Digital Twin based Asynchronous Federated Learning enabled IDS for False Data Injection Attacks in Vehicular CPS

Sunitha Safavat and Danda B. Rawat
Department of Electrical Engineering and Computer Science
Howard University, Washington, DC, 20059, USA
{sunitha.safavat, danda.rawat}@howard.edu

2024 8th International Conference on Computer, Software and Modeling (ICCSM) | 979-8-3503-6713-3/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICCSM63823.2024.00012

***Abstract*—Cyber Physical Systems (CPS) consist of integration of cyber and physical spaces through computing, communication, and control operations. In vehicular CPS, modern vehicles with multiple Electronic Control Units (ECUs) and networking with other vehicles help autonomous driving. Vehicular CPS is vulnerable to multitude of cyber attacks, including false data injection attacks. This paper presents an Asynchronous Federated Learning (AFL) with a Gated Recurrent Unit (GRU) model for identifying False Data Injection (FDI) attacks in a VCPS. The AFL model continuously monitors the network and constructs a digital twin using the data obtained from a VCPS for intrusion detection. The proposed model is evaluated using different evaluation metrics. Numerical results show that the AFL model outperforms other existing models.**

I. Introduction

Vehicular Cyber Physical Systems (VCPS) is regarded as one of the solutions to provide better traffic efficiency, traffic safety, and improve the overall transportation system [1], [2]. However, with the massive number of connectivity of personal vehicles and the critical nature of VCPS, malicious users and cyber attackers can launch a multitude of cyber attacks [3]. The securing any CPS including VCPS has gained huge attention in recent times due to the increased number of cyber-attacks [3], [4]. False Data Injection (FDI) attack is one of the attacks used in VCPS to mislead users. There are different Intrusion Detection System (IDS) proposed for detecting attacks in VCPS networks [4], [5]. In general, signature and anomaly-based IDS are used to identify intrusions. Signature-based IDS identifies unauthorized intrusions in the network based on predefined rules or signatures of the attacks [6]. A typical anomaly-based IDS monitors the network traffic in real time and compares the output with the previously learned network traffic patterns to identify the cyber attacks within the network [7]. Alternatively while information is received from multiple vehicles, malicious data (which is not aligned with majority of the vehicles) can be discarded for further consideration. Both signature and anomaly-based IDS exhibit better performance in terms of detecting intrusions, but these techniques fail to identify new or unknown attacks. Furthermore, an IDS in VCPS needs to handle large volumes of data (approx. 25 GB of data per vehicle per hour) with a very minimum processing time to identify the intrusions in the early stage. Recently, different Machine Learning (ML) techniques, including Deep Learning (DL) have been used extensively in the design of IDS [7], [8] by overcoming the drawbacks of conventional rule-based techniques, which depend on predefined strategies, labeled data, and feature sets for performing a specific task. ML and DL models can automatically learn from the dataset and do not require any predefined strategies for detecting intrusions. However, ML algorithms require labeled data samples to identify the attacks, and their performance is affected when applied to larger datasets. On the contrary, DL models use supervised or unsupervised learning. While supervised learning in DL does require a labeled dataset, an unsupervised learning mechanism for creating a hierarchical representation of the data helps them to provide solutions for complex and dynamic security problems without requiring a labeled dataset. However, to avoid risk of privacy leakage in ML and DL models, Federated Learning (FL) is used where model parameters are shared but not the actual data [9]–[11]. Furthermore, synchronous FL can suffer from communication bottlenecks and heterogeneity of participants. To overcome these problems, we propose an asynchronous FL model for detecting unknown intrusions in heterogeneous VCPS. The main contributions of this paper are as follows:

- We propose an asynchronous FL with GRU-based IDS for identifying unknown or new intrusions, including false data injection attacks in VCPS.
- A new statistical feature extraction technique is implemented for extracting contextual features for IDS.
- A Digital Twin model is implemented to work on unlabeled data samples and learn continuously in real-time for VCPS for IDS.

The paper is further structured as follows: Section II explains the system and attack models. Section III provides the details of the digital-twin based IDS for identifying FDI attacks on a vehicular CPS. Section IV deals with the details of experimental analysis and outcomes. Section V is the conclusion, which highlights the observations.

II. System Model and Threat Model

A. System Model

A typical system model is shown in Fig. 1, which consists of Road Side Units (RSUs), the Base Station (BS), and vehicles. The RSUs cache the data from the BS and other vehicles. The architecture consists of smart data transformation and an attack detection component to detect FDI attacks in vehicles and RSUs. Vehicles (RSU is considered as a vehicle with 0

979-8-3503-6713-3/24/$31.00 ©2024 IEEE
DOI 10.1109/ICCSM63823.2024.00012

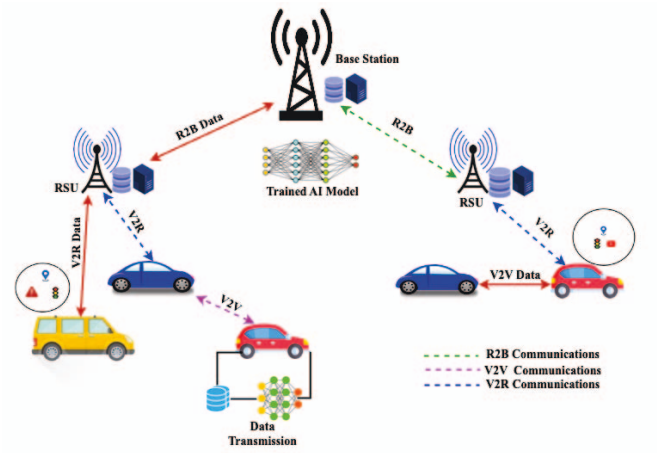

Fig. 1. Architecture of a secure VCPS model with vehicles, road side units, base stations, and Vehicle-to-vehicle (V2V) and Vehicle-to-Roadside (V2R) communications.

mph speed) use asynchronous federated learning and transform the heterogeneous data into a learned model parameters for the global learning model. Information caching and sharing are the two prominent data-aware methods in VCPS. During caching, the RSUs collect and cache data from the vehicles or BS to minimize the delivery latency to its users/vehicles. Simultaneously, during the data-sharing process, the information is shared through V2X (X being vehicle, RSU, BS) communications.

B. Threat Model

In VCPS, threat model consists of malicious users (less than 50% of all VCPS participants) manipulating the vehicular information to mislead the other users or vehicles by manipulating the information or injecting the false data in the system. Furthermore, malicious users also manipulate the actual data or learned parameters in federated learning based VCPS.

III. The Proposed Approach

The Flow diagram of the proposed approach is shown in Fig. 2. The IDS is designed to detect unknown or new intrusions in the VCPS network, which is not possible using conventional rule-based techniques. The IDS integrates the advantages of federated learning in the Digital Twin enabled VCPS to achieve the desired intrusion detection performance. Unlike traditional FL, the asynchronous FL used in this paper updates the model continuously based on the responses obtained from the devices without waiting to receive learning model parameters from all precipitants. The expected accuracy is within the tolerable limit, parameters reported by participants in FL are considered for updating global model, otherwise received parameters are considered as malicious ones and discarded for global model. This helps the model to access updated information about the network behavior and combats the potential FDI attacks either in VCPS data in each participant or in learned parameters for FL. Furthermore, the Digital Twin Model (DTM) generates adversarial samples for training the model, and this optimizes the size and volume of the training data. The DTM is considered as the virtual representation of the VCPS in Metaverse [12] form and VCPS is susceptible to adversarial attacks. For example, hackers mounted a two inch piece of tape in front of 35 mph road sign which fooled the Self driving Tesla car's camera and made the Tesla car accelerate by 50 miles per hour [13]. The generation of adversarial examples for VCPS data using DTM and the Digital Twin Capability (DTC) helps make the learning models robust. There are two factors that motivated this research to design a digital twin-based IDS for attack detection. Firstly, the model can be trained in an unsupervised manner without requiring any previous knowledge about the spatio-temporal distribution and statistical characteristics. Secondly, the concept of federated learning is effectively utilized to learn the nonlinear representation of the VCPS data and share the sensitive information through learned model parameters (instead of actual data) with multiple entities without compromising privacy. The vehicular CPS model is combined with the digital twin model, which can learn from historical and real-time data to identify FDI attacks. Next, the generation of DTM is given below.

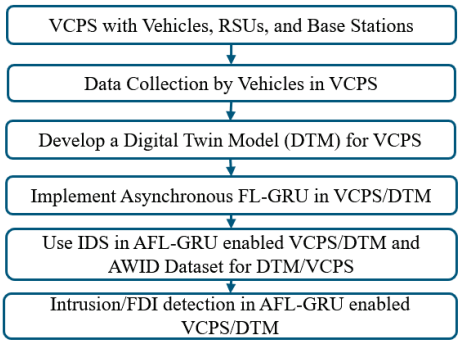

Fig. 2. The Flow diagram of the proposed approach

A. Digital Twin Model

In general, the DTM is created using a finite Time Automaton (TA) approach and is generated manually using the domain knowledge of the experts [14]. The formation of TA is represented using a tuple $A = (U, T, \delta)$, where these terms represent a finite set of states, transitions, and transition timing constraints in VCPS, respectively. In this work, each state in U i.e., $(u \subseteq U)$ is considered to be an observed state and the values obtained from sensors and actuators are included in the set defined as; $u = [u_{s1}, u_{s2}, u_{s3}, \ldots\ldots, u_{a1}, u_{a2}, u_{a3}, \ldots.]$. Similarly, the term $T \subseteq U \times U$ represents the transition set, which is defined as $\{< u, u' >\}$, and $\{u, u' \in U\}$ for source and destination states respectively. The constraint used for determining the transition timing δ is determined as $\delta : T \rightarrow I$, where I is the set of probability distribution functions that varies with respect to time. This term also defines the time required for the transition. As mentioned previously, the DTM generates adversarial samples for attack detection, and the DTC acts as an IDS in an asynchronous federated learning enabled VCPS.

B. Asynchronous Federated Learning and IDS

The proposed IDS is designed to detect intrusive events along with FDI attacks in a VCPS network using DTM and asynchronous federated learning. In general, federated learning allows multiple vehicles and RSUs (vehicles with 0 mph can be considered as RSUs for simplicity) to learn from their own data, which minimizes the latency and ensures data privacy while sharing their information with other vehicles in the network. For every iteration i, the model computes the updates for each vehicle v_i and sends the updates to the base station through V2R communication. The base station combines all updates obtained from the vehicles (FL Clients) and distributes them to all vehicles in the network. Further, the next iteration is started, and the process is continued to get an optimal global model. As FL, actual data is not shared but the learned model parameters, the risk of FDI attack is significantly reduced when attackers tries to inject false data (far from model parameters' values which would be outliers for FL) in VCPS. However, model parameters can be manipulated which is combated by either discarding the parameters which do not give model closer to optimal global or lowest possible weight is given to false data injected model parameters. In VCPS, it is difficult to maintain a synchronous FL. To overcome this problem, this paper proposes an asynchronous FL for the vehicles, which does not depend on all vehicles need to report all the time before calculating a global model. Alternatively vehicles could form a local cluster and calculate their aggregate model. This reduces the risk of waiting long time for FL approach and improves the robustness of the model from either malicious users or slow reporters of FL. The problem of FL is formulated as an optimization problem wherein the main objective is to reduce the loss function $F_i(w)$. The objective function for the asynchronous FL is given as (1)

$$\min_{w \in R_d} f(w) = \frac{1}{|D|} \sum_{i=1}^{N} |D_i| F_i(w) \tag{1}$$

where D_i is defined as the local dataset, R_d is the subset with random data samples belonging to D_i, w is the weight, $|D|$ is the cardinality of the whole dataset, and N defines the number of clients. If two vehicles v_i and v_j participate in the data transmission, their respective local models are defined as $m_i(t-1)$ and $m_j(t-1)$. During the learning phase, all other participants in the VCPS network send the updated models to the vehicle v_j, denoted as $\sum m_i(t)$. The vehicle collects and aggregates the data and updates the existing model with the updated data, as shown (2)

$$m_i(t) = m_i(t-1) \frac{1}{s_k} \sum_{k} \hat{m}_k(t) \tag{2}$$

where s_k is the previous local gradients for the device k, $\hat{m}_k(t)$ is the local server model at time instant t. After a few iterations, each vehicle v_i attempts to obtain the global model m_i by aggregating all models.

$$M = \sum_{t} m_i(t) \tag{3}$$

Eq. (1) to eq. (3) are used to train the AFL model, which is updated asynchronously either in a cluster based distributed learning in FL or centralized RSU based FL. The IDS implemented in this research mainly incorporates three phases, namely, data processing, feature extraction, and FDI attack detection. During feature extraction, the GRU model takes raw data as input and extracts network features, mainly statistical features, to improve the attack detection performance. This stage generates multi-dimensional feature vectors for identifying FDI attacks [15]. GRU requires fewer parameters, and hence it is easier to train the model. Unlike the RNN model, GRU has only three gates without any internal cell state. The data is stored in the internal cell state and is embedded into the hidden state of the GRU, and this data is forwarded to the next layer and so on. The two main gates of GRU are an update gate (z) and a reset gate (r). In addition to these two, a current memory gate $\hat{h}(t)$ is also included [16]:

1) Update Gate (z): The Update gate measures the amount of past information that needs to be forwarded into the future layers similar to the output gate in the LSTM.
2) Reset Gate (r): The Reset gate measures the amount of past information to forget similar to the operation of the input gate and the forget gate in the LSTM.
3) Current Memory Gate ($\hat{h}_t$): The current memory gate is incorporated into the reset gate, which is similar to the incorporation of the input modulation gate into the input gate. This is done to introduce nonlinearity into the input and make the input zero mean. Another important fact of incorporating the memory gate into the reset gate is to minimize the influence of previous information on the current state, which is being forwarded to the next gates. The gates of the GRU model can be expressed as follows:

$$h_t = (1 - z_t) \bigodot h_{t-1} + z_t \bigodot h_t \tag{4}$$

$$\hat{h}_t = g(W_h x_t + U_h(r_t \bigodot h_{t-1}) + b_n \tag{5}$$

where x_t is the external feature vector, W, U, and b are the two weights and the bias, respectively, g is the activation function, z_t is the update gate, and r_t is the reset gate. The update and reset gates are described as follows:

$$z_t = \sigma(W_z x_t + U_z h_{t-1} + b_z) \tag{6}$$

$$r_t = \sigma(W_r x_t + U_r h_{t-1} + b_r) \tag{7}$$

where σ is the logistic nonlinearity. The statistical features are fed to the GRU model, and the network layer of the model captures both latent and spatial attributes of the FDI attack. In this research, the GRU model is used to design IDS to detect FDI attacks. The stages involved in the IDS are as follows:

1) Data Collection and Preprocessing: The data for the experimental analysis of the attack detection approach is obtained from the Aegean Wi-Fi Intrusion Dataset (AWID). The fundamental AWID dataset is modified as AWID3 dataset in [17]. The AWID3 dataset is considered one of the most effective datasets for designing and evaluating IDS. The data in this dataset is in the pcap format along with their Pairwise Master

Key (PMK) and TLS keys. This format is highly flexible for extracting relevant features from the data based on the requirement. In this research, features related to FDI attacks are extracted. The extracted features are spread across the network layers of the VCPS environment and are distinguished based on the corresponding layer. The dataset consists of 254 manually extracted features in CSV format, wherein 253 are generic features with one additional feature for labeling. This study focuses on the attacks against local (internal) and external nodes. Attacks such as SSH brute force, Botnet, and malware are considered attacks against local nodes, while SQL injection and SSDP are considered attacks against external nodes. The raw data from the AWID3 dataset is preprocessed to filter out uncertainties such as redundant data, null values, and missing values. During preprocessing, all empty features and features with constant values were removed, and missing values were replaced with training data.

2) Feature Extraction: In this stage, the essential features are extracted to achieve better attack detection performance. It is important to select only relevant features from the dataset to reduce the computational burden on the learning model and to improve the time required for training the GRU model. Besides, feature extraction also overcomes the problem of data dimensionality and enhances the accuracy of attack detection. Based on the FDI attack-related features, the model identifies the changes in the normal behavior of the VCPS network and flags the FDI attacks. In certain cases, the destination ID is not mentioned in the communicated data, and in such cases, two distinct features are extracted for training and validating the IDS model. The first feature is the total number of data packets transmitted by the source, and the second feature is the size of the data transmitted from the source ID. The extracted features are the statistical features that contain the attack pattern, and some of the statistical features that are used to train the proposed IDS model are as follows: traffic initiated from the source ID, data transmitted from the source ID to the destination ID, the time required for data transmission, bits per second, and data sent from source to destination and vice versa. The extraction of statistical features is expected to improve the accuracy of the AFL-GRU model while detecting FDI attacks. It is assumed in this research that the statistical attributes of the normal behavior of the VCPS model will exhibit sudden change, and as a result, more stable performance can be achieved.

3) FDI Attack Detection: Here in this research, the layers of the GRU model reconstruct the VCPS data, and in this stage, the reconstruction error (which is calculated as the difference between the original and the reconstructed data) is reduced, and an optimal value is selected for classifying the data sequences based on the reconstruction error. In the final stage, the reconstruction errors are used as a validation dataset for distinguishing normal and malicious data. The data sequences whose reconstruction error is higher than the selected optimal value are considered malicious.

IV. Performance Evaluation

The proposed federated learning and digital twin-based IDS is evaluated using the AWID3 dataset in terms of its ability to detect potential attacks. For simulation, multiple vehicles are considered, and the dataset is divided into multiple subsets based on their categories and aggregated to form multiple datasets. The number of vehicles considered for simulation analysis is 50, and the maximum number of features considered for the analysis is 130. The attack detection performance is evaluated based on the detection accuracy. The dataset was split into a ratio of 80% for training and 20% for testing the performance of the model, respectively. The approximate consideration of the split ratio reduces the problem of overfitting and ensures that the model exhibits better performance. The IDS model was trained using both normal data and malicious data, which includes different types of attacks, including FDI attacks. Nine different VCPS attributes were selected for simulation analysis, namely, source IP, destination IP, source port and destination port, duration, source bytes, destination bytes, source TTL, destination TTL, source load, destination load, source packets, and destination packets. In addition, the performance of the digital twin-based IDS was evaluated in terms of various performance evaluation parameters, and the results obtained were compared with another existing model/algorithm to validate the effectiveness of the proposed approach. The dataset is split into 10 samples sequentially to find the optimal parameters for the experimental evaluation. The last sample will be considered the testing data, and the remaining samples will be used as the training data. A 9-fold cross-validation is performed on the training dataset, and the hyperparameters are set based on the validation result. The proposed IDS model is trained using both real-time data and historical data. The simulation results of the proposed IDS for different metrics are shown in Table I.

TABLE I
Attack classification report of the proposed IDS

	Accuracy	Precision	Recall	f1-Score	AUC
Class 0	0.988	0.98	0.95	0.92	0.93
Class 1	0.988	0.97	0.98	0.96	0.95
Class 2	0.992	0.98	1.00	0.99	0.98
Macro Avg	0.993	0.976	0.976	0.956	0.953
Weighted Avg	0.993	0.976	0.976	0.956	0.953

It can be inferred from the Table I that the proposed classification model achieved an accuracy of 99.3%. At the same time, the macro average of the precision, recall, F1 score, and AUC

TABLE II
Comparative Results of the proposed IDS with other techniques

Techniques	Accuracy	Precision	Recall	F1-Score	AUC
RF	0.95	0.93	0.93	0.91	0.9
NB	0.79	0.74	0.77	0.79	0.83
SVM	0.93	0.89	0.92	0.91	0.94
Decision Tree	0.94	0.92	0.91	0.91	0.93
XGBoost	0.73	0.82	0.74	0.72	0.85
DQN	0.988	0.964	0.958	0.951	0.950
DBN	0.966	0.975	0.963	0.928	0.937
Proposed AFL-GRU	0.993	0.976	0.976	0.956	0.953

(Area under the ROC Curve) is found to be 97.6%, 97.6%, 95.6%, and 95.3%, respectively. The performance of the proposed IDS was validated by comparing the simulation results of the proposed approach with other existing classification models. In this work, the performance of the digital twin-based AFL-GRU model was compared with existing Random Forest (RF), Naive Bayes (NB), Support Vector Machine (SVM), Decision Tree, XG boost, Deep Q-Networks (DQN), and Deep Belief Networks (DBN) model and presented in Table II.

Simulation results show that the proposed IDS model outperforms existing models such as RF, Decision Tree, SVM, NB, and XGBoost. In addition, models such as DQN and DBN are also considered for the comparative analysis. These models can achieve a higher classification accuracy since they learn data effectively while capturing essential features. As a result, these models are compared against the proposed AFL-GRU model. The proposed model achieves a high precision and accuracy of 97.6% and 99.3%, respectively, which is higher compared to other models. The second-best performance is achieved by the DQN model, which achieves an accuracy of 98.8%. Results show that the proposed IDS achieves better results and performance than other models. There are multiple reasons for the proposed IDS to exhibit excellent performance. Firstly, extracting the spatial and temporal attributes of VCPS models is important in making relevant predictions. During simulation, it was observed that the proposed model required less epochs to reduce the training time to acceptable limits. However, extracting the statistical features helped the model achieve better performance irrespective of the longer training time. Several works have implemented CNN and LSTM models for learning spatial features. However, the dynamic behavior of the VCPS model makes it challenging for these models to learn spatial features, thereby affecting performance efficiency. Hence, in this research, a GRU model is included instead of conventional CNN. The GRU model effectively captures the nonlinear spatial features, which improves the intrusion detection performance with better precision. On the other hand, it was observed from the experimental analysis that the existing models suffered from the problem of data sparsity. It is difficult to manually acquire the labeled data in a dynamic and heterogeneous VCPS environment since it can be expensive. This problem is addressed in this research by training the model with both adversarial samples and normal samples. Lastly, the model is trained to learn continuously while the VCPS model is operating. In addition, asynchronous federated learning helps the model obtain updated information continuously using real-time data to prevent new intrusions. Hence, the model is trained online, leveraging the real-time data obtained from the VCPS model. Otherwise, the VCPS model can become more susceptible to attacks and intrusions not present in the training dataset.

V. Conclusion

In this paper, we have presented an asynchronous Federated Learning based digital twin enabled IDS for detecting FDI attacks in VCPS, which detects unknown attacks. The digital twin concept employed in this paper evaluates the ground truth labels and enables the proposed approach to work effectively with a large amount of unlabeled data samples, which does not need labeled data samples to achieve better performance. The performance of the proposed IDS model is evaluated using the AWID3 dataset, and results show that the proposed model outperforms the other models in terms of accuracy and other metrics.

Acknowledgment

This work was supported in part by the VMware Inc. Research Gift Funds, Meta Inc. Research gift funds and Microsoft Corp. Research Gift Funds as well as by the NSF grant # 2240407.

References

[1] J. Wan, D. Zhang, S. Zhao, L. T. Yang, and J. Lloret, "Context-aware vehicular cyber-physical systems with cloud support: architecture, challenges, and solutions," *IEEE Communications Magazine*, vol. 52, no. 8, pp. 106–113, 2014.

[2] D. B. Rawat and C. Bajracharya, "Vehicular cyber physical systems," *Springer*, vol. 10, pp. 978–3, 2017.

[3] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Federated learning for data privacy preservation in vehicular cyber-physical systems," *IEEE Network*, vol. 34, no. 3, pp. 50–56, 2020.

[4] D. B. Rawat and K. Z. Ghafoor, *Smart cities cybersecurity and privacy*. Elsevier, 2018.

[5] J. Giraldo, E. Sarkar, A. A. Cardenas, M. Maniatakos, and M. Kantarcioglu, "Security and privacy in cyber-physical systems: A survey of surveys," *IEEE Design & Test*, vol. 34, no. 4, pp. 7–17, 2017.

[6] D. B. Rawat and C. Bajracharya, "Detection of false data injection attacks in smart grid communication systems," *IEEE Signal Processing Letters*, vol. 22, no. 10, pp. 1652–1656, 2015.

[7] G. Abdelmoumin, D. B. Rawat, and A. Rahman, "On the performance of machine learning models for anomaly-based intelligent intrusion detection systems for the internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 6, pp. 4280–4290, 2021.

[8] F. O. Olowononi, D. B. Rawat, and C. Liu, "Resilient machine learning for networked cyber physical systems: A survey for machine learning security to securing machine learning for cps," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 524–552, 2020.

[9] C. Zhang, Y. Xie, H. Bai, B. Yu, W. Li, and Y. Gao, "A survey on federated learning," *Knowledge-Based Systems*, vol. 216, p. 106775, 2021.

[10] B. Ghimire and D. B. Rawat, "Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things," *IEEE Internet of Things Journal*, 2022.

[11] Z. Guo, K. Yu, Z. Lv, K.-K. R. Choo, P. Shi, and J. J. Rodrigues, "Deep federated learning enhanced secure poi microservices for cyber-physical systems," *IEEE Wireless Communications*, vol. 29, no. 2, pp. 22–29, 2022.

[12] D. B. Rawat and H. El Alami, "Metaverse: Requirements, architecture, standards, status, challenges, and perspectives," *IEEE Internet of Things Magazine*, vol. 6, no. 1, pp. 14–18, 2023.

[13] Patrick Howell O'Neill, Hackers can trick a Tesla into accelerating by 50 miles per hour A two inch piece of tape fooled the Tesla's cameras and made the car quickly and mistakenly speed up, https://www.technologyreview.com/2020/02/19/868188/hackers-can-trick-a-tesla-into-accelerating-by-50-miles-per-hour.

[14] Q. Ma, B. Burns, K. Narayanaswamy, V. Rawat, and M. C. Shieh, "Network attack detection using partial deterministic finite automaton pattern matching," Mar. 8 2011, uS Patent 7,904,961.

[15] Z. Qu, X. Bo, T. Yu, Y. Liu, Y. Dong, Z. Kan, L. Wang, and Y. Li, "Active and passive hybrid detection method for power cps false data injection attacks with improved akf and gru-cnn," *IET Renewable Power Generation*, vol. 16, no. 7, pp. 1490–1508, 2022.

[16] R. Dey and F. M. Salem, "Gate-variants of gated recurrent unit (gru) neural networks," in *2017 IEEE 60th international midwest symposium on circuits and systems (MWSCAS)*. IEEE, 2017, pp. 1597–1600.

[17] E. Chatzoglou, G. Kambourakis, and C. Kolias, "Empirical evaluation of attacks against ieee 802.11 enterprise networks: The awid3 dataset," *IEEE Access*, vol. 9, pp. 34 188–34 205, 2021.