applied sciences

MDPI

Article

Towards a Hybrid Machine Learning Model for Intelligent Cyber Threat Identification in Smart City Environments

Najla Al-Taleb [1] and Nazar Abbas Saqib [2,*]

[1] Department of Computer Science, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia; 2190500053@iau.edu.sa
[2] SAUDI ARAMCO Cybersecurity Chair, Department of Networks and Communications, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia
* Correspondence: nasaqib@iau.edu.sa

Abstract: The concept of a smart city requires the integration of information and communication technologies and devices over a network for the better provision of services to citizens. As a result, the quality of living is improved by continuous analyses of data to improve service delivery by governments and other organizations. Due to the presence of extensive devices and data flow over networks, the probability of cyber attacks and intrusion detection has increased. The monitoring of this huge amount of data traffic is very difficult, though machine learning algorithms have huge potential to support this task. In this study, we compared different machine learning models used for cyber threat classification. Our comparison was focused on the analyzed cyber threats, algorithms, and performance of these models. We have identified that real-time classification, accuracy, and false-positive rates are still the major issues in the performance of existing models. Accordingly, we have proposed a hybrid deep learning (DL) model for cyber threat intelligence (CTI) to improve threat classification performance. Our model was based on a convolutional neural network (CNN) and quasi-recurrent neural network (QRNN). The use of QRNN not only resulted in improved accuracy but also enabled real-time classification. The model was tested on BoT-IoT and TON_IoT datasets, and the results showed that the proposed model outperformed the other models. Due to this improved performance, we emphasize that the application of this model in the real-time environment of a smart system network will help in reducing threats in a reasonable time.

Keywords: cyber threat intelligence; privacy; smart city; machine learning; deep learning; CNN; QRNN

Citation: Al-Taleb, N.; Saqib, N.A. Towards a Hybrid Machine Learning Model for Intelligent Cyber Threat Identification in Smart City Environments. *Appl. Sci.* **2022**, *12*, 1863. https://doi.org/10.3390/app12041863

Academic Editors: Leandros Maglaras, Helge Janicke and Mohamed Amine Ferrag

Received: 21 December 2021
Accepted: 28 January 2022
Published: 11 February 2022

1. Introduction

The transformation of cities into smart cities is on the rise, where technologies such as the Internet of Things (IoT) and cyber–physical systems (CPS) are connected through networks for the better provision of quality services to citizens [1]. The smart city concept refers to urban systems that are integrated with information and communication technologies (ICTs) to improve city services in terms of monitoring, management, and control to be more efficient and effective [2]. A smart city contains a huge number of sensors that continuously generate a tremendous amount of sensitive data such as location coordinates, credit card numbers, and medical records [3]. These data are transmitted through a network to data centers for processing and analysis so that appropriate decisions, such as managing traffic and energy, can be made in a smart city [4]. The resource limitations of technological infrastructure expose smart cities to cyber attacks [5]. For instance, sensors that generate data and devices that handle the data in a smart city have vulnerabilities that can be exploited by cybercriminals. Consequently, citizens' privacy and lives can be at risk when collected data for analysis and decision making are manipulated, which makes people intimidated by smart cities [1].

A smart city environment collects a tremendous amount of private and sensitive data and depends on ICT, which makes smart cities target for different cyber attacks, such as distributed denial of service (DDoS), using IoT devices by infecting them with bots and launch an attack against a target [6–9]. Cyber threat intelligence (CTI) can provide secure environments for smart cities, where it can rely on cloud services to monitor possible threats in real time and take appropriate prevention measures without human intervention [10–15]. Moreover, CTI can provide a light security mechanism, as it is not implemented on smart city devices; rather, it monitors attacks through the cloud to obtain information about recent threat behavior and indicator of compromise (IoC), and it reports this information to connected smart city systems. Different techniques and machine learning (ML) models have been proposed to analyze cyber threats for CTI such as deep learning (DL) models [16,17], random forest (RF) [18], and K-NN [19]. Nevertheless, artificial intelligence (AI)-based models can have a high false-positive rates (FPRs) and low true-positive rates (TPRs) if the attack traffic is not profiled and modeled well enough [20]. This limits real-time classification efficiency and degrades smart city network security. To address this issue, improve threat analysis, and lower FPRs, we propose a hybrid DL model that is based on a convolutional neural network (CNN) and quasi-recurrent neural network (QRNN). The proposed model can automatically learn spatial features using CNN and temporal features using QRNN without human intervention. The CNN model can automatically select the relevant features from the dataset and reduce the irrelevant features to improve classification performance [21]. For cyber threat analysis, several works have shown the efficiency of CNN for feature selection, such as [20,22]. The QRNN model performs computation in parallel, which improves computation time while maintaining sequence modeling [23]. Thus, this hybrid model (CNN–QRNN) can help improve real-time analysis in CTI while providing a high accuracy and low FPR. Therefore, the proposed model can improve CTI performance for smart cities. We evaluated our proposed model with two IoT network traffic datasets. The evaluation results demonstrate the effectiveness of our proposed model. The main contributions of this study are summarized as follows:

- We propose a hybrid DL model that consists of QRNN and CNN to improve cyber threat analysis accuracy, lower FPR, and provide real-time analysis.
- We evaluated our proposed model on two datasets that were simulated to represent a realistic IoT environment.

The rest of this paper is structured as follows. In Section 2, we discuss related work by comparing and analyzing different threat classification schemes that have been proposed in the literature. The proposed model is presented in Section 3. The implementation of the proposed model is discussed in Section 4, the experiment results and analysis are presented in Section 5, and conclusions are presented in Section 6.

2. Related Work

In recent years, different studies have proposed mechanisms to predict and analyze cyber attacks in smart city environments. The authors of [24] proposed an ML-based detection mechanism that focused on classifying DDoS patterns to protect a smart city from them. In [25], the authors studied how IoT devices can affect smart city cyber security; the authors proposed a detection mechanism that depends on the selected features to improve the threat detection for IoT. The results of the proposed system showed high accuracy, but the dataset, KDD CUP 99, did not represent the behavior of IoT network attacks. Soe et al. [21] proposed an algorithm to improve prediction accuracy by selecting the optimal features for each type of attack in an IoT environment. The authors used ML models to evaluate the proposed feature selection algorithm, which was able to accurately predict the threats. However, the proposed algorithm selected a static set of features for each type of attack, which could be easily bypassed if exposed to the threat environment. In [26], the authors used a DL model to select the best features for threat prediction to improve the detection time in an IoT environment. The proposed model selects a set of features that are fed into feed-forward neural networks (FFNNs) to detect cyber threats and

classify threat types. However, the proposed model showed limited accuracy in predicting information theft data.

In [19], the authors discussed how to use the ML model to rapidly and efficiently detect and classify IoT network attacks. The authors performed an experimental study by implementing various ML models and evaluating their performance. In [27], the authors proposed a hybrid ML model to detect IoT network attacks including that of the zero-day. The proposed model mainly consists of two stages: the first stage classifies the traffic into two categories (normal or attack), and the second stage classifies the type of attacks using SVM. Similarly, in [28], the authors proposed a hybrid ML model to detect and classify IoT network attacks in real time. The first layer of the proposed model uses a decision tree classifier to detect malicious behavior and the second layer classifies the type of attack using random forest (RF). In [29], the authors investigated the remote-control threat of connected cars and used an ML model to predict threats. The authors proposed a proactive anomaly detection mechanism that profiled the behavior of the autonomous connected cars using a recursive Bayesian estimator. To evaluate the effectiveness of the proposed method, the authors designed a dataset for connected cars using hypothetical events routes and global positioning system coordinates, and they then modeled the data to predict the anomalies' behavior. Lee et al. [30] proposed a technique, based on DL models, that transforms the multitude of security events into individual event profiles. The authors discussed how anomaly-based detection can be costly since it can trigger many false alerts. Therefore, they focused on improving security information and event management system by using DL to reduce the cost to differentiate between true and false alerts. In [31], the authors proposed a hybrid ML method to detect cyber threats. The authors focused on how to improve detection accuracy to handle an attacker's methods to evade detection tools. To evaluate the proposed method, the authors used different datasets including KDD Cup and UNSW-NB15. In [32], the authors discussed how to improve the threat analysis and classification, including novel attacks. The authors proposed a model based on a stacked autoencoder to enhance and automate feature selection to classify the threats.

Various scientific studies have proposed a hybrid DL model to improve threat analysis and classification. In [33], the authors proposed an improved version of grey wolf optimization (GWO) and a CNN. In the proposed hybrid model, the first GWO model is used to select the features and the second CNN model is used for threat classification. Other studies have used a hybrid DL model that is based on CNNs and RNNs for spatial and temporal feature extraction to improve attack classification. In [34], the authors used a CNN for feature selection since it could provide fast feature selection to support real-time analysis. For threat classification, the authors used one of the variants of the LSTM model: weight-dropped LSTM (WDLSTM). The proposed hybrid model showed good performance in terms of execution time. Vinayakumar et al. [35] studied the effect of CNN in threat classification and intrusion detection system (IDS). The authors investigated different hybrid DL models with CNNs including CNN-LSTM, CNN-GRU, and CNN-RNN, and the model implementing CNN-LSTM outperformed the other models. Moreover, the authors highlighted that selecting a minimum set of features for threat classification degraded the performance of the classification. Therefore, DL models can perform well in terms of feature selection. In [36], the authors proposed a hierarchical model based on CNN-LSTM. The authors used stacked CNN layers for spatial features learning using image classification and then stacked LSTM for temporal features learning. Similarly, in [20], the authors proposed an LuNet model based on CNN-LSTM. The authors discussed how stacking LSTM layers after CNN layers could drop some of the temporal features. Thus, the authors proposed the LuNet block, which consists of LSTM layer stacked after the CNN layer, and they then stacked the LuNet block in multiple layers to improve classification performance and lower the FPR.

As shown in Table 1, different network traffic benchmark datasets have been used to analyze the low-level IoC such as UNSW-NB15, NSL-KDD, and KDD CUP 99. For IoT attack classification, the BoT-IoT dataset has been used in multiple studies to evaluate

the performance of proposed models. Different ML and DL models, such as the SVM, CNN, and LSTM, have been used to analyze threats and provide accurate results, and the CNN-LSTM hybrid model has been used in multiple studies to improve threat classification performance.

Table 1. Comparison between proposed attack classification methods.

Ref	Cyber Threats	Algorithm	Data Sources	Accuracy	FPR
[24]	DDoS	Restricted Boltzmann machine and FFNN	Simulated smart water system dataset	97.5%	-
[21]	Information theft, reconnaissance, and DDoS	J48	BoT-IoT UNSW	-	0.41
[26]	Information theft, reconnaissance, and DDoS	FFNN	BoT-IoT UNSW	-	-
[19]	DDoS, DoS, data exfiltration, keylogging, OS fingerprinting, and service scan	K-nearest neighbors (K-NN)	BoT-IoT UNSW	99.00%	-
[27]	DDoS, DoS, keylogging, and reconnaissance	C5-SVM	BoT-IoT UNSW	99.97%	0.001
[28]	DDoS, DoS, data exfiltration, keylogging, OS fingerprinting, and service scan	Decision tree-RF	BoT-IoT UNSW	99.80%	-
[29]	Remote car control	Recursive Bayesian estimation	Route data for connected cars	-	-
[30]	DoS, probe, R2L, and U2R	FCNN, CNN, and LSTM	Network events	94.7%	0.049
[31]	Tor traffic (anonymous IP)	C4.5, Multilayer perceptron (MLP), SVM, and linear discriminant analysis (LDA)	UNB-CIC TOR Network Traffic dataset	100	0
	Worms, DoS, backdoors, reconnaissance, exploits, analysis, generic, fuzzers, and shellcode		UNSW-NB15	97.84%	0.23
[32]	Injection, Flooding, Impersonation	Stacked auto-encoder (SAE)	AWID-CLS-R	98.66%	-
[33]	DoS, probe, R2L, and U2R	GWO-CNN	DARPA1998	97.92%	3.60
			KDD CUP 99	98.42%	2.22
[34]	Worms, DoS, backdoors, reconnaissance, exploits, analysis, generic, fuzzers, and shellcode	CNN-LSTM	UNSW-NB15	98.43%	-
[35]	DoS, probe, R2L, and U2R	CNN-LSTM	KDD CUP 99	98.7%	0.005
[36]	DoS, probe, R2L, U2R, BruteForce SSH, DDoS, and infiltrating	CNN-LSTM	ISCX2012	99.69%	0.22
			DARPA1998	99.68%	0.07
[20]	Worms, DoS, backdoors, reconnaissance, exploits, analysis, generic, fuzzes, and shellcode	CNN-LSTM	UNSW-NB15	84.98%	1.89
	DoS, probe, R2L, and U2R		NSL-KDD	99.05%	0.65

In terms of the CTI for smart cities, multiple papers, including [24,25], have analyzed the threats pattern based on network traffic. Additionally, in [37], the authors proposed a trustworthy privacy-preserving secured framework (TP2SF) for smart cities; the authors used the optimized gradient tree boosting system (XGBoost) and blockchain, and they evaluated the proposed framework on two datasets: BoT-IoT and TON_IoT. DDoS is one of the challenging threats in a smart city that has been studied by different researchers, who have proposed methods to analyze IP addresses and track the sources to prevent this attack or to identify the behavior of the network when there is overload traffic. Data theft, which can be described as privacy and identity theft, is another threat that has been studied by

various researchers. Data theft threats include reconnaissance, information theft, probe, R2L, and U2R, which may lead to the exposure of various vulnerabilities that can help in launching data theft attacks such as sniffing passwords and unauthorized access. Some of the proposed models for smart cites set a fixed threshold to detect attacks, which is not effective and can raise a lot of false alarms that affect the power consumption of the connected systems. In smart cities, the normal behavior of a system can change due to the increasing number of connected devices, so some researchers have achieved high accuracy but bad performance in terms of FPR.

Even though different researchers have proposed models to enhance threat classification for IoT environments, many aspects still require improvement. One of the limitations that is common between different methods is performance time. Low-level IoCs that are collected from network traffic have been used to analyze the threats in various papers to provide timely information to the CTI knowledge base and update the detection and prevention information for all systems connected to the CTI. However, to enhance classification performance, various models have multiple stacked ML model layers. Therefore, it may take time to train a model and classify threats while not taking advantage of these IoCs. Secondly, when some models are not provided with enough data for each type of threat, threat traffic cannot be profiled and modeled well enough. Consequently, ML models can have high FPRs. Furthermore, some models only provide accurate results when their system has precise details of threats. Consequently, the system is not able to recognize threats that do not have enough data for model training, which affects classification accuracy.

Moreover, we observed that few papers have addressed diverse patterns for threat analysis while considering time, accuracy, and FPR. Several works have proposed hybrid models based on the CNN and LSTM to learn spatial and temporal data. However, LSTM is computationally complex and requires a long time for analysis [38]. The QRNN model is a type of RNN that allows for sequence modeling by implementing computation in parallel while maintaining the data's long- and short-term sequence dependencies [23]. We could not find a work that used the QRNN model to improve cyber threat classification time while demonstrating high accuracy. Thus, in this work, we propose a hybrid DL model for CTI for smart cities that addresses the abovementioned challenges and uses the QRNN model. The proposed hybrid model can improve threat classification accuracy and lower the FPR in a reasonable time. Therefore, it can predict different attacks to protect citizens' data and enhance the security of smart cities.

3. Proposed Model

In this section, we discuss the proposed hybrid DL model in terms of its structure, the selected DL algorithms, and relevant theoretical concepts. The selected DL models (CNN and QRNN) can be used to classify a threat type in real time while providing a low FPR. The architecture of the proposed model is presented in Figure 1.

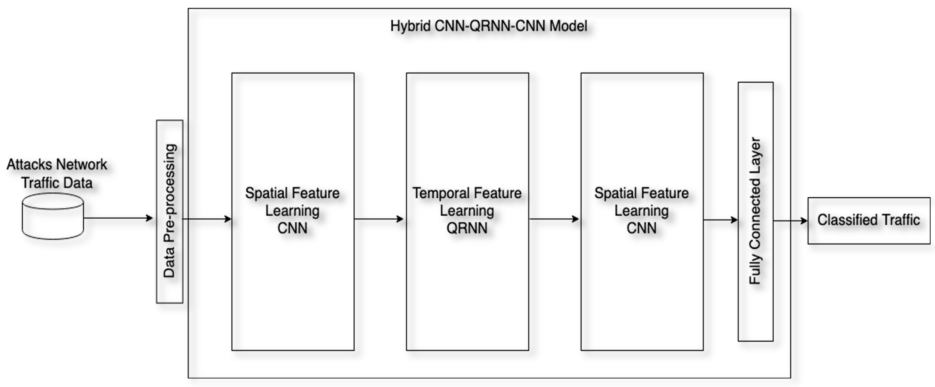

Figure 1. The architecture of the proposed hybrid model.

A CNN is an extension of a neural network [39] and it is effective at extracting features at a low level from the source data, especially spatial features [40].

CNNs are used widely in image processing due to their ability to automate feature extraction [41]. Additionally, CNNs have demonstrated their effectiveness in many fields such as biomedical text analysis and malware classification [30]. Based on the shape of the input data, a CNN can be classified into different types including a two-dimensional (2D) CNN, which uses data such as images, and a one-dimensional (1D) CNN, which uses data such as text. A CNN consists of a convolution layer, pooling layer, fully connected (FC) layer, and activation function [42]. The convolution layer is fundamental building block in CNNs that takes two sets of information as inputs and performs a mathematical operation with these inputs. The two sets of information are the data and a filter, which can be referred to as kernel. The filter is applied to an entire dataset to produce a feature map [41]. Each CNN filter extracts a set of features that are aggregated to a new feature map as output [30]. The pooling layer is implemented to reduce feature map dimensions and to remove irrelevant data to improve learning [20]. The output of the pooling layer is fed into the FC layer to classify the data [43].

The LSTM-RNN is one of the most powerful neural network models that is used in cyber security due to its ability to accurately model temporal sequences and their long-term dependencies [44]. However, LSTM usually takes a longer time for model training and high computation cost [45]. The QRNN model [23] was designed to overcome the RNN limitations in terms of each timestep's computation dependency on the previous timestep, which limits the power of parallelism. The QRNN combines the benefits of the CNN and RNN by using convolutional filters on the input data and allowing the long-term sequence dependency to store the data of previous timestamps [23]. The computation structure of the QRNN is presented in Figure 2. The QRNN consists of convolutional layers and recurrent pooling function, which allow the QRNN to work faster than LSTM due to its a 16-times-increase in speed while achieving the same accuracy as LSTM [46]. The convolutional and pooling layers allow for the parallel computation of the batch and feature dimensions [23]. The QRNN has been used in different applications such as video classification [45], speech synthesis [46], and natural language processing [47].

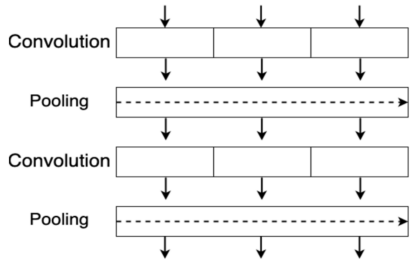

Figure 2. The computation structure of the QRNN.

Our hybrid DL model consists of a 1D convolutional layer, 1D max-pooling layer, a QRNN, and FC layers. The first 1D convolutional layer selects the spatial features and produces a feature map that will be processed by the activation function. The Rectified Linear Unit (ReLU) activation function is used in the convolutional layers because of its rapid convergence of gradient descent, which made it a good choice for our proposed model [41]. Then, the feature map is processed by the second layer that uses the max-pooling operation. The max-pooling operation selects the maximum value in the pooling operation [41]. The pooling layer reduces dimensionality and removes irrelevant features. The output of the CNN model retains the temporal feature that is extracted by the QRNN model. Figure 3 provides details of our proposed model and shows that we used two QRNN layers to extract the temporal features. In the two layers of the QRNN, the hidden size represents the number of the hidden units and the output dimension. The hidden units can be selected based on the value of the number of features [45]. One of the problems

of a neural network is overfitting, which means that a model learns the data too well. Consequently, the model is not able to identify variants in new data [22]. We added a dropout layer to prevent overfitting.

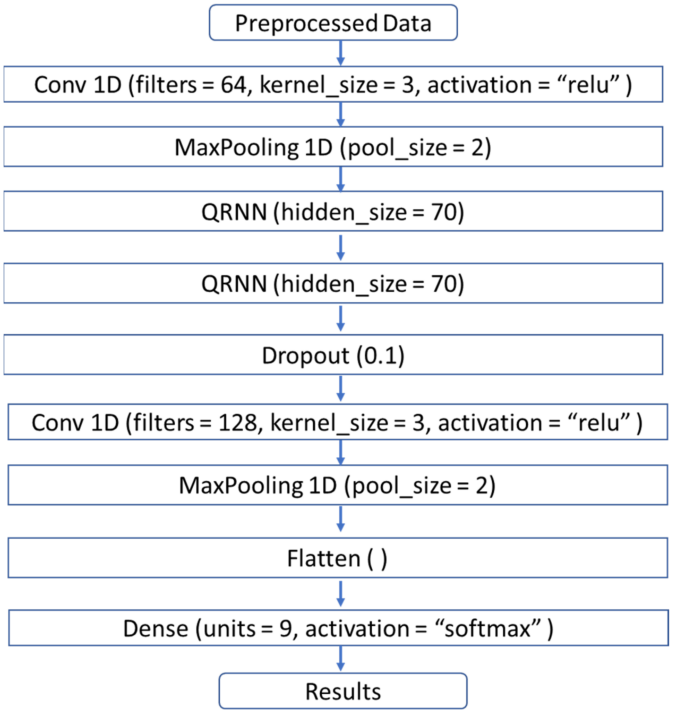

Figure 3. Illustration of the details of the proposed model.

Then, a 1D convolutional layer and max-pooling layer are used to extract more spatial-temporal features. The output of the CNN model is passed to the Flatten layer, which is a fully connected input layer that transforms the output of the pooling layer into one vector to be an input for the next layer [48]. Finally, the dense layer, which is also a fully connected layer, with the SoftMax activation function is used to classify the threats by calculating the probabilities for each class [34].

4. Implementation

In this section, we describe the datasets that we selected to evaluate the proposed model. Additionally, we discuss the data preprocessing steps, model parameter selection process, and selected evaluation metrics.

4.1. Datasets

In this work, we selected the BoT-IoT and TON-IoT datasets because they have been simulated to represent realistic IoT environments such as smart homes and cities. The datasets had a heterogeneity of simulated IoT devices including weather-monitoring systems, smart lights, smart thermostats, and a variety of cyber threats.

4.1.1. BoT-IoT Dataset

In previous studies, different datasets, such as KDD99, ISCX, and CICIDS2017, have been used to evaluate ML models; however, few datasets have been produced to reflect realistic IoT network traffic. These datasets were either not diverse enough in terms of attacks or not realistic in terms of the testbed [19]. Therefore, Koroniotis et al. [49] designed the BoT-IoT dataset to address these limitations. The BoT-IoT dataset is used in forensic analysis and to evaluate IDS. The dataset contains normal IoT traffic and different types of attack traffic with subcategories for each type, which are listed in Table 2. Reconnaissance

is one of the privacy threats, and it allows a threat actor to collect data about a victim via port scanning and OS fingerprinting, among other ways. Information theft includes data theft by unauthorized access and keylogging. On the other hand, a DoS threat affects the availability of services and can damage systems, which make it one of the biggest threats to smart cities. In this dataset, UDP, TCP, and HTTP protocols were used to perform both DoS and DDoS attacks.

Table 2. Attack categories in BoT-IoT dataset.

Attack	Attack Subcategory	Number of Instances
Reconnaissance	Service scan	73,168
	OS fingerprinting	17,914
DoS	TCP	615,800
	UDP	1,032,975
	HTTP	1485
DDoS	TCP	977,380
	UDP	948,255
	HTTP	989
Information theft	Keylogging	73
	Data theft	6

4.1.2. TON_IoT Dataset

The ToN_IoT dataset [50] is one of the newest cyber security datasets; it as collected from a testbed network for industry 4.0 IoT and Industrial IoT (IIoT), which makes it suitable to evaluate CTI for a smart city. We used the TON_IoT train–test dataset, which is in the CSV format. The dataset contains a total of 461,043 instances and 9 types of attacks, which are presented in Table 3 along with the number of instances for each type.

Table 3. Attack categories in TON_IoT dataset.

Attack	Number of Instances
DoS	20,000
DDoS	20,000
Scanning	20,000
Ransomware	20,000
Backdoor	20,000
Injection	20,000
Cross-Site Scripting (XSS)	20,000
Password	20,000
Man-In-The-Middle (MITM)	1043

4.2. Data Preprocessing

Since we were interested in evaluating CTI for threat classification, we deleted the normal traffic from the datasets. Additionally, in the BoT-IoT dataset, we omitted the pkSeqID feature since it represented an identifier for the traffic records. The datasets contains some categorical features that could not be processed by the neural network. Thus, we converted the nominal values into numeric using sklearn LabelEncoder. LabelEncoder converts categorical values into numerical values [22]. We implemented sklearn StandardScaler to scale the data. For training and evaluation, several papers have split the dataset into training and testing, with a ratio of 20% for testing s in [19] and 30% for testing in [21]. However, due to

the size of the BoT-IoT dataset and the resource constraints of our device, we divided the data into training and testing sets, with a ratio of 35% for testing, while having the same ratio of classes in both parts by using the stratify parameter.

4.3. Model Implementation

The parameters of the hybrid model were obtained during the training phase by trial and error including the number of CNN filters, the number of QRNN hidden units, and the dropout rate. As mentioned in different studies [35], kernel size values of 3 and 5 are the most common, so we used kernel size 3 with both datasets in our experiment. A filter can help in extracting more details from a dataset by increasing the number of filters [51]. Thus, for the first CNN layer, we used 64 filters, and for the other CNN, we used 128 filters. Additionally, we set the value of the batch size for the training at 128 and the value of the number of epochs at 10. The details and the selected parameters of the hybrid DL model are presented in Figure 3.

4.4. Evaluation Tools and Metrics

Different evaluation metrics were used in this work to evaluate the performance of the proposed model including accuracy, FPR, TPR, precision, recall, and F-Score. Accuracy represents the ratio of correctly classified threats to the total number of classified threats, so it demonstrates how accurate an model in classifying threats [52]. The FPR represents the ratio of misclassified data as a different type of threat, and the TPR represents a model's ability to correctly classify threats. A low FPR and a high TPR demonstrate the ability of a model to correctly classify cyber threats [53]. Precision, recall, and F-Score were used to evaluate the overall performance of the proposed model; a high value of precision indicates a low FPR, and recall represents a model's ability to correctly classify threats. Equations (1)–(6) represent the evaluation metrics, where FP is false positive, TP is true positive, TN is true negative, and FN is false negative.

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

$$\text{FPR} = \frac{FP}{FP + TN} \tag{2}$$

$$\text{TPR} = \frac{TP}{TP + FN} \tag{3}$$

$$\text{Precision} = \frac{TP}{TP + FP} \tag{4}$$

$$\text{Recall} = \frac{TP}{TP + FN} \tag{5}$$

$$\text{F} - \text{Score} = \frac{2(\text{Precision} \times \text{Recall})}{\text{Precision} + \text{Recall}} \tag{6}$$

5. Results and Discussion

5.1. Results and Analysis

This section presents the results and analysis for model implementation. We used Jupyter Notebook software with the Python programming language. We used the Keras and scikitlearn packages for data pre-processing and implementing the proposed model. We trained the proposed model on a MacBook Air with an Intel Core i5 CPU 1.6 GHz processor and 8 GB RAM. Additionally, we implemented different state-of-the-art ML models on the datasets to compare their performance with that of our proposed model. Figure 4 presents the confusion matrix of our proposed model on the BoT-IoT dataset. The results show that the model correctly classified most of the cyber threat categories. Furthermore, to illustrate the quality of the proposed model, the receiver operating characteristic (ROC) curve is plotted in Figure 5 for the BoT-IoT dataset.

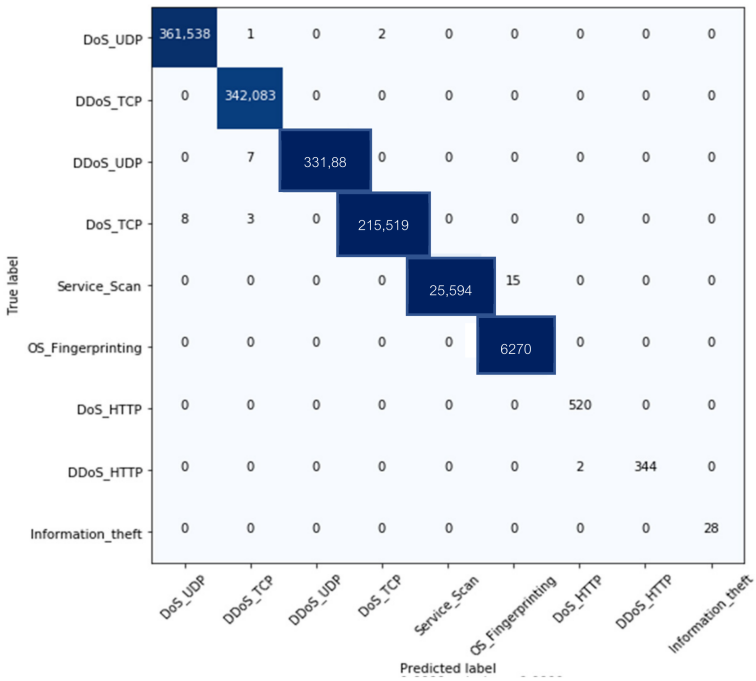

Figure 4. Confusion matrix based on the BoT-IoT dataset.

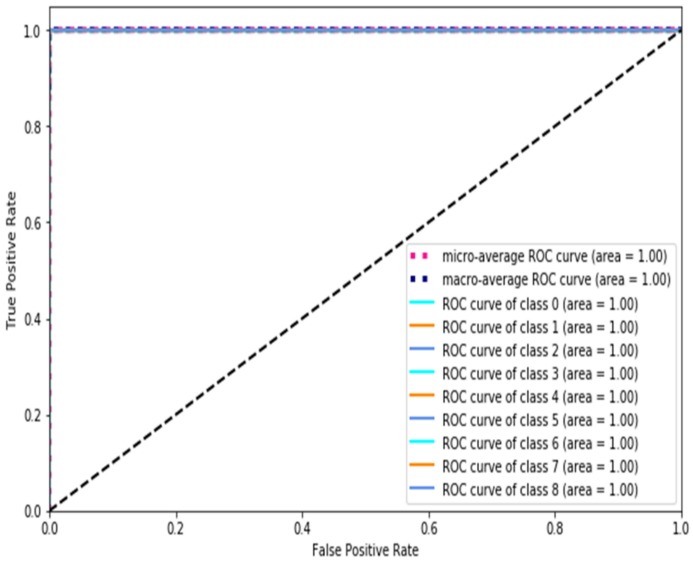

Figure 5. ROC curve of using our proposed model on the BoT-IoT dataset.

Figure 6 presents the confusion matrix of our proposed model on the TON_IoT dataset, and the ROC curve is presented in Figure 7. Both ROC curves show that our proposed model achieved the highest value of 1. Thus, our proposed model performed very well with all the classes.

The results of our proposed model on the testing datasets are presented in Table 4.

Table 4. Results of cyber threat classification on both datasets.

Dataset	Accuracy%	TPR%	FPR
BoT-IoT	99.99	99.92	0.0003
TON_IoT	99.99	99.99	0.001

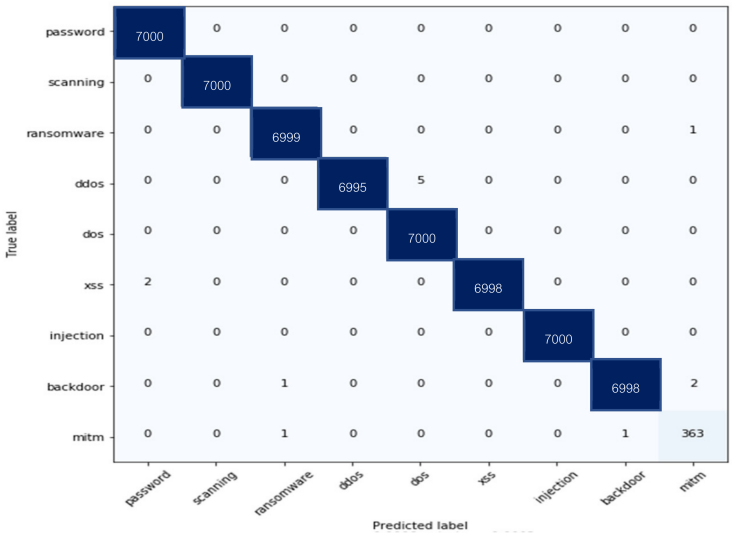

Figure 6. Confusion matrix based on the TON_IoT dataset.

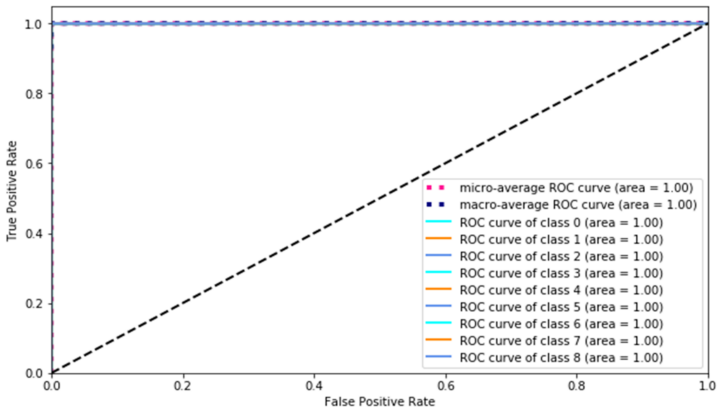

Figure 7. ROC curve of using our proposed model on the TON_IoT dataset.

As shown in Table 4, the proposed model achieved high accuracy, with an average of 99.99% on both datasets. The TPR reached averages of 99.92% with the BoT-IoT dataset and 99.99% with the TON_IoT dataset. The proposed model achieved a low FPR of 0.0003 with the BoT-IoT dataset and 0.001 with the TON_IoT dataset. Thus, the proposed model showed good performance in classifying the threats with both datasets. Moreover, to demonstrate the effectiveness of the QRNN, we implemented our proposed model with LSTM instead of the QRNN to compare performance. Cybersecurity threats are very critical [54–56], and the results shown in Tables 5 and 6 highlight that our proposed approach could be very effective in dealing with them.

Table 5. Comparison of our proposed model while using LSTM and QRNN based on BoT-IoT dataset.

Model	Accuracy	Precision	Recall	F-Score	Avg. Training Time per Epoch	Classification Time
With LSTM	99.99%	100%	100%	100%	1717.4 s	326 s
With QRNN	99.99%	100%	100%	100%	1299.1 s	251 s

Table 6. Comparison of our proposed model while using LSTM and the QRNN based on TON_IoT dataset.

Model	Accuracy	Precision	Recall	F-Score	Avg. Training Time per Epoch	Classification Time
With LSTM	99.99%	100%	100%	100%	86.3 s	16 s
With QRNN	99.99%	100%	100%	100%	66.5 s	13 s

According to the results in Tables 5 and 6, our proposed model with the QRNN showed the same performance as our proposed model with LSTM in terms of accuracy, precision, recall, and F-Score. In terms of time, the proposed model with the QRNN showed better performance for training the model and testing. The average training time per epoch demonstrated that the QRNN performed faster than LSTM in terms of training the model on both datasets, with a 418.3 s difference on the BoT-IoT dataset and a 19.8 s difference on the TON_IoT dataset. Additionally, for the classification time on the test dataset, the QRNN model performed faster than LSTM, with a 75 s difference on the BoT-IoT dataset and a 3 s difference on the TON_IoT dataset. The QRNN showed its effectiveness in increasing the speed of the model while providing a high accuracy and low FPR. Therefore, the model can be used for real-time CTI. We further compared the performance of our proposed model on the BoT-IoT and TON_IoT datasets against the state-of-the-art models for the multi-class classification of threats. The results of these comparisons are shown in Tables 7 and 8.

Table 7. Comparison of our proposed model with state-of-the-art models based on the BoT-IoT dataset.

Model	Accuracy%	Precision%	Recall%	F-Score%
K-NN [19]	99.00	99.00	99.00	99.00
Hybrid IDS [27]	99.97	-	-	95.7
RF [28]	99.80	99.00	99.00	98.80
RF [37]	99.99	79.76	62.98	65.08
TP2SF [37]	99.99	99.97	94.92	97.08
Our model	99.99	100	100	100

Table 8. Comparison of our proposed model with state-of-the-art models based on the TON_IoT dataset.

Model	Accuracy%	Precision%	Recall%	F-Score%
RF [37]	97.81	87.55	85.43	86.41
TP2SF [37]	98.84	97.23	94.03	95.28
Our model	99.99	100	100	100

As shown in Tables 7 and 8, though K-NN [19] and RF [28] showed good performance for recall and F-score on the BoT-IoT dataset, our proposed model outperformed the state-of-the-art models on both datasets. Additionally, we implemented different ML models to compare their performance with that of our model. The accuracy, TPR, and FPR values of each model are given are Tables 9 and 10. Our model performed better than the other four models, with accuracy measured as 99.99% on both datasets and low FPR values of 0.0003 on the BoT-IoT dataset and 0.001 on the TON_IoT dataset. The LSTM model showed good performance in terms of accuracy and FPR, while the GRU showed a high TPR compared to the LSTM on the BoT-IoT dataset. On the TON_IoT dataset, the GRU performed poorly compared to the other models.

Table 9. Comparison of our proposed model with other ML models based on BoT-IoT dataset.

Model	Accuracy%	TPR%	FPR
MLP	99.98	86.42	0.002
CNN	99.98	88.13	0.001
GRU	99.98	96.06	0.001
LSTM	99.99	94.69	0.0004
Our model	99.99	99.92	0.0003

Table 10. Comparison of our proposed model with other ML models based on TON_IoT dataset.

Model	Accuracy%	TPR%	FPR
MLP	99.67	99.51	0.03
CNN	99.88	99.75	0.01
GRU	97.85	96.95	0.27
LSTM	99.83	99.79	0.02
Our model	99.99	99.99	0.001

5.2. Theoretical and Practical Implications

This work describes a model that can correctly classify cyber threats with a low FPR while considering time performance. Thus, the proposed model can improve decision making for risk mitigation so that appropriate protection measures against cyber attacks in smart cities can be taken [57,58]. Additionally, this model will benefit organizations and services providers in smart cities because of the high costs of implementing and maintaining cyber security solutions [59]. The organizations and service providers in smart cities can take accurate proactive measures against detected cyber attacks such as data breaches, which will help in saving costs [60]. Furthermore, our proposed model can be implemented in the cloud to monitor cyber security and collect and update cyber threat data from the connected systems in smart cities.

6. Conclusions

A smart city facilitates the life of its citizens by providing better services than non-smart cities. Due to the extensive presence of digital data, smart cities are also vulnerable to various types of attacks. Machine-learning-based cyber threat intelligence can secure smart city environments by monitoring attacks and analyzing data threats in order to take prevention measures. In this paper, we have proposed a hybrid deep learning model to classify threats. The proposed model uses a CNN and a QRNN to improve feature extraction, increases classification accuracy, and lower the FPR. We evaluated our model on the BoT-IoT and TON_IoT datasets, and our results showed the effectiveness of our model in improving classification accuracy and lowering the FPR. In addition, the results showed that the QRNN model could improve classification time performance while providing high accuracy and lower FPR than LSTM. Thus, the proposed model for CTI for smart cities can accurately analyze and classify data in real time.

One of the limitations of this work is the authors' use of datasets. Due to the security and privacy of smart city citizens, it was difficult to evaluate the proposed model on real-time data. Additionally, for implementation, we evaluated the model as a centralized system. In future work, we can implement the proposed model in a distributed environment with parallel training to improve classification performance.

Author Contributions: Data curation, N.A.-T.; Formal analysis, N.A.-T.; Funding acquisition, N.A.S.; Investigation, N.A.S. and N.A.-T.; Project administration, N.A.S.; Resources, N.A.S.; Supervision, N.A.S.; Validation, N.A.-T.; Writing—original draft, N.A.-T. All authors have read and agreed to the published version of the manuscript.

Funding: The authors would like to thank SAUDI ARAMCO Cybersecurity Chair, Imam Abdulrahman Bin Faisal University for funding this project.

Acknowledgments: The authors would like to thank Attaur-Rahman and Sujata Dash for their feedback on an earlier non-peer-reviewed version of the manuscript which was shared on the Arxiv repository.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. AlZaabi, K.A.J.A. The Value of Intelligent Cybersecurity Strategies for Dubai Smart City. In *Smart Technologies and Innovation for a Sustainable Future*; Springer International Publishing: Cham, Switzerland, 2019; pp. 421–445, ISBN 9783030016593.
2. Behzadan, V.; Munir, A. Adversarial Exploitation of Emergent Dynamics in Smart Cities. In Proceedings of the 2018 IEEE International Smart Cities Conference (ISC2), Kansas City, MO, USA, 16–19 September 2018; pp. 1–8.
3. Butt, T.A.; Afzaal, M. Security and Privacy in Smart Cities: Issues and Current Solutions. In *Smart Technologies and Innovation for a Sustainable Future*; Springer International Publishing: Cham, Switzerland, 2019; pp. 317–323, ISBN 9783030016593.
4. Lee, J.; Kim, J.; Seo, J. Cyber attack scenarios on smart city and their ripple effects. In Proceedings of the 2019 International Conference on Platform Technology and Service (PlatCon), Jeju, Korea, 28–30 January 2019; pp. 1–5.
5. Ahmad, F.; Adnane, A.; Franqueira, V.N.L.; Kurugollu, F.; Liu, L. Man-In-The-Middle Attacks in Vehicular Ad-Hoc Networks: Evaluating the Impact of Attackers' Strategies. *Sensors* **2018**, *18*, 4040. [CrossRef] [PubMed]
6. Alibasic, A.; Junaibi, R.A.; Aung, Z.; Woon, W.L.; Omar, M.A. Cybersecurity for Smart Cities: A Brief Review. In *International Workshop on Data Analytics for Renewable Energy Integration*; Springer: Cham, Switzerland, 2017; pp. 22–30.
7. Braun, T.; Fung, B.C.M.; Iqbal, F.; Shah, B. Security and privacy challenges in smart cities. *Sustain. Cities Soc.* **2018**, *39*, 499–507. [CrossRef]
8. Cui, L.; Xie, G.; Qu, Y.; Gao, L.; Yang, Y. Security and Privacy in Smart Cities: Challenges and Opportunities. *IEEE Access* **2018**, *6*, 46134–46145. [CrossRef]
9. Kettani, H.; Cannistra, R.M. On Cyber Threats to Smart Digital Environments. In Proceedings of the 2nd International Conference on Smart Digital Environment, Rabat, Morocco, 18–20 October 2018; ACM: New York, NY, USA, 2018; pp. 183–188.
10. Sookhak, M.; Tang, H.; Yu, F.R. Security and Privacy of Smart Cities: Issues and Challenges. In Proceedings of the 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Exeter, UK, 28–30 June 2018; pp. 1350–1357.
11. Liu, M.; Xue, Z.; He, X.; Chen, J. Cyberthreat-Intelligence Information Sharing: Enhancing Collaborative Security. *IEEE Consum. Electron. Mag.* **2019**, *8*, 17–22. [CrossRef]
12. Zhang, K.; Ni, J.; Yang, K.; Liang, X.; Ren, J.; Shen, X.S. Security and Privacy in Smart City Applications: Challenges and Solutions. *IEEE Commun. Mag.* **2017**, *55*, 122–129. [CrossRef]
13. Abu, S.; Selamat, S.R.; Ariffin, A.; Yusof, R. Cyber Threat Intelligence—Issue and Challenges. *Indones. J. Electr. Eng. Comput. Sci.* **2018**, *10*, 371–379.
14. Conti, M.; Dehghantanha, A.; Dargahi, T. Cyberthreat intelligence: Challenges and opportunities. In *Cyber Threat Intelligence*; Springer: Cham, Switzerland, 2018; pp. 1–6.
15. Myat, K.; Win, N.; Myo, Y.; Khine, K. Information Sharing of Cyber Threat Intelligence with their Issue and Challenges. *Int. J. Trend Sci. Res. Dev.* **2019**, *3*, 878–880.
16. Diro, A.A.; Chilamkurti, N. Distributed attack detection scheme using deep learning approach for Internet of Things. *Futur. Gener. Comput. Syst.* **2018**, *82*, 761–768. [CrossRef]
17. Berman, D.S.; Buczak, A.L.; Chavis, J.S.; Corbett, C.L. A Survey of Deep Learning Methods for Cyber Security. *Information* **2019**, *10*, 122. [CrossRef]
18. Abawajy, J.; Huda, S.; Sharmeen, S.; Hassan, M.M.; Almogren, A. Identifying cyber threats to mobile-IoT applications in edge computing paradigm. *Futur. Gener. Comput. Syst.* **2018**, *89*, 525–538. [CrossRef]
19. Alsamiri, J.; Alsubhi, K. Internet of Things Cyber Attacks Detection using Machine Learning. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*, 627–634. [CrossRef]
20. Wu, P.; Guo, H. LuNet: A Deep Neural Network for Network Intrusion Detection. In Proceedings of the 2019 IEEE Symposium Series on Computational Intelligence (SSCI), Xiamen, China, 6–9 December 2019; pp. 617–624.
21. Soe, Y.N.; Feng, Y.; Santosa, P.I.; Hartanto, R.; Kouichi, S. Towards a Lightweight Detection System for Cyber Attacks in the IoT Environment Using Corresponding Features. *Electronics* **2020**, *9*, 144. [CrossRef]
22. Wu, P.; Guo, H.; Moustafa, N. Pelican: A Deep Residual Network for Network Intrusion Detection. In Proceedings of the 2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), Valencia, Spain, 29 June–2 July 2020.
23. Bradbury, J.; Merity, S.; Xiong, C.; Socher, R. Quasi-Recurrent Neural Networks. *arXiv* **2017**, arXiv:1611.01576.
24. Elsaeidy, A.; Munasinghe, K.S.; Sharma, D.; Jamalipour, A. A Machine Learning Approach for Intrusion Detection in Smart Cities. In Proceedings of the 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), Honolulu, HI, USA, 22–25 September 2019; pp. 1–5.

25. Li, D.; Deng, L.; Lee, M.; Wang, H. IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning. *Int. J. Inf. Manag.* **2019**, *49*, 533–545. [CrossRef]
26. Ge, M.; Fu, X.; Syed, N.; Baig, Z.; Teo, G.; Robles-kelly, A. Deep Learning-based Intrusion Detection for IoT Networks. In Proceedings of the 2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC), Kyoto, Japan, 1–3 December 2019.
27. Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J.; Alazab, A. A Novel Ensemble of Hybrid Intrusion Detection System for Detecting Internet of Things Attacks. *Electronics* **2019**, *8*, 1210. [CrossRef]
28. Ullah, I.; Mahmoud, Q.H. A Two-Level Flow-Based Anomalous Activity Detection System for IoT Networks. *Electronics* **2020**, *9*, 530. [CrossRef]
29. Al-Khateeb, H.; Epiphaniou, G.; Reviczky, A.; Karadimas, P.; Heidari, H. Proactive Threat Detection for Connected Cars Using Recursive Bayesian Estimation. *IEEE Sens. J.* **2018**, *18*, 4822–4831. [CrossRef]
30. Lee, J.; Kim, J.; Kim, I.; Han, K. Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles. *IEEE Access* **2019**, *7*, 165607–165626. [CrossRef]
31. Sornsuwit, P.; Jaiyen, S. A New Hybrid Machine Learning for Cybersecurity Threat Detection Based on Adaptive Boosting. *Appl. Artif. Intell.* **2019**, *33*, 462–482. [CrossRef]
32. Thing, V.L.L. IEEE 802.11 Network Anomaly Detection and Attack Classification: A Deep Learning Approach. In Proceedings of the 2017 IEEE Wireless Communications and Networking Conference (WCNC), San Francisco, CA, USA, 19–22 March 2017; pp. 1–6.
33. Garg, S.; Kaur, K.; Kumar, N.; Kaddoum, G.; Zomaya, A.Y.; Ranjan, R. A Hybrid Deep Learning-Based Model for Anomaly Detection in Cloud Datacenter Networks. *IEEE Trans. Netw. Serv. Manag.* **2019**, *16*, 924–935. [CrossRef]
34. Hassan, M.M.; Gumaei, A.; Alsanad, A.; Alrubaian, M.; Fortino, G. A hybrid deep learning model for efficient intrusion detection in big data environment. *Inf. Sci.* **2020**, *513*, 386–396. [CrossRef]
35. Vinayakumar, R.; Kp, S.; Poornachandran, P. Applying Convolutional Neural Network for Network Intrusion Detection. In Proceedings of the 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Udupi, India, 13–16 September 2017; pp. 1222–1228.
36. Wang, W.; Sheng, Y.; Wang, J.; Zeng, X.; Ye, X.; Huang, Y.; Zhu, M. HAST-IDS: Learning Hierarchical Spatial-Temporal Features Using Deep Neural Networks to Improve Intrusion Detection. *IEEE Access* **2018**, *6*, 1792–1806. [CrossRef]
37. Kumar, P.; Gupta, G.P.; Tripathi, R. TP2SF: A Trustworthy Privacy-Preserving Secured Framework for sustainable smart cities by leveraging blockchain and machine learning. *J. Syst. Archit.* **2021**, *115*, 101954. [CrossRef]
38. Niu, X.; Ma, J.; Wang, Y.; Zhang, J.; Chen, H.; Tang, H. A Novel Decomposition-Ensemble Learning Model Based on Ensemble Empirical Mode Decomposition and Recurrent Neural Network for Landslide Displacement Prediction. *Appl. Sci.* **2021**, *11*, 4684. [CrossRef]
39. LeCun, Y.; Bengio, Y.; Hinton, G. Deep learning. *Nature* **2015**, *521*, 436–444. [CrossRef]
40. Ferrag, M.A.; Maglaras, L.; Moschoyiannis, S.; Janicke, H. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *J. Inf. Secur. Appl.* **2020**, *50*, 102419. [CrossRef]
41. Hasan, M.N.; Toma, R.N.; Nahid, A.; Islam, M.M.M.; Kim, J. Electricity Theft Detection in Smart Grid Systems: A CNN-LSTM Based Approach. *Energies* **2019**, *12*, 3310. [CrossRef]
42. Kwon, D.; Natarajan, K.; Suh, S.C.; Kim, H.; Kim, J. An Empirical Study on Network Anomaly Detection using Convolutional Neural Networks. In Proceedings of the In 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), Vienna, Austria, 2–6 July 2018; pp. 1595–1598.
43. Liu, H.; Lang, B.; Liu, M.; Yan, H. Knowledge-Based Systems CNN and RNN based payload classification methods for attack detection. *Knowl.-Based Syst.* **2019**, *163*, 332–341. [CrossRef]
44. Khan, A.; Sarfaraz, A. RNN-LSTM-GRU based language transformation. *Soft Comput.* **2019**, *23*, 13007–13024. [CrossRef]
45. Bolelli, F.; Baraldi, L.; Pollastri, F.; Grana, C. A Hierarchical Quasi-Recurrent approach to Video Captioning. In Proceedings of the 2018 IEEE International Conference on Image Processing, Applications and Systems (IPAS), Sophia Antipolis, France, 12–14 December 2018; pp. 162–167.
46. Wang, M.; Wu, X.; Wu, Z.; Kang, S.; Tuo, D.; Li, G.; Su, D.; Yu, D.; Meng, H. Quasi-fully Convolutional Neural Network with Variational Inference for Speech Synthesis. In Proceedings of the ICASSP 2019–2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Brighton, UK, 12–17 May 2019; pp. 7060–7064.
47. Huang, J.; Feng, Y. Optimization of Recurrent Neural Networks on Natural Language Processing. In Proceedings of the Proceedings of the 2019 8th International Conference on Computing and Pattern Recognition, New York, NY, USA, 23–25 October 2019; pp. 39–45.
48. Yao, D.; Wen, M.; Liang, X.; Fu, Z.; Zhang, K.; Yang, B. Energy Theft Detection with Energy Privacy Preservation in the Smart Grid. *IEEE Internet Things J.* **2019**, *6*, 7659–7669. [CrossRef]
49. Koroniotis, N.; Moustafa, N.; Sitnikova, E.; Turnbull, B. Towards the Development of Realistic Botnet Dataset in the Internet of Things for Network Forensic Analytics: Bot-IoT Dataset. *Futur. Gener. Comput. Syst.* **2018**, *100*, 779–796. [CrossRef]
50. Moustafa, N. TON_IoT Datasets. In Proceedings of the IEEE Dataport, Brisbane, Australia, 16 October 2019. [CrossRef]

51. Safa, H.; Nassar, M.; Al Orabi, W.A.R. Benchmarking Convolutional and Recurrent Neural Networks for Malware Classification. In Proceedings of the 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), Tangier, Morocco, 24–28 June 2019; pp. 561–566.
52. Shafiq, M.; Tian, Z.; Sun, Y.; Du, X.; Guizani, M. Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city. *Futur. Gener. Comput. Syst.* **2020**, *107*, 433–442. [CrossRef]
53. Vinayakumar, R.; Alazab, M.; Member, S.; Soman, K.P. Deep Learning Approach for Intelligent Intrusion Detection System. *IEEE Access* **2019**, *7*, 41525–41550. [CrossRef]
54. Obaidan, F.A.; Saeed, S. Digital Transformation and Cybersecurity Challenges: A Study of Malware Detection Using Machine Learning Techniques. In *Handbook of Research on Advancing Cybersecurity for Digital Transformation*; IGI Global: Pennsylvania, PA, USA, 2021; pp. 203–226.
55. Naeem, H.; Ullah, F.; Naeem, M.R.; Khalid, S.; Vasan, D.; Jabbar, S.; Saeed, S. Malware detection in industrial internet of things based on hybrid image visualization and deep learning model. *Ad. Hoc. Netw.* **2020**, *105*, 102154. [CrossRef]
56. Khadam, U.; Iqbal, M.M.; Saeed, S.; Dar, S.H.; Ahmad, A.; Ahmad, M. Advanced security and privacy technique for digital text in smart grid communications. *Comput. Electr. Eng.* **2021**, *93*, 107205. [CrossRef]
57. Yamin, M.M.; Katt, B.; Nowostawski, M. Serious games as a tool to model attack and defense scenarios for cyber-security exercises. *Comput. Secur.* **2021**, *110*, 102450. [CrossRef]
58. Poleto, T.; Carvalho VD, H.D.; Silva AL, B.D.; Clemente TR, N.; Silva, M.M.; Gusmão AP, H.D.; Costa, A.P.C.S.; Nepomuceno, T.C.C. Fuzzy cognitive scenario mapping for causes of cybersecurity in telehealth services. *Healthcare* **2021**, *9*, 1504. [CrossRef]
59. Shayan, S.; Kim, K.P.; Ma, T.; Nguyen, T.H.D. The first two decades of smart city research from a risk perspective. *Sustainability* **2020**, *12*, 9280. [CrossRef]
60. Kumar, S.; Biswas, B.; Bhatia, M.S.; Dora, M. Antecedents for enhanced level of cyber-security in organisations. *J. Enterp. Inf. Manag.* **2021**, *34*, 1597–1629. [CrossRef]