Using Bayesian Network for Cyber-physical Threat Model in Railway Transport System

O.Y. Ogunlola, O. Owolafe, A.O. Oronti, B.K. Alese
Department of CyberSecurity
Federal University of Technology Akure
Nigeria

Abstract

Railway transportation systems are critical infrastructures, but they also face vulnerabilities from both cyber and physical threats. This research proposes a comprehensive approach using Bayesian Networks to model and analyze these threats. The model classifies, identifies, and assesses risks to railway networks by analyzing conditional dependencies. This research proposes a comprehensive approach to modeling and analyzing these threats using Bayesian Networks. Bayesian networks are graphical models that depict complex relationships among variables in a probabilistic framework. The proposed method involves modeling the interactions between cyber threats, physical components, and their potential consequences by identifying key system elements, defining possible cyber threats and physical impacts, constructing a Bayesian network structure, and estimating probability tables with conditions. The model seeks to classify, identify, and assess the risks to railway networks by analyzing the conditional dependencies among system vulnerabilities and potential threat vectors. Using the ML.NET library and C# programming language, a probabilistic framework was developed for real-time threat detection and risk assessment. The model demonstrated high accuracy, precision, and recall, offering a practical and scalable solution for detecting and mitigating cyber-physical threats.

1. Introduction

Cyber-physical systems (CPS) consist of interacting physical, digital, analog, and human components that have been designed with integrated logic and physics for their intended use [9]. The word "CPS" was first used in 2006 by the U.S. National Science Foundation to refer to a sophisticated, interdisciplinary, system of the future that incorporates embedded system into the real world. CPS belongs to a class of systems that incorporate physical processes, computation, and networking [12]. In a time when physical and cyber systems are increasingly integrated, protecting the security of cyber-physical systems (CPS) is essential. A smart decision system may link and integrate several components, including actuators and sensors, to form a CPS [8]. Physical system comprises physical devices, while the cyber portion consists of computer processes utilizing web, cloud, and embedded activities. These activities interact with real-world data for decision-making as shown in Figure 1.

Railway systems, consisting of rolling stock, control, communication, and network infrastructure, face uncertainties that can disrupt operations and cause delays. Factors making railway systems attractive targets for cyber-attacks include distributed architecture, extended equipment lifecycle, diverse supply chains, and growing digital connectivity, increasing vulnerability of critical signaling systems.

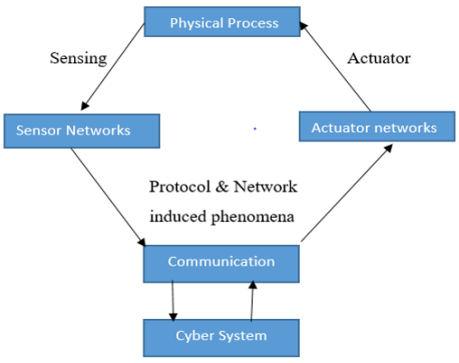


Figure 1. Structure of Cyber-Physical system

Bayesian Networks (BNs) represent a probabilistic graphical model that captures the probabilistic connections between a set of variables [4]. These networks are rooted in Bayesian probability theory, allowing them to model and reason about uncertainty and dependencies in a systematic manner. Because physical and cyber systems are interrelated, they may be utilized to estimate the likelihood of cyber-attacks and their possible outcomes. Cyber-physical threat modeling using Bayesian networks is a promising approach to addressing cyber threats, as it allows for the analysis of complex systems and the

 | DOI: 10.20533/jitst.2046.3723.2024.0106

identification of potential threats. The possibility of sophisticated attacks that can take advantage of weaknesses in both physical and cyber components has grown as a result of the convergence of the digital and physical worlds.

2. Literatures Review

Cyber-Physical Systems (CPS) are systems made up of software, hardware, and human systems that are interconnected and networked. They are used in various industries like energy, transportation, home automation, healthcare, and agriculture. Researchers have studied cyber-attacks on CPS, focusing on their cyber security. CPS combines computational and physical components, improving functionality, reliability, and safety. However, successful cyberattacks can lead to safety violations and operational disruptions, resulting in injuries, deaths, or equipment damage.

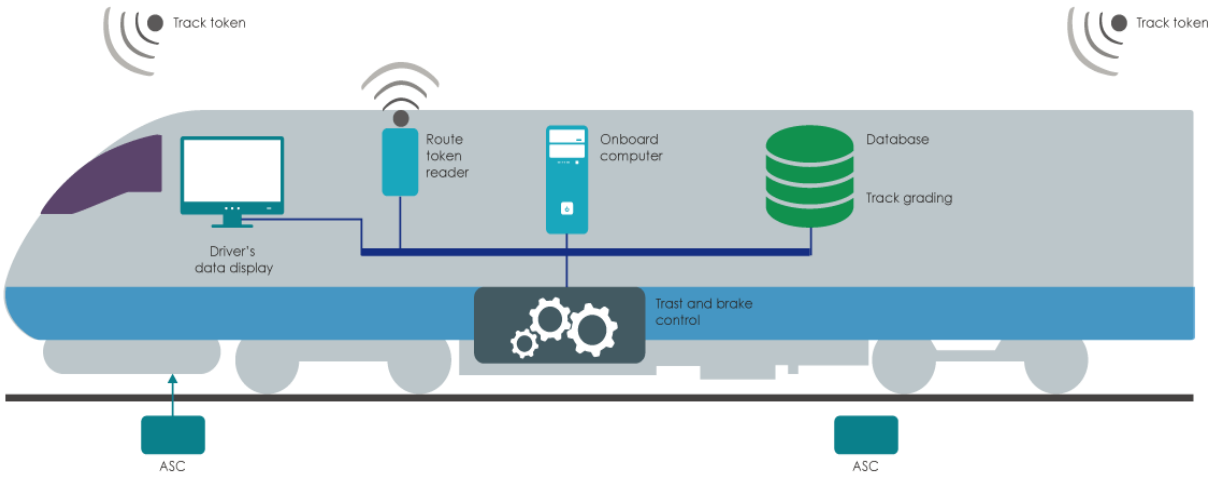


Figure 2: Schematic Structure of an Automatic Train Operation

Cyberattacks against rail CPSs have been common since the early 21st century and continue to expand globally. Bayesian Networks are a powerful tool for threat modeling, representing complex relationships between cyber and physical variables. They incorporate observed data, enabling inference of probabilities for unobserved variables, making them ideal for modeling uncertain and dynamic cyber-physical threats. Equation below represents the generic rule of the Bayesian theorem.

$$P(H/E) = \frac{P\left(\frac{E}{H}\right) * P(H)}{P(E)} \quad (1)$$

Where E is proof of an occurrence and H is a hypothesis. The marginal probability linked to hypothesis H is revised using the Bayes theorem in light of the evidence E. The probability of H for a given E is determined by multiplying the posterior probability P(H/E) by the prior probability P(H).

Rasha [12] used Artificial Intelligence and Machine Learning algorithms to detect cyberattacks in physical systems. They used the Heuristic Multi-Swarm Optimization (HMS) algorithm and Self-tuned Fuzzy Logical Hidden Markov Model (SFL-HMM) to outperform previous detection algorithms. Kabanda [10] designed a Bayesian Network-based structure for intrusion detection and prevention in Zimbabwe. Ullah [17] studied the cyber resilience of smart grids using Bayesian Networks, highlighting the importance of mitigating vulnerabilities in access domains. Quentin [16] introduced a framework for authority transfers in remote railway automation. Simone [15] conducted a survey on railway cyber-security in the age of interconnected systems, focusing on the cybersecurity features of railroad signaling systems. They also explored the use of specialized cyber ranges to simulate attack-defense scenarios and analyze vulnerabilities. Davide [4] used a Bayesian network approach to analyze the cyber security resilience of digital infrastructures in power systems.

3. System Design

CPS frequently consists of hardware components like sensors, actuators, and other embedded systems that communicate with both sophisticated software and the outside environment [7]. A wide range of socially significant industries, including energy, transportation, home automation, healthcare, and agriculture, are examples of CPSs. To effortlessly monitor and regulate physical processes, a Cyber-Physical System (CPS) combines computational and physical components [5].

 | DOI: 10.20533/jitst.2046.3723.2024.0106

Modern railways are no longer just physical networks of tracks and trains. They are evolving into complex CPS, incorporating the actual train world, locomotives, and stations with the digital world of information technology (IT), communication networks, and control systems [21].

3.1. System Architecture

The threat detection system uses C# and a Bayesian Network library for machine learning. It includes dataset pre-processing, Bayesian Network classification model, and Inference Analyzer for incoming network traffic analysis. These components classify new data.

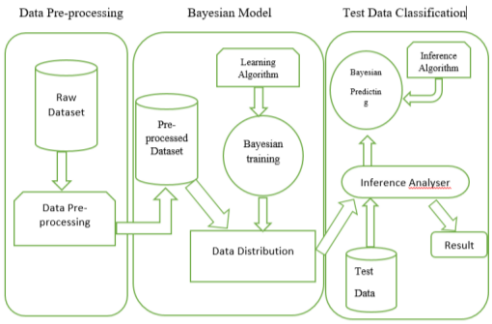


Figure 3. Railway CPS Threat Model using Bayesian Network

3.1.1. System Framework: The Rail CPS, a system that identifies various types of attacks, uses a Bayesian network classification model to produce precise detection outcomes, ensuring a small percentage of attacks evade it, demonstrating its primary uniqueness.

i. The following are included in the model's conceptual framework:

- Threat Categories: Clearly specify the types of cyberthreats that will be modelled, such as malware, physical sabotage, network intrusions, denial-of-service assaults, and signal manipulation.

ii. Determine the variables and nodes:

- Threat Nodes: These stand for the particular dangers that fall under each heading.
- Vulnerability Nodes: These point to areas of the system that might be exploited.
- Impact Nodes: Calculate the possible outcomes of an assault that is successful.
- Additional Relevant Nodes: Take into account system statuses or environmental elements (weather, time of day) that might affect risks.

iii. Build Communication: identifying the nodes' causal relationships. This creates the structure of the Bayesian network.

3.1.2. Feature Extraction and Data Preprocessing: Feature extraction is a crucial process in machine learning and data analysis, identifying and isolating relevant features from raw data. This process minimizes data dimensionality, making analysis easier and improving the efficiency of machine learning systems. It also involves feature engineering and data modification. Important data preparation procedures include:

i. Data Cleaning: The goal of this stage is to identify and correct errors or inconsistencies in the data, such as duplicates, outliers, and missing values. Cleaning techniques including imputation, removal, and transformation are frequently employed.

ii. Data Integration: To produce a coherent dataset, data from many sources is combined in this procedure. Due to variations in formats, structures, and meanings, data integration can be challenging. To overcome these obstacles, techniques like data fusion and record linking are employed.

iii. Data Transformation: Data is transformed into a suitable format for analysis using techniques like standardisation, normalisation, and discretisation, which convert continuous data into categorical data.

iv. Data reduction involves reducing the size of a dataset by converting it into a lower-dimensional form and selecting a subset of relevant characteristics.

3.2. Bayesian Network Construction

Bayesian network classifiers are created using training data from data distributors, constructing probability distribution tables and learning parameters and structures. They use structured learning, or casual discovery, to learn parameters and structure from input data. The model uses the library's API to define network structure and specify conditional probability distributions (CPDs) for each node. Learning algorithms like expectation-maximization and maximum likelihood estimation determine CPD parameters using the training data.
Nodes: The main event model includes a Cyber Attack (CA), vulnerabilities (V), Threat Actor Capability (TAC), security controls (SC), and external factors (EF). CA represents the main event, V represents system vulnerabilities, TAC represents potential attackers' skill and resources, SC represents security measures, and EF includes geopolitical tensions and vulnerabilities.

 | DOI: 10.20533/jitst.2046.3723.2024.0106

Dependencies (Edges): The probability of a cyber-attack increases with vulnerabilities, threat actor capability, and weak security controls. Strengthening controls depends on V, while external factors can influence TAC.

Using Bayes' Theorem, we can express the probability of a cyber-attack given the evidence of other variables as shown in equations 2 and 3 while equation 1 shows the generic rile of BN saying the probability of hypothesis H to a proof of occurrence E is the probability of E to H over the probability of E:

$$P(H/E) = \frac{P\left(\frac{E}{H}\right) * P(H)}{P(E)} \quad (1)$$

$$P(CA|V, TAC, S, EF) = [P(V, TAC, SC, EF\ |CA) * P(CA)]/ P(V, TAC, SC, EF) \quad (2)$$

$$P(CA, V, TAC, SC, EF = \prod_{i=1}^{n} P\left(Parent(CA_i)\right) * \prod_{j=1}^{n} P\left(Parent\left(V_j\right)\right) * \prod_{k=1}^{n} P\left(Parent(TAC_k)\right) * \prod_{l=1}^{n} P\left(Parent(S_l)\right) * \prod_{m=1}^{n} P(EF_m|Parent(EF_m)) \quad (3)$$

Where:

- P(CA | V, TAC, SC, EF): The likelihood of a cyberattack in the future, based on detected vulnerability, threat actor, security control, and external factor values.
- P(V, TAC, SC, EF | CA): The likelihood of observing the given values of the other variables if a cyber-attack has occurred.
- P(CA): The prior probability of a cyber-attack.
- P(V, TAC, SC, EF): The marginal probability of observing the given combination of the other variables.

4. System Implementation

In order to simulate cyber-physical dangers in railway transport systems, this study makes use of Bayesian networks (BN). With ML.NET and C#, a comprehensive and scalable framework for threat identification and risk analysis is provided. The goal is to develop a system that can identify, classify, and gauge the seriousness of cyber-physical threats in order to efficiently reduce risks for the rail sector.

Tools

Visual Studio 2022
C# Programming Language
ML.Net (Machine Learning Probabilistic Libraries)
CSVHelper

ML.NET integrates machine learning into.NET applications, enabling automatic prediction using available data patterns. Its core is a machine learning model, which can be trained using algorithms or pre-trained models from TensorFlow and ONNX. ML.NET is compatible with Windows, Linux, macOS, and Windows using.NET Framework, with 32-bit support limited to Windows (see Figure 4).

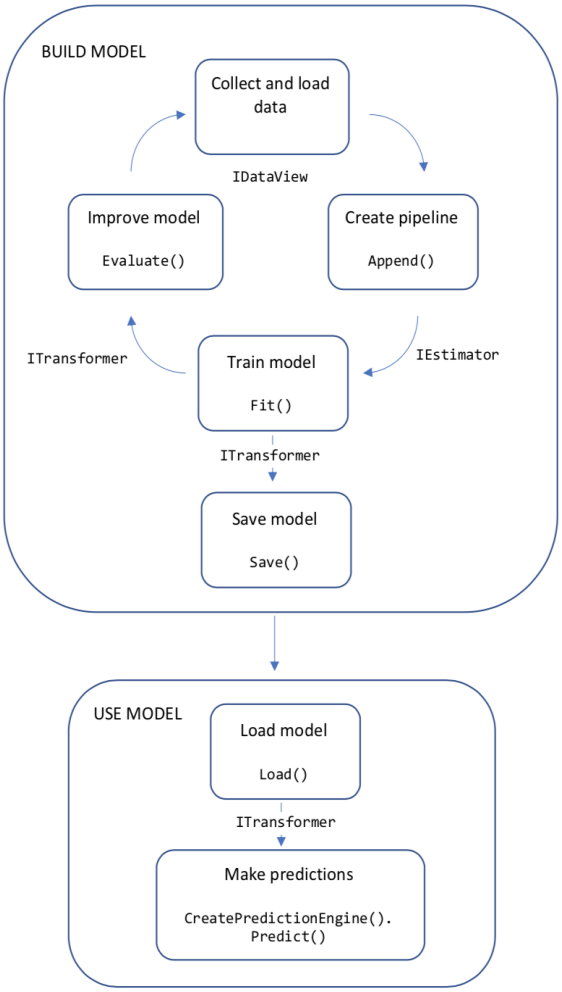


Figure 4. ML.NET workflow

C# is a high-level programming language developed by Anders Hejlsberg, Scott Wiltamuth, and Peter Golde, primarily at Microsoft. It supports multiple paradigms and is recognized as an international standard. Microsoft introduced C# alongside the.NET Framework and Visual Studio, initially as a closed-source product. Later, they released Visual Studio Code, Roslyn compiler, and unified.NET platform (see Figures 5, 6, and 7).

CsvHelper is a C# utility that simplifies CSV file reading and writing in.NET applications, enabling serialization, deserialization, syntactic parsing, data type recognition, and compatibility with LINQ and anonymous types (see Figure 8).

 | DOI: 10.20533/jitst.2046.3723.2024.0106

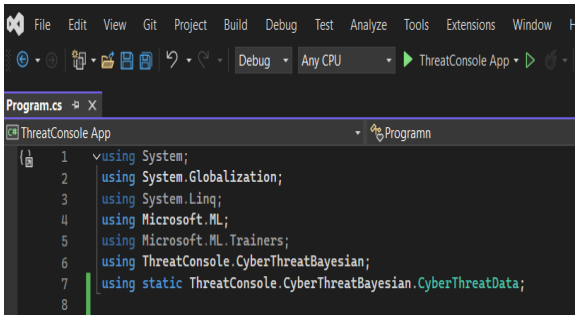


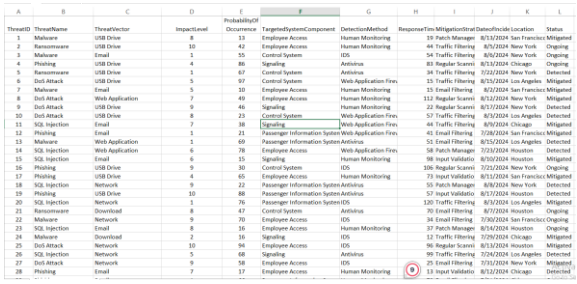
Figure 5. Usage of libraries

```
var split = mlContext.Data.TrainTestSplit(data, testFraction: 0.2);

// Define your Bayesian model pipeline (with potential feature engineering)
var pipeline = mlContext.Transforms.Categorical.OneHotEncoding("ThreatNameEncoded", "ThreatName")
    .Append(mlContext.Transforms.Categorical.OneHotEncoding("ThreatVectorEncoded", "ThreatVector"))
    // ... more one-hot encodings as needed
    .Append(mlContext.Transforms.Concatenate("Features", "ThreatID", "ThreatNameEncoded", "ThreatVectorEncoded", "ImpactLevel",
                                             "TargetedSystemComponent", "DetectionMethod", "ResponseTime", "MitigationStrategy",
    .Append(mlContext.MulticlassClassification.Trainers.NaiveBayes(labelColumnName: "IsThreat", featureColumnName: "Features"));

// Train the model
var model = pipeline.Fit(split.TrainSet);

// Evaluate the model
```

Figure 6. Script showing data splitting

```
// Step 4: Train the model
Console.WriteLine("Training the model...");
var model = pipeline.Fit(splitData.TrainSet);

// Step 5: Evaluate the model
Console.WriteLine("Evaluating the model...");
var predictions = model.Transform(splitData.TestSet);
var metrics = _mlContext.MulticlassClassification.Evaluate(predictions);

Console.WriteLine($"Macro Accuracy: {metrics.MacroAccuracy:F2}");
Console.WriteLine($"Micro Accuracy: {metrics.MicroAccuracy:F2}");
Console.WriteLine($"Log Loss: {metrics.LogLoss:F2}");

// Step 6: Save the model
_mlContext.Model.Save(model, splitData.TrainSet.Schema, _modelPath);
Console.WriteLine($"Model saved to: {_modelPath}");

// Step 7: Make a prediction
var predictionEngine = _mlContext.Model.CreatePredictionEngine<ThreatRecord, ThreatPrediction>(model);

var sampleThreat = new ThreatRecord
{
    ThreatVector = "Network",
    ImpactLevel = 3.0f,
```

Figure 7. Prediction and evaluation Script



ThreatID	ThreatName	ThreatVector	ImpactLevel	ProbabilityOf Occurrence	TargetedSystemComponent	DetectionMethod	ResponseTim	MitigationStrat	DateofIncide	Location	Status
1	Malware	USB Drive	8	13	Employee Access	Human Monitoring	19	Patch Manager	8/13/2024	San Francisc	Mitigated
2	Ransomware	USB Drive	10	42	Employee Access	Human Monitoring	44	Traffic Filtering	8/9/2024	New York	Ongoing
3	Malware	Email	1	55	Control System	IDS	54	Traffic Filtering	8/6/2024	New York	Ongoing
4	Phishing	USB Drive	4	86	Signaling	Antivirus	83	Regular Scanni	8/13/2024	Chicago	Ongoing
5	Ransomware	USB Drive	1	67	Control System	Antivirus	34	Traffic Filtering	7/22/2024	New York	Detected
6	DoS Attack	USB Drive	5	97	Control System	Web Application Firev	15	Traffic Filtering	8/15/2024	Los Angeles	Mitigated
7	Malware	Email	5	10	Employee Access	Human Monitoring	15	Email Filtering	8/2/2024	San Francisc	Mitigated
8	DoS Attack	Web Application	7	49	Employee Access	Human Monitoring	112	Regular Scanni	8/12/2024	New York	Mitigated
9	DoS Attack	USB Drive	9	46	Signaling	Human Monitoring	22	Regular Scanni	8/17/2024	New York	Detected
10	DoS Attack	USB Drive	8	23	Control System	Web Application Firev	57	Traffic Filtering	8/3/2024	Los Angeles	Detected
11	SQL Injection	Email	7	38	Signaling	Web Application Firev	44	Traffic Filtering	8/9/2024	Chicago	Mitigated
12	Phishing	Email	1	21	Passenger Information System	Web Application Firev	41	Email Filtering	7/28/2024	San Francisc	Mitigated
13	Malware	Web Application	1	69	Passenger Information System	Antivirus	51	Email Filtering	8/15/2024	Los Angeles	Detected
14	SQL Injection	Web Application	6	78	Employee Access	Web Application Firev	58	Patch Manager	7/23/2024	Houston	Detected
15	SQL Injection	Email	6	15	Signaling	Human Monitoring	98	Input Validatio	8/10/2024	Houston	Mitigated
16	Phishing	USB Drive	9	30	Control System	IDS	106	Regular Scanni	7/21/2024	New York	Ongoing
17	Phishing	USB Drive	4	65	Employee Access	Human Monitoring	73	Input Validatio	8/11/2024	San Francisc	Mitigated
18	SQL Injection	Network	9	22	Passenger Information System	Antivirus	55	Patch Manager	8/8/2024	New York	Detected
19	Phishing	USB Drive	10	88	Passenger Information System	Antivirus	57	Input Validatio	8/17/2024	Houston	Detected
20	SQL Injection	Network	1	76	Passenger Information System	IDS	120	Traffic Filtering	8/3/2024	Los Angeles	Mitigated
21	Ransomware	Download	8	47	Control System	Antivirus	70	Email Filtering	8/7/2024	Houston	Ongoing
22	Malware	Network	9	70	Employee Access	IDS	34	Email Filtering	7/30/2024	San Francisc	Ongoing
23	SQL Injection	Email	8	16	Employee Access	Human Monitoring	27	Patch Manager	8/14/2024	Houston	Ongoing
24	Malware	Download	2	16	Signaling	IDS	12	Traffic Filtering	7/29/2024	Chicago	Mitigated
25	DoS Attack	Network	10	94	Employee Access	IDS	96	Regular Scanni	8/13/2024	Houston	Mitigated
26	SQL Injection	Network	5	68	Signaling	Antivirus	99	Traffic Filtering	7/24/2024	Los Angeles	Detected
27	DoS Attack	Network	9	58	Employee Access	IDS	25	Email Filtering	7/31/2024	New York	Mitigated
28	Phishing	Email	7	17	Employee Access	Human Monitoring	13	Input Validatio	8/12/2024	Chicago	Detected

Figure 8. Screenshot of CSV file containing railway Cyber Threat dataset

4.1. Result

A Bayesian Network (BN) allows various types of analysis, including predictive, diagnostic, and combined diagnostic / predictive studies. The probability of a successful attack is a useful predictive analysis for early threat identification. The evaluation model shows that malware has the highest occurrence of attacks based on the predicted causes, providing guidance for early threat identification (see Figure 9).

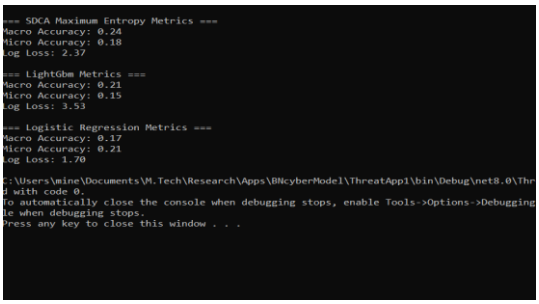


Figure 9. Result after Training

5. Conclusion

The study developed a cyber-physical threat modelling framework using Bayesian networks to evaluate and manage security risks in the integration of physical and cyber systems. The model identifies and quantifies cyber threats within the railway system using machine learning techniques, particularly multiclass classification. The model uses probabilistic models with nodes and edges for predictive analysis. ML.NET's algorithms can transform non-numeric data into a format suitable for the model. The model was trained using 70% of the data and assessed using log loss, micro accuracy, and macro accuracy. It accurately forecasted cyber threats using characteristics like attack vectors, impact degree, likelihood of occurrence, and reaction time. The BN-based threat modeling framework can be used by cybersecurity professionals to develop mitigation strategies and cybersecurity regulations.

6. Recommendation

Cybersecurity is crucial in information technology and systems, especially in railway systems. The digitalization of railway systems has combined cyber and physical infrastructure issues. This report highlights threats and issues related to railway systems and discusses data security techniques. Organizations should focus on cybersecurity challenges and incorporate safeguard technologies into digital platforms to reduce attacks.

7. References

[1] Association of American Railroads. (2022). Freight Rail: Designed to Drive a Nation. Association of American Railroads.

[2] Ahmed, Chuadhry M., Venkata R., and Aditya P.

 | DOI: 10.20533/jitst.2046.3723.2024.0106

(2017). WADI: a water distribution tested for research in the design of secure cyber physical systems." In Proceedings of the 3rd International Workshop on Cyber-Physical Systems for Smart Water Networks, pp. 25-28.

[3] Ci Liang, Mohamed G., Olivier C., and El-Koursi E. (2017). Bayesian Network Modelling Applied on Railway Level Crossing Safety. International Conference on Reliability, Safety and Security of Railway Systems.

[4] Davide C, Daniele C., Giovanna D. Lavinia E., and Giuliana F. (2019). A Bayesian Network Approach for the Interpretation of Cyber Attacks to Power Systems. Published in Intalian Conference of Cyber security; vol-2315/paper11.

[5] Eduardo B. (2016). Threat Modelling in Cyber-Physical Systems. Conference Paper publication at Florida Atlantic University. DOI: 10.1109/DASC-PICom-DataComCyberSciTec.2 016.89.

[6] Fernling F., Junjie J., Ailan L. Chengguang L. (2022). Bayesian network-based risk evaluation model for the operational requirements of the China Railway Express under the Belt and Road initiative. Transportation Safety and Environment, Volume 4, Issue 3, September.

[7] George S., Mari-Anais S., Ioana P., Daniel P., Luca V., Silvai A. (2021). Cyber-physical Threat Detection Platform Designed for Health Care Systems. Annals of Disaster Risk Sciences. Vol 3, No 1 (2020): Special issue on cybersecurity of critical infrastructure.

[8] Hu L, Xie N, Kuang Z, Zhao K. (2012). Review of cyber-physical system architecture. In: Proceedings of the IEEE International Symposium on Object/Component/ Service-Oriented Real-Time Distributed Computing Workshops (ISORCW). Shenzhen, China.

[9] Imen G., Slim K., Nawal G., Ahmed H. . (2018). A comprehensive survey on modeling of cyber-physical systems. Issue Paper DOI:10.1002/cpe :4850.

[10] Kabanda Gabriel. (2020). A Bayesian Network Model for a Zimbabwe Cyber security System. Oriental Journal of Computer Science and Technology, Vol.12, No 3.

[11] Lessan, J., Fu, L., Wen, C. (2018) A Hybrid Bayesian Network Model for Predicting Delays in Train Operations, Computers and Industrial Engineering, DOI: 10.1016/j.cie. 2018.03.017.

[12] Rasha A., Amer I., Abedallah Z., Naha M. and Faris A. (2022). Using machine learning algorithm for detection of cyber-attacks in cyber physical systems, College of Computer Information Technology; American University in Emirates, Dubai, UAE. Periodicals of Engineering and Natural Sciences, vol. 10, No.3, pp.261-275.

[13] Sabarathinam C., Wolter P., Andre T., and Pieter V. (2017). Bayesian Network Models in Cyber Security: A Systematic Review. `Proceedings of the Nordic Conference on Secure IT Systems, Springer under DOI: 10.1007/978-3-319-70290-2_7.

[14] Sdca Maximum Entropy Multiclass Trainer class (n.d). ML. NET 3.0.0. https://learn.microsoft.com/en-us/dotnet/api/microsoft.ml.trainers.sdcamaximumentropymulticlasstrainer?view=ml-dotnet (Access Date: 11 December 2024).

[15] Simone S., Daniele M., Yuriy Z. (2023). Railway Cyber-Security in the Era of Interconnected Systems: A Survey. IEEE Transactions on Intelligent Transportation Systems, Volume: 24, Issue: 7, July 2023.

[16] Quentin G., Philippe R., Jean-Christophe P., and Chouki S. (2022). Railway Automation: A framework for authority transfers in a remote environment. IFAC-PapersOnLine Volume 55, Issue 29, Pages 85-90.

[17] Ullah N., Morteza N., Raed J., Shah C. Randy B., Michael H. (2020). Modeling and assessing cyber resilience of smart grid using Bayesian network-based approach: a system of systems problem; Mississippi State University. Journal of Computational Design and Engineering. DOI:10.1093/jcde/qwaa029.

[18] Wahida F., Mohammed N., Ashraf U., Alamin T., Rahat H., Souvik P., Faisal I., and Rakib H. (2024). A stacked ensemble approach to detect cyber attacks based on feature selection techniques. International Journal of Cognitive Computing in Engineering Volume 5, 2024, Pages 316-331.

[19] Xiaoyan Sun, Jun Dai, Peng Liu, Anoop Singhal, and John Yen. (2017) Using Bayesian networks to fuse intrusion evidences and detect zero-day attack paths. In Network Security Metrics, pages 95,115. Springer.

[20] Yaa Takyiwaa A. and Roy K. (2024). Exploration of Ensemble Methods for Cyber Attack Detection in Cyber-Physical Systems. In book: Artificial Intelligence Applications and Innovations.

[21] Zezhou W. and Xiang L. (2022) “Cyber Security of railway cyber-physical system (CPS)-A risk management methodology”. Communications in Transportation Research Journal.

 | DOI: 10.20533/jitst.2046.3723.2024.0106