Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 5 (2023)

Identification and Attribution of Cyber Physical Attack Using Rnn and Random Forest Algorithm

[1]Vignesh. P., [2]Marees Kannan. M.,[3]Praveen. P.,[4]Sebathirani.K.,[5]Manimegalai. M.,

[1]Dept. Of Information Technology,National Engineering College Kovilpatti, India

[2]Dept. Of Information Technology, National Engineering College Kovilpatti, India

[3]Dept. Of Information Technology, National Engineering College Kovilpatti, India

[4]Dept. Of Eee, Sri Ramakrishna Engineering College Coimbatore, India

[5]Dept. Of Information Technology, National Engineering College Kovilpatti, India

***Abstract*—** Securing Cyber-Physical Systems (CPS) within the Internet of Things (IoT) paradigm poses significant challenges, particularly in mitigating attacks on sensors and preventing the transmission of falsified data to centralized servers. Traditional cybersecurity measures struggle to address the complexities inherent in these systems, leading to vulnerabilities exploited by malicious actors. This project introduces an innovative approach aimed at addressing the issue of data imbalance, a persistent challenge encountered in existing attack detection algorithms. The first component utilizes an Autoencoder trained on an imbalanced dataset to extract salient features. These features are subsequently processed through ensemble learning models, such as Random Forest and Recurrent Neural Network (RNN) algorithms, to enhance the detection accuracy in identifying anomalous patterns within the data. The second component integrates a predictive labeling mechanism for both known and unknown attack instances. Leveraging reduced feature sets derived from Independent Component Analysis (ICA), the RNN algorithm is trained to differentiate and classify records containing attack signatures, assigning appropriate labels to detected anomalies. This novel approach mitigates the challenges posed by data imbalance without relying on conventional resampling techniques, thereby bolstering the accuracy and efficacy of attack detection in IoT-enabled CPS environments. The proposed framework's effectiveness is validated through comprehensive evaluations utilizing real-world datasets, showcasing superior performance when compared to existing methodologies.

Keywords*—Internet of Things, Cyber-Physical Systems, Random Forest, Recurrent Neural Network, Independent Component Analysis, Attack Detection, Data Imbalance.*

Introduction

Sensors find widespread use across various applications, encompassing everything from monitoring bodily functions to facilitating automated driving. Moreover, they serve as pivotal components in executing detection and vision-oriented functions within contemporary scientific and technological landscapes dominated by computer vision. One intriguing and burgeoning realm harnessing smart sensors is the Internet of Things (IoT), focused on wireless networks and distributed sensors capturing live data for tailored outputs via adept processing. Within IoT devices, sensors and artificial intelligence (AI) stand out as the core elements, endowing these devices with their intelligence and smart capabilities. Artificial intelligence empowers sensors to become 'smart sensors,' enabling their effective deployment across diverse applications like general environmental monitoring [1], monitoring of different environmental factors, weather prediction, use of satellite imagery, applications based on remote sensing, and observation of important events like the identification of landslides. Furthermore, in the

healthcare industry, the notable recent increase in the use of smart devices in hospitals and diagnostic centers makes it easier to evaluate and track a variety of medical conditions among patients with disabilities, both locally and remotely [2]. Virtually every scientific field or research domain leverages modern sensors smartly, emphasizing their indispensable role in advancing research and innovation. The widespread necessity for sensors and their integration into the Internet of Things across remote sensing, environmental monitoring, and human health drives the intelligence of various applications. In the last ten years, the agricultural industry [3] has come to rely more and more on a variety of sensor types for monitoring and controlling a wide range of environmental factors, including radiation, temperature, humidity, soil quality, pollution, and contamination of the air and water. The purpose of this paper is to highlight the use of sensors and IoT in agricultural and remote sensing applications, promoting a thorough overview and discussion. Moreover, structural health monitoring (SHM) of buildings has emerged as a pivotal research focus in recent times, enabling the identification of structural damage and offering early alerts regarding unsafe structural conditions.
Over time, civil infrastructure like bridges faces degradation attributed to factors such as heavy vehicular traffic, environmental stressors, and dynamic forces like seismic activity. These changes predominantly affect older structures, necessitating various methodologies for damage detection. Structural health monitoring (SHM) involves continuous observation of these structures, capturing periodic data measurements, extracting relevant features, and conducting analyses to determine the structure's current condition. Recommended data guides the assessment, allowing for periodic updates in monitoring. Leveraging the data gleaned from structure monitoring enables informed decisions on reinforcement, repairs, and comprehensive restoration and maintenance [5]. Internet of Things (IoT) devices, an essential part of Cyber Physical Systems (CPS), are being integrated more and more into critical infrastructure domains such as power plants and dams. These devices, commonly referred to as Industrial IoT (IIoT) devices, function within these environments and are essential to industrial control systems (ICS) that guarantee the infrastructure's reliable functionality. ICS includes distributed control systems (DCS), systems with programmable logic controllers (PLCs) and Modbus protocols, and supervisory control and data acquisition (SCADA) systems. However, connecting ICS or IIoT systems to open networks increases their susceptibility to potential cyberattacks and raises the possibility that they will be targeted maliciously by cybercriminals. Take prominent examples of cyberattacks that caused significant damage, such as the Stuxnet campaign that allegedly targeted Iran's nuclear enrichment centrifuges in 2010 [1], [2In addition, in 2011 an Illinois hydroelectric plant failed due to a pump-related incident [3]. In 2015, the BlackEnergy3 campaign targeted the power grids in Ukraine, resulting in blackouts that affected about 230,000 people [4]. Moreover, the cyberattacks that occurred in April 2018 against three US gas pipeline companies resulted in the prolonged suspension of electronic customer communication systems [1].

The complex interdependence between controlled physical environments and cybernetic systems may limit the direct applicability of security solutions for IT and OT systems, despite their relative maturity in these domains.

Hence, implementing system-level security measures becomes imperative to assess physical behaviors and ensure sustained system availability [1]. ICS security focuses on availability, integrity, and confidentiality priorities, unlike the typical sequence in IT/OT systems [5]. Cyberattacks on Industrial Control Systems (ICS) can have serious societal and environmental repercussions due to the close relationship between feedback control loop variables and physical processes. This emphasizes the need for strong security protocols to identify and stop intrusions.

Typical attack detection techniques include anomaly- and signature-based methods, with hybrid models being worked on to address known shortcomings [6]. Frequent network upgrades, however, present reliability issues for these hybrids and result in a variety of intrusion detection system typologies [7]. Moreover, network metadata analysis plays a major role in conventional attack detection techniques, which has led to a renewed focus on machine learning (ML) or deep neural network (DNN)-based approaches for accurate attack detection and attribution [8].

Additionally, attack detection techniques are divided into host-based and network-based categories. Real-time traffic data is analyzed by methods like supervised clustering, support vector machines (SVM), fuzzy logic,

artificial neural networks (ANN), and DNN to identify potentially malicious activity. However, concentrating only on host and network data may miss sophisticated or insider attacks.

Problem Statement

As our world becomes more interconnected through cyber-physical systems, the risk of sophisticated attacks exploiting vulnerabilities in this network grows. The key challenge is quickly and accurately pinpointing these cyber-physical attacks and tracing their origins to respond promptly with effective mitigation strategies.

This research endeavors to create an advanced framework that harnesses the power of Recurrent Neural Network (RNN) and Random Forest algorithms. The goal is to reliably identify and attribute cyber-physical attacks, ensuring robustness in detection and attribution. The primary aims are:

1. Identification of Cyber-Physical Attacks:

Temporal Pattern Recognition: Create an RNN-powered model designed to scrutinize sequential data streams, pinpointing anomalies or variations that may signal cyber-physical attacks. This involves spotting irregularities within network traffic, sensor readings, and system logs.

Anomaly Detection: Leverage the RNN model to discern nuanced deviations from typical system behavior, differentiating between harmless fluctuations and potentially malevolent actions.

Multi-class Classification: Harness the Random Forest algorithm to categorize identified anomalies into distinct attack types, utilizing learned patterns and extracted features from a range of data sources.

2. Attribution of Attacks:

Source Tracing: Explore various methodologies, potentially incorporating network forensics and threat intelligence, to attribute detected cyber-physical attacks, pinpointing their sources.

Origin Identification: Devise strategies to trace the origins of attacks, aiming to unveil the perpetrators or entities initiating these malicious activities

Literature Survey

Ullo et. al concentrated on an expansive investigation into the progression of smart sensors and the Internet of Things in remote sensing [1], spanning agricultural applications like weather assessment, soil quality evaluation, crop monitoring, robotic utilization in harvesting and weeding, and the integration of drones. The study extensively covered various sensor types and technologies, providing in-depth analyses, reviews, comparisons, and recommendations to propel IoT advancements. Its goal was to aid researchers, farmers, remote sensing scientists, and policymakers in their research endeavors and practical implementations. Sivasuriyan et al. offer a comprehensive exploration of bridge monitoring, delving into the diverse array of sensors employed and the detection of various types of damage—such as strain, displacement, acceleration, and temperature—tailored to different bridge conditions (such as abrasion, hinge failure, bolt and cable disconnection) and environmental wear under static and dynamic loads. The article encompasses insights into numerous methodologies, approaches, case studies, cutting-edge technologies, real-time experiments, simulated models, data mining, and predictive analytics. Additionally, it discusses the future scope and research avenues regarding Structural Health Monitoring (SHM) implementation in bridges. Ultimately, this research aims to furnish researchers with a deeper comprehension of bridge monitoring mechanisms.

Dazhe Zhao et al. demonstrated a tiny, easily produced untethered triboelectric patch by using the human body as the conductor and polytetrafluoroethylene (PTFE) as the triboelectric layer. Their findings demonstrated the untethered patch's strong output capability and long-lasting nature by indicating that the conductive qualities of the human body had minimal impact on the outputs. These patches serve dual purposes as both sensor patches and energy harvesters. The study demonstrates three key applications: machine learning-driven objects achieving accuracy rates between 93.09% and 94.91%, wireless communication transmitting typical words to a mobile phone, and harvesting energy from human movements to directly power electronics or charge devices for energy storage.

Bacco et. al provided a comprehensive account, combining analytical and empirical insights, detailing a practical test setting that implemented IEEE 802.15.4-based communications linking UAVs with stationary ground sensors. Within this context, our observations indicated that the aerial mobility significantly restricts the effective IEEE 802.15.4 transmission range between UAVs and ground nodes, reducing it to approximately one-third of the nominal value [4]. Additionally, we offer essential design considerations for deploying sensors in precision agriculture scenarios.

Verma et al. provided an in-depth exploration into the contemporary landscape of advanced smart functionalities, control parameters, and the requisite Internet of Things (IoT) infrastructure crucial for the evolution of smart buildings. Their primary focus revolved around sensing capabilities and the management of IoT infrastructure, facilitating the utilization of virtual sensing infrastructure by cloud clients through communication protocols. The discussion encompassed various key smart features inherent in smart buildings, such as privacy and security, network architecture, health services, sensor deployment, security protocols, and overall management.

The integration of Internet of Things (IoT) principles enables the interconnection and management of appliances within smart buildings through network systems. This ongoing development in sensing technologies, control mechanisms, and IoT infrastructure contributes significantly to the enhanced efficiency of smart buildings. Consequently, the review highlighted emerging innovations and challenges within the context of IoT-driven smart buildings, offering a structured scientific overview that identifies current limitations and points towards future research directions.

Hu et al. introduced an intricate and energy-efficient real-time air quality monitoring system that integrates aerial and ground-based sensing capabilities. The system's architecture comprises distinct layers: a sensing layer for comprehensive data collection, a transmission layer enabling bidirectional communication [6], a processing layer dedicated to data analysis and manipulation, and a presentation layer offering a graphical user interface. The study investigates three primary techniques focusing on data processing, deployment strategies, and power management.

Spatial fitting and short-term prediction techniques were used in data processing to lessen the effects of imperfect measurements and delayed data uploads. Aerial and ground-based sensing deployment strategies were investigated in order to improve the overall quality of the data that was gathered. In addition, strategies for power management were developed to balance data accuracy and power consumption.

Since its implementation in February 2018, this system at Peking University and Xidian University has produced close to 100,000 useful data values.

Family et. al [7] introduced an enhanced optimization approach, IABCOCT (Improved Artificial Bee Colonies ClusTering Algorithm), integrating the Grenade Explosion Into the conventional Artificial Bee Colony (ABC) algorithm, the Cauchy Operator and the Method (GEM) are incorporated. This augmentation using the Cauchy operator and GEM effectively keeps the algorithm from becoming stuck in local optima and greatly accelerates convergence. To be more precise, the Onlooker Bee and Scout Bee stages incorporate the GEM and Cauchy operator improvements, which significantly increase the use and exploration levels in the Cluster Head (CH) selection procedure. The outcomes of the simulations showed that the IABCOCT algorithm outperformed more recent approaches like competitive clustering technique (CCT), particle swarm optimization technique (EPSOCT), and hierarchical clustering-based CH selection (HCCHE). The IABCOCT algorithm performed exceptionally well in terms of throughput, packet loss, delay, power consumption, and network lifetime, among other metrics.

proposed Framework

Cyber-physical attack detection and attribution within IoT-enabled cyber–physical systems, our research introduces a comprehensive two-level ensemble framework. At the first level, deploy a robust attack detection system. The system utilizes a Random Forest in conjunction with a groundbreaking ensemble deep representation-learning model. The combination enables the early detection of cyber-attacks, even in imbalanced industrial control system (ICS) environments where traditional methods may struggle. Notably, our

first-level system excels in identifying anomalous activities and potential threats. Subsequently, at the second level, our framework integrates an ensemble Recurrent neural network tailored to the task of attack attribution.

The second-level system plays a pivotal role in tracing the source and origin of the detected cyber-attacks. By combining these two levels, our framework provides a holistic approach to enhancing the security of IoT-enabled cyber-physical systems, particularly within the context of industrial control systems (ICS). The approach not only excels in attack detection but also facilitates the crucial task of attack attribution, offering a comprehensive solution for safeguarding these complex systems.

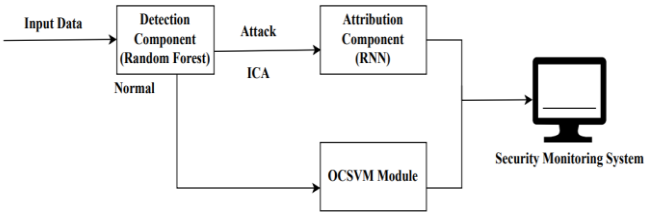

Fig..1 Cyber Physical System Detection Design.

A. Attack Detection Method

Attack Detection refers to the process of identifying and categorizing potentially malicious activities or anomalies within a computer system or network. In the context of the framework for IoT-enabled cyber–physical systems (CPS), attack detection involves monitoring the system for any unusual patterns of behavior that may indicate a cyber-attack. In The detection process typically relies on a combination of techniques, including signature-based detection, anomaly detection, and machine learning algorithms. In the two-level approach for attack detection, the first level employs a decision tree combined with a novel ensemble deep representation-learning model. In The combination allows for the identification of attacks in environments with imbalanced data, which is common in industrial control systems. The decision tree helps classify events, while the deep learning model is capable of learning complex patterns and anomalies, enhancing the system's ability to detect both known and unknown threats.

1) Random Forest

This algorithm is renowned for its reliability, consistently generating highly accurate classifiers, particularly when handling large datasets and files. Its versatility allows for seamless implementation of numerous strategies without any interruptions, providing vital estimates for essential variables within the distribution.

Feature and Advantages of Random Forest:

This learning algorithm ranks among the most precise available, consistently generating remarkably accurate classifiers across a wide range of datasets. It efficiently manages large databases and copes adeptly with thousands of input variables, maintaining their integrity without requiring elimination. Furthermore, it provides crucial estimates for pivotal classification variables and constructs an unbiased estimate of generalization error during forest creation. Notably, it possesses an efficient approach to estimating missing data, preserving accuracy even when a substantial portion of the data is absent.

Disadvantages of Random Forest:

Random forests have shown instances of being excessive for datasets involving noisy classification or regression tasks. In scenarios where categorical variables have varying levels, random forests exhibit bias toward attributes with more levels. Consequently, in such data types, relying on variable importance scores generated by a random forest might not yield reliable outcomes.

B. Attack Attribution Method

The second level of the framework focuses on attack attribution and utilizes an ensemble Recurrent neural network. In the network is designed to analyze various attributes and characteristics of the attack, such as its signature, tactics, techniques, and infrastructure used. By correlating these attributes with known threat actors or patterns, the system can attribute the attack to a specific group or entity. Attack attribution is essential not only for responding to cyber-attacks effectively but also for taking legal and diplomatic actions against threat actors.

2) Recurrent Neural Network

Recurrent Neural Networks stand as a pivotal machine learning technique, particularly within supervised learning paradigms. RNNs are designed to discern the temporal relationships within sequential data. An RNN model presumes connections between new data instances and existing ones, categorizing the new data based on its similarity to the sequences in the dataset. The algorithm processes all available data, accommodating new data points by determining their likeness to the existing dataset. Unlike parametric models, RNNs are non-parametric, signifying their absence of assumptions about the underlying data distribution. This attribute allows RNNs to adapt flexibly to different data structures. RNNs function as 'eager learners,' meaning they do not instantaneously learn from the training set. Instead, they retain the dataset and perform operations on it during classification. Upon encountering new data, RNNs categorize it into the most analogous sequence within the stored dataset.

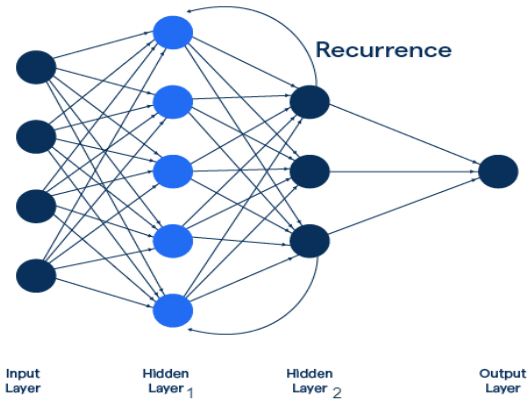

Fig. 3.1 Recurrent Neural Network

Input Layer(Layer 1): In the RNN structure, this layer represents input features. Suppose there are n_1 neurons in this layer, each corresponding to an input feature.

Hidden Layers: Similar to the DNN's hidden layers, the RNN comprises multiple hidden layers. For instance:

Hidden Layer 1(Layer 2): With n_2 neurons, this is the first hidden layer.

Hidden Layer 2 (Layer 3): uses n_3 neurons to represent the second hidden layer.

Output Layer (Layer 4): Comparable in operation to the DNN, this layer in an RNN consists of one neuron for binary classification tasks and several neurons for multi-class classification or regression tasks.

Hidden Layer 1 (Layer 2): Computing activations for the first hidden layer involves:

$$z^{j}_{2,t}=\sum_i(w^{j,i}_2,\cdot x_{t,i})+b_2^j \quad (1)$$

$$a^{j}_{2,t} = \text{activation function}(z_2^j,_t)$$

Hidden Layer 2 (Layer 3): Calculating activations for the subsequent hidden layer can be represented as:

$$Z^{k}_{3,t}=\sum_j(w^{k,j}_3,\cdot a_2^j,_t)+b_3^k \quad (2)$$

$$a^{k}_{3,t} = \text{activation function}(z_3^k,_t)$$

In this case, x_{t,i} represents the input from the i-th input neuron at time step t, b_{2}^ indicates the weight of the connection between the i-th and the j-th neuron in the first hidden layer, and w_2^{j,i} denotes that weight.In the first hidden layer, j denotes the bias term for the j-th neuron; element-wise, the activation function is applied to z_{2, t}^j.

Similar to this, a_{2, t}^j represents the activation from the first hidden layer at time step t, b_{3}^k denotes the bias term for the k-th neuron in the second hidden layer, and activation function is applied element-wise to z_{3, t}^k. Additionally, w_3^{k,j} indicates the weight of the connection between the j-th neuron in the first hidden layer and the k-th neuron in the second hidden layer.

Advantages of RNNs:

- ✓ Ease of implementation.
- ✓ Robustness against noisy training data.
- ✓ Increased efficiency with large training datasets.

Steps to Implement the RNN Algorithm:

- ✓ Data preprocessing stage.
- ✓ Adapting the RNN model to the training dataset.
- ✓ Predicting outcomes based on the test data.
- ✓ Assessing result accuracy through techniques like creating a confusion matrix.
- ✓ Visualization of test set results.

Iv. Results And Discussion

A. Dataset

We evaluated the suggested framework on two real-world Industrial Control Systems (ICS) datasets. The first dataset came from a pipeline system at Mississippi State University that combined sensors, actuators, a communication network, and supervisory control. This dataset includes seven different types of attacks: Denial of Service (DoS), Complex Malicious Response Injection (CMRI), Malicious State Command Injection (MSCI), Malicious Parameter Command Injection (MPCI), Malicious Function Code Injection (MFCI), Naive Malicious Response Injection (NMRI), and Reconnaissance (Recon). The dataset included 60,048 (21.86%) attack samples and 214,580 (78.14%) normal samples out of a total of 274,628 reported observations. It also included 17 features that defined the states of the network and fields.

B. Pre-Processing

Multiple Recurrent Neural Networks (RNNs) are incorporated into the framework shown in Figure 5.2. RNNs are in charge of using raw features as input to create new representations for attack detection and matching. Like other approaches, the data was normalized using the min-max technique to guarantee that features were treated fairly before processing. This was all there was to pre-processing in this suggested framework. To obtain the results, 10-fold cross-validation was also used.

Regarding data preprocessing, measures like normalization, scaling, or other preprocessing techniques were employed to optimize the effectiveness of Independent Component Analysis (ICA) in identifying independent components across diverse data sources.

The ICA transformation was implemented as an initial step to preprocess the raw data, aiming to create a space where the derived components represent statistically independent sources. This step aimed to enhance the efficacy of subsequent feature extraction processes.

C. Evaluation Metrics

This study compared the suggested attack attribution method with approaches previously used on the same datasets in their original studies in order to fairly assess its efficacy using the DT classifier on the original representation. Nevertheless, attempts to identify comparable approaches for the suggested auto-debugging attack assignment method were not successful. In contrast to our model's ability to assign all eight classes, a comparison with Fuzzy C-Mean (FCM) clustering [25] showed that FCM only detected four of the eight classes in the pipeline dataset. This implies that attacks are highly similar, which makes classification difficult. In keeping with industry norms, this study evaluated machine learning algorithm performance using traditional metrics.

D. Feature Extraction

Independent Component Analysis (ICA) serves as a technique geared towards blind source separation and feature extraction, seeking to unveil statistically independent components within multivariate data. Integrating ICA into the feature extraction process for cyber-physical attack identification and attribution can shed light on the independent sources contributing to these attacks.

The application of ICA involves decomposing network traffic data into statistically independent components. Features are extracted from these components, emphasizing distinctive patterns or anomalies that may signify potential cyber-physical attacks. Activation patterns within these independent components, deviating significantly from regular traffic behavior, can indicate attack signatures or abnormal system behavior. Similarly, ICA can be applied to system logs or sensor data to extract independent features that capture anomalous behaviors, focusing on components representing unusual system events or irregular sensor readings. For the utilization of ICA in model development:

- ICA-derived independent components serve as input features for RNN models, leveraging their ability to capture unique temporal dependencies or sequential patterns.
- Incorporating ICA-derived features into the Random Forest algorithm enhances the feature set, bolstering the algorithm's capacity to classify cyber-physical attacks based on independent characteristics.
- It's crucial to maintain interpretability when integrating ICA-extracted features with other feature sets for model training.
- Proper parameter tuning for ICA, such as determining the number of components and algorithm variations, is pivotal for optimal feature extraction relevant to cyber-physical attack patterns.

V. Experimental Results

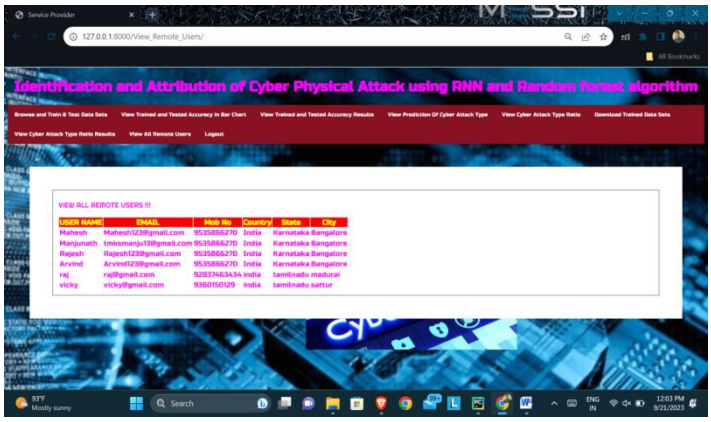

Fig 5.1: View remote Users

In Fig 5.1 provides an overview of the distribution of user authority levels within the system, specifically focusing on the number of users who possess account authority.

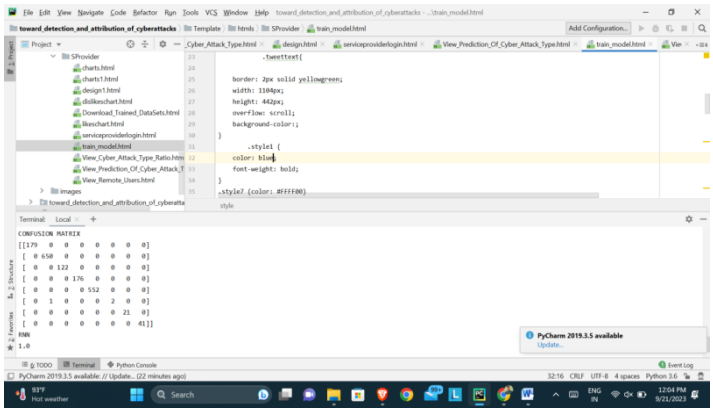

Fig 5.2: Training and Testing Dataset1

In Fig 5.2 describes the system that depict different aspects of datasets used for training and testing purposes.

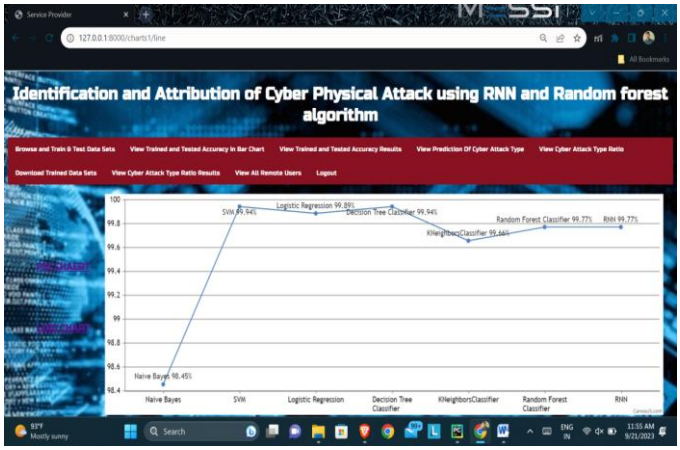

Fig 5.3: Train and Test Accuracy Result

In Fig 5.3 describes the Attack Detection Accuracy Using line Chart representation that illustrates the accuracy of attack detection using a line chart.

Fig 5.4: Training and Testing Result of Cyber Dataset

In Fig 5.4 illustrates the training and testing outcomes of the Cyber Dataset, showcasing performance metrics like accuracy. This visual aids in understanding the model's learning process and its ability to generalize while maintaining reliability in detecting cyber threats.

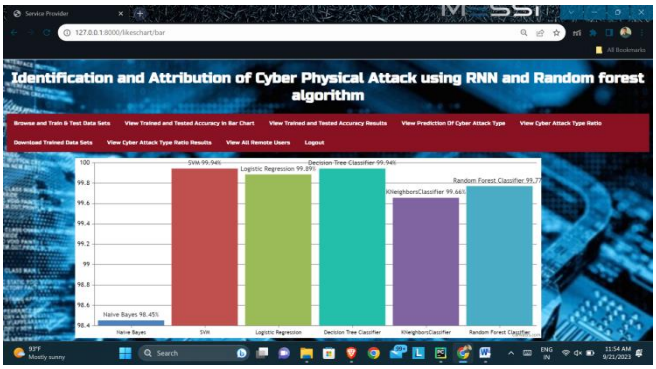

Fig 5.5: Train and Test Accuracy Chart Report

In Fig 5.5 presents the Train and Test Accuracy Chart Report, delineating the performance metrics of the model on both training and testing data. This visual depiction offers insights into the model's learning progress and its ability to generalize, critical for assessing its reliability in real-world scenarios.

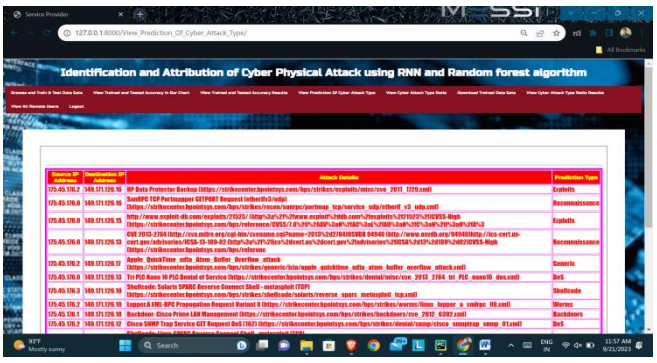

Fig 5.6: Cyber Attack Details

In Fig 5.6 encapsulates Cyber Attack Details, offering a comprehensive breakdown of specific cyber threats within the dataset. This visual representation provides an in-depth analysis, showcasing various attack types.

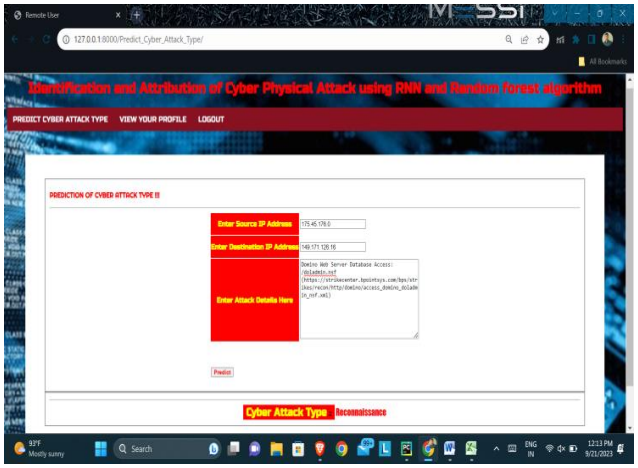

Fig 5.7: Prediction of Cyber Attack

In Fig 5.7, the determining the specific type of cyber attack that has occurred within a cyber-physical system.

Conclusion

In summary, the fusion of Independent Component Analysis (ICA) with Recurrent Neural Networks (RNNs) and Random Forest algorithms offers a promising direction for cyber-physical attack identification and attribution. This hybrid framework leverages ICA's ability to unveil statistically independent components from diverse data streams in cyber-physical systems, enriching feature extraction processes. It empowers the detection of nuanced attack signatures and unusual behaviors, often elusive with traditional methods. These extracted independent components serve as valuable inputs, augmenting RNNs and Random Forest models to capture intricate temporal dependencies and unique patterns related to cyber-physical attacks. This synergy between statistical independence extraction and machine learning models shows promise in advancing the understanding and response to evolving cyber threats targeting interconnected systems. Continued refinement of this hybrid approach holds significant potential in fortifying the security of cyber-physical infrastructures against increasingly sophisticated attacks.

References

[1] F. Zhang, H. A. D. E. Kodituwakku, J. W. Hines, and J. Coble, "Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data," IEEE Transactions on Industrial Informatics, vol. 15, no. 7, pp. 4362–4369,2019.

[2] R. Ma, P. Cheng, Z. Zhang, W. Liu, Q. Wang, and Q. Wei, "Stealthy Attack Against Redundant Controller Architecture of Industrial CyberPhysical System," IEEE Internet of Things Journal, vol. 6, no. 6, pp.9783–9793, 2019.

[3] G. Falco, C. Caldera, and H. Shrobe, "IIoT Cybersecurity Risk Modeling for SCADA Systems," IEEE Internet of Things Journal, vol. 5, no. 6, pp. 4486–4495, 2018.

[4] J. Yang, C. Zhou, S. Yang, H. Xu, and B. Hu, "Anomaly Detection Based on Zone Partition for Security Protection of Industrial Cyber-Physical Systems," IEEE Transactions on Industrial Electronics, vol. 65, no. 5, pp. 4257–4267, 2018.

[5] S. Ponomarev and T. Atkison, "Industrial control system network intrusion detection by telemetry analysis," IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 2, pp. 252–260, 2016.

[6] J. F. Clemente, "No cyber security for critical energy infrastructure," Ph.D. dissertation, Naval Postgraduate School, 2018.

[7] C. Bellinger, S. Sharma, and N. Japkowicz, "One-class versus binary classification: Which and when?" in 2012 11th International Conference on Machine Learning and Applications, vol. 2, 2012, pp. 102–106.

[8] I. Goodfellow, Y. Bengio, and A. Courville, Deep learning. MIT Press, 2016. [Online]. Available: http://www.deeplearningbook.org.

[9] E. Nakashima. Foreign Hackers Targeted U.S. Water Plant in Apparent Malicious Cyber Attack, Expert Says. Accessed: Mar. 23, 2021. [Online].

[10] I. A. Khan, D. Pi, Z. U. Khan, Y. Hussain, and A. Nawaz, "HML-IDS: A hybrid-multilevel anomaly prediction approach for intrusion detection in SCADA systems," IEEE Access, vol. 7, pp. 89507–89521, 2019.

[11] T. K. Das, S. Adepu, and J. Zhou, "Anomaly detection in industrial control systems using logical analysis of data," Comput. Security, vol. 96, Sep. 2020, Art. no. 101935.

[12]] M. M. N. Aboelwafa, K. G. Seddik, M. H. Eldefrawy, Y. Gadallah, and M. Gidlund, "A machine-learning-based technique for false data injection attacks detection in industrial IoT," IEEE Internet Things J., vol. 7, no. 9, pp. 8462–8471, Sep. 2020.

[13] M. Alaeiyan, A. Dehghantanha, T. Dargahi, M. Conti, and S. Parsa, "A multilabel fuzzy relevance clustering system for malware attack attribution in the edge layer of cyber-physical networks," ACM Trans. Cyber Phys. Syst., vol. 4, no. 3, pp. 1–22, 2020.

[14] U. Noor, Z. Anwar, T. Amjad, and K.-K. R. Choo, "A machine learning-based FinTech cyber threat attribution framework using highlevel indicators of compromise," Future Gener. Comput. Syst., vol. 96, pp. 227–242, Jul. 2019.

[15] A. N. Jahromi, J. Sakhnini, H. Karimpour, and A. Dehghantanha, "A deep unsupervised representation learning approach for effective cyberphysical attack detection and identification on highly imbalanced data," in Proc. 29th Annu. Int. Conf. Comput. Sci. Softw. Eng. (CASCON), 2019, pp. 14–23