
Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2024 SCPE. Volume 25, Issues 1, pp. 577–591, DOI 10.12694/scpe.v25i1.2405

VULNERABILITY DETECTION IN CYBER-PHYSICAL SYSTEM USING MACHINE LEARNING

BHARATHI V*AND C. N. S. VINOTH KUMAR†

Abstract. The cyber-physical system is a specific type of IoT communication environment that deals with communication through innovative healthcare (medical) devices. The traditional medical system has been partially replaced by this application, improving healthcare through efficiency, accessibility, and personalization. The intelligent healthcare industry utilizes wireless medical sensors to gather patient health information and send it to a distant server for diagnosis or treatment. The healthcare industry must increase electronic device accuracy, reliability, and productivity. Artificial intelligence (AI) has been applied in various industries, but cybersecurity for cyber-physical systems (CPS) is still a recent topic. This work presents a method for intelligent threat recognition based on machine learning (ML) that enables run-time risk assessment for better situational awareness in CPS security monitoring. Several machine learning techniques, including Nave Bayes (65.4%), Support Vector Machine (64.1%), Decision Tree (89.6%), Random Forest (92.5%), and Ensemble crossover (EC) XG boost classifier (99.64), were used to classify the malicious activities on real-world testbeds. The outcomes demonstrate that the Ensemble crossover XG boost enabled the best classification accuracy. When used in industrial reference applications, the model creates a safe environment where the patient is only made aware of risks when categorization optimism exceeds a specific limit, minimizing security managers' pressure and efficiently assisting their choices.

Key words: Cyber-Physical Systems, Trustworthy Artificial Intelligence, Cybersecurity, Healthcare, Machine Learning, Critical Infrastructures.

1. Introduction. The healthcare landscape has changed due to the assumption of developing automation like the Internet of Things (IoT), intelligent bio-medical sensors (BMSs), and the cloud that have increased life expectancy rates. As a result, it raised people's living standards. The fifth industrial revolution (industry 5.0) is based on a cyber-physical system that connects digital diagnostic products, like computers and the Internet, to physical processes[33]. Healthcare professionals can use H-CPS to process the sensed data and make wise decisions. Medical practitioners must adhere to H-CPS-based procedures to provide better treatment for less money. IoMT smart devices can gather, evaluate, and broadcast various data in a healthcare setting that uses H-CPS.

Additionally, these wearable sensors continuously monitor the patient's health characteristics, such as blood pressure, temperature, and pulse rate, and communicate the information to nearby access systems for computation and feature selection. Using Artificial Intelligence (AI)-enabled technology, the pre-processed data is sent to remote computing equipment for disease detection or prognosis [18]. The medical sector has recently been exposed to more complex and extensive cyber risks, drawing attention to the lack of cybersecurity skills. For instance, the healthcare supply chain has just been exposed to a new cyber threat, becoming more widespread and stable each year. This threat revealed the industry's overall inadequate cybersecurity architecture. Cyber risk is related explicitly to two concurrent advancements: First, the increasingly pervasive incorporation of technologies, modernization, and novel healthcare systems [34], including automated treatment pathways, electronic health records, individualized therapies, and widely scattered IoMT (Internet of Medical Things) equipment.

On the contrary side, cybersecurity practice upgrading and invention procedures find it challenging to keep up with the rate of advancements in technology. Because of the intersection of these two tendencies, the healthcare industry is highly vulnerable to cyber threat, which has increased in both severity and frequency in

*Department of Networking and Communications, College of Engineering and Technology (CET), SRM Institute of Science and Technology, Kattankulathur Chennai, India (bv3994@srmist.edu.in)

†Corresponding Author, Department of Networking and Communications, College of Engineering and Technology (CET), SRM Institute of Science and Technology, Kattankulathur Chennai, India. (vinothks1@srmist.edu.in).

recent years. The availability of the data, therefore making it impossible for legitimate owners to access the data to make it susceptible to exploitation, as well as the integrity, correctness, and alteration of the accuracy, are three potential targets for cyberattacks in the health sector. Knowing an individual's or a portion of the population's health figure could have financial implications. The requirement to strike a balance between the necessity for security and information privacy and the accessibility of information to maintain the essential benefit of the person's health adds another layer of complexity to many crucial professions, such as healthcare. The above explains why it can be challenging to put stringent cybersecurity controls in place that hamper healthcare, especially in times of need and urgency[11].

The use of AI as a decision support tool while leaving ultimate decision-making in the hands of people was agreed upon by machine learning (ML), artificial intelligence, and cybersecurity. The multiple contributions to this topic proposed some ML 'anomaly-based' approaches. Unfortunately, there are fewer comparative studies to determine the best effective learning method for improved detection capacity and fewer false alarms than for ML approaches. The possibilities of boosting ML approaches' dependability and the extent to which they apply to real-world situations are also major open questions. Even though many security strategies for Critical Infrastructure (CI) have been presented, there are still many obstacles to overcome to autonomously spot risks in the face of complexity, uncertainty, and change, especially when considering phenomena like sensors are compromised [30]. Additionally, a novel perspective on CIs has emerged recently, which they have seen as complicated Medical Cyber-Physical Systems (HCPS).

Modern CPS comprises real and intangible elements, including databases and software algorithms for data elaboration and electro-mechanical devices, sensors, and actuators. Threats can be both tangible and intangible because of the nature of CPS. Cyberthreats, for example, could directly affect the physical components' integrity and indirectly affect the environment's and the related parties' overall health. These threats may also have a chain of associated repercussions. This paper's essential contribution is as follows: We offer a vulnerability assessment technique for CPSs that considers cyber-physical and physical-cyber interdependencies to derive goal-oriented attack routes. The suggested procedure:

- Artificial intelligence is a paradigm for coordinating the efforts of many machine learning algorithms to detect and prevent harmful or malicious occurrences.
- Exposes sophisticated cyber-physical assaults by using vulnerability analysis techniques to deduce the motivations of adversaries.
- Attack route analysis is made more efficient by switching from a blind analysis to an algorithmic analysis with clear end goals.
- It is a practical approach to computing risk and evaluating Likelihood and Impact based on security-relevant criteria.

The remainder of the paper is organized as follows: This document is organized for the remaining portions: The relevant work's outline is presented 2, while the material and methods are presented in Section 3. In Section 4, experimental analysis is presented. Section 5 serves as the paper's conclusion.

2. Related Work. The CPS explosive expansion, security, and privacy are necessary for reliable communication in innovative healthcare [37]. Sun et al. [24] addressed the privacy and security concerns with IoT in the healthcare sector and remarked on the potential routes for further study. Hu et al. [16] used attribute-based encryption to address the issue of safe communication between a BAN and its data consumer (end-user). According to Chandrasekaran et al. [7], the technique [16]is ineffective for repeated data transfer, and they provide a novel system for safely transmitting data in WBAN. Blockchain technology was used by Egala et al. [10] to create a safe and decentralized platform for sharing health data records without jeopardizing system privacy. Kumar and Chand [22] presented a blockchain-based privacy-privacy data-sharing system for the healthcare sector, where an Identity-based broadcast group encryption technique protects each transaction. As a result, interest in managing complex cybersecurity systems increased, and AI techniques were incorporated to assist with automation [4][13]. AI is revolutionizing cybersecurity due to extensive analysis of data, faster reaction times, and effective customization of threat detection for limited records. Further, Artificial Intelligence has already-existing and synergistic applications for pattern recognition and computer vision to identify physical threats [12]. The authors of [15] have created a hybrid IoT generator, a framework for estimating cellular network performance. This platform was combined with big data and Machine Type Communications traffic

models.[6][1] provides information on the various ML-based strategies. The authors systematically explain how machine learning approaches operate and offer their assessments. An overview of ML algorithms in IoT of healthcare data is provided in [5]. This study uses supervised learning, semi-supervised learning, and unsupervised learning ML model types to classify data from the healthcare industry and show the work on the data. The threat modeling tools STRIDE [1], Factor Analysis of Information Risk (FAIR)[5], and OCTAVE [9] have all been utilized in the process of assessing the level of risk present in CPSs across a variety of application areas. Another prevalent strategy[35] combines two or more methodologies: STRIDE and CVSS. It is possible that the "traditional" impact criteria of confidentiality, integrity, and availability will not be sufficient for CPSs; consequently, the methods used to assess the cyber risk posed by these systems must typically be industry-specific. This is why research on the safety and security of CPSs is carried out simultaneously. In [20], we comprehensively analyze different approaches to co-engineering of safety and security. In [23], we summarize risk assessment techniques applicable to the smart grid scenario. Kandasamy et al. [19] presented a general overview of the methods for assessing the Internet of Things risks. A rundown of a few methods for determining how vulnerable SCADA systems are to attack is provided for us in reference [8][26] delves into the various approaches that can be taken to perform risk assessments in the automotive sector. Recent research, such as that presented in [25], examines various risk assessment strategies for CPS from the perspectives of safety, security, and the integration of all three and proposes specific categorization criteria. Current approaches to risk assessment for CPSs, which primarily focus on either one or the other of these two types of interdependencies, ignore, for the most part, cyber-physical and physical-cyber interdependencies. When researching the system, the authors of[29] focused on its physical components, whereas Homer et al. [14] investigated only the system's cyber components. It has been demonstrated by Krotofil et al. [27] that this is not the case, despite the fact that attackers may use the physics of the mechanism that is behind a CPS. When it comes to developing security policies, these same authors argued that the physical process layer should be considered. According to[28], research into cyber-physical systems needs to adopt a more comprehensive methodology because of the complex intertwining of computer networks and physical processes.

Regrettably, to the best of our knowledge from Table 3.1, no risk assessment method that satisfies this criterion has ever been made public. This study covers a knowledge gap with its recommended practices. The recommended strategy facilitates research of the entire cyber-physical system for each undesired event, in contrast to present methodologies. As a result, the review shows some of the disadvantages over existing methods; hence, in this work, three possibilities were evaluated to find the optimum strategy that will build up the existing research gaps.

Possibility 1: This work uses binary classification to alert the customer whenever an abnormality has been found by identifying its kind or context. Knowing the nature of a threat is necessary to take adequate preventative measures, even though its identification is crucial.

Possibility 2: Given the four components that make up the system, this instance seeks to tell the operator about the one that the anomaly has affected. As a result, it is an inter-categorization. The classes investigated are 5: pulse rate, temperature, SpO2, blood pressure, and the scenario in which an anomaly impacts no sensor.

Possibility 3: The most recent experiment aimed to categorize the incidents into the following categories: failure, damage, accident/damage, cyberattack, failure/damage, and, ultimately, the lack of abnormalities. The response time could be significantly shortened by resorting to relevant risk management by providing the user only with the known malicious scenario.

3. Materials and Methods. This paper examines five machine-learning techniques to discover trends in PCA information. They categorize strange events using the selected models, including hardware (sensor issues), cyberattacks, and sabotage. Naive Bayes, SVM, DT, RT, and Ensemble crossover XG boost classifiers are the models that have been chosen depending on the latest research and taking into account the FPR rates attained by prior research. The overall system architecture was shown in Figure 3.1.

Data are periodically gathered from various patients. These data comprise multiple situations structured in CSV files across a range of time—the length of the file changes according to the circumstance and malfunctioning element. Typical operational occasions and strange events include physical malfunctions and cybersecurity issues. For example, a decision-maker may need to understand these scenarios or become aware of them when malicious activity occurs. Attack analysis are crucial because poorly handled circumstances may result in highly

Table 2.1: Comparative analysis of existing methodology

Tag	Year	Protocol	Attack	Entrypoint	Control	Evaluation metric	Type
1	2022 Khadr et al. (2022)[21]	ZigBee	Jamming	S-S	Parallel-Channel Security-aware Medium Access Control (PCS-MAC) algorithm	Throughput	Physical
2	2022 Yu and Park (2022)[39]	IEEE 802.15.6	Eavesdropping, brute force, service disruption, masquerading	E-S, S-C	Authentication protocol based on blockchain technology and PUFs	Computation time, communication overhead	Simulated
3	2022 Pu et al. (2022)[32]	IEEE 802.15.6	Eavesdropping, data manipulation, replay, service disruption, masquerading	E-S, S-C	Lightweight, anonymous authentication and key agreement protocol	Communication overhead, computation time, energy consumption, CPU time, CPU cycles	Simulated
4	2021 Alzahrani et al. (2021)[3]	IEEE 802.15.6	Eavesdropping, brute force, replay, masquerading	E-S, S-C	Authenticated key agreement based on Burrows-Abadi-Needham (BAN) Burrows et al. (1990) logic	Computation time, communication overhead, energy consumption	Simulated
5	2021 Wang et al. (2021)[38]	IEEE 802.15.6	Eavesdropping, data manipulation, replay, service disruption, masquerading	E-S, S-C	Authentication protocol based on blockchain technology and PUFs	Computation time, communication overhead	Simulated
6	2021 Hussain et al. (2021)[17]	IEEE 802.11	Eavesdropping, data manipulation	S-C, W-C	Physical layer scheme (Gray code)	N/A	Physical
7	2021 Surminski et al. (2021)[36]	IEEE 802.11	Eavesdropping, buffer overflow	C-A	Remote attestation	Runtime, energy consumption, communication overhead, race conditions	Hybrid
8	2020 Alladi et al. (2020)[2]	IEEE 802.15.6	Eavesdropping, data manipulation, masquerading, ARP spoofing, replay	S-C, W-C	Two-way, two-stage authentication protocol using PUFs	Computation time	Simulated

negative operating costs.

The following stages can be used to breakdown the suggested method:

3.1. Data Collection. The dataset was obtained from iot-healthcare-security-dataset. The provided dataset includes regular and malicious traffic data for IoT healthcare use cases. A use case was developed for an Internet of Things (IoT)-based Intensive Care Unit (ICU) consisting of two beds. Each bed has nine patient monitoring devices (See Figure 3.2), sensors, and one control unit known as the Bedx-Control-Unit. All of these devices were developed with the IoT-Flock tool.

The proposed ICU system is based on the Internet of Things (IoT) technology and has a capacity of two beds. Each bed is equipped with nine patient monitoring devices, often called sensors, along with one control unit. The term used to refer to this entity is the Bedx-Control-Unit, where 'x' is the number assigned to each bed, ranging from Bed1 to Bed2. The responsibility of the Bedx-Control-Unit encompasses several tasks,

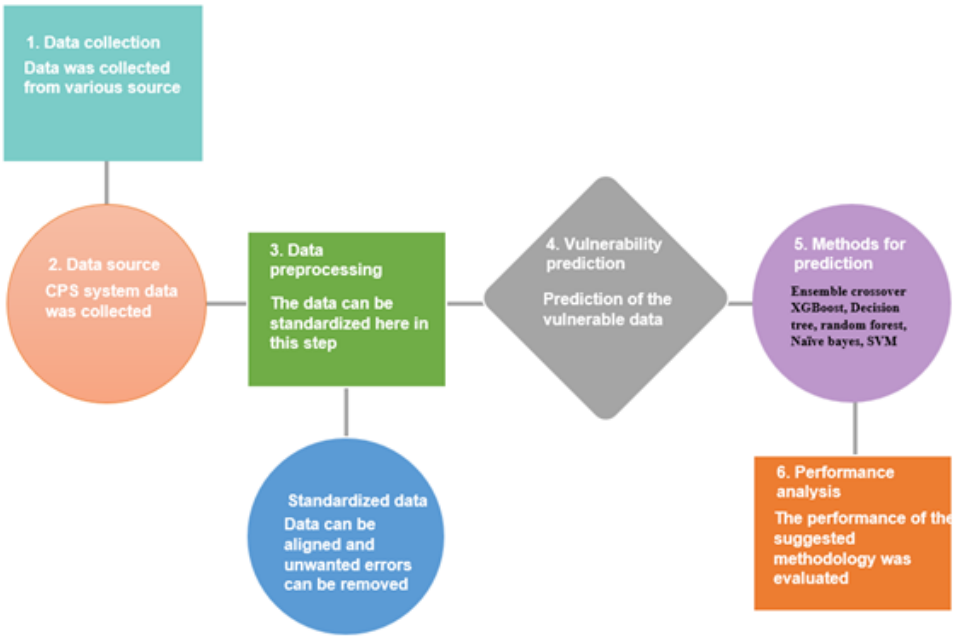

Fig. 3.1: Suggested Architecture of Cyber-Physical System

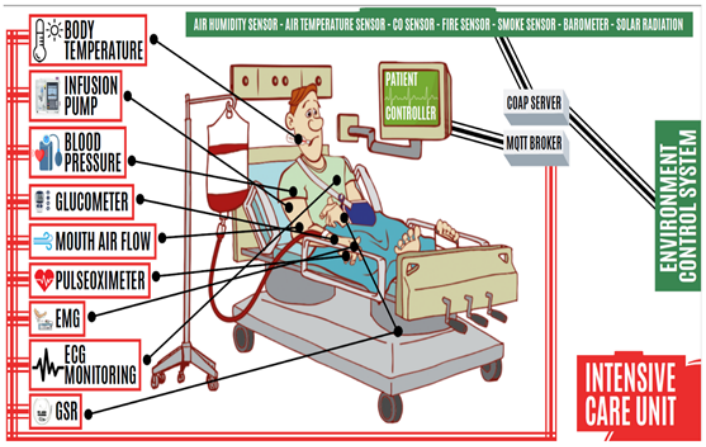

Fig. 3.2: Dataset description

including but not limited to configuring the time profile, determining the dosage administered by an infusion pump, and activating emergency alarms. These activities are contingent upon the patient's physical status, as monitored by the patient monitoring devices.

In a similar vein, an additional control unit was included to facilitate the monitoring of environmental equipment, which was that named the Environment-Control-Unit. The Environment-Control-Unit is tasked with regulating the environmental conditions inside the Intensive Care Unit (ICU), including maintaining specific temperature and humidity levels, detecting the presence of smoke, and activating an emergency alert in

Table 3.1: Patient monitoring sensors

Device Name	**Description**	**Data Profile**	**Time Profile**
Remote Electrocardiogram (ECG) monitoring	Test the electrical and muscular functions of the heart	Pulse Rate (0-200 bpm)	1.0 s
Infusion Pump	A generic device is used to deliver the nutrients and drugs to the patients at a controlled amount	Dose (10-100 mL)	10.0 min
Pulsoximeter (SPO2)	A device that tells the oxygen saturation (i.e.,amount of oxygen dissolved) in blood	Oxygen in blood (35-100%)	1.0 s
Nasal/Mouth AirFlow Sensor	Provides the (breathing) respiratory rate of a patient	Device Respiratory rate (0-60ppm peaks/min)	1.0 s
Blood Monitor Sensor	Measure the pressure of the blood in the arteries when the heart beats	Systolic & diastolic pressure (0-300 mmHg)	2.0 s
Glucometer	A device used to determine the amount of glucose in the blood.	Glucose in Blood (10-150 mg/dL)	10.0 min
Body Temperature	Sensor Measures the temperature of the body	Temperature (0-120 F)	10.0min
Electro-myography (EMG) Sensor	Measures the electric potential produced by the body's muscles	Muscle rate(contractions/min)(0-60cpm)	5.0min
Galvanic skin response (GSR) Sensor	Measures the electrical conductance of skin	Conductance(0-20uS)(micro Siemens)	5.0 min

the event of critical situations in order to uphold the necessary ICU environment. In our specific scenario, both the devices used for patient monitoring operate on the MQTT protocol. The MQTT protocol is characterized by its connection-oriented nature and ability to guarantee the appropriate transmission of packets. Table 3.1 presents an overview of the use case for IoT-based intensive care units.

The attacks identified using this dataset include an MQTT distributed denial-of-service, MQTT publish flood, brute force, and SlowITE attack. The following sections describe the types of attacks that IoT-Flock supports.

- MQTT Publish Flood— A Distributed Denial of Service (DDoS) attack has the potential to deplete the available network bandwidth and exhaust the resources of the targeted victim system. Due to the implementation of more effective mitigation strategies at the network and transport layers, DDoS attackers have shifted their focus towards attacking the application layer. Internet of Things (IoT) devices adhere to either the periodic or event-driven paradigm when transmitting data via application layer protocols. The systematic model device transmits data at regular intervals, such as the temperature sensor sending temperature data to the server every five seconds. In the context of event-driven models, devices transmit data only in response to specific events. For instance, inside an intensive care unit, a motion sensor will only transmit data to the server upon detecting activity in the designated area. According to recent literature, it has been observed that the act of publishing messages at a rapid rate using the MQTT protocol might potentially lead to a denial of service attack. These assaults can potentially impede data transmission significantly and pose substantial risks, particularly in critical sectors such as industrial operations, smart hospitals, and smart transport systems. The potential consequences of data transmission delays may result in the destruction of assets and pose significant risks to human life.
- MQTT Authentication Bypass Attack —To establish a connection with the MQTT broker, which necessitates authentication, MQTT clients transmit MQTT connect requests that include fields for username and password. The discovery was made that the authentication mechanism of MQTT may be circumvented by omitting the password field from the MQTT packet and just supplying a valid username. Despite the mitigation measures used in recent versions of MQTT brokers, the processing

of erroneous packets by an MQTT broker may still result in operational delays, particularly when such packets are sent in substantial quantities. Hence, using IPS to block such an unauthorized packet can mitigate the latency problem associated with the MQTT broker.

- MQTT Packet Crafting Attack —The present assault involves deliberately manipulating MQTT packets to cause a targeted application to malfunction or cease functioning entirely. The assailant initiated a connection with the MQTT broker at the Transport layer and started publication without first issuing a connection request to the MQTT broker.
- COAP Replay Attack— During this attack, an unauthorized individual does an initial network scan to get the addresses of COAP clients and servers and payload information. Subsequently, the unauthorized individual modifies the payload by substituting it with inaccurate data and transmits it to the COAP server, using a deceptive technique that mimics the Sensors 2021, 21, 3025 12 of 19 COAP client IP. The magnitude of this assault becomes apparent when examining instances in which environmental sensors use COAP protocols to relay ambient data to the COAP server. This may be illustrated when the temperature sensor transmits fluctuations in the intensive care unit's temperature. Subsequently, the condition is established by using the data mentioned above. In the event that an assailant employs IP spoofing techniques, they may transmit a manipulated ICU temperature reading, including anomalous values, hence instigating severe and detrimental consequences inside the ICU environment.

3.2. Data pre-processing. This step aims to clarify the information more understandable for the user. The first three steps in pre-processing are: a) Data arrangement: The information must be shown in a logical manner. b) Data scrubbing: Any corrupted or missing data must be removed, replaced, or added to the data. c) Sampling Data: Data must have been sampled regularly before being transferred via communication channels to eliminate redundancy without compromising information.

Transform the data following the algorithm and your understanding of the issue. Feature scaling, deconstruction, or aggregation are all examples of transformation. Features can be aggregated to merge numerous instances into a single element or decomposed to retrieve the valuable components embedded in the data. Three distinct yet interconnected steps can be used to describe this process:

3.3. Vulnerability prediction. For the prediction of the CPS vulnerability in which the visualized data can be split up into train and test data, are separately given as input for the Nave Bayes, Support Vector Machine, Decision Tree, Random Forest, and Ensemble crossover XG boost classifier listed below,

a.Decision Tree (DT) Classifier. A DT is a simple classifier that may be used to put data into groups. In DT, the data is continuously segmented according to a predetermined criterion. Well-known in the field of supervised classification are the DTs. They are effective at categorization tasks, have straightforward decision-making processes, and can be created (trained) quickly and easily thanks to an efficient algorithm. Since it was one of the first elite regression analysis techniques taught to those studying predictive modeling, it has become one of the most well-known approaches in the field.

$$\mathrm{X} = [D_x, D_y] \tag{3.1}$$

where D_x and D_y are the factors that go into the equation,

$$D_x = \frac{1}{3} \frac{\sum_{i=0}^{n-1} (X_i + X_{i+1}) (Y_i X_{i+1} - Y_{i+1} X_i)}{\sum_{i=0}^{n-1} (Y_i X_{i+1} - X_{i+1} X_i)} \tag{3.2}$$

and

$$C_y = \frac{1}{3} \frac{\sum_{i=0}^{n-1} (X_i + X_{i+1}) (\mathrm{X} Y_{i+1} - X_{i+1} Y_i)}{\sum_{i=0}^{n-1} (X_i x_{i+1} - X_{i+1} Y_i)} \tag{3.3}$$

b.Random Forest (RT) Classifier. The supervised ML model includes the ML approach known as Random Forest. There are several different types of DTs that make up the RF classifier. The predicted accuracy is increased by averaging the subsets of all trees. Instead of relying on only one set of decision trees,

RF takes the average of all the votes to determine the outcome. Each branch of the decision tree responds to a question regarding the current state of affairs.

Possible values for the X_i property of a nominal (divided) data set are $L_i, \ldots, L_j$. To get the Gini Index for this characteristic, use the following Equation (3.4) formula.

$$G\left(X_i\right)=\sum_{j=1}^{j} \Pr\left(Y_i=L_j\right)\left(1-\Pr\left(Y_i=L_j\right)\right)=1-\sum_{j=1}^{j} \Pr\left(Y_i=L_j\right)^2 \tag{3.4}$$

c.Naïve Bayes (NB) Classifier. It is easy to estimate conditional probabilities using the Bayes' theorem. The Equation (3.5) looks like this:

$$P(A \mid R)=\frac{P(R \mid A) * P(A)}{P(R)} \tag{3.5}$$

where R and A are random variables, $P(A \mid R)$ is the probability that Y if X is true,$P(R \mid A)$ is the probability that X if R is true, P(R) is the probability of X, and P(A) is the probability of Y if A is true.

d.Support Vector Machine.Data vulnerability Classification and Estimation Using a Support Vector Machine Model. In this investigation, we focus on the classification of signal quality, which is often a two-classification issue. In several cases involving categorization into two groups, the SVM-based model performed well. For a given training set $\{x_i, y_i\}, i=1 \ldots, K$, where x_i is a feature vector of length$x_i \in R^d$, and y_i is the label, it is possible to train a classifier. Therefore, the SVM-based model may be used for both estimating and classifying signal quality. The quality estimate label is $y_i \in \{1,0\}$, where excellent and terrible represent extremes. $y_i \in \{1,-1\}$ is the categorization label for abnormal and normal cases. The goal of a support vector machine (SVM) classifier is not only to differentiate between the classes, but also to create a hyperplane between them. It is also possible to build the ideal hyperplane by solving Equation (3.6),the following optimisation issue.

$$\min \phi(\mathbf{V})=\frac{1}{2}\left(\mathbf{V}^T \mathbf{V}\right)+C \sum_{i=1}^{K} \xi_i \tag{3.6}$$

subject to

$$y_i\left(\left(\mathbf{V}^T \varphi\left(\mathbf{x}_i\right)\right)+b\right) \geq 1, i=1, \cdots, K.$$

Here ξ_i is a error relaxation variable and $\xi_i \geq 0$, C is a factor of penalty, and w is the coefficient vector. $\varphi(x_i)$ is presented in order to construct a nonlinear SVM. Converting the optimisation issue into Equation (3.7).

$$\max L(\boldsymbol{\alpha})=\sum_{i=1}^{K} \alpha_i-\frac{1}{2} \sum_{i,j=1}^{K} \alpha_i \alpha_j y_i y_j \kappa\left(\mathbf{Y}_i, \mathbf{Y}_j\right) \tag{3.7}$$

subject to

$$\sum_{i=1}^{K} \alpha_i y_i=0, 0 \leq \alpha_i \leq C, i=1, \cdots, K$$

where $k\left(x_i, y_i\right)$ is a kernel function. In this work, the RBF kernel function is used. Furthermore, sigma has been determined experimentally to be 14.

e. Ensemble crossover XGBoost. This DT ensemble uses gradient boosting, which allows it to scale very well. Similar to gradient boosting, XGBoost maximises an objective function by minimising a loss function. Due to XGBoost's exclusive reliance on DTs as base classifiers, a modified loss function is used to regulate the tree complexity, as shown in Equations (3.8) and (3.9).

$$\begin{aligned} L_{\mathrm{xgb}} &=\sum_{i=1}^{N} L\left(y_i, F\left(Y_i\right)\right)+\sum_{m=1}^{M} \Omega\left(h_m\right), \\ \Omega(h) &=\gamma T+\frac{1}{-\lambda}\|\omega\|^2. \end{aligned} \tag{3.8}$$

where the leaf output scores are indicated by the symbol ω and T is the number of leaves on the tree. A prepruning method can be created by incorporating this loss function into the split criterion for decision trees. Higher values result in simpler trees. The amount of loss reduction gain needed to split an internal node is determined by γ. In XGBoost, shrinkage is a further regularisation parameter that lowers the additive expansion step size. Lastly, other strategies, like tree depth, can be employed to keep the complexity of the trees to a minimum. Reduced tree complexity has the added benefit of accelerating model training and requiring less storage space.

The number of records classified as normal, uncertain, or abnormal in each of the reference categories is used to calculate the overall score.

These numbers are denoted by $Nn_k, Nq_k, Na_k, An_k, Aq_k, andAa_k$. The various categories of risk level are represented as follows (based on the distribution of the complete test set):

$$\begin{aligned} Va_1 &= \frac{\text{Particular attack abnormal records}}{\text{total abnormal records}}, \\ Va_2 &= \frac{\text{Particular attack abnormal records}}{\text{total abnormal records}}. \\ Vn_1 &= \frac{\text{Dataset cluster normal records}}{\text{total normal records}}, \\ Vn_2 &= \frac{\text{Dataset cluster normal records}}{\text{total normal records}}. \end{aligned} \tag{3.9}$$

The sensitivity and specificity ratio are defined as (based on a subset of the test set) Equations (3.10) and (3.11).

$$\text{SeVa}_1 \frac{Aa_1}{Aa_1 + Aq_1 + An_1} + Va_2 \frac{Aa_2 + Aq_2}{Aa_2 + Aq_2 + An_2} \tag{3.10}$$

$$\begin{aligned} Sp =& Vn_1 \frac{Nn_1}{Na_1 + Nq_1 + Nn_1} \\ &+ Vn_2 \frac{Nn_2 + Nq_2}{Na_2 + Nq_2 + Nn_2}. \end{aligned} \tag{3.11}$$

The overall risk score is then the average of these two values:

$$\text{Overall vulnerable score } = \frac{(Se + Sp)}{2}$$

4. Experimental Analysis. The software Matlab has been used to implement the algorithms. The outcomes for each scenario are displayed below.

The simulated output is illustrated in Figure 4.1. The vulnerability was classified as normal and abnormal depending on the obtained risk score. Then, the attack type was identified as MQTT publish flood.

When applied to all of the information that makes up an entire epoch, the loss function yields a numeric estimate of the loss during that time. While developing an iterative curve, some data will inevitably be lost. The resultant curve shows that training and testing the classifier took much less time and effort when compared to previous approaches. Our model is underfitted if there is a substantial gap between the training and validation losses. The training loss may be reduced if more data were included in the sample. (either the overall number of layers or the number of neurons in each layer). Figure 4.2 displays the data we used to calculate the validation loss. However, when evaluating a model's performance on the validation set, the validation loss statistic is the statistic of choice. The validation set is a subset of the data used to evaluate the performance of the model. The sum of all false positives in both the validation set and the training set is the testing loss. The proposed EC-XG boost strategy results in much lower amounts of level loss than the currently available mechanisms.

The simulated output of the vulnerable values in the dataset by the suggested algorithm was demonstrated using a sample illustrated in Figure 4.3.

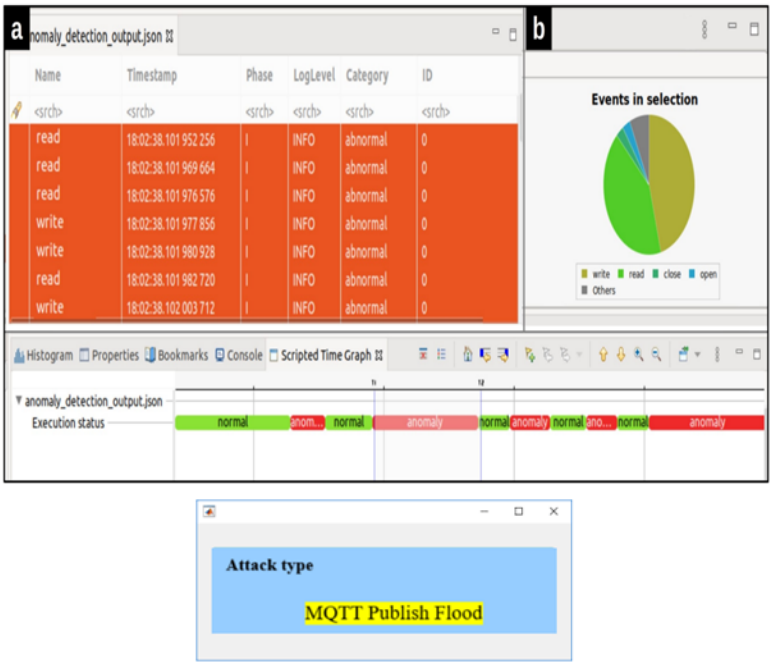

Fig. 4.1: Simulated output

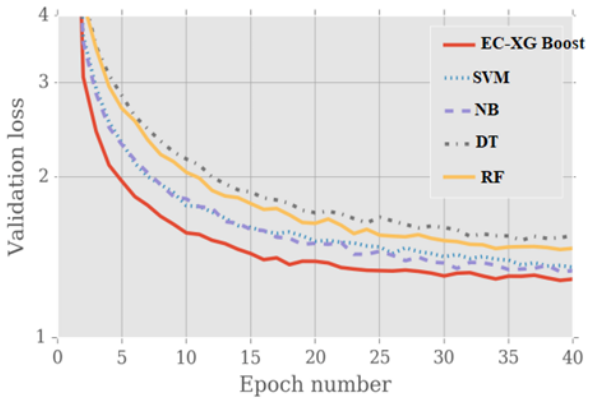

Fig. 4.2: Epoch Vs. Loss

As of from Figure 4.4, training and validation accuracy was calculated. Here, a high level of training and testing accuracy was obtained, showing the mechanism's efficiency.

Some performance measures are shown below that may be used to verify the effectiveness of the proposed technique. The following metrics have been calculated using the equations (4.1) (4.2) (4.3) to evaluate the trained models:

Accuracy: It counts how many potential exploits were accurately identified. How well the findings mirror the

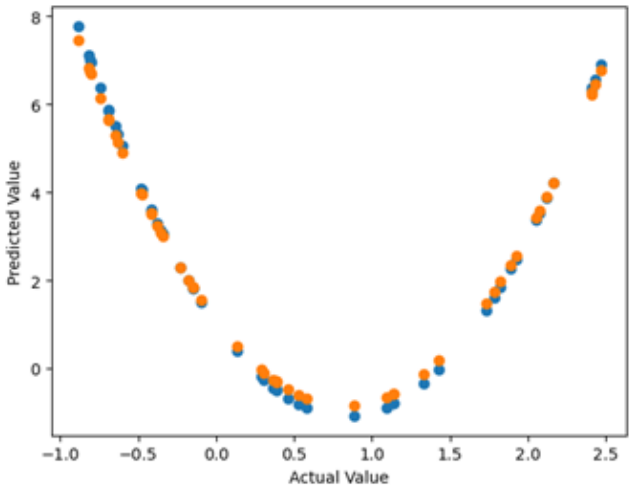

Fig. 4.3: Simulated vulnerability data prediction output

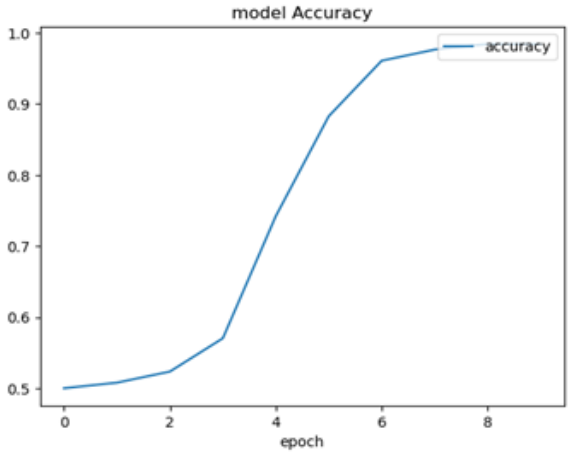

Fig. 4.4: Epoch Vs. accuracy

actual outcomes is determined by this factor.

$$\text{Accuracy} = \frac{(TP + TN)}{(FN + FP + TN + TP)} \tag{4.1}$$

Precision: It determines how accurate the suggested technique behavior is by separating required vulnerable code from the dataset

$$\text{Precision} = \frac{TP}{(TP + FP)} \tag{4.2}$$

Recall: The ratio of correctly predicted instances and all instances

$$\text{Recall} = \frac{TP}{(TP + FN)} \tag{4.3}$$

Table 4.1: Binary classification comparision

Methodology	**Accuracy**(%)
SVM	64.1 %
NB	65.4 %
DT	89.6%
RF	92.5 %
EC-XG boost	99.64 %

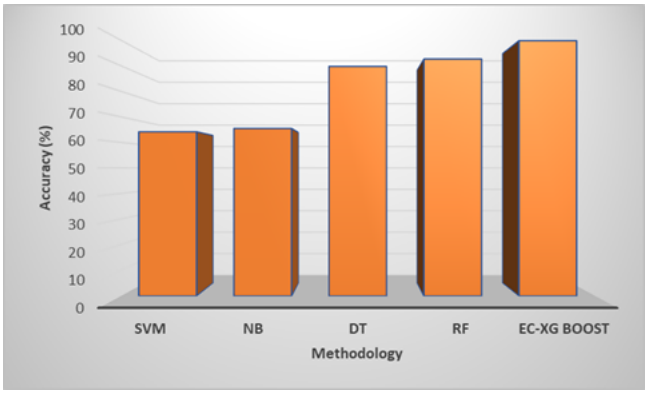

Fig. 4.5: Classification outcome of an algorithm.

Table 4.2: Comparative analysis of the different classifiers

Classes	Decision Tree		SVM		RF		NB		Ensemble XG Boost	
	Recall	Precision	Recall	Precision	Recall	Precision	Recall	Precision	Recall	Precision
Class 1	87.1	86.2	6.2	68.5	91.7	92.4	14.1	50.2	98.5	99.1
Class 2	84.3	86	9.7	16.5	90.5	91.2	73	10.3	97.2	98.3
Class 3	86.2	87	32.1	10.4	91.3	92.7	25.5	10.1	99.4	98.9
Class 4	87.4	87.3	23.5	11.5	90.4	92.5	80.3	10.5	99.5	99.3

where
True Positive (TP) : actual = 1, predicted = 1
True Negative (TN) : actual = 0, predicted = 0
False Positive (FP) : actual = 1, predicted = 0
False Negative (FN) : actual = 0, predicted = 1

The classification results of the five algorithms applied to the dataset are shown in Figure 3.2. For Ensemble crossover XG boost, RF, and DT, the maximum accuracy was attained at 99.64%, 92.5%, and 89.6%, respectively.

As of from the table 4.1 and figure 4.5 Ensemble crossover XG boost, RF performs the best, with 99.64% and 92.5% accuracy. The importance of highlighting that both techniques exhibit high Recall and Precision per class, as well as increased sensitivity and a low number of false positives, cannot be overstated and is highlighted in Figure 4.6. 99.64% and 92.5% accuracy are obtained using XG boost and RF, respectively. Due to a correlation between the various cases, which prevents a clear differentiation, the remaining algorithms under examination perform worse than those previously analyzed.

The comparative analysis of the different classifiers over precision and recall was done in Figure 4.6 and Table 4.2. From the analysis, the crossover XG boost classifier overcomes the other methodology by obtaining

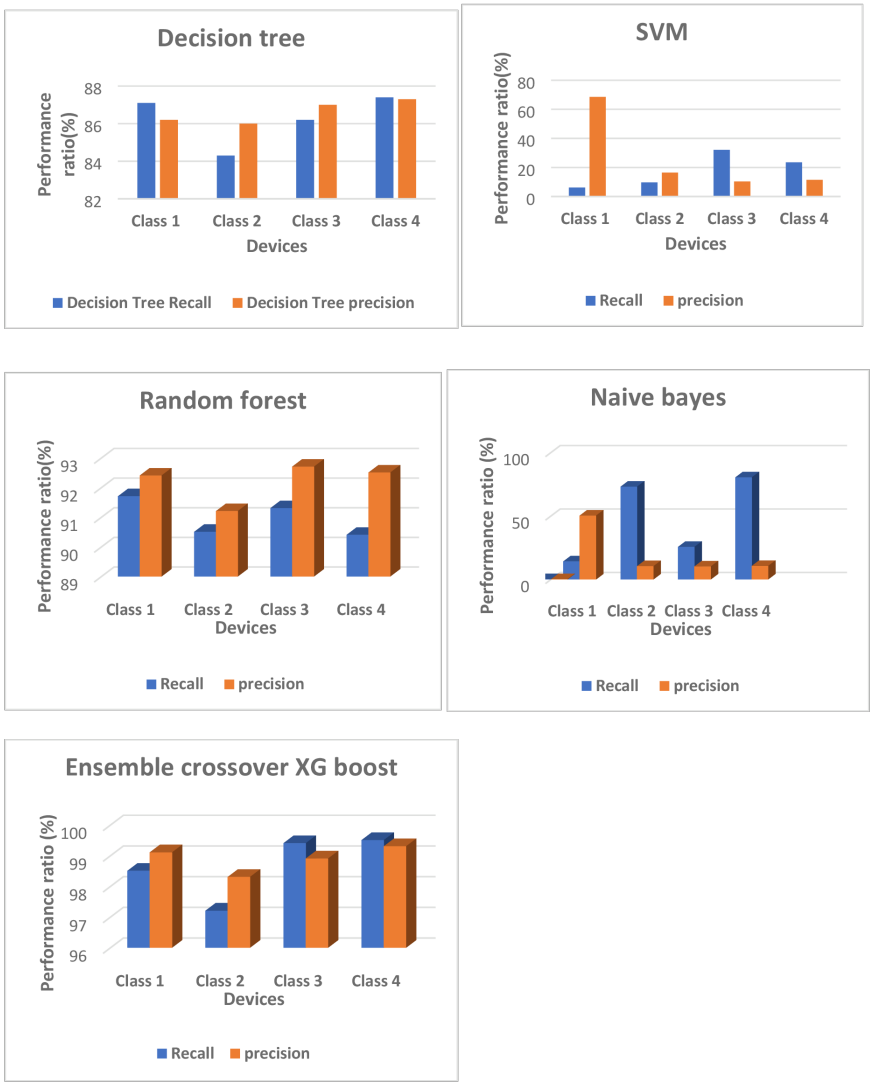

Fig. 4.6: Comparison of Recall and Precision.

a high range of precision and recall.

To prove the efficiency of the suggested methodology it can be compared with the existing methodologies [31].

From the result obtained from the above analysis (See Table 4.3), it was revealed that the suggested EC-XGboost methodology expresses more satisfied results than other existing mechanisms by getting a higher range of performance ratio over CPS vulnerability prediction than the other mechanism in use.

Table 4.3: Comparative performance analysis

S.No	Methods	AUC	TN	FP	FN	TP	Accuracy(%)	F1	Time (s)
1	ResNet	0.8490	82.270	11.320	3.490	2.920	85.190	28.290	6330
2	Inception	0.9610	93.500	0.200	4.100	2.310	95.710	51.760	9760
3	FCN	0.9550	88.160	5.430	3.920	2.490	90.650	34.760	10160
4	MLP	0.7580	72.220	21.370	4.860	1.550	73.770	10.550	1130
5	GC-LSTM + Resnet	0.9740	93.290	0.310	3.270	3.140	96.420	63.770	10560
6	GC-LSTM + Inception	0.9760	92.100	1.490	3.350	3.060	95.160	55.870	14090
7	GC-LSTM + FCN	0.9720	92.280	1.30	3.680	2.730	95.010	52.260	1342. 0
8	GC-LSTM + MLP	0.9370	93.400	0.190	6.130	0.280	93.680	8.140	765. 0
9	CyResGrid	0.9840	93.470	0.130	3.420	2.990	96.450	65.030	714. 0
10	Ensemble crossover XG Boost	0.990	94.0	0.0010	2.000	3.200	99.60	98.90	50

5. Conclusion. To enhance the maintenance of the integrity of CI based on CPS, this work aimed to construct computational mathematics on a pertinent case analysis with appropriate information. The overall evaluation revealed that Ensemble crossover XG boost, RF, and DT outperformed SVM and Naive Bayes in performance. Ensemble crossover XG boost demonstrated the best performance across all algorithms, with 99.64% accuracy in scenario classification. The dataset's instance count should be increased to improve Ensemble crossover XG boost accuracy. Cyber-physical security significantly impacts society, business, and the economy and is crucial to safeguarding vital infrastructure. Protection against cyber threats can be considerably enhanced by awareness of the most recent technology and dangers. To improve scenario identification, rescue operations, and strategic planning, it will be essential for CPS security in the future to automate threat detection and the activation of suitable remedies using Security Orchestration, Automation, and Response (SOAR) systems. Our proposed approach will eventually be used for virtual and distributed Linux deployments. We also aim to use a caching method and batch processing to boost our solution's speed. Each microservice in our architecture will use a "PROSPECT" secure data container, allowing for granular role-based and attribute-based access control to be applied to the settings stored within. A relational database management system would be combined with this.

REFERENCES

[1] A. Aldahiri, B. Alrashed, and W. Hussain, *Trends in using iot with machine learning in health prediction system*, Forecasting, 3 (2021), pp. 181–206.

[2] T. Alladi, V. Chamola, et al., *Harci: A two-way authentication protocol for three entity healthcare iot networks*, IEEE Journal on Selected Areas in Communications, 39 (2020), pp. 361–369.

[3] B. A. Alzahrani, A. Irshad, A. Albeshri, and K. Alsubhi, *A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks*, Wireless Personal Communications, 117 (2021), pp. 47–69.

[4] N. B. Amor, S. Benferhat, and Z. Elouedi, *Naive bayes vs decision trees in intrusion detection systems*, in Proceedings of the 2004 ACM symposium on Applied computing, 2004, pp. 420–424.

[5] ———, *Naive bayes vs decision trees in intrusion detection systems*, in Proceedings of the 2004 ACM symposium on Applied computing, 2004, pp. 420–424.

[6] M. Binkhonain and L. Zhao, *A review of machine learning algorithms for identification and classification of non-functional requirements*, Expert Systems with Applications: X, 1 (2019), p. 100001.

[7] B. Chandrasekaran, R. Balakrishnan, and Y. Nogami, *Secure data communication using file hierarchy attribute based encryption in wireless body area networks*, Journal of Communications Software and Systems, 14 (2018), pp. 75–81.

[8] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, *A review of cyber security risk assessment methods for scada systems*, Computers & security, 56 (2016), pp. 1–27.

[9] C. A. A. Dorofee, *Managing information security risks: the octave (sm) approach*, 2002.

[10] B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, *Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control*, IEEE Internet of Things Journal, 8 (2021), pp. 11717–11731.

[11] A. Fiaschetti, F. Lavorato, V. Suraci, A. Palo, A. Taglialatela, A. Morgagni, R. Baldelli, and F. Flammini, *On the use of semantic technologies to model and control security, privacy and dependability in complex systems*, in Computer Safety, Reliability, and Security: 30th International Conference, SAFECOMP 2011, Naples, Italy, September

19-22, 2011. Proceedings 30, Springer, 2011, pp. 467–479.
[12] G. Garibotto, P. Murrieri, A. Capra, S. De Muro, U. Petillo, F. Flammini, M. Esposito, C. Pragliola, G. Di Leo, R. Lengu, et al., *White paper on industrial applications of computer vision and pattern recognition*, in Image Analysis and Processing–ICIAP 2013: 17th International Conference, Naples, Italy, September 9-13, 2013, Proceedings, Part II 17, Springer, 2013, pp. 721–730.
[13] M. A. M. Hasan, M. Nasser, B. Pal, and S. Ahmad, *Support vector machine and random forest modeling for intrusion detection system (ids)*, Journal of Intelligent Learning Systems and Applications, 6 (2014), pp. 45–52.
[14] J. Homer, A. Varikuti, X. Ou, and M. A. McQueen, *Improving attack graph visualization through data reduction and attack grouping*, in Visualization for Computer Security: 5th International Workshop, VizSec 2008, Cambridge, MA, USA, September 15, 2008. Proceedings, Springer, 2008, pp. 68–79.
[15] W.-H. Hsu, Q. Li, X.-H. Han, and C.-W. Huang, *A hybrid iot traffic generator for mobile network performance assessment*, in 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), IEEE, 2017, pp. 441–445.
[16] C. Hu, H. Li, Y. Huo, T. Xiang, and X. Liao, *Secure and efficient data communication protocol for wireless body area networks*, IEEE Transactions on Multi-Scale Computing Systems, 2 (2016), pp. 94–107.
[17] A. M. Hussain, K. Abualsaud, E. Yaacoub, T. Khattab, A. Gehani, and M. Guizani, *A testbed for implementing lightweight physical layer security in an iot-based health monitoring system*, in 2021 International Wireless Communications and Mobile Computing (IWCMC), IEEE, 2021, pp. 486–491.
[18] M. A. Jan, M. Usman, X. He, and A. U. Rehman, *Sams: A seamless and authorized multimedia streaming framework for wmsn-based iomt*, IEEE Internet of Things Journal, 6 (2018), pp. 1576–1583.
[19] K. Kandasamy, S. Srinivas, K. Achuthan, and V. P. Rangan, *Iot cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process*, EURASIP Journal on Information Security, 2020 (2020), pp. 1–18.
[20] G. Kavallieratos, S. Katsikas, and V. Gkioulos, *Cybersecurity and safety co-engineering of cyberphysical systems—a comprehensive survey*, Future Internet, 12 (2020), p. 65.
[21] M. H. Khadr, H. B. Salameh, M. Ayyash, H. Elgala, and S. Almajali, *Jamming resilient multi-channel transmission for cognitive radio iot-based medical networks*, Journal of Communications and Networks, 24 (2022), pp. 666–678.
[22] M. Kumar and S. Chand, *Medhypchain: A patient-centered interoperability hyperledger-based medical healthcare system: Regulation in covid-19 pandemic*, Journal of Network and Computer Applications, 179 (2021), p. 102975.
[23] V. Lamba, N. Šimková, and B. Rossi, *Recommendations for smart grid security risk management*, Cyber-Physical Systems, 5 (2019), pp. 92–118.
[24] D. Liu, J. Shen, Y. Chen, C. Wang, T. Zhou, and A. Wang, *Privacy-preserving data outsourcing with integrity auditing for lightweight devices in cloud computing*, in Information Security and Cryptology: 14th International Conference, Inscrypt 2018, Fuzhou, China, December 14-17, 2018, Revised Selected Papers 14, Springer, 2019, pp. 223–239.
[25] X. Lyu, Y. Ding, and S.-H. Yang, *Safety and security risk assessment in cyber-physical systems*, IET Cyber-Physical Systems: Theory & Applications, 4 (2019), pp. 221–232.
[26] G. Macher, E. Armengaud, E. Brenner, and C. Kreiner, *Threat and risk assessment methodologies in the automotive domain*, Procedia computer science, 83 (2016), pp. 1288–1294.
[27] M. Malatji, *Industrial control systems cybersecurity: Back to basic cyber hygiene practices*, in 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET), IEEE, 2022, pp. 1–7.
[28] J. Mendel et al., *Smart grid cyber security challenges: Overview and classification*, e-mentor, 68 (2017), pp. 55–66.
[29] S. Pan, T. Morris, and U. Adhikari, *Classification of disturbances and cyber-attacks in power systems using heterogeneous time-synchronized data*, IEEE Transactions on Industrial Informatics, 11 (2015), pp. 650–662.
[30] P. Perrone, F. Flammini, and R. Setola, *Machine learning for threat recognition in critical cyber-physical systems*, in 2021 IEEE International Conference on Cyber Security and Resilience (CSR), IEEE, 2021, pp. 298–303.
[31] A. Presekal, A. Ştefanov, V. S. Rajkumar, and P. Palensky, *Attack graph model for cyber-physical power systems using hybrid deep learning*, IEEE Transactions on Smart Grid, (2023).
[32] C. Pu, H. Zerkle, A. Wall, S. Lim, K.-K. R. Choo, and I. Ahmed, *A lightweight and anonymous authentication and key agreement protocol for wireless body area networks*, IEEE Internet of Things Journal, 9 (2022), pp. 21136–21146.
[33] H. Qiu, M. Qiu, M. Liu, and G. Memmi, *Secure health data sharing for medical cyber-physical systems for the healthcare 4.0*, IEEE journal of biomedical and health informatics, 24 (2020), pp. 2499–2505.
[34] I. C. Reinhardt, J. C. Oliveira, and D. T. Ring, *Industry 4.0 and the future of the pharmaceutical industry*, Pharm Eng, (2021), pp. 1–11.
[35] N. Shevchenko, B. R. Frye, and C. Woody, *Threat modeling for cyber-physical system-of-systems: Methods evaluation*, Software Engineering Institute: Pittsburgh, PA, USA, (2018).
[36] S. Surminski, C. Niesler, F. Brasser, L. Davi, and A.-R. Sadeghi, *Realswatt: remote software-based attestation for embedded devices under realtime constraints*, in Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, 2021, pp. 2890–2905.
[37] S. Verma, S. Kaur, M. A. Khan, and P. S. Sehdev, *Toward green communication in 6g-enabled massive internet of things*, IEEE Internet of Things Journal, 8 (2020), pp. 5408–5415.
[38] W. Wang, Q. Chen, Z. Yin, G. Srivastava, T. R. Gadekallu, F. Alsolami, and C. Su, *Blockchain and puf-based lightweight authentication protocol for wireless medical sensor networks*, IEEE Internet of Things Journal, 9 (2021), pp. 8883–8891.
[39] S. Yu and Y. Park, *A robust authentication protocol for wireless medical sensor networks using blockchain and physically unclonable functions*, IEEE Internet of Things Journal, 9 (2022), pp. 20214–20228.

Edited by: Polinpapilinho Katina
Special issue on: Scalable Dew Computing for Future Generation IoT Systems
Received: Jul 7, 2023
Accepted: Oct 17, 2023