detection systems through deep learning. *Computers & Security*, *102*, 102151.
9. Lansky, J., Ali, S., Mohammadi, M., Majeed, M. K., Karim, S. H. T., Rashidi, S., ... & Rahmani, A. M. (2021). Deep learning-based intrusion detection systems: a systematic review. *IEEE Access*, *9*, 101574-101599.
10. Xu, W., Jang-Jaccard, J., Singh, A., Wei, Y., & Sabrina, F. (2021). Improving performance of autoencoder-based network anomaly detection on nsl-kdd dataset. *IEEE Access*, *9*, 140136-140146.
11. Nixon, C., Sedky, M., & Hassan, M. (2020, August). Autoencoders: a low cost anomaly detection method for computer network data streams. In *Proceedings of the 2020 4th International Conference on Cloud and Big Data Computing* (pp. 58-62).
12. Azam, Z., Islam, M. M., & Huda, M. N. (2023). Comparative analysis of intrusion detection systems and machine learning based model analysis through decision tree. *IEEE Access*.
13. Mohammadpour, L., Ling, T. C., Liew, C. S., & Aryanfar, A. (2022). A survey of CNN-based network intrusion detection. *Applied Sciences*, *12*(16), 8162.
14. Zarai, R. (2020). Recurrent Neural Networks & Deep Neural Networks Based on Intrusion Detection System. *Open Access Library Journal*, *7*(03), 1.
15. Song, Y., Hyun, S., & Cheong, Y. G. (2021). Analysis of autoencoders for network intrusion detection. *Sensors*, *21*(13), 4294.
16. Qureshi, A. S., Khan, A., Shamim, N., & Durad, M. H. (2020). Intrusion detection using deep sparse auto-encoder and self-taught learning. *Neural Computing and Applications*, *32*(8), 3135-3147.
17. Sood, K., Nosouhi, M. R., Nguyen, D. D. N., Jiang, F., Chowdhury, M., & Doss, R. (2023). Intrusion detection scheme with dimensionality reduction in next generation networks. *IEEE Transactions on Information Forensics and Security*, *18*, 965-979.
18. Singh, R., Srivastava, N., & Kumar, A. (2024). Network Anomaly Detection Using Autoencoder on Various Datasets: A Comprehensive Review. *Recent Patents on Engineering*, *18*(9), 63-77.
19. Kimanzi, R., Kimanga, P., Cherori, D., & Gikunda, P. K. (2024). Deep Learning Algorithms Used in Intrusion Detection Systems--A Review. *arXiv preprint arXiv:2402.17020*.
20. Naidu, G., Zuva, T., & Sibanda, E. M. (2023, April). A review of evaluation metrics in machine learning algorithms. In *Computer Science On-line Conference* (pp. 15-25). Cham: Springer International Publishing.
21. Saranya, T., Sridevi, S., Deisy, C., Chung, T. D., & Khan, M. A. (2020). Performance analysis of machine learning algorithms in intrusion detection system: A review. *Procedia Computer Science*, *171*, 1251-1260.
22. Pratomo, B. A., Burnap, P., & Theodorakopoulos, G. (2018, June). Unsupervised approach for detecting low-rate attacks on network traffic with autoencoder. In *2018 international conference on cyber security and protection of digital services (Cyber Security)* (pp. 1-8). IEEE.
23. Mijalkovic, J., & Spognardi, A. (2022). Reducing the false negative rate in deep learning based network intrusion detection systems. *Algorithms*, *15*(8), 258.