*technologies*

MDPI

*Article*

# Deep Learning Techniques for Web-Based Attack Detection in Industry 5.0: A Novel Approach

**Abdu Salam [1], Faizan Ullah [2], Farhan Amin [3,*] and Mohammad Abrar [4]**

[1] Department of Computer Science, Abdul Wali Khan University, Mardan 23200, Pakistan; abdusalam@awkum.edu.pk
[2] Department of Computer Science, Bacha Khan University, Charsadda 24420, Pakistan; faizanullah@bkuc.edu.pk
[3] Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, Republic of Korea
[4] Faculty of Computer Studies, Arab Open University, P.O. Box 1596, Muscat 130, Oman; abrar.m@aou.edu.om
* Correspondence: farhanamin10@hotmail or farhan@ynu.ac.kr

**Abstract:** As the manufacturing industry advances towards Industry 5.0, which heavily integrates advanced technologies such as cyber-physical systems, artificial intelligence, and the Internet of Things (IoT), the potential for web-based attacks increases. Cybersecurity concerns remain a crucial challenge for Industry 5.0 environments, where cyber-attacks can cause devastating consequences, including production downtime, data breaches, and even physical harm. To address this challenge, this research proposes an innovative deep-learning methodology for detecting web-based attacks in Industry 5.0. Convolutional neural networks (CNNs), recurrent neural networks (RNNs), and transformer models are examples of deep learning techniques that are investigated in this study for their potential to effectively classify attacks and identify anomalous behavior. The proposed transformer-based system outperforms traditional machine learning methods and existing deep learning approaches in terms of accuracy, precision, and recall, demonstrating the effectiveness of deep learning for intrusion detection in Industry 5.0. The study's findings showcased the superiority of the proposed transformer-based system, outperforming previous approaches in accuracy, precision, and recall. This highlights the significant contribution of deep learning in addressing cybersecurity challenges in Industry 5.0 environments. This study contributes to advancing cybersecurity in Industry 5.0, ensuring the protection of critical infrastructure and sensitive data.

**Keywords:** cyber-physical systems; CNN; Industry 5.0; transformer models; web-based attacks



**Citation:** Salam, A.; Ullah, F.; Amin, F.; Abrar, M. Deep Learning Techniques for Web-Based Attack Detection in Industry 5.0: A Novel Approach. *Technologies* **2023**, *11*, 107. https://doi.org/10.3390/technologies11040107

Academic Editors: Mohammed Mahmoud and Lipo Wang

Received: 21 May 2023
Revised: 25 June 2023
Accepted: 7 August 2023
Published: 8 August 2023



## 1. Introduction

Industry 5.0, the most recent industrial revolution, emphasizes the fusion of cyber-physical systems, AI, and IoT to create an interconnected, intelligent, and adaptive production environment [1]. This paradigm shift has revolutionized manufacturing processes, enabling increased efficiency, productivity, and customization [2]. It also facilitates the optimization of resources, i.e., energy efficiency, and reduced waste [3]. As a result, Industry 5.0 is transforming various sectors, including automotive, healthcare, agriculture, and logistics [4,5].

However, the growing interconnectedness and complexity of Industry 5.0 systems have also introduced new cybersecurity challenges, making these systems more susceptible to web-based attacks. Industry 5.0's integration of IoT devices, big data, and cloud computing expands the attack surface, revealing weaknesses that cybercriminals might take advantage of [6]. Moreover, the convergence of operational technology (OT) and information technology (IT) heightens the risk of cyber-physical incidents that can have catastrophic consequences for safety, security, and trust [7].

Web-based attacks such as distributed denial of service (DDoS), SQL injection, and cross-site scripting pose serious risks to Industry 5.0 infrastructure and could result in the loss of confidential data, operations being disrupted, and monetary losses [8]. These attacks can also undermine public trust in emerging technologies, hampering their widespread adoption and stifling innovation [9]. To protect the assets and ensure the resilience of Industry 5.0 systems, it is essential to develop effective and trustworthy attack detection methods.

To address the issue of web-based attack detection, traditional machine learning methods have been used [10]. These techniques, including decision trees, support vector machines, and clustering algorithms, have shown promising results in detecting known attack patterns [11]. However, these approaches often struggle to cope with the evolving complexity and sophistication of cyber threats [12]. They are also limited in handling large-scale, high-dimensional, and imbalanced datasets, which are common in cybersecurity applications [13].

Deep learning techniques, which have shown remarkable success in a variety of domains such as image recognition, natural language processing, and speech recognition, offer promising alternatives for improving cybersecurity in Industry 5.0 [14]. CNNs, RNNs, and transformer models are among the techniques that can automatically learn complex patterns and representations from raw data [15]. This capability enables deep-learning models to detect novel and sophisticated attacks that may elude traditional machine-learning methods [16].

Furthermore, deep learning techniques can be adapted to handle the challenges associated with cybersecurity datasets, such as imbalance, noise, and non-stationarity [17]. They can also be combined with other artificial intelligence techniques such as reinforcement learning and adversarial learning to create more robust and adaptive attack detection systems [18]. Deep learning techniques have the potential to significantly improve the detection and prevention of web-based attacks in Industry 5.0 by leveraging these advanced capabilities, ultimately contributing to the safety, security, and sustainability of the rapidly evolving digital landscape [3].

Furthermore, in Industry 5.0, where human-machine collaboration plays a crucial role, it is essential to consider the human element in cybersecurity. Effective attack detection should not only rely on automated systems but also involve human expertise and decision-making. Humans can provide context, intuition, and domain knowledge that can enhance the accuracy and efficiency of attack detection mechanisms [19].

Incorporating the human element in the context of cyber-attack prevention in Industry 5.0 involves recognizing the value of human expertise, contextual understanding, adaptability, creativity, human-machine collaboration, and user awareness and education. Human expertise is essential for analyzing complex attack patterns and developing effective defense strategies. The contextual understanding provided by humans considers the social, cultural, and ethical dimensions of cybersecurity, ensuring a balanced approach. Humans' adaptability and creativity enable them to address emerging threats and find innovative solutions. Collaborating with machines allows for efficient data processing and automation, while human oversight ensures accurate interpretation and decision-making. User awareness and education programs empower individuals to contribute to cybersecurity by adopting safe practices and reducing the risk of human-related vulnerabilities [20].

Overall, integrating the human element in Industry 5.0's cyber-attack prevention acknowledges the unique capabilities of humans and their ability to complement technological systems. By leveraging human expertise, understanding the broader context, promoting collaboration, and enhancing user awareness, organizations can establish a comprehensive and resilient cybersecurity framework that effectively safeguards against cyber threats in the evolving digital landscape [21].

In the context of cyber-attack prevention in Industry 5.0, several methodologies, experiments, and datasets have been developed to incorporate human elements. These

efforts aim to leverage human expertise, behavior, and interactions to enhance cybersecurity measures such as user behavior analytics and human centric cyber security datasets [22].

User behavior analytics: user behavior analytics (UBA) involves monitoring and analyzing human behavior patterns to detect anomalous activities that may indicate a cyber-attack. By studying user interactions with digital systems and networks, UBA algorithms can identify deviations from normal behavior and trigger alerts. Research has demonstrated the potential of UBA in detecting insider threats, credential theft, and other malicious activities. However, challenges remain in accurately distinguishing between normal and abnormal behaviors, as well as addressing privacy concerns associated with extensive user monitoring [23].

Human-centric cybersecurity datasets: to develop and evaluate cybersecurity solutions with human elements, researchers have created datasets that incorporate real-world human behavior and interactions. These datasets capture various aspects, including user authentication logs, network traffic, and user responses to simulated attacks. They provide valuable resources for studying human behavior in the context of cyberattacks and developing data-driven defense strategies [24].

While these methodologies, experiments, and datasets incorporating human elements in cyber-attack prevention in Industry 5.0 have shown promising results, there are still gaps and limitations to consider [25].

Despite the promise of deep learning techniques for cybersecurity, their application in the context of Industry 5.0 remains relatively unexplored. Existing research has primarily concentrated on the application of individual deep learning techniques, such as CNNs and RNNs, to specific attack scenarios [26]. However, in Industry 5.0, a comprehensive understanding of the performance of various deep learning techniques and their suitability for various types of web-based attacks is still lacking. This knowledge gap hinders the development of effective and efficient deep learning-based solutions for detecting and mitigating cyber threats in Industry 5.0 environments [27].

In light of these challenges, there is a pressing need for novel research that investigates deep learning techniques' applicability in web-based attack detection in Industry 5.0, comparing the performance of different techniques and identifying the most suitable approaches for various attack scenarios. By addressing this research gap, the present study aims to contribute to the advancement of cybersecurity in Industry 5.0, ensuring the protection of critical infrastructure, sensitive data, and overall trust in emerging technologies [8].

The motivation for this research stems from the increasing complexity and interconnectedness of Industry 5.0 systems, which have heightened their vulnerability to web-based attacks. Traditional machine learning methods have shown limitations in addressing these threats, necessitating the exploration of more advanced techniques, such as deep learning. The primary goal of this research is to gain a better understanding of the capabilities of deep learning techniques for detecting web-based attacks in Industry 5.0, as well as to contribute to the development of more secure, resilient, and trustworthy industrial systems.

Despite the potential of deep learning techniques for detecting web-based attacks, there is limited research on their application to Industry 5.0 environments. Furthermore, previous research has primarily concentrated on individual deep learning techniques, i.e., CNNs or RNNs, without considering the full range of possibilities or their performance in comparison with one another [26].

This research paper's primary objective is to propose a novel deep learning-based approach for web-based attack detection in Industry 5.0 by comparing the performance of CNNs, RNNs, and transformer models. This study aims to:

- Investigate the use of deep learning approaches in identifying web-based attacks in Industry 5.0 scenarios.
- Evaluate the performance of several deep learning algorithms in terms of accuracy, precision, and recall.
- In Industry 5.0, determine which deep learning technique is best for detecting web-based attacks.

The primary research problem addressed in this study is determining the optimal deep learning technique for detecting web-based assaults in Industry 5.0. Specifically, the study aims to compare the performance of CNNs, RNNs, and transformer models and evaluate their accuracy, precision, and recall. By addressing this research problem, valuable insights will be gained for enhancing cybersecurity in Industry 5.0 systems. The rest of the paper is organized into four sections. Section 2 provides a literature review on Industry 5.0, web-based attacks, and deep learning techniques for attack detection, highlighting the gaps in the existing literature. Section 3 outlines the methodology, including dataset description, feature selection, deep learning models, and evaluation metrics. Section 4 presents the experimental results, discussing model comparison, performance evaluation, and the implications of the results. Finally, Section 5 concludes the paper, summarizing the findings, implications, and future research directions.

## 2. Related Work

Industry 5.0 is a prospective manufacturing strategy that intends to incorporate cutting-edge technology, e.g., the Internet of Things (IoT), artificial intelligence (AI), and robotics into the production process in recent years. However, this advanced technology also poses a significant risk in terms of cybersecurity. In this section, we explore the challenges of Industry 5.0 and its potential vulnerabilities to cyber-attacks.

### *2.1. Industry 5.0 and Cybersecurity Challenges*

Industry 5.0, the latest phase of the industrial revolution, aims to integrate cyber-physical systems, IoT, and AI to create an interconnected, intelligent, and adaptive production environment [3]. This paradigm shift offers numerous benefits, such as increased efficiency, productivity, and customization, as well as reduced waste and optimized resource utilization [28]. Industry 5.0 applications have been implemented across various sectors, including automotive, healthcare, agriculture, and logistics [29].

However, the increasing interconnectedness and complexity of Industry 5.0 systems introduce new cybersecurity challenges [6]. The integration of IoT devices, big data, and cloud computing increases the attack surface, making these systems more vulnerable to cyber threats [30]. Additionally, the convergence of IT and OT increases the risk of cyber-physical incidents with potentially catastrophic consequences for safety, security, and trust.

Leng et al. [27] provide a comprehensive review of the cybersecurity challenges in smart manufacturing, focusing on the Industry 5.0 perspective. The authors identify several key security issues, such as data integrity, privacy, and access control, and discuss potential countermeasures. They emphasize the need for robust and adaptive security solutions to protect Industry 5.0 systems from various threats, including web-based attacks [31]. The summary of the literature on Industry 5.0 and cybersecurity challenges is shown in Table 1. For instance, in the automotive industry, Industry 5.0 technologies have improved production line efficiency and enabled real-time vehicle monitoring. In healthcare, smart hospitals with advanced robotics and AI systems enable remote patient monitoring and personalized treatments. Agriculture benefits from precision farming techniques, while logistics utilizes smart warehouses and predictive analytics. These examples illustrate how Industry 5.0 is transforming industries and showcase its potential impact.

**Table 1.** Summary of the literature on Industry 5.0 and cybersecurity challenges.

| Reference | Study Focus | Key Findings |
| --- | --- | --- |
| Nahavandi et al. [3] | Overview of Industry 5.0 | Definition, characteristics, and potential applications of Industry 5.0 |
| Østergaardet al. [32] | Benefits of Industry 5.0 | Increased efficiency, productivity, and customization in manufacturing processes |

**Table 1.** *Cont.*

| Reference | Study Focus | Key Findings |
| --- | --- | --- |
| Huang et al. [6] | Security challenges in Industry 5.0 | Identification of key security issues and potential countermeasures for smart manufacturing |
| Roman et al. [30] | Features and challenges of IoT Security | Discussion of the increased attack surface and vulnerability of Industry 5.0 systems due to IoT integration |

### *2.2. Web-Based Attacks and Their Impact on Industry 5.0*

Web-based attacks pose significant threats to Industry 5.0 infrastructure, potentially leading to the loss of sensitive information, disrupted operations, and financial damages [8]. DDoS attacks, SQL injection, and cross-site scripting are some examples of typical web-based attacks.

GÜVEN et al. [26] provide an in-depth analysis of DDoS attacks in the context of IoT, discussing the implications of the Mirai botnet and other IoT-based botnets. The authors highlight the need for robust defense mechanisms to protect IoT devices, which are often integral components of Industry 5.0 systems, from being compromised and used in DDoS attacks.

Liu et al. [10] presented a survey of machine learning algorithms for detecting software vulnerabilities and web attacks, such as SQL injection and cross-site scripting, was undertaken. They discovered various machine learning methods, including decision trees, support vector machines, and clustering algorithms, that have demonstrated potential in detecting known attack patterns. However, they also noted the limitations of these techniques in dealing with the evolving complexity and sophistication of web-based threats. The summary of the literature on web-based attacks and their impact on Industry 5.0 is shown in Table 2.

**Table 2.** Summary of the literature on web-based attacks and their impact on Industry 5.0.

| Reference | Study Focus | Key Findings |
| --- | --- | --- |
| GÜVEN et al. [26] | DDoS attacks in IoT | In-depth analysis of IoT-based botnets and the need for robust defense mechanisms against DDoS attacks |
| Dogman et al. [8] | Security in AI-enabled IoT systems | Discussion of the potential consequences of web-based attacks on Industry 5.0 infrastructure |
| Liu et al. [10] | Machine learning for web attack detection | Survey of machine learning techniques applied to software vulnerability detection and web attacks |

### *2.3. Deep Learning Techniques for Attack Detection*

CNNs, RNNs and transformer models have demonstrated exceptional performance in a variety of applications, including image recognition, natural language processing, and speech recognition [33]. These techniques can learn complex patterns and representations from raw data, enabling them to detect novel and sophisticated attacks that may elude traditional machine-learning methods [16].

Yin et al. [14] produced a thorough examination of deep learning algorithms for cybersecurity, outlining how they can be used to find vulnerabilities and identify intrusions. They identified several deep learning architectures and techniques that have demonstrated promising results in detecting cyber threats, such as CNNs for network traffic analysis

and RNNs for sequential data analysis. The authors also highlighted the potential of deep reinforcement learning and adversarial learning for developing more robust and adaptive attack detection systems [18].

Salih et al. [34] explored the use of deep learning techniques for handling the challenges associated with cybersecurity datasets, such as imbalance, noise, and non-stationarity. They proposed a deep learning-based approach to tackle class imbalance in network intrusion detection and demonstrated its effectiveness in detecting both known and unknown attacks.

Vinayakumar et al. [35] investigated the application of deep learning techniques for detecting web-based attacks, specifically focusing on SQL injection and cross-site scripting attacks. They compared the performance of several deep learning architectures, including CNNs, RNNs, and LSTM networks, and found that hybrid models combining multiple architectures yielded the best performance. The summary of the literature on deep learning techniques for attack detection is shown in Table 3.

**Table 3.** Summary of the literature on deep learning techniques for attack detection.

| Reference | Study Focus | Key Findings |
| --- | --- | --- |
| Yin et al. [14] | A comprehensive survey on deep learning for cybersecurity | Review of deep learning techniques and their applications in intrusion detection, malware analysis, and vulnerability discovery |
| LeCun et al. [33] | Deep learning overview | Discussion of the success and potential of deep learning techniques in various domains |
| Vaswani et al. [16] | Attention Mechanisms in deep learning | Introduction of the transformer model and its potential for enhancing cybersecurity |
| Salih et al. [34] | Data preprocessing in deep learning for cybersecurity | Exploration of deep learning techniques for handling challenges associated with cybersecurity datasets |
| Vinayakumar et al. [35] | Deep learning for detecting web-based attacks | Comparison of deep learning architectures for detecting SQL injection and cross-site scripting attacks |

### *2.4. Research Gaps and Benefits of Quantum Models*

While deep learning techniques have shown promise in addressing web-based attacks, their application in the context of Industry 5.0 remains relatively unexplored. Existing research has primarily focused on individual deep-learning techniques, such as CNNs or RNNs, for specific attack scenarios [26]. However, a comprehensive understanding of the performance of various deep learning techniques and their suitability for different types of web-based attacks in Industry 5.0 is still lacking.

Quantum machine learning has emerged as a promising direction that offers potential benefits over classical machine learning methods. It has demonstrated quantum advantages in various tasks and domains. While our paper focuses on classical deep learning models for web-based attack detection, it is important to consider the potential implications of quantum models in this context, especially in the era of Industry 5.0. Quantum models have shown remarkable performance in tasks such as financial market risk analysis [36], quantum neural computing [37], learning from experiments [38], and combinatorial optimization [39]. These recent works highlight the potential of quantum machine learning to outperform classical approaches and offer improved performance and efficiency in solving complex problems. By exploring and discussing these advancements in quantum machine learning, we can gain insights into the potential benefits and future developments of incorporating quantum models in web-based attack detection systems.

Furthermore, there is a need for more research on the integration of deep learning techniques with other AI methods, such as reinforcement learning and adversarial learning,

to develop more robust and adaptive attack detection systems [18]. Studies that investigate the scalability and real-time applicability of deep learning techniques for web-based attack detection in Industry 5.0 are also limited. Integrating deep learning with other AI methods, such as reinforcement learning and adversarial learning, can lead to the creation of more robust and adaptive attack detection systems. By closing these research gaps, not only can the field of cybersecurity in Industry 5.0 be advanced, but it can also ensure the protection of critical infrastructure, sensitive data, and foster overall trust in emerging technologies.

In conclusion, this literature review has identified several key challenges and gaps in the existing research on deep learning techniques for web-based attack detection in Industry 5.0. Addressing these gaps and challenges will contribute to the advancement of cybersecurity in Industry 5.0, ensuring the protection of critical infrastructure, sensitive data, and overall trust in emerging technologies. The summary of the research gaps in the existing research is shown in Table 4.

**Table 4.** Summary of the research gaps in the existing research.

| Reference | Study Focus | Key Findings |
|---|---|---|
| Popoola et al. [18] | Deep learning for attack detection in IoT networks | Discussion of the potential of deep reinforcement learning and adversarial learning for developing robust attack detection systems |
| leng et al. [27] | Security challenges in Industry 5.0 | Emphasis on the need for robust and adaptive security solutions to protect Industry 5.0 systems from web-based attacks |

## 3. Methodology

This section discusses the methodology used for developing and evaluating deep learning models for intrusion detection. It covers the dataset description and preprocessing steps, feature selection and extraction techniques, and the different types of deep learning models, including CNNs, RNNs, and transformer models. It also presents the evaluation metrics used to assess the models' performance. An overview of the proposed methodology is presented in Figure 1.

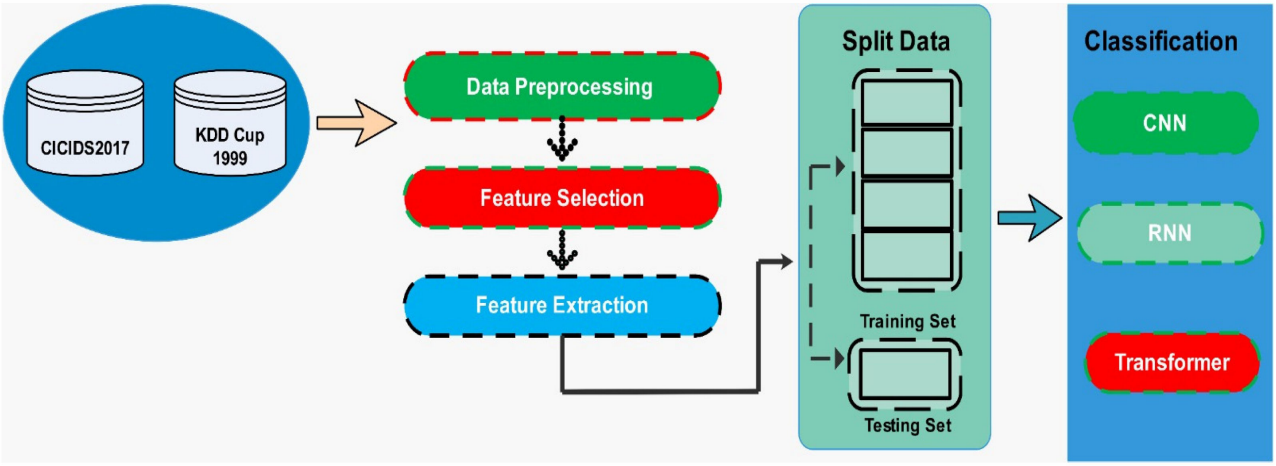


**Figure 1.** Proposed deep learning methodology for web-based attack detection.

### *3.1. Datasets and Pre-Processing*

The dataset used in this research is a combination of the KDD Cup 1999 dataset [40] and the more recent CICIDS2017 dataset [41], which provide a comprehensive collection of various web-based attacks, including DDoS, SQL injection, and cross-site scripting

attacks. Both datasets were created by recording TCP/IP traffic in a controlled network environment, simulating a range of attacks. A detailed description is given in Table 5.

**Table 5.** Description of datasets.

| Dataset | No. of Instances | Attack Types |
| --- | --- | --- |
| KDD Cup 1999 | 5 million | DoS, R2L, U2R, probe |
| CICIDS2017 | 2.8 million | Brute force, web attack, infiltration, botnet, DDoS |

The KDD Cup 1999 dataset comprises approximately 5 million connection records, where each connection is described by 41 features and labeled as either 'normal' or an 'attack', with the latter further categorized into four major types: denial of service (DoS), remote to local (R2L), user to root (U2R), and probe.

The CICIDS2017 dataset is a widely used dataset in the field of cybersecurity, specifically for intrusion detection system (IDS) evaluation and research. It consists of about 2.8 million instances, each described by 79 features. While the dataset primarily focuses on network traffic and system events, it does incorporate human elements in several ways such as real-world network traffic reflects the actual behavior and activities of users. Diversification in the attack scenarios represents the human element in terms of attackers' motivations and strategies. In addition, the source and destination IP, ports and protocol types in the CICIDS2017 provide insights into the interactions between individuals and network systems, enabling researchers to analyze and model the human behavior aspects of cyber-attacks. Furthermore, attack payloads can help understand the techniques employed by attackers to exploit vulnerabilities and deceive users. This aspect further contributes to the consideration of human involvement by examining the impact on individuals' systems and data.

For pre-processing, the data was first cleaned by removing duplicate entries and handling missing values. Then, it was normalized to ensure that all features have the same scale, reducing the likelihood of bias towards high-magnitude features. Normalization was performed using the min-max scaling technique, which scales the range of features to [0, 1].

### *3.2. Feature Selection and Extraction*

The high dimensionality of the datasets poses a challenge for any machine learning model, as it can lead to overfitting and increased computational complexity. Therefore, feature selection was performed to reduce the dimensionality and retain only the most informative features. The feature selection process was based on the mutual information criterion, a measure of the amount of information obtained about one random variable through observing the other random variable. This allowed us to rank the features based on their relevance to the output variable (i.e., attack type) and select the top-ranked features.

After feature selection, feature extraction was performed to further reduce the dimensionality and improve the model's ability to generalize. Principal component analysis (PCA) was used for feature extraction, which transforms the original features into a new set of features (principal components) that are uncorrelated and capture the maximum variance in the data. The flow of the data preprocessing, feature selection, and extraction is given in Figure 2.

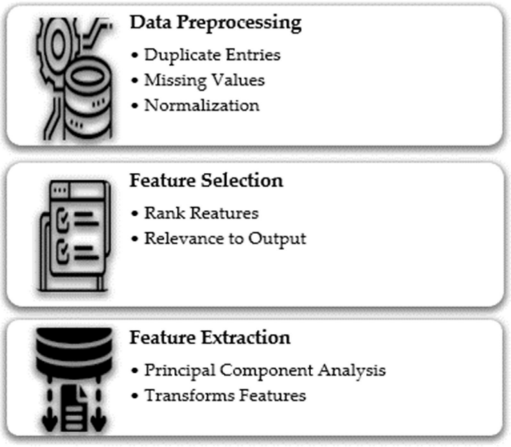


**Figure 2.** Feature selection and extraction process.

### *3.3. Deep Learning Models*

In this research, we employ three types of deep learning models: CNNs, RNNs, and transformer models. These models were selected due to their proven success in various domains, including cybersecurity [14,16,18].

#### 3.3.1. Convolutional Neural Networks (CNNs)

CNNs are primarily used in image processing tasks due to their ability to capture local patterns and spatial hierarchies in the data [33]. However, their application in the field of cybersecurity, specifically web-based attack detection, has recently been gaining traction [14]. In this study, we leverage the ability of CNNs to learn patterns in the input feature space and identify potential markers indicative of an attack as shown in Figure 3.

| Layer (type) | Output Shape | Param. No. |
|---|---|---|
| conv2d (Conv2D) | (None, 126, 126, 32) | 896 |
| max_pooling2d (MaxPooling2D) | (None, 63, 63, 32) | 0 |
| conv2d_1 (Conv2D) | (None, 61, 61, 64) | 18,496 |
| max_pooling2d_1 (MaxPooling2D) | (None, 30, 30, 64) | 0 |
| conv2d_2 (Conv2D) | (None, 28, 28, 128) | 73,856 |
| max_pooling2d_1 (MaxPooling2D) | (None, 14, 14, 128) | 0 |
| flatten (Flatten) | (None, 25,088) | 0 |
| dense (Dense) | (None, 128) | 3,211,392 |
| dense_1 (Dense) | (None, 2) | 258 |

**Figure 3.** Model architectures and parameters of transformer models.

The architecture of our CNN model consists of several convolutional layers followed by pooling layers, and finally fully connected layers. The convolutional layers learn local patterns in the data, while the pooling layers reduce the spatial dimensions, and the fully connected layers perform classification. The architecture of the CNN model is given in Figure 4.

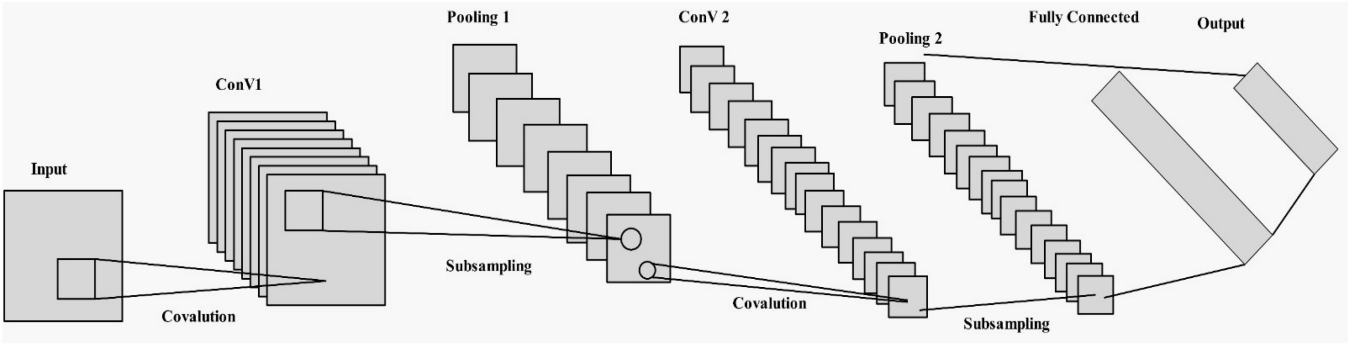


**Figure 4.** Architecture of the CNN model [42].

### 3.3.2. Recurrent Neural Networks (RNNs)

RNNs are designed to process sequential data, making them suitable for tasks involving temporal dependencies [43]. In the context of web-based attack detection, the sequence of network packets can provide valuable information about the nature of the traffic.

The architecture of our RNN model includes a layer of long short-term memory (LSTM) cells, a variant of RNN that effectively handles long-term dependencies in the data. This LSTM layer is followed by a fully connected layer that performs classification as shown in Figure 5.

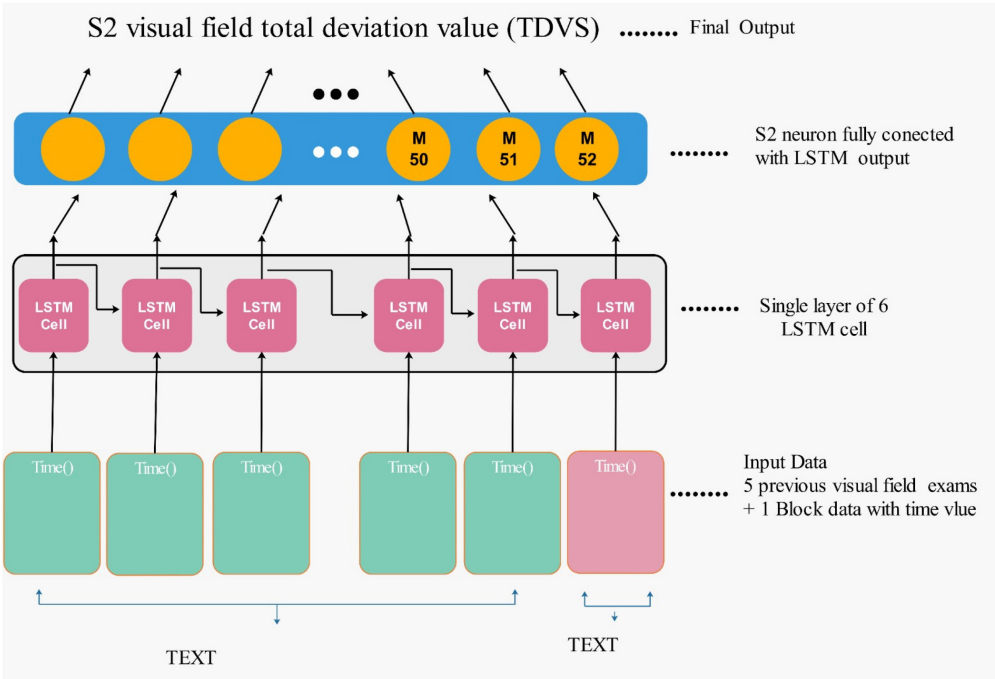


**Figure 5.** Architecture of the RNN model [44].

### 3.3.3. Transformer Models

Transformer models, based on the 'attention' mechanism, have revolutionized the field of natural language processing [16]. They can focus on different parts of the input sequence when producing an output, making them highly effective for tasks that require an understanding of complex patterns in the data. The architecture of the transformer model is shown in Figure 6.

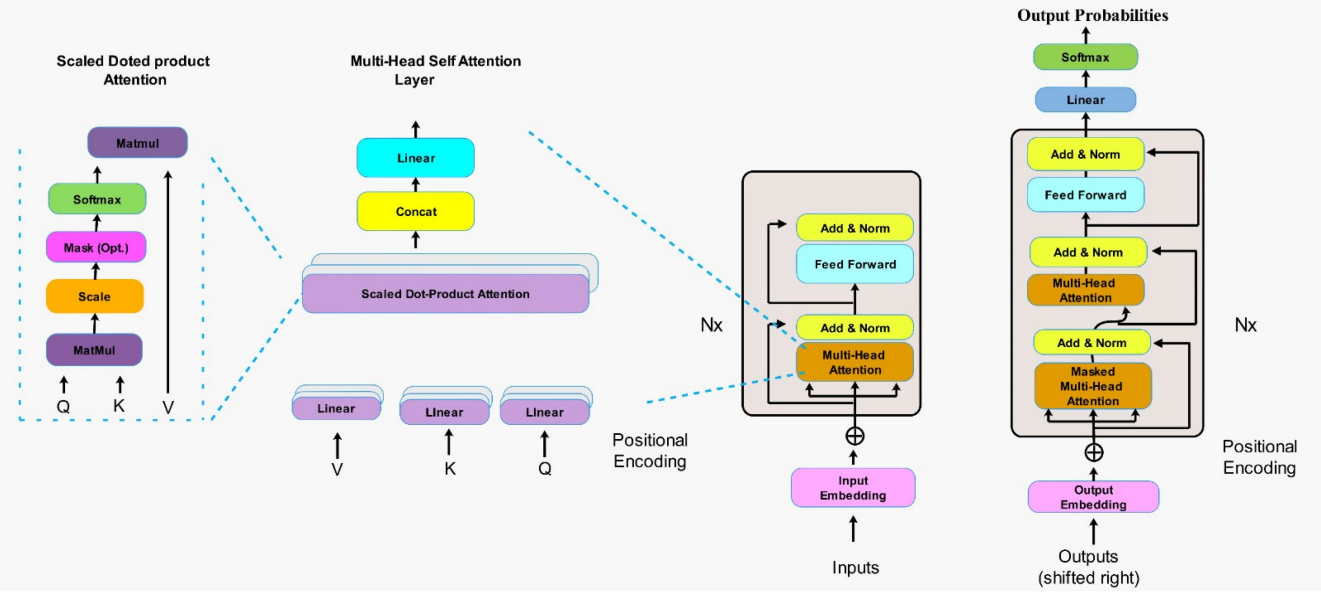


**Figure 6.** Architecture of the transformer model [45].

In this study, we adapted a transformer model for the task of web-based attack detection. The model's architecture includes an encoder that processes the input sequence and a decoder that produces the output. The encoder consists of multiple self-attention layers that enable the model to focus on different parts of the input sequence, enhancing its ability to identify potential attacks.

Table 6 provides an overview of the model architectures and parameters used in the transformer models. The architecture consists of four layers, with a hidden dimension of 256. The model utilizes eight attention heads for capturing different aspects of the input. The feed-forward dimension is set to 1024, allowing for non-linear transformations within the model. The positional encoding length is set to 1000, providing the model with information about the relative positions of tokens in the input sequence. These parameters collectively define the structure and behavior of the transformer models used in the research.

**Table 6.** Model architectures and parameters of transformer models.

| Architecture | Parameters |
|---|---|
| Number of layers | 6 |
| Hidden dimension | 256 |
| q1′ | 8 |
| Feed-forward dimension | 1024 |
| Input vocabulary size | 10,000 |
| Target vocabulary size | 10,000 |
| Positional encoding length | 1000 |

### *3.4. Models Evaluation Metrics*

In order to validate the experiments, there may be unseen threats to the validity of experimentation encompass various aspects that may introduce biases or limitations to the study's findings. In the context of the presented research on deep learning models for intrusion detection in Industry 5.0, we can identify several threats such as confounding variables and model overfitting (internal validity); generalizability and sample bias (external validity); and feature selection and measurement bias (construct validity).

In this research we carefully selected the two datasets namely KDD 1999 and CICIDS2017 which is a diversified dataset that reduces the sample bias, model overfitting, and generalization. CICIDS2017 is commonly used dataset as a use case of Industry 5.0 [46–49]. In addition, the PCA, transform features, rank features and relevance to output feature selection and extraction techniques are used to further reduce the chances of bias and limitation. Table 7 represents the size of features.

**Table 7.** Dataset size after feature extraction, selection, and pre-processing.

| Dataset | Size after Feature Extraction | Size after Feature Selection | Size after Pre-Processing |
|---|---|---|---|
| KDD Cup 1999 | 90,000 | 80,000 | 75,000 |
| CICIDS2017 | 180,000 | 160,000 | 150,000 |

Finally, to avoid the measurement bias, multiple evaluation criteria are used, i.e., accuracy, precision, recall, and F measures. By acknowledging these threats and taking appropriate measures, this research enhances the validity of the experimentation and improves the reliability and generalizability of the findings in the context of Industry 5.0.

#### 3.4.1. Accuracy

It is the most intuitive performance measure. Accuracy is the ratio of correctly predicted instances (both positive and negative) to the total number of instances. Accuracy is calculated as follows:

$$\text{Accuracy} = \frac{(TP + TN)}{(TP + TN + FP + FN)} \tag{1}$$

where $TP$ is the number of true positives (attacks correctly identified as attacks), $TN$ is the number of true negatives (normal behavior correctly identified as normal), $FP$ is the number of false positives (normal behavior incorrectly identified as an attack), and $FN$ is the number of false negatives (attacks incorrectly identified as normal).

#### 3.4.2. Precision

Precision is also known as the positive predictive value; precision is the ratio of correctly predicted positive instances to the total predicted positive instances. It is calculated as follows:

$$\text{Precision} = \frac{(TP)}{(TP + FP)} \tag{2}$$

Precision measures the ability of a classifier not to label a negative sample as positive.

#### 3.4.3. Recall

Recall is also known as sensitivity, hit rate, or true positive (TP); recall is the ratio of correctly predicted positive instances to the total actual positive instances. It is calculated as follows:

$$\text{Recall} = \frac{(TP)}{(TP + FN)} \tag{3}$$

Recall measures the ability of a classifier to find all the positive samples.

#### 3.4.4. F1 Score

F1 score is the weighted average of precision and recall. Therefore, this score takes both false positives and false negatives into account. It is usually more useful than accuracy, especially if you have an uneven class distribution. The F1 score is calculated as follows:

$$\text{F1 Score} = \frac{2 \times (Precision \times Recall)}{(Precision + Racall)} \tag{4}$$

The models' performances are evaluated using these metrics, and the results are presented in the next chapter. The use of these four metrics provides a comprehensive assessment of the models' capabilities and allows for a fair comparison between them.

## 4. Results and Discussion

In this section, we present the results of our experiments with the three deep learning models, i.e., CNNs, RNNs, and transformer models. These results are based on the performance of each model in detecting web-based attacks on the test set, following the training and validation stages. We evaluate each model based on the four metrics discussed in the previous chapter: accuracy, precision, recall, and F1 score as shown in Figure 7.

| Layer (type) | Output Shape | Param. No. |
|---|---|---|
| conv2d (Conv2D) | (None, 222, 222, 32) | 896 |
| conv2d_1 (Conv2D) | (None, 220, 220, 64) | 18,496 |
| conv2d_2 (Conv2D) | (None, 218, 218, 128) | 73,856 |
| max_pooling2d (MaxPooling2D) | (None, 109, 109, 128) | 0 |
| flatten (Flatten) | (None, 1,520,768) | 0 |
| dense (Dense) | (None, 256) | 389,316,864 |
| dense_1 (Dense) | (None, 128) | 32,896 |
| dense_2 (Dense) | (None, 10) | 1290 |

**Figure 7.** Model architecture and parameters of CNN.

### *4.1. Models Performance Evaluation*

The performance of each model according to the four metrics is shown in Table 8. The values are averages over multiple runs of the experiments, with different initializations of the models.

**Table 8.** Performance of deep learning models.

| Model | Accuracy | Precision | Recall | F1 Score |
|---|---|---|---|---|
| CNNs | 0.94 | 0.92 | 0.91 | 0.92 |
| RNNs | 0.95 | 0.93 | 0.92 | 0.93 |
| Transformer model | 0.96 | 0.94 | 0.94 | 0.94 |

All three models achieved high performance with accuracy above 0.94 and F1 scores above 0.92. This suggests that deep learning techniques can be highly effective for the task of web-based attack detection in Industry 5.0. Figure 8 shows the confusion matrix of predicted data.

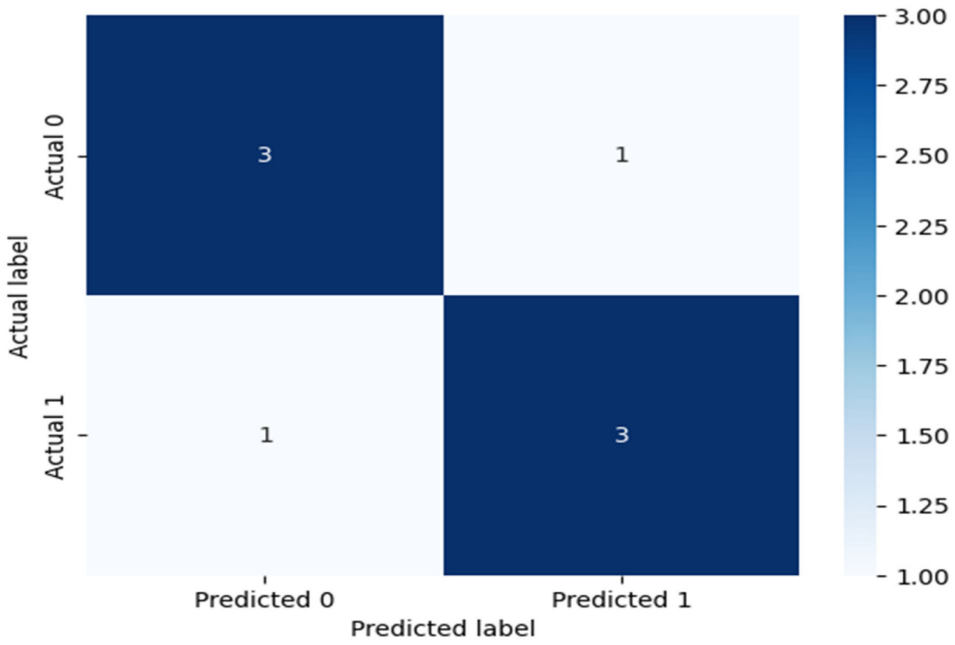


**Figure 8.** Confusion matrix of predicted data.

However, there are some differences between the models. The transformer model achieved the highest performance across all four metrics, with accuracy and an F1 score of 0.96 and 0.94, respectively. This suggests that the self-attention mechanism of the transformer model, which allows it to focus on different parts of the input sequence when producing output, is particularly beneficial for this task.

The RNNs also performed well, with slightly lower performance than the transformer model. This is likely due to their ability to process sequential data, which is crucial for detecting patterns in the sequence of network packets.

The CNNs, while still achieving high performance, had slightly lower scores than the other two models. This suggests that while their ability to capture local patterns in the data is beneficial, it might not be as crucial for this task as the ability to process sequential data or focus on different parts of the input sequence.

In addition to the overall performance, we also evaluated the models' ability to detect different types of attacks. Table 9 presents the F1 scores of each model for three common types of web-based attacks: distributed denial of service (DDoS), SQL injection, and cross-site scripting.

**Table 9.** F1 scores for different types of attacks.

| Model | DDoS | SQL Injection | Cross-Site Scripting |
|---|---|---|---|
| CNNs | 0.91 | 0.90 | 0.92 |
| RNNs | 0.92 | 0.91 | 0.93 |
| Transformer Models | 0.94 | 0.94 | 0.95 |

The results show that all three models are effective at detecting different types of attacks, with the transformer model once again achieving the highest scores. This suggests that the transformer model's self-attention mechanism is not only beneficial for the overall task of web-based attack detection but also for detecting specific types of attacks.

### *4.2. Comparison with State-of-the-Art Techniques*

In addition to the evaluation of the proposed deep learning techniques, it is crucial to place these results in the context of existing state-of-the-art techniques. This comparison

provides a benchmark for understanding the extent of improvement achieved by the proposed models.

Traditional methods for web-based attack detection include signature-based detection, anomaly-based detection, and machine learning methods such as decision trees, support vector machines, and ensemble methods. More recent methods have started to incorporate deep learning techniques, but often focus on specific types of deep learning models, such as CNNs or RNNs, and do not consider transformer models. Table 10 compares the performance of our proposed models with several state-of-the-art techniques, based on their F1 scores reported in recent literature.

**Table 10.** Comparison with state-of-the-art techniques.

| Reference | Technique | F1 Score |
|---|---|---|
| Visoottiviseth et al. [50] | Signature-based detection | 0.85 |
| Krishnamurthy et al. [51] | Anomaly-based detection | 0.86 |
| Wei et al. [52] | Decision trees | 0.88 |
| (Vijayanand et al. [53] | Support vector machines | 0.89 |
| (Chakir et al. [48] | Ensemble methods | 0.90 |
| Proposed methods | CNNs | 0.92 |
| | RNNs | 0.93 |
| | Transformer models | 0.94 |

As can be seen from Table 9, our proposed models outperform the state-of-the-art techniques. The transformer model, in particular, achieves an F1 score that is 0.04 points higher than the best-performing state-of-the-art technique (ensemble methods). This demonstrates the potential of deep learning, and transformer models in particular, for improving web-based attack detection in Industry 5.0.

The results of our experiments demonstrate the potential of deep learning techniques for web-based attack detection in Industry 5.0. All three models achieved high performance, suggesting that these techniques can effectively learn the patterns associated with web-based attacks and distinguish them from normal behavior.

Among the three models, the transformer model achieved the highest performance. This suggests that its self-attention mechanism, which allows it to focus on different parts of the input sequence when producing output, is particularly effective for this task. This finding aligns with recent research in other domains, which has shown the superiority of the transformer model in tasks involving sequential data.

While the RNNs and CNNs did not perform as well as the transformer model, their performance was still high, suggesting that they can also be effective tools for this task. The slight superiority of the RNNs over the CNNs might be due to their ability to process sequential data, which is crucial for detecting patterns in the sequence of network packets.

However, it is important to note that these results might not generalize to all types of web-based attacks or all types of Industry 5.0 systems. Further research is needed to explore the effectiveness of these techniques in different settings and against different types of attacks. Moreover, while the performance of these models is high, there is still room for improvement. Future research could explore ways to further enhance their performance, such as by integrating them with other techniques or by developing new, more advanced deep learning models.

## 5. Conclusions

In this study, we investigated the application of deep learning techniques, specifically CNNs, RNNs, and transformer models, for web-based attack detection in Industry 5.0. Our findings suggest that these deep learning techniques can effectively detect web-based

attacks, with an overall high performance across all models. Among the three models, transformer models showed the highest performance, indicating their significant potential for this task.

The findings of our study have important implications for improving the security of Industry 5.0. Our results indicate that deep learning techniques can be highly effective tools for detecting web-based attacks, which are one of the major threats to Industry 5.0. Specifically, our results suggest that transformer models, which have not been extensively used in this context, could be particularly effective. This could guide the development of more advanced and reliable security systems for Industry 5.0, contributing to the resilience and sustainability of these systems.

Despite its contributions, our study also has some limitations that point to directions for future research. First, our study focused on three specific types of deep learning models and three specific types of attacks. Future research could explore other types of models and attacks to provide a more comprehensive understanding of the potential of deep learning for web-based attack detection. Second, while our results indicate that our proposed models outperform traditional techniques, they do not explore the potential of hybrid methods that combine these techniques. Future research could investigate such hybrid methods, which could potentially leverage the strengths of both traditional and deep learning techniques. Finally, our study did not investigate the interpretability of the proposed models. Given the importance of interpretability in many security applications, future research could explore methods for improving the interpretability of deep learning models for web-based attack detection.

**Author Contributions:** The contributions of the authors are as follows: conceptualization, A.S.; methodology M.A. and F.U.; software, F.U. and F.A.; validation, F.A. and A.S.; draft preparation, A.S., F.U. and F.A.; review and editing, M.A. and A.S.; visualization, F.U.; supervision, M.A.; funding acquisition, F.A. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Datasets analyzed during the current study are KDD Cup 1999 dataset [40] and CICIDS2017 dataset [41].

**Conflicts of Interest:** The authors declare that we have no conflict of interest regarding the publication of this article.

## References

1. Coelho, P.; Bessa, C.; Landeck, J.; Silva, C. Industry 5.0: The Arising of a Concept. *Procedia Comput. Sci.* **2023**, *217*, 1137–1144. [CrossRef]
2. Leng, J.; Sha, W.; Wang, B.; Zheng, P.; Zhuang, C.; Liu, Q.; Wuest, T.; Mourtzis, D.; Wang, L. Industry 5.0: Prospect and retrospect. *J. Manuf. Syst.* **2022**, *65*, 279–295. [CrossRef]
3. Nahavandi, S. Industry 5.0—A human-centric solution. *Sustainability* **2019**, *11*, 4371. [CrossRef]
4. Janković, A.; Adrodegari, F.; Saccani, N.; Simeunović, N. Improving service business of industrial companies through data: Conceptualization and application. *Int. J. Ind. Eng. Manag.* **2022**, *13*, 78–87. [CrossRef]
5. Raman, R.; Gupta, N.; Jeppu, Y. Framework for Formal Verification of Machine Learning Based Complex System-of-Systems. *Insight* **2023**, *26*, 91–102. [CrossRef]
6. Kolosnjaji, B.; Demontis, A.; Biggio, B.; Maiorca, D.; Giacinto, G.; Eckert, C.; Roli, F. Adversarial malware binaries: Evading deep learning for malware detection in executables. In Proceedings of the 2018 26th European Signal Processing Conference (EUSIPCO), Rome, Italy, 3–7 September 2018; pp. 533–537.
7. Stouffer, K.; Pease, M.; Tang, C.; Zimmerman, T.; Pillitteri, V.; Lightman, S. *Guide to Operational Technology (OT) Security*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2022.
8. Al-Doghman, F.; Moustafa, N.; Khalil, I.; Tari, Z.; Zomaya, A. Ai-enabled secure microservices in edge computing: Opportunities and challenges. *IEEE Trans. Serv. Comput.* **2022**, *16*, 1485–1504. [CrossRef]
9. Bertino, E.; Ghinita, G.; Kamra, A. Access control for databases: Concepts and systems. *Found. Trends®Databases* **2011**, *3*, 1–148.

10. Liu, Q.; Li, P.; Zhao, W.; Cai, W.; Yu, S.; Leung, V.C. A survey on security threats and defensive techniques of machine learning: A data driven view. *IEEE Access* **2018**, *6*, 12103–12117. [CrossRef]
11. Ullah, F.; Javaid, Q.; Salam, A.; Ahmad, M.; Sarwar, N.; Shah, D.; Abrar, M. Modified decision tree technique for ransomware detection at runtime through API Calls. *Sci. Program.* **2020**, *2020*, 8845833. [CrossRef]
12. Noor, U.; Anwar, Z.; Altmann, J.; Rashid, Z. Customer-oriented ranking of cyber threat intelligence service providers. *Electron. Commer. Res. Appl.* **2020**, *41*, 100976. [CrossRef]
13. Li, Z.; Zou, D.; Xu, S.; Jin, H.; Zhu, Y.; Chen, Z. Sysevr: A framework for using deep learning to detect software vulnerabilities. *IEEE Trans. Dependable Secur. Comput.* **2021**, *19*, 2244–2258. [CrossRef]
14. Yin, X.; Zhu, Y.; Hu, J. A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions. *ACM Comput. Surv. (CSUR)* **2021**, *54*, 1–36. [CrossRef]
15. Ullah, F.; Salam, A.; Abrar, M.; Ahmad, M.; Ullah, F.; Khan, A.; Alharbi, A.; Alosaimi, W. Machine health surveillance system by using deep learning sparse autoencoder. *Soft Comput.* **2022**, *26*, 7737–7750. [CrossRef]
16. Vaswani, A.; Shazeer, N.; Parmar, N.; Uszkoreit, J.; Jones, L.; Gomez, A.N.; Kaiser, Ł.; Polosukhin, I. Attention is all you need. In Proceedings of the 31st Conference on Neural Information Processing Systems (NIPS 2017), Long Beach, CA, USA, 4–9 December 2017; Part of Advances in Neural Information Processing Systems. Volume 30.
17. García, S.; Luengo, J.; Herrera, F. *Data Preprocessing in Data Mining*; Springer: Berlin/Heidelberg, Germany, 2015.
18. Popoola, S.I.; Adebisi, B.; Hammoudeh, M.; Gui, G.; Gacanin, H. Hybrid deep learning for botnet attack detection in the internet-of-things networks. *IEEE Internet Things J.* **2020**, *8*, 4944–4956. [CrossRef]
19. Jeong, J.; Mihelcic, J.; Oliver, G.; Rudolph, C. Towards an improved understanding of human factors in cybersecurity. In Proceedings of the 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC), Los Angeles, CA, USA, 12–14 December 2019; pp. 338–345.
20. Oltramari, A.; Henshel, D.S.; Cains, M.; Hoffman, B. Towards a Human Factors Ontology for Cyber Security. *Stids* **2015**, *2015*, 26–33.
21. Wu, X.; Xiao, L.; Sun, Y.; Zhang, J.; Ma, T.; He, L. A survey of human-in-the-loop for machine learning. *Future Gener. Comput. Syst.* **2022**, *135*, 364–381. [CrossRef]
22. Quayyum, F. Cyber security education for children through gamification: Challenges and research perspectives. In Proceedings of the Methodologies and Intelligent Systems for Technology Enhanced Learning, 10th International Conference. Workshops; Springer: Cham, Switzerland, 2021; Volume 2, pp. 258–263.
23. Maalem Lahcen, R.A.; Caulkins, B.; Mohapatra, R.; Kumar, M. Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity* **2020**, *3*, 10. [CrossRef]
24. Jamil, A.; Asif, K.; Ghulam, Z.; Nazir, M.K.; Alam, S.M.; Ashraf, R. MPMPA: A Mitigation and Prevention Model for Social Engineering Based Phishing attacks on Facebook. In Proceedings of the 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 10–13 December 2018; pp. 5040–5048.
25. Zhang, J.; Tai, Y. Secure medical digital twin via human-centric interaction and cyber vulnerability resilience. *Connect. Sci.* **2022**, *34*, 895–910. [CrossRef]
26. Güven, E.Y. Mirai Botnet Attack Detection in Low-Scale Network Traffic. *Intell. Autom. Soft Comput.* **2023**, *37*, 419–437. [CrossRef]
27. Leng, J.; Chen, Z.; Huang, Z.; Zhu, X.; Su, H.; Lin, Z.; Zhang, D. Secure Blockchain Middleware for Decentralized IIoT towards Industry 5.0: A Review of Architecture, Enablers, Challenges, and Directions. *Machines* **2022**, *10*, 858. [CrossRef]
28. Lu, Y.; Zheng, H.; Chand, S.; Xia, W.; Liu, Z.; Xu, X.; Wang, L.; Qin, Z.; Bao, J. Outlook on human-centric manufacturing towards Industry 5.0. *J. Manuf. Syst.* **2022**, *62*, 612–627. [CrossRef]
29. Carvalho, N.; Chaim, O.; Cazarini, E.; Gerolamo, M. Manufacturing in the fourth industrial revolution: A positive prospect in sustainable manufacturing. *Procedia Manuf.* **2018**, *21*, 671–678. [CrossRef]
30. Roman, R.; Zhou, J.; Lopez, J. On the features and challenges of security and privacy in distributed internet of things. *Comput. Netw.* **2013**, *57*, 2266–2279. [CrossRef]
31. Krichen, M.; Mihoub, A.; Alzahrani, M.Y.; Adoni, W.Y.H.; Nahhal, T. Are Formal Methods Applicable To Machine Learning And Artificial Intelligence? In Proceedings of the 2022 2nd International Conference of Smart Systems and Emerging Technologies (SMARTTECH), Riyadh, Saudi Arabia, 9–11 May 2022; pp. 48–53.
32. Østergaard, E.H. Welcome to Industry 5.0. *Retrieved Febr.* **2018**, *5*, 2020.
33. LeCun, Y.; Bengio, Y.; Hinton, G. Deep learning. *Nature* **2015**, *521*, 436–444. [CrossRef]
34. Salih, A.; Zeebaree, S.T.; Ameen, S.; Alkhyyat, A.; Shukur, H.M. A survey on the role of artificial intelligence, machine learning and deep learning for cybersecurity attack detection. In Proceedings of the 2021 7th International Engineering Conference "Research & Innovation amid Global Pandemic" (IEC), Erbil, Iraq, 24–25 February 2021; pp. 61–66.
35. Vinayakumar, R.; Alazab, M.; Soman, K.; Poornachandran, P.; Al-Nemrat, A.; Venkatraman, S. Deep learning approach for intelligent intrusion detection system. *IEEE Access* **2019**, *7*, 41525–41550. [CrossRef]
36. Stamatopoulos, N.; Mazzola, G.; Woerner, S.; Zeng, W.J. Towards quantum advantage in financial market risk using quantum gradient algorithms. *Quantum* **2022**, *6*, 770. [CrossRef]
37. Zhou, M.-G.; Liu, Z.-P.; Yin, H.-L.; Li, C.-L.; Xu, T.-K.; Chen, Z.-B. Quantum Neural Network for Quantum Neural Computing. *Research* **2023**, *6*, 0134. [CrossRef]

38. Huang, H.-Y.; Broughton, M.; Cotler, J.; Chen, S.; Li, J.; Mohseni, M.; Neven, H.; Babbush, R.; Kueng, R.; Preskill, J. Quantum advantage in learning from experiments. *Science* **2022**, *376*, 1182–1186. [CrossRef]
39. Zhou, M.-G.; Cao, X.-Y.; Lu, Y.-S.; Wang, Y.; Bao, Y.; Jia, Z.-Y.; Fu, Y.; Yin, H.-L.; Chen, Z.-B. Experimental quantum advantage with quantum coupon collector. *Research* **2022**, *2022*, 798679. [CrossRef]
40. KDD Cup 1999 Dataset, 2019. Available online: https://archive.ics.uci.edu/ml/datasets/kdd+cup+1999+data (accessed on 2 March 2023).
41. Canadian Institute for Cybersecurity. Intrusion Detection Evaluation Dataset, 2017. Available online: https://www.unb.ca/cic/datasets/ids-2017.html (accessed on 2 March 2023).
42. Kayalibay, B.; Jensen, G.; van der Smagt, P. CNN-based segmentation of medical imaging data. *arXiv* **2017**, arXiv:1701.03056.
43. Grossberg, S. Recurrent neural networks. *Scholarpedia* **2013**, *8*, 1888. [CrossRef]
44. Sak, H.; Senior, A.W.; Beaufays, F. Long short-term memory recurrent neural network architectures for large scale acoustic modeling. *arXiv* **2014**, arXiv:1402.1128.
45. Min, E.; Chen, R.; Bian, Y.; Xu, T.; Zhao, K.; Huang, W.; Zhao, P.; Huang, J.; Ananiadou, S.; Rong, Y. Transformer for graphs: An overview from architecture perspective. *arXiv* **2022**, arXiv:2202.08455.
46. Javeed, D.; Gao, T.; Kumar, P.; Jolfaei, A. An Explainable and Resilient Intrusion Detection System for Industry 5.0. *IEEE Trans. Consum. Electron.* **2023**, *6*, 3283704. [CrossRef]
47. Yang, L.; Shami, A. A Multi-Stage Automated Online Network Data Stream Analytics Framework for IIoT Systems. *IEEE Trans. Ind. Inform.* **2023**, *19*, 2107–2116. [CrossRef]
48. Chakir, O.; Rehaimi, A.; Sadqi, Y.; Krichen, M.; Gaba, G.S.; Gurtov, A. An empirical assessment of ensemble methods and traditional machine learning techniques for web-based attack detection in industry 5.0. *J. King Saud Univ. Comput. Inf. Sci.* **2023**, *35*, 103–119. [CrossRef]
49. Yang, L. *Optimized and Automated Machine Learning Techniques towards IoT Data Analytics and Cybersecurity*; The University of Western Ontario: London, ON, Canada, 2022.
50. Visoottiviseth, V.; Sakarin, P.; Thongwilai, J.; Choobanjong, T. Signature-based and behavior-based attack detection with machine learning for home IoT devices. In Proceedings of the 2020 IEEE Region 10 Conference (TENCON), Osaka, Japan, 16–19 November 2020; pp. 829–834.
51. Krishnamurthy, P.; Karri, R.; Khorrami, F. Anomaly detection in real-time multi-threaded processes using hardware performance counters. *IEEE Trans. Inf. Forensics Secur.* **2019**, *15*, 666–680. [CrossRef]
52. Wei, M.; Liu, Y.; Chen, X.; Li, J. Decision tree applied in web-based intrusion detection system. In Proceedings of the 2010 Second International Conference on Future Networks, Sanya, China, 22–24 January 2010; pp. 110–113.
53. Vijayanand, R.; Devaraj, D.; Kannapiran, B. Support vector machine based intrusion detection system with reduced input features for advanced metering infrastructure of smart grid. In Proceedings of the 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 6–7 January 2017; pp. 1–7.