International Journal of Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: 10.31695/IJASRE.2024.8.11

Volume 10, Issue 8
August - 2024

Subject Review: Anomaly Detection in Cyber Security Using Convolution Neural Network

Haitham Salman Chyad[1], Raniah Ali Mustafa[2], Dena Nadir George[3]

[1,2]Computer Science Department,

College of Education, Mustansiriyah University,

Baghdad, Iraq

ABSTRACT

Security concerns are multiplying as a result of the rapid advancement of computer and communications technology. Cybersecurity is evolving into different types of techniques to reduce these concerns. Amongst these techniques is anomaly detection (AD). Anomaly identification (AI) is a major problem in many academic fields and practical applications. It has been presented that Convolution Neural Networks (CNNs) be used to identify anomalies from different type; however, there is currently no guide over which model to apply in a specific instance. In this study presented the most relevant Convolution Neural Networks (CNNs) as a key solution for anomaly detection (AD) in the literature, compares between anomaly detection (AD) techniques which current in the previous studies. In addition, the pros and cons of this technique are examined in various application contexts, and their results are presented. Finally, this study offers a number of recommendations for future studies that will assist readers in their subsequent efforts in this field.

Key Words: Cyber Security, Anomaly Detection (AD), Relevant Convolution Neural Networks (CNNs), Deep learning (DL).

1. INTRODUCTION

The challenge of identifying patterns in data that deviate from expected behavior is referred as anomaly detection (AD). In various application areas, these non-conforming patterns are also referred to as anomalies, conflicting results, exceptions, outliers, surprises, deviations, oddities, or contaminants. Two of these terms that are most commonly used in the context of anomaly detection (AD) are anomalies and outliers. Anomaly detection technology (ADT) is widely used in a variety of fields, including cybersecurity intrusion detection (CSID), credit card fraud detection (CCFD), detecting fraud in healthcare and insurance, disturbance detection in safety-critical systems, and military monitoring of enemy activities. Because anomalies in data translate to meaningful (and frequently crucial) actionable information across a broad range of application fields, which makes anomaly identification crucial. An unusual traffic pattern within a computer network (CN), for instance, may indicate that a compromised machine is transmitting private information to an unauthorized location. The existence of malignant tumors may be indicated by an abnormal MRI scan. Anomalies in credit card transaction data may point to identity or credit card theft, or unusual sensor readings from a space craft may indicate a malfunction in one or more space craft components [1,2].

Using a variety of approaches and methodologies for detecting these anomalies is known as anomaly detection (AD); these approaches include statistical analysis (SA) and artificial intelligence (AI). The first difficulty of anomaly detection derives from the need to analyze numerous factors. Establishing the line that separates normal behavior and abnormal behaviors. The second is the persistent development of malevolent behavior. The variety of applications is other issue. For instance, applications involving transportation may not be suitable for the health care anomaly detection system. In cybersecurity, anomaly detection (AD) refers to the detection of patterns or actions which deviate significantly from the norm and may indicate risks or malicious activities [3,4].

1.1 Techniques of Anomaly Detection (AD) for Cybersecurity

Cybersecurity anomaly detection techniques (CSADT) come in a variety of forms, each with their own advantages and disadvantages as well as appropriate applications. Following is a comparison of a few popular techniques [5]:

- Signature-Based on Detection (S-BD):

  Brief Description: Depends on preset patterns or signs of recognized threats.
  Benefits: Efficient of identifying attacks with recognizable signatures or known malware.
  Drawbacks: Signature databases require frequent updates; inefficient against novel or unidentified threats.
- Machine Learning-Based on Detection (ML-BD):

  Brief Description: uses machine learning techniques to find patterns in typical behavior and detect anomalies.
  Benefits: The ability to recognize unexpected anomalies and adapt to changing threats.
  Drawbacks: lacks labeled training data, has the potential to generating FP (false positives), and might experience issues in highly dynamic environments.
- Behavioural Analytics (BA):

  Brief Description: looks at scheme and user activities to identify anomalies that do not match pre-defined criteria.
  Benefits: effectively in identifying suspicious activity and insider threats.
  Drawbacks: Establishing a baseline can be challenges, and FP (false positives) might occur during scheme changes or updates.
- Statistical Anomaly Detection (SAD):

  Brief Description: applied statistical models to identify deviations from predicted statistical properties.
  Benefits: efficient in identifying minute deviations without the expected patterns.
  Drawbacks: It might present FP (false positives) in dynamic environments due of its sensitivity to variations in usual behavior.
- Clustering-Based on Detection (C-BD):

  Brief Description: Comparable data points are combined to form clusters, and data points that don't fit into any cluster are referred to as anomalies.
  Benefits: Effective for identifying spatial outliers and classifying correlated anomalies.
  Drawbacks: sensitive to the use of distance measurement; problems with high-dimensional data may occur.
- Ensemble Techniques (ET):

  Brief Description: combines multiple anomaly detection (AD) strategies to increase efficiency overall.
  Benefits: Strong against specific model practical and limitations in a variety of scenarios.
  Drawbacks: A variety of models are carefully selected, which may lead to increased computational complexity.
- Deep Learning-Based on Detection (DL-BD):

  Brief Description: constructs hierarchical data representations designing use of autoencoders, a kind of DNN , for detecting anomalies.
  Benefits: The ability to effectively address complicated patterns and handle high-dimensional data effectively.
  Drawbacks: demanded a significant amount of computational capacity and might not be interpretable.
- One-Class Support Vector Machines (SVM):

  Brief Description: The training process exclusively utilizes normal data, and anomalies are defined as occurrences that depart from the normal class.
  Benefits: The scheme is capable of dealing with high-dimensional data and is efficient in scenarios with imbalanced databases.
  Drawbacks: Very sensitive to changes in the hyperparameter (HYP); perhaps unstable when there are several anomaly densities.
- Flow-Based on Detection (F-BD):

  Brief Description: The scheme finds anomalies through analyzing packet-level data and network flows.
  Benefits: Efficiency in identifying network anomalies and intrusions is critical.
  Drawbacks: Higher OSI model layers may not capture anomalies e.g. application layer attacks (LA).
- Hybrid Approaches (HA):

DOI: 10.31695/IJASRE.2024.8.11

Brief Description: The scheme integrates various anomaly detection (AD) strategies, each taking advantage of a different anomaly.
Benefits: Enhanced agility, precision, and flexibility.
Drawbacks: The setup and configuration process is complex, and might require additional processing power.

1.2 Type of Anomaly Detection Technique (ADT)

The desired anomaly characteristics are an essential component of any anomaly detection technique. Three categories can be used to classify anomalies [6,7,8]:

1. Point Anomalies (PA): A single data condition is indicating to as a point anomaly if it can be considered anomalous with respect to other data. The majority of anomaly detection research focuses on this type of anomaly because it is the most basic.
2. Contextual Anomalies (CA): A data instance is considered contextually anomalous (also known as conditionally anomalous) if it is anomalous in a certain context but not in any other.
   The structure of the data set creates the idea of a context, that should be defined as part of the problem formulation process. The two sets of attributes listed below are used to define each data instance:
   - Contextual Attributes (CA): The context (or neighborhood) for that instance is ascertained using the contextual attributes. Contextual attributes in spatial data sets include, for instance, a location's latitude and longitude. Time is a contextual attribute in time series data that identifies where an event occurs into the sequence as an entire.
   - Behavioral Attributes (BA): The non-contextual traits of an instance are specified by its behavioral attributes. For instance, the amount of rainfall at any given place is a behavioral attribute in a spatial data set that describes the global average rainfall.
3. Collective Anomalies (CA): A set of connected data examples is indicating to as a collective anomaly if they are anomalous for the entire data set. Even if individual data examples in a group anomaly may not constitute an anomaly in themselves, their existence as a group is unusual.

Anomaly detection techniques (ADT) can be divided according to learning methods as follows [9]:

- Supervised anomaly detection (SAD): Both typical and abnormal data are covered in this class. The objective is to create a prediction model that works for both normal and anomalous classes.
- Semi-supervised anomaly detection (SSAD): This type of algorithm only uses normal data for training. Anything that isn't classified in that method is known as anomaly.
- Unsupervised anomaly detection (USAD): In this case, training is not necessary. This kind of algorithm makes the assumption that normal events occur far more frequently than anomalies. But if this assumption is incorrect, the algorithm generates a lot of false positives (FP).

By using unlabeled data for training, multiple semi-supervised methods can be modified to function in an unsupervised manner. This kind of adaptation supposes which the test data contains a small number of strong anomalies.

2. CONVOLUTIONAL NEURAL NETWORK (CNN) ARCHITECTURE

Convolutional neural networks (CNN) are the best choice for deep learning (DL) implementations when it is difficult for standard neural networks to handle multi-dimensional inputs, such as images. Multiple construction components, comprise convolution layers, pooling layers, and fully connected layers, are part of the convolutional neural networks (CNN) architecture. Repetitions of a stack of multiple convolution layers (CL), a pooling layer (PL), and one or more fully connected layers follow in a typical structure. Ward propagation is the process through which input data are transformed into output through these layers as shown in figure 1. CNN architecture layers are described as follows [10-14]

1. Input Layer (IL): This layer feeds the input to the subsequent layer, which could have a single dimension or several.

DOI: 10.31695/IJASRE.2024.8.11

2. Convolution layer (CL): The convolution layer is the essential component of the convolutional neural network (CNN) design that deals with feature extraction (FE). To extract features, this layer often combines linear and nonlinear techniques such as the activation function (AF) and convolution operation.
3. Pooling layer (PL): reducing the in-plane dimensionality of the feature maps, a pooling layer offers a typical down sampling operation which can translate variance to slight shifts and distortions and the minimum number of additional learnable parameters. The filter size (FZ), stride, and padding are hyperparameters (HYP) in pooling operations, which are comparable to convolution operations, but there isn't a learnable parameter in any of the pooling layers.

Fully connected layer (FCL): The final convolution or pooling layer's output feature maps are often flattened, or converted into a one-dimensional (1D) array of numbers (or vectors), and then connected to one or more fully connected layers, sometimes referred to as dense layers, where every input and each output are connected through a learnable weight. A subset of fully connected layers maps the features provided through the convolution layers and the pooling layers' downsampled features to the final outputs of the network, which in classification tasks are probabilities for every class. The number of output nodes in the last fully connected layer is often equal to the number of classes. After every completely linked layer, a nonlinear function like ReLU comes next [15].

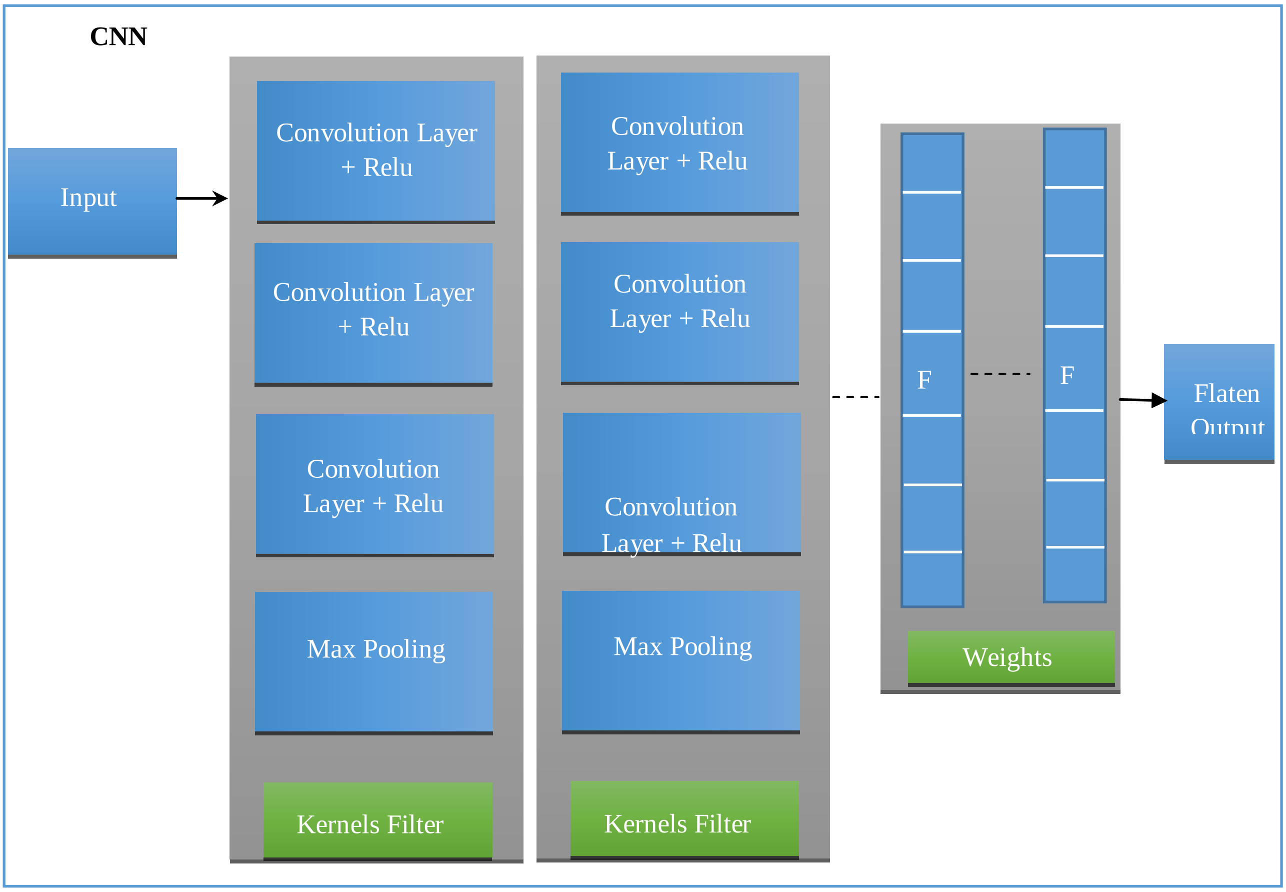

Fig. 1 Show architectural description of a convolutional neural network (CNN). [15].

3. RELATED WORKS

The current studies in the areas of deep learning (DL), machine learning (ML) techniques, and anomaly detection (AD) algorithms have covered a variety of topics related to this integration. Z. Zhao, H. Guo, and Y. Wang [16] This research paper constructs a multi-information fusion model by employing an AutoEncoder and a convolutional neural network (CNN). The model utilizes an AutoEncoder to encode the statistical features extracted from the raw traffic data and a convolutional neural network (CNN) to extraction features directly from the raw traffic data in order to make up for the information loss caused through cropping. The load information from the original traffic data and the global information of the original traffic data obtained from the statistical features are combined to form a novel integrated feature for network traffic. This feature enhances the model's capacity for detection and offers an

DOI: 10.31695/IJASRE.2024.8.11

accurate representation of the data observed in network traffic. The findings of the studies demonstrate that this model works much better to conventional machine learning (ML) techniques in terms of classification accuracy for network traffic anomaly detection (AD). I. Al-Turaiki and N. Altwaijry [17] this reference, we suggested two deep learning rely on models to deal with network attack classification, each multiclass and binary. For our models, we perform a convolutional neural network structure. Furthermore, a two-step hybrid pre-processing strategy is suggested to provide significant features. The suggested method combines deep feature synthesis feature engineering with dimensionality reduction. Two benchmark datasets are utilized to assess the performance of our models: The University of New South Wales Network depend 2015 database and the Network Security Laboratory Knowledge Discovery in databases. The results are contrasted with cutting-edge classification models and comparable deep learning techniques found in the literature. According to experimental results, our models outperform comparable models in the literature in terms of recall and accuracy (ACC). J. J. Hephzipah, et al., [18] the authors study that cybersecurity is commonly used to identify malicious activities because previous machine learning algorithms used inaccurate feature analysis to forecast outcomes. In order to address this issue, a cutting-edge cyber security solution based on flow-depend on anomaly detection (AD) employing an artificial neural network (ANN) optimized for maximum game theory (MMGT-ANN) is proposed. KDD crime dataset was used for the reprocessing. The feature margins and defect scaling rate are then tracked using a data-driven network model. Transmission based on the feature scaling rate to choose the feature limitations, the flow defect rate is calculated and applied using the Min-Max Game theory. Next, to detect the crime rate, features are trained using an optimal neural network. In comparison to the other system, the suggested system performs better in terms of precision rate, resulting in higher detection accuracy and less time complexity. Z. Hussien [19] this research developed a deep neural network (DNN) approach for non-identifiable anomaly detection (NIDS). Dropout is a regularized method for reducing overfitting in DNN models. The NSL_KDD database was subjected to the experimental outcomes. Different classifications have been applied to the suggested model, with one label being normal and four being attacks (Probe, U2L, R2L, and Dos). The SoftMax output layer has been employing in conjunction with a cross-entropy loss function. The model's performance was assessed using the accuracy metric. 99.45% accuracy was attained with the suggested model. Feature selection (FS) technique is a typical way to shorten the recognition time in NIDS. With the utilize of a feature selection (FS) strategy, the created DNN classifier achievement an accuracy of (99.27%). S. Rana [20] the authors employ three approach to assessment of Performance applying the KDD-NSL database in this research. The objective of this research is to introduce an overall examination of the diverse methods utilized in machine learning (ML) and deep learning (DL) to identify anomalies in networks. Additionally, it will further improve network security. This study evaluates the performances of three methods using the KDD-NSL database and presents the outcomes. The SVM is referred to a support Vector Machine, RF is referred to a Random Forest, and ANN is referred to an artificial Neural Network are the three methods. Accuracy, recall, and F1-score will be compared between them. The impact of feature selection on the algorithm's performance is also investigated in this study. The investigation's conclusions will be taken into consideration while developing novel methods for boosting network security. Analysing the effectiveness of different methods for identifying network anomalies is made possible by the KDD NSL dataset. A. Handa, A. Sharma, and S. K. Shukla [21] in this review, the authors provide a comprehensive study of a variety of cybersecurity domains where machine learning is used as a technique. To render such tools ineffective, we also provide a few glimpses of adversarial attacks on machine learning algorithms that alter the test and training data of classifiers. B. Sharma, L. Sharma, and C. Lal [22] the authors provide an overview of anomaly detection (AD) in internet of things (IoT) applications utilizing deep learning and machine learning techniques is given. IoT components and devices can be used to analyse both typical and abnormal behavior with the utilize of machine learning (ML) and deep learning (DL). In this paper, we summarize the main research questions and difficulties in applying deep anomaly detection approaches for devices with limited resources in real-world Internet of Things scenarios. Fog computing moves computation to the edge or device to address a few network security and latency estimation issues. A. K. Pathak, et al. [23] this article explores the problem of tampering with IoT sensors in an office environment. We gather real-world data and use machine learning to identify two types of sensor manipulation. Firstly, our isolation forest-based unsupervised machine learning algorithm for anomaly identification is trained using a real-time view of the traffic patterns. Secondly, in our unique Anomaly Detection using Machine Learning (AD-ML) system, labels are generated and the decision tree supervised approach is applied based on traffic patterns. The two suggested models' accuracy is shown. With the isolation forest's silhouette metric accuracy, we

DOI: 10.31695/IJASRE.2024.8.11

discovered (84%). Furthermore, the supervised machine learning model's decision trees produced the best classification accuracy of (91.62%) with the lowest false positive rate, according to the outcome based on ten cross-validations. A. S. Saabith, et al. [24] this article provides a comprehensive overview of machine learning algorithms for anomaly detection in cybersecurity, with a focus on malware and network intrusion detection. We review the advantages and disadvantages of many machine learning (ML) techniques and emphasize the significance of feature engineering and selection for creating efficient anomaly detection (AD) models. We also look at the estimation measures that are utilized to define how well these techniques work and offer actual instances of how they are employed. Eventually, we examine the possibility for further study and advancement in this domain, comprise combining several strategies and utilizing behavioral analysis and machine learning to increase detection accuracy. The purpose of this survey is to serve as a useful tool for machine learning (ML) and cybersecurity (CS) researchers and practitioners. M. Qasim and E. Verdu [25] in this work, an automated anomaly detection system in videos is built using a deep convolutional neural network (CNN) and a simple recurrent unit (SRU). While the SRU obtains temporal characteristics, the ResNet architecture uses the incoming video frames to extract high-level feature representations. The expressive recurrence and highly parallelized implementation capabilities of the SRU improve the accuracy of the video anomaly detection system. Three models—ResNet18 + SRU, ResNet34 + SRU, and ResNet50 + SRU—are proposed in the study to identify anomaly. The UCF-Crime dataset is utilized to analyze the proposed models. This study demonstrated that CNN + SRU could accurately classify each unexpected behavior into the appropriate group by clearly differentiating between typical and unusual activities. ResNet18 + SRU achieved (88.92%) accuracy, ResNet34 + SRU achieved (89.34%) accuracy, and ResNet50 + SRU achieved (91.24%) accuracy using the UCF-Crime dataset. Moreover, the proposed models outperformed similar deep learning models and showed significantly better performance accuracy. L. Sana, et al. [26] objective of the article is to utilize deep learning (DL) to improve intrusion and anomaly detection security (ADS) schemes for the internet of things (IoT). To find out "How to be implemented data transformation analyses of IoT database to find anomaly detection (AD) for cyber IoT attacks?," a systematic literature review (SLR) is carried out in this context. twenty-four databases were utilized to analyse the IoT, thirty-five performance metrics were utilized to evaluation the internet of things (IoT) problems, six to forty-two attributes were identified to be discoverable, forty-two pre-processing procedures were utilized to adjust the data, and twenty-two distinctive approaches and models were utilized to solve the given problem, accordingly to the SLR outcome. The SLR draws attention to additional improvements for the issue and the identification of IoT cyber-security. After a careful examination of SLR, anomaly detection (AD) could be carried out utilizing reinforcement learning (RL) deep learning (DL). V. S. Rao, et al [27] the authors propose a unique architecture of hybrid convolutional neural network (HCNN) and generative adversarial network (GAN) for network anomaly detection (AD). The hybrid approach enhancements network anomaly detection (AD) through utilizing the benefits of both (CNN and GAN). The CNN component may identify complicated patterns and relationships in network traffic data through extracting high-level attributes from the data. The GAN component performs the dual roles of generator and discriminator at the same time. It learns to produce typical network traffic patterns and discern anomalies from them. Utilizing a sizable dataset of labeled network traffic that comprise typical and abnormal behaviors, the hybrid model was trained. In order to train the CNN and improve its ability to generalize to changes in network traffic, the GAN creates synthetic normal traffic during training. This results in a varied set of normal data. When compared to conventional techniques, the hybrid CNN-GAN model performs better in studies at identifying network anomalies. Utilizing MATLAB software, it has an increased detection rate (DR) and a low number of false positives (FP), making it a promising tool for improving network security. Through utilizing AI-driven anomaly detection, the suggested techniques adds to the continuing efforts to protect critical network infrastructures from evolving cyber threats. R. B. Varugu and G. A. Kumar [28] this work explores the difficulties associated with internet of things (IoT) device authentication. It examines a variety of technologies, comprise multi-factor authentication, biometric authentication, and cryptographic protocols, and examines their drawbacks and benefits in various internet of IoT contexts. In-depth analysis of anomaly detection strategies in internet of things (IoT) environments is provided in this research, which emphasizes the value of machine learning (ML) algorithms e.g. supervised, unsupervised, and semi-supervised approaches in identifying anomalous behavior patterns and possible security risks. This work describes the growing trends, unresolved issues, and potential future research directions in this important area of IoT device authentication and anomaly detection (AD). It also thoroughly covers the theoretical underpinnings and technical specifics of these

DOI: 10.31695/IJASRE.2024.8.11

topics. R. Alhajri, R. Zagrouba, and F. Al-Haidari [29] the primary focus of the research is machine learning techniques to identify security risks related to the IoT. It looks into whether auto-encoders can be utilized to identify Internet of Things botnets. Because no single technique has shown the ability to effectively counteract this security danger, botnets can generate DDoS attacks and pose a serious security risk in IoT networks. These techniques frequently fall short of IoT environment requirements, including those related to energy and processing power. One option for detecting botnets is to use auto-encoders. The potential that auto-encoders offer for identifying IoT botnets must be investigated in future studies.

4. COMPARATIVE ANALYSIS FOR ANOMALY DETECTION (AD)

In the Table 1 provides a summarization of all the above explained related works for anomaly detection techniques.

Table 1: A comparison between previous anomaly detection techniques (ADT).

Ref.	Year	Scope of Use	Summary of the review
Z. Zhao, et al.,	2024	Convolutional Neural Network (CNN) + Auto Encoder (AE)	-Improve anomaly detection (AD) performance in network traffic -The information classification and identification capabilities of CNN are taken into account to determine the effect of f obtaining multiple information source detection. -The Auto Encoder (AE)features for feature extraction (FE) and data reconstruction.
I. Al-Turaiki and N. Altwaijry	2021	Deep Learning (DL)+ Network Attacks (NA)	Introduce a two-step hybrid preprocessing method that uses deep feature synthesis (DFS) to combine feature engineering and dimensionality reduction. Suggest new binary classification ADNIDS based on DNNs offers a comprehensive architecture comparison about ADNIDS
J. J. Hephzipah et al.,	2023	Artificial Neural Network (Ann)	-Introduce a novel approach to cyber security that uses an Optimal Min-Max Game Theory Artificial Neural Network (MMGT-ANN) for flow-based anomaly detection. -Cybersecurity (CS) assists in avoiding data loss, personal loss, privacy loss, financial loss, and computer outages through enhancing integrity, confidentiality, reliability, and authentication.
Z. Hussien	2020	Deep Neural Network (Dnn)	Proposed a novel deep neural network (DNN) method for NIDS anomaly detection (AD).
S. Rana	2019	Machine Learning (Ml) + Deep Learning (Dl)	Analysis of the various techniques Support Vector Machine (SVM), the Random Forest (RF), and the Artificial Neural Network (ANN)
A. Handa, A. Sharma, and S. K. Shukla	2019	Machine Learning (Ml)	Describe the various applications of machine learning (ML) in cyber security (CS).
B. Sharma, L. Sharma, and C. Lal	2019	Machine Learning (Ml) + Deep Learning (Dl)	highlight the main research questions and difficulties with deep anomaly detection (AD) methods for devices with limited resources in real-world Internet of Things scenarios.
A. K. Pathak, et al.,	2021	Machine Learning (ML) + Internet Of Things (Iot)	Using unsupervised learning techniques (isolation forest) and supervised learning algorithms (decision trees) to detect sensor tampering depend on network traffic patterns.
A. S. Saabith, et al.,	2023	Machine Learning (Ml)	Analyses different machine learning techniques utilized in cybersecurity to detect anomalies
M. Qasim and E. Verdu	2023	Deep Convolutional Neural Network (CNN)	Suggested a simple recurrent unit (SRU) system and a deep convolutional neural network (CNN) for anomaly detection (AD) in videos. The proposed method uses Transfer Learning technique to avoid label distortion issues, and CNN+SRU is pre-trained utlizing 1000 sets of images from the ImageNet dataset.
L. Sana, et al.,	2022	Cyber Iot Attacks	Using Deep Learning (DL) to Enhance Intrusion and Anomaly Detection (AD) Security Systems for the Internet of Things (IoT).

DOI: 10.31695/IJASRE.2024.8.11

V. S. Rao, et al.,	2024	Convolutional Neural Network (CNN) + Generative Adversarial Network (GAN) architecture	Introduce a unique techniques for detecting network anomalies that makes use of a hybrid architecture of a generative adversarial network (GAN) and convolutional neural network (CNN).
R. B. Varugu and G. A. Kumar	2023	Machine Learning (ML) + Internet of Things (IoT)	Highlighting the significance of algorithms for machine learning (ML) Investigates strategies for anomaly detection (AD) in IoT environments.
R. Alhajri, R. Zagrouba, and F. Al-Haidari	2019	Internet of Things (IoT)	Discussing machine learning (ML) techniques for detecting IoT security threats.

Table 2 indicates the aspects that this review has identified as requiring further attention in the future.

Table 2: Summary of future work

Ref.	Future Work
I. Al-Turaiki and N. Altwaijry	- Planned to combine our classifiers' output into an ensemble to enhance predictions. - The classification result can be generated in a single step by combining the neural networks (NN) in a variety of methods.
S. Rana	Focus on creating more efficient algorithms than those currently in existence. Additionally, efforts should be made to create models that can adjust to cyberthreats (CT).
A. K. Pathak, et al.,	Develop a real-time online system by collecting more data from various IoT sensor types and employing additional unsupervised based machine learning (ML) algorithms.
A. S. Saabith, et al.,	- Focusing on creating novel algorithms that can manage diverse and complicated data, as well as improving the robustness and interpretability of machine learning (ML) models for CPS security.
M. Qasim and E. Verdu	Attention more intently on the anomaly events that occur in a video. Since silent videos are typically the only ones accessible, they can be utilized to identify anomalies in audio signals. Thus, we can increase the effectiveness of video surveillance through utilizing audio signal synthesis.
L. Sana, et al.,	The specific model of cyber IoT can be deeply analyzed.
V. S. Rao, et al.,	Using real-time information streams and building defenses against zero-day attacks are two ways to enhance the hybrid approach. Furthermore, efforts should be taken to deploy and integrate this technology into operational networks in order to guarantee its scalability and usability.
R. B. Varugu and G. A. Kumar	- By using machine learning and a holistic approach to IoT security, stakeholders can build robust and reliable IoT systems that drive innovation and raise consumer standards around the world.
R. Alhajri, R. Zagrouba, and F. Al-Haidari	- Representation of the security specification set for a robot detection system and the combination of required attributes for an autoencoder (AE). By modeling these criteria, a framework for creating efficient detection systems that counter the security threat posed through IoT botnets can be developed.

5. CONCLUSION

The study focuses on recent years and provides state-of-the-art tools with convolutional neural network (CNN) as the basis for anomaly detection techniques in the field of cybersecurity. The main goal is find best deep learning (DL), machine learning (ML) techniques for anomaly detection (AD). In this study also, we highlight most of the algorithms for anomaly detection (AD). Although every technology has benefits as well as drawbacks, new technologies have been developed. Finally, this study suggests that in the future, comprehensive studies will develop more efficient algorithms and high-precision systems as well as develop a real-time system.

REFERENCES

[1] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM computing surveys (CSUR)*, vol. 41, no. 3, pp. 1-58, 2009.

[2] V. Kumar, "Parallel and distributed computing for cybersecurity," *IEEE Distributed Systems Online*, vol. 6, no. 10, 2005.

[3] R. Fujimaki, T. Yairi, and K. Machida, "An approach to spacecraft anomaly detection problem using kernel feature space," in *Proceedings of the eleventh ACM SIGKDD international conference on Knowledge discovery in data mining*, 2005, pp. 401-410.

[4] X. Song, M. Wu, C. Jermaine, and S. Ranka, "Conditional anomaly detection," *IEEE Transactions on knowledge and Data Engineering*, vol. 19, no. 5, pp. 631-645, 2007.

[5] S. Tatineni, "A Comprehensive Overview of DevOps and Its Operational Strategies," *International Journal of Information Technology and Management Information Systems (IJITMIS)*, vol. 12, no. 1, pp. 15-32, 2021.

[6] N. Görnitz, M. Kloft, K. Rieck, and U. Brefeld, "Toward supervised anomaly detection," *Journal of Artificial Intelligence Research*, vol. 46, pp. 235-262, 2013.

[7] O. Chapelle, B. Scholkopf, and A. Zien, "Semi-supervised learning (chapelle, o. et al., eds.; 2006)[book reviews]," *IEEE Transactions on Neural Networks*, vol. 20, no. 3, pp. 542-542, 2009.

[8] T. Schlegl, P. Seeböck, S. M. Waldstein, U. Schmidt-Erfurth, and G. Langs, "Unsupervised anomaly detection with generative adversarial networks to guide marker discovery," in *International conference on information processing in medical imaging*, 2017, pp. 146-157: Springer.

[9] J. E. de Albuquerque Filho, L. C. Brandão, B. J. T. Fernandes, and A. M. Maciel, "A review of neural networks for anomaly detection," *IEEE Access*, vol. 10, pp. 112342-112367, 2022.

[10] M. Vakalopoulou, S. Christodoulidis, N. Burgos, O. Colliot, and V. Lepetit, "Deep learning: basics and convolutional neural networks (CNNs)," *Machine Learning for Brain Disorders*, pp. 77-115, 2023.

[11] F. Rofii, G. Priyandoko, and M. I. Fanani, "Modeling of Convolutional Neural Networks for Detection and Classification of Three Vehicle Classes," in *Journal of Physics: Conference Series*, 2021, vol. 1908, no. 1, p. 012018: IOP Publishing.

[12] N. Bačanin Džakula, "Convolutional neural network layers and architectures," in *Sinteza 2019-International Scientific Conference on Information Technology and Data Related Research*, 2019, pp. 445-451: Singidunum University.

[13] J. Mendoza-Bernal, A. González-Vidal, and A. F. Skarmeta, "A Convolutional Neural Network approach for image-based anomaly detection in smart agriculture," *Expert Systems with Applications*, vol. 247, p. 123210, 2024.

[14] R. Chalapathy and S. Chawla, "Deep learning for anomaly detection: A survey," *arXiv preprint arXiv:1901.03407*, 2019.

[15] R. Yamashita, M. Nishio, R. K. G. Do, and K. Togashi, "Convolutional neural networks: an overview and application in radiology," *Insights into imaging*, vol. 9, pp. 611-629, 2018.

[16] Z. Zhao, H. Guo, and Y. Wang, "A multi-information fusion anomaly detection model based on convolutional neural networks and AutoEncoder," *Scientific Reports*, vol. 14, no. 1, p. 16147, 2024.

[17] I. Al-Turaiki and N. Altwaijry, "A convolutional neural network for improved anomaly-based network intrusion detection," *Big Data*, vol. 9, no. 3, pp. 233-252, 2021.

[18] J. J. Hephzipah, R. R. Vallem, M. S. Sheela, and G. Dhanalakshmi, "An efficient cyber security system based on flow-based anomaly detection using Artificial neural network," *Mesopotamian Journal of Cybersecurity*, vol. 2023, pp. 48-56, 2023.

[19] Z. Hussien, "Anomaly detection approach based on deep neural network and dropout," *Baghdad Science Journal*, vol. 17, no. 2 (SI), pp. 0701-0701, 2020.

[20] S. Rana, "Anomaly Detection in Network Traffic using Machine Learning and Deep Learning Techniques," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 10, no. 2, pp. 1063-1067, 2019.

[21] A. Handa, A. Sharma, and S. K. Shukla, "Machine learning in cybersecurity: A review," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 9, no. 4, p. e1306, 2019.

DOI: 10.31695/IJASRE.2024.8.11

[22] B. Sharma, L. Sharma, and C. Lal, "Anomaly detection techniques using deep learning in IoT: a survey," in *2019 International conference on computational intelligence and knowledge economy (ICCIKE)*, 2019, pp. 146-149: IEEE.

[23] A. K. Pathak, S. Saguna, K. Mitra, and C. Åhlund, "Anomaly detection using machine learning to discover sensor tampering in IoT systems," in *ICC 2021-IEEE International Conference on Communications*, 2021, pp. 1-6: IEEE.

[24] A. S. Saabith, T. Vinothraj, M. Fareez, and M. Marzook, "A survey of machine learning techniques for anomaly detection in cybersecurity."

[25] M. Qasim and E. Verdu, "Video anomaly detection system using deep convolutional and recurrent models," *Results in Engineering*, vol. 18, p. 101026, 2023.

[26] L. Sana, M. M. Nazir, M. Iqbal, L. Hussain, and A. Ali, "Anomaly Detection for Cyber Internet of Things Attacks: A Systematic Review," *Applied Artificial Intelligence*, vol. 36, no. 1, p. 2137639, 2022.

[27] V. S. Rao, R. Balakrishna, Y. A. B. El-Ebiary, P. Thapar, K. A. Saravanan, and S. R. Godla, "AI Driven Anomaly Detection in Network Traffic Using Hybrid CNN-GAN," *Journal of Advances in Information Technology*, vol. 15, no. 7, 2024.

[28] R. B. Varugu and G. A. Kumar, "A Survey on IoT Device Authentication and Anomaly Detection for Cyber Security using Machine Learning," *Available at SSRN 4798899*, 2023.

[29] R. Alhajri, R. Zagrouba, and F. Al-Haidari, "Survey for anomaly detection of IoT botnets using machine learning auto-encoders," *Int. J. Appl. Eng. Res*, vol. 14, no. 10, pp. 2417-2421, 2019.

dr.haitham@uomustansiriyah.edu.iq
rania83computer@uomustansiriyah.edu.iq
dena.my@uomustansiriyah.edu.iq

DOI: 10.31695/IJASRE.2024.8.11