electronics

MDPI

Article

Detection of Fake Replay Attack Signals on Remote Keyless Controlled Vehicles Using Pre-Trained Deep Neural Network

Qasem Abu Al-Haija [1,*] and Abdulaziz A. Alsulami [2]

[1] Department of Cybersecurity, Princess Sumaya University for Technology (PSUT), Amman 11941, Jordan
[2] Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia
* Correspondence: q.abualhaija@psut.edu.jo

Abstract: Keyless systems have replaced the old-fashioned methods of inserting physical keys into keyholes to unlock the door, which are inconvenient and easily exploited by threat actors. Keyless systems use the technology of radio frequency (RF) as an interface to transmit signals from the key fob to the vehicle. However, keyless systems are also susceptible to being compromised by a threat actor who intercepts the transmitted signal and performs a replay attack. In this paper, we propose a transfer learning-based model to identify the replay attacks launched against remote keyless controlled vehicles. Specifically, the system makes use of a pre-trained ResNet50 deep neural network to predict the wireless remote signals used to lock or unlock doors of a remote-controlled vehicle system. The signals are finally classified into three classes: real signal, fake signal high gain, and fake signal low gain. We have trained our model with 100 epochs (3800 iterations) on a KeFRA 2022 dataset, a modern dataset. The model has recorded a final validation accuracy of 99.71% and a final validation loss of 0.29% at a low inferencing time of 50 ms for the model-based SGD solver. The experimental evaluation revealed the supremacy of the proposed model.

Keywords: artificial intelligence; cybersecurity; remote control; fake signals; replay attack; deep learning; ResNet50; transfer learning

Citation: Abu Al-Haija, Q.; Alsulami, A.A. Detection of Fake Replay Attack Signals on Remote Keyless Controlled Vehicles Using Pre-Trained Deep Neural Network. *Electronics* **2022**, *11*, 3376. https://doi.org/10.3390/electronics11203376

Academic Editors: Juan M. Corchado, Byung-Gyu Kim, Carlos A. Iglesias, In Lee, Fuji Ren and Rashid Mehmood

Received: 4 October 2022
Accepted: 18 October 2022
Published: 19 October 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

1. Introduction

Rapid technological advancement allows the usage of computers and wireless devices with modern vehicles to increase customer security and convenience [1]. Keyless systems are considered a vital component of modern vehicles because they perform several functions, such as locking and unlocking the doors, opening and closing the trunk, and starting the engine [2]. The first remote keyless system used with a vehicle was introduced in 1982 [3]. Keyless systems have replaced the old fashion methods of inserting physical keys into the keyhole to unlock the door, which are inconvenient and easily exploited by threat actors [4]. Generally, there are two types of keyless systems, remote keyless entry (RKE) and passive keyless entry (PKE) [5]. Both keyless systems use the technology of radio frequency (RF) as an interface to transmit signals from the key fob to the vehicle. In the RKE system, the driver needs to press the fob button to send the intended command to the vehicle, i.e., unlock the door. Then, the authenticated protocol is used to validate the vehicle's owner [6]. However, the PKE system does not require drivers to press any button. Still, once the fob becomes close to the proximity distance of the vehicle, an authentication protocol establishes before the automated command is sent to the vehicle [7].

The early keyless system was developed based on static code sent from the key fob to the receiver, which is easily compromised by a thread actor who intercepts the transmitted signal and performs a replay attack [6]. A replay attack is also called a playback attack, when authorized legitimated data are captured and copied during transmission

by a threat actor to be repeated for fraudulent purposes, as illustrated in Figure 1 [8]. Rolling codes attempted to overcome this issue by producing a changed code based on a counter. Therefore, a new code is generated every time the keyless system is used; however, a rolling code is also suspectable to different types of replay attacks [9]. Due to the vulnerability of the keyless systems, threat actors can exploit them to steal vehicles or owner belongings. For example, United Kingdom police broadcasted a video illustrating how a threat actor can steal a vehicle within 1 min using relay devices [10]. Furthermore, increasing the number of installed communication technologies, such as keyless, WiFi, and Bluetooth systems in a vehicle, leverages drivers' and passengers' convenience and enables fast transformation into automation. However, this opens the gate to more opportunities for establishing cyberattacks [11].

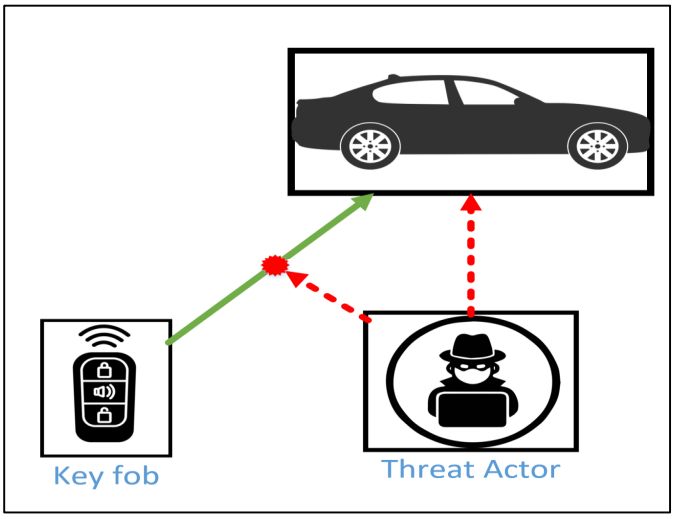

Figure 1. Replay Attack Targeting keyless system.

The theory of the CIA triad model, which is the conditionality, integrity, and availability, can be used to measure the security level of a system [11]. Conditionality assures that data will not be accessed by unauthorized users, programs, or procedures. To guarantee that only authorized users can access the data, sufficient control mechanisms are used. Integrity has much to do with reliability; thus, unauthorized users must not modify the data. Finally, availability ensures that data must be available and not prevented when users need it [12].

Recently, researchers used different authentication techniques to mitigate and prevent threats on keyless systems, such as authentication using smartphones [13], authentication using bioinformatics [14], and authentication using blockchain [15,16]. However, this field still needs more research to investigate how to resist malicious activities on keyless systems.

This research uses transfer learning to enhance the security of remote keyless vehicle systems. Transfer learning is a pre-trained neural network that uses existing, generalizable knowledge from previous related tasks to learn a new task with a small amount of data [17]. This research proposed a deep transfer learning based on the ResNet50 deep neural network to overcome fake replay attack signals targeting remote keyless systems of modern vehicles. Our pre-trained model distinguishes fake signals caused by a threat actor and true signals caused by a vehicle's owner. We evaluated our model using the KeFRA 2022 dataset. In addition, we measured the performance of our model using accuracy, precision, F1-score, and recall, and we found that our model scored 99.71% for all metrics. This reveals the superiority of the proposed model over the existing models in the same area of study. For the novelty of using transfer learning in our research, in addition to the use of signal frequency images describing the real and fake signals, we have noticed a limitation in research on applying transfer learning to enhance the security of

remote keyless systems on vehicles. Although transfer learning shows its power in detecting/classifying cyberattacks in security sectors, there is still a need to use it with remote keyless systems, as we did in this research. In addition, our ResNet50-based model scored high-performance indicators compared with the most recent research models in the detection/classification of cyberattacks in the security field.

The rest of this paper is arranged as follows: Section 2 summarizes the related research work. Section 3 elaborates on the proposed detection system modeling and architecture. Section 4 provides comprehensive experimental results and discussion. Finally, Section 5 concludes the research article.

2. Literature Review

Modern vehicles are designed to rely on the keyless system when starting the engine and unlocking and locking doors instead of using traditional keys for the convenience of vehicle owners. However, there is a cost to using such technology because keyless systems are susceptible to various attacks, such as replay, relay, and man-in-the-middle (MITM) attacks [18].

Cryptography could be used to eliminate replay attacks, as the authors of [6] developed an encryption algorithm to prevent replay attacks on remote keyless vehicles. Their model was built based on asymmetrical and hashing methods to allow authentication between the vehicle and the owner. The authors of [19] also used cryptography methods to mitigate replay attacks in remote keyless systems by enhancing the performance of the KeeLoq algorithm. However, the authors of [4] illustrated that encryption techniques are insufficient for authentication, and there is a need for more security layers; therefore, they proposed the HODOR technique to detect attacks targeting keyless systems using a classifier algorithm they implemented. The vehicle owner needs to hold the door handle, and radio frequency fingerprinting is used to detect unauthorized commands based on collected features.

To enhance the authentication mechanism of the remote keyless system, [20] introduced an authentication protocol based on challenge-response pairs integrated with the RKE system. Therefore, the command sent from the key fob to the vehicle is first verified then a challenge is computed. Next, the computed challenge is sent from the vehicle to the key fob. Finally, the key fob computes the challenge and sends the response to the vehicle that verifies the response and executes the command.

Smart vehicles that use a controlled area network (CAN) for communication purposes are vulnerable to cyberattacks since CAN protocol has limited security mechanisms to provide comprehensive, secure communication [21]. There are several reasons for CAN vulnerabilities of cyberattacks, such as that the exchanged messages between the physical components are not encrypted, and all components are connected with the same CAN bus; therefore, the same message can be broadcasted to all components [21]. Aldhyani et al. [22] implemented a deep learning model that integrates a convolution neural network (CNN) with long short-term memory (LSTM) to defend the self-driving car network from various cyberattacks, such as packets, replaying, and spoofing attacks. The authors evaluated their model using a collected dataset from real network traffic of CAN that was injected with the cyberattacks above. They achieved 97.30% using the classification accuracy metric.

The authors of [23] proposed a biometric method to enhance the security of the keyless system. Their model integrates two security levels: face recognition and fingerprint. In the face recognition phase, the driver's face is captured using a camera attached to the vehicle door, and a spoofing algorithm is used to perform anomaly detection to identify the legitimacy of the driver. In the fingerprint phase, the driver's fingerprint is scanned using another spoofing algorithm; therefore, if the fingerprint is confirmed, the driver can access the vehicle. However, this model has a challenge in finding the perfect position of the camera used for face recognition.

Blockchain is a recent technology that can also be used to enhance the security of the keyless system. It is an advanced technology built to increase the security of pair-to-pair networks. Blockchain is considered a decentralized distributed system. It is a well-known technology used to secure transactions in the cryptocurrency market, such as Bitcoin [24]. The authors of [8] proposed an authentication model based on a Blockchain system. Basically, the transmitted data between the key fob and the vehicle is encrypted using hash algorithms. The authors compared secure hash algorithms: SHA-1, SHA-256, SHA-512, and message digest (Md5).

Machine learning (ml) techniques can be used to mitigate the impacts of attacks targeting keyless systems. The authors of [25] implemented a data-intensive model using ml to prevent relay attacks on the PKE system. The authors developed their models based on artificial neural networks (ANN), K-nearest neighbors (KNN), support vector machines (SVM), and decision trees. They trained their ml algorithms using the following features: date, time, elapsed time, location, type of day, key fob signal strength, and key fob acceleration. According to the authors, the decision tree outperformed the other ml algorithms and reached 99% accuracy based on the classification accuracy metric.

Most keyless systems use radio-frequency identification (RFID) technology as an interface to transmit a command from the key fob to the vehicle. However, RFID could be vulnerable to various malicious attacks, such as relay attacks. Therefore, the authors of [26] used several security features to proximity identify the location of the vehicle based on contextual information, such as global positioning system (GPS) coordinates, receiving signal strength indicator (RSSI), and WiFi access points. Therefore, their technique helps to overcome the vulnerability of RFDI, which can be compromised using a variety of attacks, such as relay attacks. Moreover, the authors of [10] proposed a context detection method to detect relay attacks on passive keyless entry systems using a smartphone. Therefore, a secure connection between the vehicle owner's smartphone and the vehicle is established using Bluetooth low energy (BLE) technology to track the location of the vehicle's owner and determine their proximity to the vehicle, then evaluate the legality of the owner.

The authors of [27] proposed a timestamp-based method to defend remote keyless systems from replay attacks. The authors enhanced the rolling-code algorithm by adding a timestamp factor (time in seconds) to the generated code. Therefore, each time the rolling-code algorithm generates code, the time in seconds is added as a parameter with the generated code. Even though a threat actor captures the generated code, they still need to know when the code was generated. However, this method requires the clock to be synchronized between the sender and receiver. Table 1. lists a summary of the most recent proposed solutions to leverage the security of the keyless system.

Table 1. Summary of recently proposed solutions for the security of the keyless system.

Research	Proposed Solution
[6] Poolat et al.	Asymmetrical and hashing methods
[19] Madhumitha et al.	Enhanced KeeLoq algorithm
[4] Kyungho et al.	HODOR
[20] Jinita et al.	Challenge-response pairs
[22] Aldhyani et al.	CNN and LSTM
[23] Béatrix-May et al.	Biometric
[8] Husain et al.	Blockchain
[25] Usman et al.	ML
[26] Juan et al.	Contextual information
[10] Jing et al.	Contextual information
[27] Greene et al.	Timestamp-based

3. Detection System Modeling

In this research, we aim to develop a new detection system for the replay attack signals (false signals) over the remote-controlled keyless entry used to lock or unlock the vehicle doors. The overall system modeling architecture is provided in Figure 2. According to the figure, the system can mainly be decomposed into three subsystems: (a) image dataset and preprocessing subsystem, (b) transfer learning subsystem, and (c) assessment and detection subsystem.

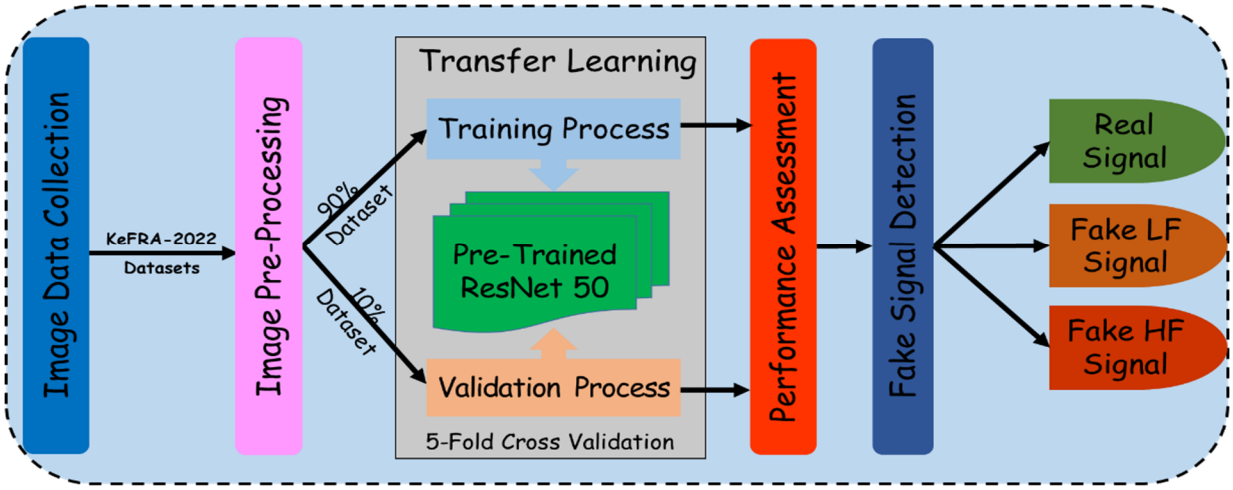

Figure 2. The overall architecture for the proposed detection system.

3.1. Image Dataset and Preprocessing Subsystem

In this research, we have used the KeFRA-2022 Image dataset [28] of the Ad hoc communication signals of remote keyless entry (RKE) used to lock or unlock doors distantly. Specifically, a key fob, a small handheld remote-control device that controls a remote keyless entry system of a 2016 model vehicle, was used to produce the real experimentation signals collected in the dataset (110 samples, known as real signal). Moreover, a Hack RF-SDR, an open-source remote-control hardware platform that acts as an attacker, was used in a replay attack mode to produce the fake signals in the replay scheme. Two types of fake signals were produced: Fake_Signal_High_Gain (110 samples, resulting from configuring the Hack RF-SDR with high radio frequency (RF)) gain, and, Fake_Signal_Low_Gain (120 samples, resulting from configuring the Hack RF-SDR with low radio frequency (RF). Finally, the dataset examples are modeled as RGB bitmap images of 1288 X 421 pixels with 3-channels-pixel.

Figure 3 demonstrates three samples of the KeFRA-2022 Image dataset: (A) real remote signal, (B) Fake_Signal_Low_Gain, and (C) Fake_Signal_High_Gain. The differences between the signals are very deep, requiring a powerful deep neural network such as the ResNet50 CNN used in this research.

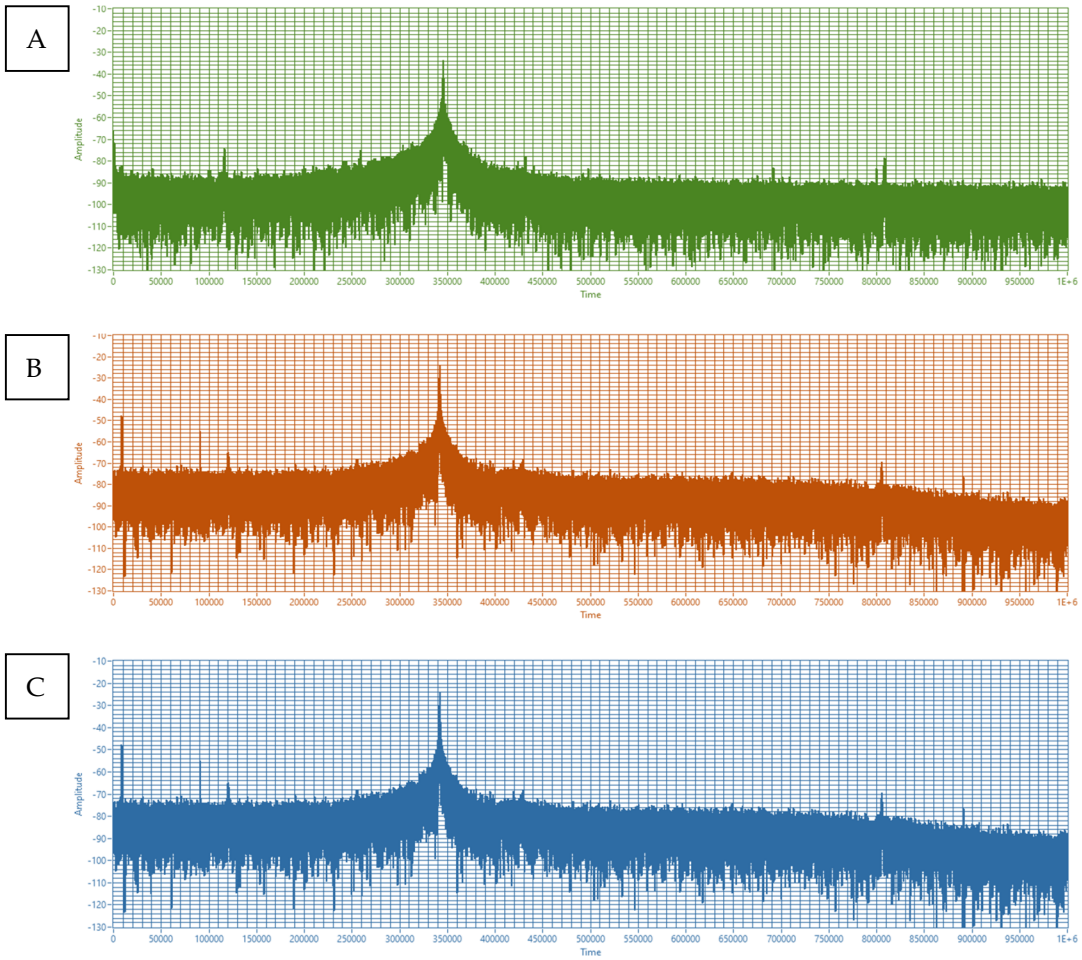

Figure 3. Three samples of the KeFRA-2022 Image dataset: (**A**) real remote signal (Green), (**B**) Fake_Signal_Low_Gain (Orange), and (**C**) Fake_Signal_High_Gain (Blue).

Then, once the dataset is acquired, it undergoes a number of image preprocessing stages before it can be handled by the deep neural network at the next subsystem. These include:

- **Image Resizing**: All images have been resized to accommodate the input layer of pre-trained ResNet50 CNN. Therefore, the original size of the image samples, 1288 × 421 × 3, was downsized to 224 × 224 × 3;
- **Image augmentation**: This is a process concerned with applying simple and complex image transformations in order to increase the number of data samples in the dataset. Several image transformations were applied here, including (1) random reflection axis X, (2) random reflection axis Y, (3) random image rotation using min-max degrees, (4) random image rescaling using min-max factors, (5) random horizontal translation using min-max pixels, and (6) random vertical translation using min-max pixels. Since the number of images in the accumulated dataset is relatively small, with a small frequency for each class (340 images in total distributed in 110 images for the real signal, 110 images for the fake signal with high gain, and 120 images for the fake signal with low gain). Therefore, the images in the dataset have undergone the image argumentation phase to increase the number of images and improve the learning process of the employed classifier. The images were subject to six transformation processes, including (1) random reflection axis X, (2) random reflection axis Y, (3) random image rotation using min-max degrees, (4) random image rescaling using min-max factors, (5) random horizontal translation using min-max pixels, and (6) random vertical translation. This, in turn, has resulted in increasing the frequency of images for each class by a factor of 6. The following

figure shows the frequency graph image before and after augmentation. Figure 4 shows the frequency graph image of the classes contained in the dataset before and after applying image argumentation processes. The total number of images before and after the data argumentation (using 6 different transformations): (1) before the data argumentation, 340 images, and (2) after the data argumentation, 2040 images;

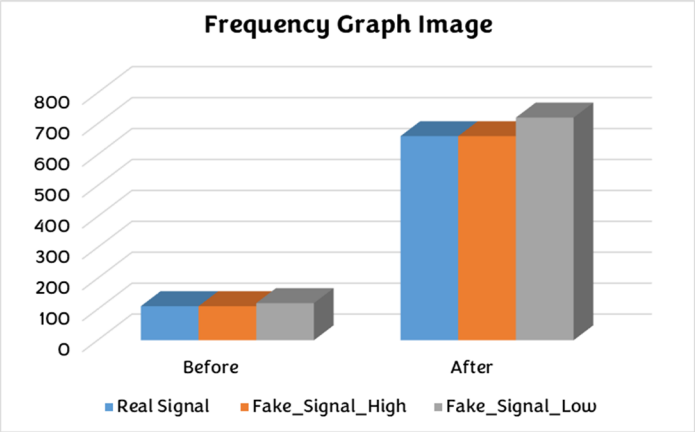

Figure 4. The frequency graph image of the classes contained in the dataset before and after applying image argumentation processes.

- **Image Shuffling**: All images have been randomly redistributed before starting the learning process. This is necessary to ensure that each data sample creates an "independent" change in the model without being biased by the same points [29];
- **Image Distribution**: Finally, the dataset is divided into two separate datasets: (A) training dataset (90% of the images in the dataset) and (B) testing dataset (10%) of the images in the dataset). Five-fold cross-validation (CV) was implemented to test the effectiveness of the learning model and provide a re-sampling procedure to evaluate a model in case of limited data [30]. The valuation process is repeated five times using different random validation sets (fold) using a Five-fold CV. For each validation experiment, the performance is evaluated and recorded for the specific fold. Finally, the overall performance is evaluated as the average of all experiments (i.e., five folds). To ensure the random distribution for splitting data for training and testing, we use the DivideRand algorithm [31] implemented in MATLAB to divide targets into sets using random indices. DivideRand takes the number of targets to divide up, the ratio of vectors for training, the ratio of vectors for validation, and the ratio of vectors for testing, and returns the training indices, the validation indices, and the test indices.

3.2. Transfer Learning Subsystem

In this subsystem, we leverage the transfer learning technology to gain the benefits of the pre-trained deep convolutional neural networks. In transfer learning, a model developed for a task is reused as the starting point for a model on a second task. However, fine-tuning is required for the learning hyperparameters employed by pre-trained CNN to accommodate the new learning tasks [32]. Figure 5 shows the main idea of the transfer learning technique where the core part of network A (transfer parameters) is frozen and transferred to network B. The adjustment will be performed at the hyperparameters of the output fully connected layer that is tuned to accommodate the output for the new classification task (at network B).

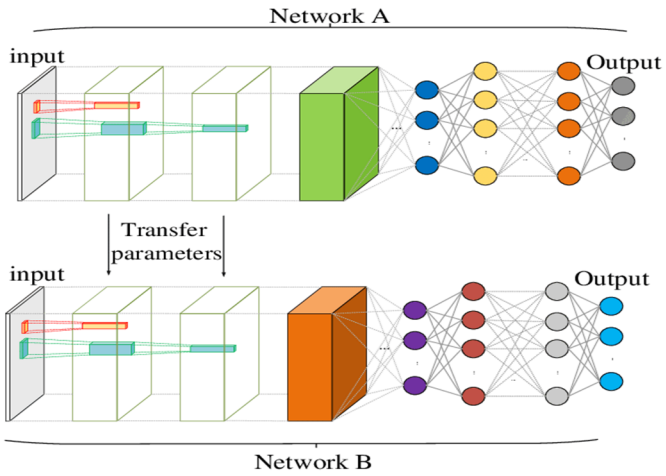

Figure 5. Demonstration of transfer learning technique where all layers in networks A and B are identical except for the output layer, which is tuned to fit the new classification task.

In this work, we are utilizing the transfer learning of ResNet-50 CNN, which is pre-trained on the ImageNet dataset [33] after preprocessing the collected dataset to fit into the input layer of ResNet50. Fine-tuning for the network hyperparameters at the output layer is performed to accommodate the output of our three-classes classification task in this research (real signal, fake signal high gain, and fake signal low gain). Figure 6 demonstrates the developmental stages of the proposed learning model subsystem. Once the images are preprocessed and resized to 224 × 224 × 3, they are fed through the 50 frozen residual layers. Finally, proper tuning and other learning parameters are performed for the fully connected layer and classification layer.

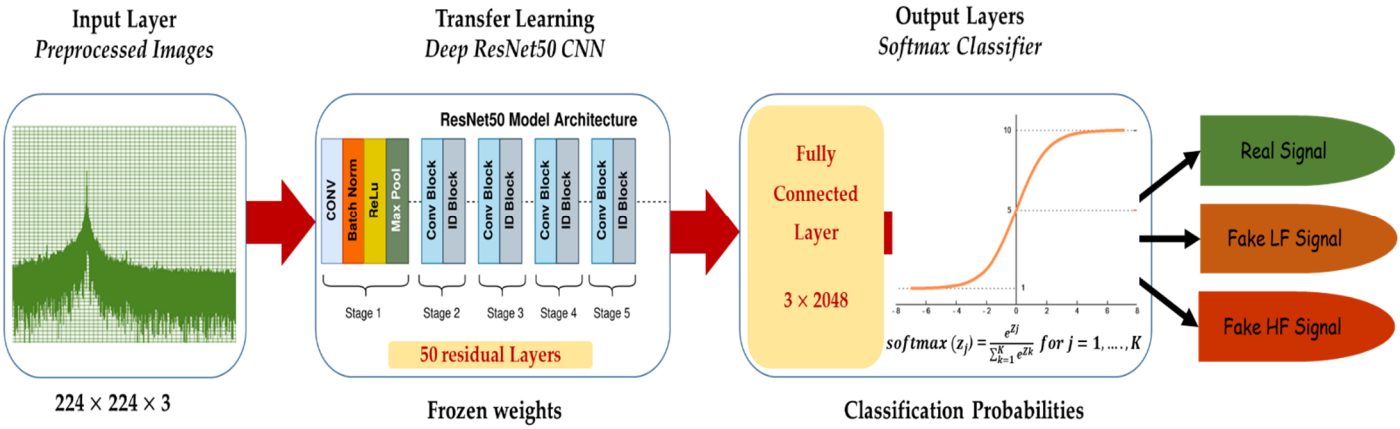

Figure 6. Demonstration of developmental stages of the proposed learning model subsystem.

The other learning hyperparameters are configured as follows: the learning rate (α = 0.001), solver = {Adam optimizer; stochastic gradient descent (SGD) optimizer; root mean squared propagation (RMSProp) optimizer}, maximum number of epochs = 100 each with 38 iterations (total number of iterations = 3800), and mini-batch size = 8. Moreover, the models were developed, trained, and tested using MATLAB R2021b system on a high-performance commodity laptop with Windows 11 professional, Intel I7 of 11th Gen, 16 GB of memory, and NVIDIA GeForce RTX 3050 Ti GPU.

3.3. Assessment and Detection Subsystem

Like any other learning-based system, its performance must be assessed to ensure its effectiveness and readiness for deployment and operation in a real-time environment to

provide the intended functionality. Several common evaluation factors are commonly used to assess the performance of the learning-based models, such as the model's positive and negative rates (confusion matrix analysis), the model accuracy, the model precision, the model sensitivity (recall), and the model inferencing time (detection time, generated by the simulation platform). These factors have been extensively defined and described in the literature [34].

Finally, once the system is assessed and assured to reach the intended performance in order to provide the intended detection functionality, it can be deployed to perform a real-time detection process for the replay attacks targeted against the remotely accessed locking control system for the vehicle. In this work, the deployed system should be able to receive any signal and provide the proper classification for every remote signal as a real signal (by the key fob) or a fake signal (by the attacker), which is with low or high-frequency gain.

4. Experimental Results and Discussion

In this section, we provide results from evaluating the proposed overall 3-class detection system to identify the replay attacks launched against remote keyless controlled vehicles. In Figure 7, we demonstrate the 3-class confusion matrix analysis for the proposed transfer learning based ResNet50 model using three optimizers (solver) techniques: (A) using SGD solver, (B) using Adam solver, and (C) using RMSProp solver. The matrix considers the three types of remote signals: the real signal (non-malicious), the fake signal with high frequency (HF/malicious), and the fake signal with low frequency (LF/malicious). According to the figure, the model-based SGD solver recorded 339 true classifications (99.71%) and 1 false classification (0.29%), the model based-Adam solver recorded 320 true classifications (94.12%) and 20 false classifications (5.88%), and the model-based-RMSProp solver recorded 270 true classifications (79.41%) and 70 false classifications (20.59%).

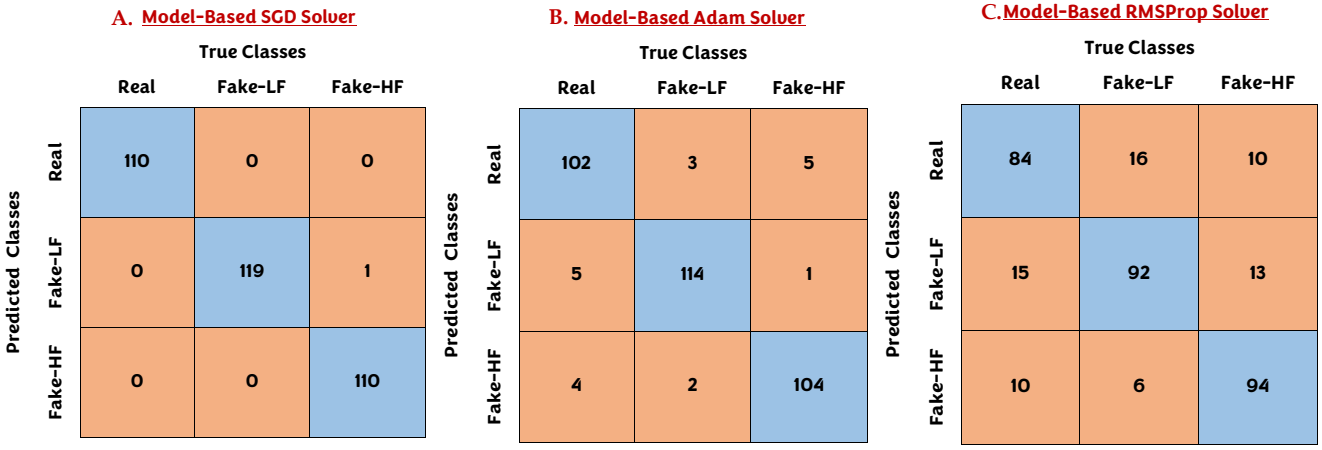

Figure 7. Confusion matrix analysis for the proposed transfer learning based ResNet50 model using three optimizers (solver) techniques: (**A**) using SGD solver, (**B**) using Adam solver, and (**C**) using RMSProp solver.

Furthermore, Table 2, along with Figure 8, compares the three models (model-based SGD solver, model based-Adam solver, and model-based- RSMProp solver) in terms of seven performance indicators, including the number of correctly classified samples (NCC = TP + TN), the number of Incorrectly classified samples (NIC = FP + FN), the overall detection accuracy (ACC), the overall detection precision (PRC), the overall detection sensitivity/recall (RCL), the overall detection harmonic mean/F1 Score (F1S), and the overall detection (inferencing) overhead/time (INF). Based on the results obtained from the confusion matrix and the other evaluation metrics, it can be clearly seen that the model-based SGD solver outperforms other models in all the performance factors. However,

inferencing time shows very close values as it is mainly affected by a deep convolutional neural network (i.e., ResNet50) with a slight difference impacted by changing the solver algorithm.

Table 2. Summary of performance indicators of the three model-based techniques.

Model	NCC	NIC	ACC	PRC	RCL	F1S	INT
SGD Based Model	339	1	99.71%	99.71%	99.71%	99.71%	50 ms
Adam Based Model	320	20	94.11%	94.14%	94.12%	94.12%	52 ms
RSMProp Based Model	270	70	79.41%	79.65%	79.39%	79.45%	55 ms

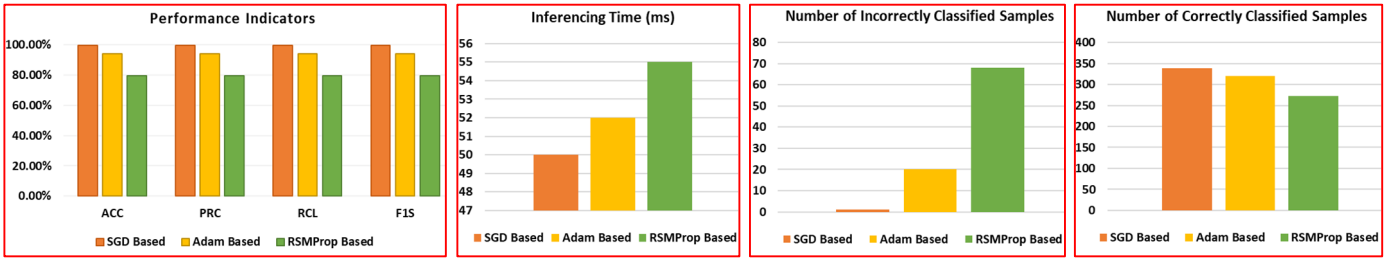

Figure 8. Comparing the performance indicators of the three model-based techniques.

Based on the earlier evaluation and analysis, the model-based SGD solver is selected to be deployed in the final detection model. Therefore, the next results will focus on the detection of fake replay attack signals on remote keyless controlled vehicles using pre-trained ResNet50 CNN with the SGD solver technique. Moreover, Figure 9 illustrates the classifier performance plots for the loss function and classification accuracy trajectory for 100-epochs training using the SGD solver technique. According to the figure, both evaluation metrics (i.e., loss function and classification accuracy) consistently advance along with the evolving training epochs. Nevertheless, the detection loss function showed a decreasing tendency toward the minimum loss (i.e., zero MSE). In contrast, the detection accuracy function exhibits an increasing tendency toward the highest possible detectability (i.e., 100% accuracy). Moreover, both functions appeared to be saturated after almost 75 training epochs recording an error value of ≤0.5% and an accuracy rate of ≥99.5%.

While the intrusion detection systems for automated controlled vehicles are widely investigated and studied in the literature, to the best of our knowledge, this is the first work that focuses mainly on the detection of fake signals over the remote-controlled electronic access system of a model vehicle. The majority of state-of-the-art detection models focused on intrusion/cyberattack detection on the whole control system in the vehicles (such as [35–37]) or the controller area network (CAN) for connected vehicles (such as [38–40]). Nevertheless, there are some other related models that, to some extent- provide comparable detection systems to our proposed system. Table 3 presents a comparative analysis of the proposed and other state-of-the-art models in the same area of study to provide more insights into the solution approach. The table compares the models in terms of learning approach, number of classes, detection accuracy, detection precision, and detection recall. Furthermore, the table considers the comparison of the proposed model with six other models, including (1) Roh et al. model [41], which is implemented using a hybrid deep learning technique comprising the use of the convolutional neural network (CNN) along with the long, short-term memory (LSTM); (2) Tariq et al. model [42], which is called CANTransfer and implemented using the transfer learning technique of deep cascaded model comprising several CNN-LSTM units; (3) Javed et al. model [43], which is called CANintelliIDS and implemented using convolutional attention incorporated with gated

recurrent neural network (GRU); (4) Song et al. model [44], which is implemented using a deep convolutional neural network (DCNN); (5) Kang et al. model [45], which is implemented by incorporating the deep neural networks with deep belief networks (DNN-DBN); and finally, (6) Seo et al. model [46], which is called GIDS-CNN (Generative Adversarial Nets IDS -CNN). According to the table, the proposed model outperforms others in several performance indicators.

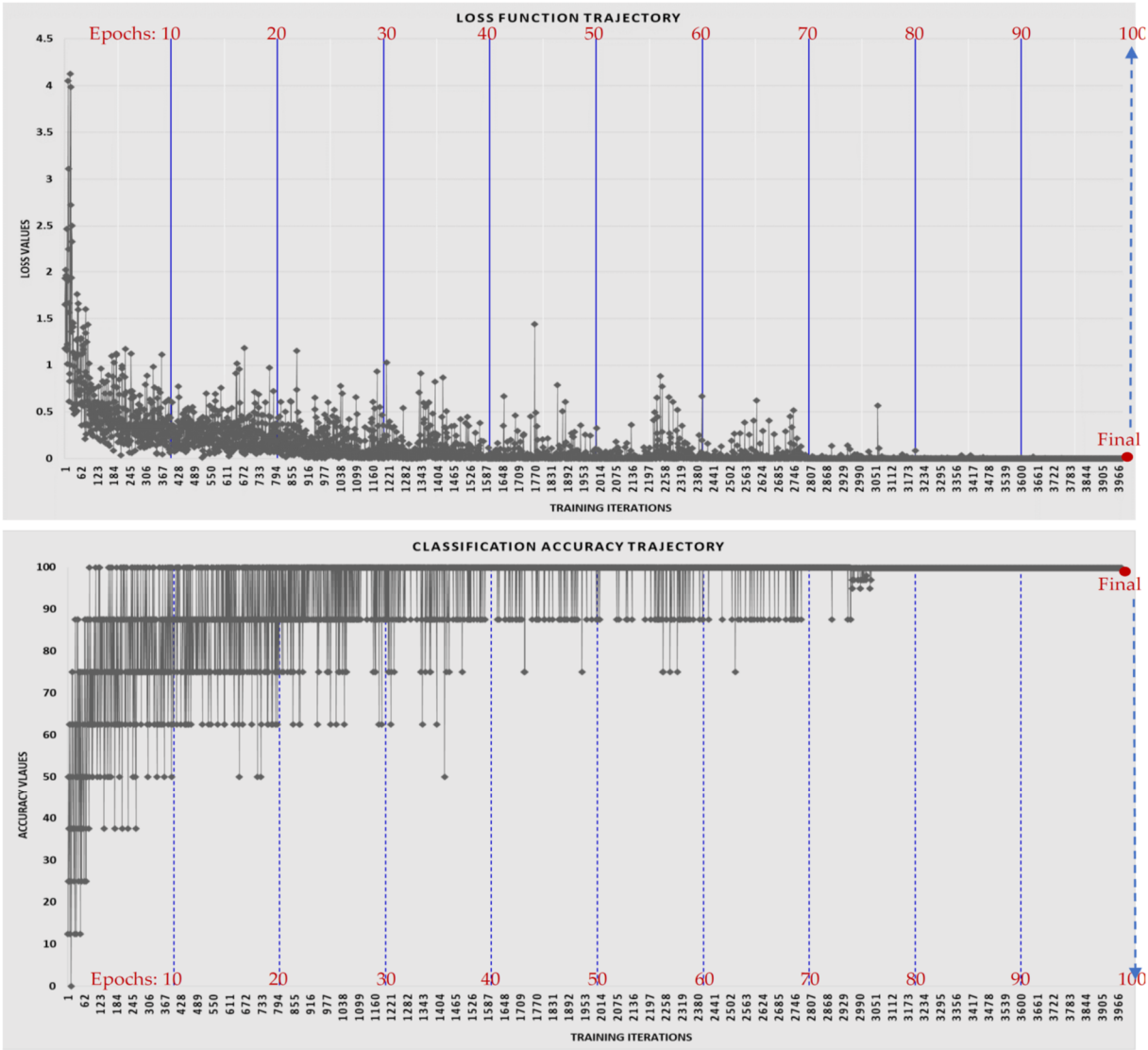

Figure 9. Loss function trajectory vs. classification accuracy trajectory for 100-epochs training using SGD solver technique.

Table 3. Comparing the performance of our proposed model with existing detection models.

Research	ML Model	Number of Classes	Accuracy	Precision	Recall
Roh et al. [41]	CNN-LSTM	Two	92.03%	-	-
Tariq et al. [42]	CANTransfer	Two	-	99.00%	91.00%
Javed et al. [42]	CANinyelliIDS	Two	-	93.69%	93.91%
Song et al. [44]	DCNN	Two	-	87.97%	88.97%
Kang et al. [45]	DNN-DBN	Three	98.00%		
Seo et al. [46]	GIDS-CNN	Three	98.00%	98.00%	98.00%
Proposed method	ResNet50 CNN	Three	99.95%	99.71%	99.71%

5. Conclusions and Remarks

An autonomous intelligent detection system to recognize the replay attacks (playback attacks) over a remote keyless entry (RKE) of a remotely controlled vehicle has been suggested, implemented, and evaluated in this paper. The proposed system leverages the power of transfer learning techniques for the ResNe50 deep convolutional neural network (DCNN) that is pre-trained on the ImageNet dataset. Fine-tuning for the output and classification layers has been performed to fit the new classification task. Moreover, several image preprocessing processes have been implemented and performed before the input layer of ResNet50 to ensure the readiness of input images for the learning and validation process via DCNN. The system aims to uncover the replay attack signals (fake signals) at low and high gain with a fast and high detection rate. The experimental evaluation reported high-performance metrics for the proposed detection system recording a 99.71% of classification accuracy at a very low detection overhead. Furthermore, the comparison with other existing models indicated the supremacy of the proposed detection system in several performance factors.

Author Contributions: Conceptualization, Q.A.A.-H.; methodology, Q.A.A.-H.; software, Q.A.A.-H. and A.A.A.; validation, Q.A.A.-H. and A.A.A.; formal analysis, Q.A.A.-H.; investigation, Q.A.A.-H. and A.A.A.; resources, Q.A.A.-H.; data curation, Q.A.A.-H. and A.A.A.; writing—original draft preparation, Q.A.A.-H. and A.A.A.; writing—review and editing, Q.A.A.-H. and A.A.A.; visualization, Q.A.A.-H. and A.A.A.; funding acquisition, Q.A.A.-H. and A.A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: For more information about the data used in this study, we refer the readers to the following link: https://data.mendeley.com/datasets/zkstkgkxvd (accessed on 11 June 2022).

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

References

1. Lennert, W.; Benedikt, G.; Bart, P. My other car is your car: Compromising the Tesla Model X keyless entry system. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* **2021**, *2021*, 149–172.
2. Kyle, G.; Deven, R.; Henry, D.; Quamar, N.; Khair, A.S.; Vijay, D. A Defense Mechanism Against Replay Attack in Remote Keyless Entry Systems Using Timestamping and XOR Logic. *IEEE Consum. Electron. Mag.* **2021**, *10*, 101–108.
3. Marin, E.; Ashur, T.; Gierlichs, B.; Preneel, B. Fast, Furious and Insecure: Passive Keyless Entry and Start Systems in Modern Supercars. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* **2019**, *2019*, 66–85.
4. Kyungho, J.; Wonsuk, C.; Hoon, L.D. Hold the Door! Fingerprinting Your Car Key to Prevent Keyless Entry Car Theft. *arXiv* **2020**, arXiv:2003.13251.
5. KiranRaj, K.S.; Ananya, C.; Ratan, S.; Ajeenky. Analysing Remote Keyless Entity Systems. *Int. J. Res. Anal. Rev.* **2019**, *6*, 136–138.
6. Poolat, P.R.; Biplab, S. An Authentication Mechanism for Remote Keyless Entry Systems in Cars to Prevent Replay and RollJam Attacks. In *IEEE Intelligent Vehicles Symposium (IV)*; IEEE: Aachen, Germany, 2022.
7. Abu Al-Haija, Q.; Al Badawi, A. High-performance intrusion detection system for networked UAVs via deep learning. *Neural Comput. Appl.* **2022**, *34*, 10885–10900. https://doi.org/10.1007/s00521-022-07015-9.
8. Husain, R.; Khan, R.; Tyagi, R.K. Novel Technique for Secure Keyless Car Authentication using Block-Chain System. *I-Manag. J. Comput. Sci.* **2020**, *8*, 12020.
9. Tobias, V.C.; Carlo, M.; Veelasha, M.; Erik, P. *Security Analysis of Aftermarket Remote Keyless Entry Systems for Consumer Vehicles*; Radboud University Nijmegen: Nijmegen, The Netherlands, 2020.
10. Jing, L.; Yabo, D.; Shengkai, F.; Haowen, Z.; Duanqing, X. User Context Detection for Relay Attack Resistance in Passive Keyless Entry and Start System. *Sensors* **2020**, *20*, 4446.
11. Al-Haija, Q.A.; Alsulami, A.A. High-Performance Classification Model to Identify Ransomware Payments for Heterogeneous Bitcoin Networks. *Electronics* **2021**, *10*, 2113. https://doi.org/10.3390/electronics10172113.
12. De la Cruz, J. E. C.; Romero, G.C.A.; Delgado, C.C. Open VProxy: Low-Cost Squid Proxy Based Teleworking Environment with OpenVPN Encrypted Tunnels to Provide Confidentiality, Integrity and Availability. In Proceedings of the IEEE Engineering International Research Conference (EIRCON), Lima, Peru, 21–23 October 2020.

13. Paul, S.; Kai, J.; Christian, Z.; Christof, P. Securing Phone as a Key Against Relay Attacks. In Proceedings of the 18th Escar Europe: The World's Leading Automotive Cyber Security Conference (Konferenzveröffentlichung), Berlin, Germany, 11–12 November 2020.
14. Asadullah, A.; Karthik, P.; Sharath, D.; Mohammad, A.; Sourik, M.; Chidambaram, V. *Mechanism to Identify Legitimate Vehicle User in Remote Keyless Entry System*; SAE Technical Paper; SAE International: Warrendale, PA, USA, 2022.
15. Pouyan, R.; Abdollah, K.-F.; Morteza, D.; Tao, J.; Wencong, S. Ultra-Lightweight Mutual Authentication in the Vehicle Based on Smart Contract Blockchain: Case of MITM Attack. *IEEE Sens. J.* **2020**, *21*, 15839–15848.
16. Ibrahim, R.F.; Abu Al-Haija, Q.; Ahmad, A. DDoS Attack Prevention for Internet of Thing Devices Using Ethereum Blockchain Technology. *Sensors* **2022**, *22*, 6806. https://doi.org/10.3390/s22186806.
17. Chenjing, C.; Shiwei, W.; Youjun, X.; Weilin, Z.; Ke, T.; Qi, O.; Luhua, L.; Jianfeng, P. Transfer Learning for Drug Discovery. *J. Med. Chem.* **2020**, *63*, 8683–8694.
18. Juan, W.; Karim, L.; Mohammad, Z. CSKES: A Context-Based Secure Keyless Entry System. In Proceedings of the EEE 43rd Annual Computer Software and Applications Conference (COMPSAC), Milwaukee, WI, USA, 15–19 July 2019.
19. Madhumitha, S.S.; Rohini, P.; Arunkumar, R.; Gunasekaran, R. Effective Cryptography Mechanism for Enhancing Security in Smart Key System. In Proceedings of the Tenth International Conference on Advanced Computing (ICoAC), Chennai, India, 13–15 December 2018.
20. Jinita, P.; Lal, D.M.; Sukumar, N. On the Security of Remote Key Less Entry for Vehicles. In Proceedings of the IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Indore, India, 16–19 December 2018.
21. Emad, A.; Omer, R.; Charith, P.; Peter, B. Cyberattacks and Countermeasures for In-Vehicle Networks. *ACM Comput. Surv.* **2022**, *54*, 1–37.
22. Theyazn, H.A.; Orcid, H.; Hasan, A. Attacks to Automatous Vehicles: A Deep Learning Algorithm for Cybersecurity. *Sensors* **2022**, *22*, 360.
23. Béatrix-May, B.; Ştefan, S.I.; Claudia, P.-N.A.; Florin, P. Cyber-Physical Systems—A New Approach for Keyless Entry Systems. In Proceedings of the 23rd International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania, 26–28 May 2021.
24. Odeh, A.; Keshta, I.; Al-Haija, Q.A. Analysis of Blockchain in the Healthcare Sector: Application and Issues. *Symmetry* **2022**, *14*, 1760. https://doi.org/10.3390/sym14091760.
25. Usman, A.; Hong, S.; Awais, B.; Mamoun, A.; Alireza, J. Secure Passive Keyless Entry and Start System Using Machine Learning. Security, Privacy, and Anonymity in Computation. *Commun. Storage* **2018**, *11342*, 304–313.
26. Wang, J. A Secure Keyless Entry System Based on Contextual Information, Proquest. Ph.D. Thesis, Queen's University, Kingston, ON, Canada, 2019.
27. Kyle, G.; Deven, R.; Henry, D.; Kyle, M.; Quamar, N.; Khair, A.S. Timestamp-based Defense Mechanism Against Replay Attack in Remote Keyless Entry Systems. In Proceedings of the IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 4–6 January 2020.
28. Martinez Quintero, J.C.; Estupinan Cuesta, E.P.; Ramirez Lopez, L. *KeFRA Images: Key-fob RKE Replay Attack*; Mendeley Data: 2022. https://doi.org/10.17632/zkstkgkxvd.1.
29. Al-Haija, Q.A.; Adebanjo, A. Breast Cancer Diagnosis in Histopathological Images Using ResNet-50 Convolutional Neural Network. In Proceedings of the 2020 IEEE International IoT, Electronics and Mechatronics Conference (IEMTRONICS), Vancouver, BC, Canada, 9–12 September 2020; pp. 1–7. https://doi.org/10.1109/IEMTRONICS51293.2020.9216455.
30. Sanjay, M. Why and How to Cross Validate a Model? Importance and Types of Cross-Validation Techniques; Towards Data Science: Medium, 2018. Available online: https://towardsdatascience.com/why-and-how-to-cross-validate-a-model-d6424b45261f (accessed on 11 June 2022).
31. Abu Al-Haija, Q.; Al-Dala'ien, M. ELBA-IoT: An Ensemble Learning Model for Botnet Attack Detection in IoT Networks. *J. Sens. Actuator Netw.* **2022**, *11*, 18. https://doi.org/10.3390/jsan11010018.
32. Al-Haija, Q.A. Leveraging ShuffleNet transfer learning to enhance handwritten character recognition. *Gene Expr. Patterns* **2022**, *45*, 119263.
33. He, K.; Zhang, X.; Ren, S.; Sun, J. Deep Residual Learning for Image Recognition. *arXiv* **2015**, arXiv:1512.03385v1.
34. Abu Al-Haija, Q. Top-Down Machine Learning-Based Architecture for Cyberattacks Identification and Classification in IoT Communication Networks. *Front. Big Data* **2022**, *4*, 782902. https://doi.org/10.3389/fdata.2021.782902.
35. Alsulami, A.A.; Abu Al-Haija, Q.; Alqahtani, A.; Alsini, R. Symmetrical Simulation Scheme for Anomaly Detection in Autonomous Vehicles Based on LSTM Model. *Symmetry* **2022**, *14*, 1450. https://doi.org/10.3390/sym14071450.
36. Sarwar, A.; Hasan, S.; Khan, W.U.; Ahmed, S.; Marwat, S.N.K. Design of an Advance Intrusion Detection System for IoT Networks. In Proceedings of the 2022 2nd International Conference on Artificial Intelligence (ICAI), Islamabad, Pakistan, 30–31 March 2022.
37. Almasoud, A.S.; Eisa, T.A.E.; Al-Wesabi, F.N.; Elsafi, A.; Al Duhayyim, M.; Yaseen, I.; Hamza, M.A.; Motwakel, A. Parkinson's Detection Using RNN-Graph-LSTM with Optimization Based on Speech Signals. *Comput. Mater. Contin.* **2022**, *72*, 872–886.
38. Abdallah, R.G.; Ahmed, A.N.; Tamer, M.B. Intrusion Detection System Using Machine Learning for Vehicular Ad Hoc Networks Based on ToN-IoT Dataset. *IEEE Access* **2021**, *14*, 37–52.

39. Seonghoon, J.; Boosun, J.; Boheung, C.; Kang, K.H. Convolutional neural network-based intrusion detection system for AVTP streams in automotive Ethernet-based networks. *Veh. Commun.* **2021**, *29*, 100338.
40. Francesco, P.; Andrea, A.E.; Simone, C.; Emanuele, S. Cybersecurity in Automotive: An Intrusion Detection System in Connected Vehicles. *Electronics* **2021**, *10*, 1765.
41. Roh, H.; Oh, S.; Song, H.; Han, J.; Lim, S. Deep Learning-based Wireless Signal Classification in the IoT Environment. *Comput. Mater. Contin.* **2022**, *71*, 5717–5732.
42. Tariq, S.; Lee, S.; Woo, S.S. CANTransfer: Transfer learning-based intrusion detection on a controller area network using convolutional LSTM network. In Proceedings of the 35th Annual ACM Symposium on Applied Computing, Brno, Czech Republic 30 March 2020; pp. 1048–1055.
43. Javed, A.R.; Ur Rehman, S.; Khan, M.U.; Alazab, M.; Reddy, T. CANintelliIDS: Detecting In-Vehicle Intrusion Attacks on a Controller Area Network Using CNN and Attention-Based GRU. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 1456–1466. https://doi.org/10.1109/TNSE.2021.3059881.
44. Song, H.M.; Woo, J.; Kim, H.K. In-vehicle network intrusion detection using deep convolutional neural network. *Veh. Commun.* **2020**, *21*, 100198.
45. Kang, M.-J.; Kang, J.-W. Intrusion Detection System Using Deep Neural Network for In-Vehicle Network Security. *PLoS ONE* **2016**, *11*, e0155781. https://doi.org/10.1371/journal.pone.0155781.
46. Seo, E.; Song, H.M.; Kim, H.K. GIDS: GAN based Intrusion Detection System for In-Vehicle Network. In Proceedings of the 2018 16th Annual Conference on Privacy, Security and Trust (PST), Belfast, Ireland, 28–30 August 2018; pp. 1–6. https://doi.org/10.1109/PST.2018.8514157.