International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST229489

A Novel Study on Design and Implementation of a Cyber Physical Industrial Control System by Using Cyber Security Techniques

Yagnasri Ashwini[1], Chetluru Rohini[2], Kondabathula Durga Charan[3], Ramakrishna Gandi[3]
[1]Assistant Professor, CSE (AI&DS) Department, Madanapalle Institute of Technology & Science, Andhra Pradesh, India
[2]Assistant Professor, IT Department, Keshav Memorial Institute of Technology, Hyderabad, Telangana State, India
[3]Assistant Professor, CSE (AI&DS) Department, Madanapalle Institute of Technology & Science. Andhra Pradesh, India
[4]Assistant Professor, CSE (AI&DS) Department, Madanapalle Institute of Technology & Science, Andhra Pradesh, India

Article Info
Volume 9, Issue 5
Page Number : 76-86

Publication Issue
September-October-2022

Article History
Accepted : 01 Sep 2022
Published : 10 Sep 2022

ABSTRACT

Because of late expansion in arrangement of Cyber-Physical Industrial Control Systems in various basic frameworks, tending to network protection difficulties of these frameworks is essential for guaranteeing their dependability and secure activity in presence of malignant digital assaults. In the ongoing scene that is controlled by innovation and organization associations, it is vital to know what digital protection is furthermore, to have the option to really utilize it. Frameworks, significant documents, information, and other significant virtual things are in danger on the off chance that there is no security to safeguard it. Securing the data have become perhaps of the greatest test in the current day. Whenever we ponder the network protection the primary thing that rings a bell is 'digital violations' which are expanding monstrously step by step. Different Governments and organizations are going to numerous lengths to forestall these digital wrongdoings. Other than different measures digital protection is as yet an extremely large worry to a large number. Towards this end, fostering a testbed to produce ongoing informational indexes for basic foundation that would be used for approval of constant assault recognition calculations are without a doubt profoundly required. This paper investigates and proposes the design and implementation of a cyber-physical industrial control system testbed where the Tennessee Eastman process is simulated in real-time on a PC and the closed-loop controllers are implemented on the Siemens PLCs. Misleading information infusion digital assaults are infused to the created testbed through the man-in-the-center construction where the vindictive programmers can continuously adjust the sensor estimations that are shipped off the PLCs. Moreover, different digital assault location calculations are created and executed continuously on the testbed and their exhibition and capacities are looked at and assessed.

Keywords : Cyber Security, Cyber Attacks, Industrial Control Systems, Hybrid Testbed, Cybercrime, Attack Detection Algorithms, Cyber Physical System.

I. INTRODUCTION

Today man can send and get any type of information might be an email or a sound or video just by the snap of a button yet did he at any point suppose how safely his information id being communicated or shipped off the other individual securely with practically no spillage of data?? The response lies in network protection. Today Internet is the quickest developing foundation in each day life. In the present specialized climate numerous most recent advancements are changing the substance of the humanity. Yet, because of these arising innovations we can't defend our confidential data in an extremely successful manner and thus these days digital wrongdoings are expanding step by step. Today in excess of 60% of complete business exchanges are done on the web, so this field required an excellent of safety for straightforward and best exchanges. Thus network safety has turned into a most recent issue. The extent of network protection isn't simply restricted to getting the data in IT industry yet additionally to different fields like the internet and so on.

A successful network protection technique has various layers of safeguard spread across the networks, PCs, projects, or information that one expects to keep non-poisonous. In a general public, the processes, individuals and apparatuses should all backup one choice to create a genuine safeguard on or after digital assaults. A brought together danger the board framework can automate increases across select Cisco Security merchandise and accelerate key security processes capabilities: revelation, assessment, and remediation.

Ongoing mechanical advances in charge, processing, and correspondences have produced serious interest being developed of new age of exceptionally interconnected and sensor rich frameworks that is known as basic Cyber-Physical Frameworks (CPS) foundation with application to assortment of designing spaces like interaction and computerization frameworks, savvy matrix and shrewd urban communities, and medical services frameworks. These complicated frameworks are turning out to be more appropriated what's more, PC arranged that have required the turn of events of novel checking, diagnostics, and disseminated control advances. Administrative Control and Data Acquisition (SCADA) systems, Wireless Sensor Networks (WSN), and PLCs, are presently settled ideal models that are used in numerous basic CPS framework. Then again, the imagined complex CPS foundation accomplish like never before require advancement of novel and proactive security innovations, as these frameworks are persistently being designated by digital assaults and interruptions by shrewd malignant enemies.

The foes are proficient of going after center control frameworks that are utilized in all key digital actual framework’s foundation. These situations don't exist and are impractical or like security challenges that are available in customary IT frameworks. Hence, there exists a pressing need to concentrate on the weaknesses, examine the dangers, what's more, foster guarded and moderation components for basic CPS foundation. Because of responsiveness and high significance of the wellbeing basic frameworks, in actuality, any examination action that is straightforwardly applied to the actual framework can prompt disruption, unexpected harms or misfortunes, and thus advancement of testbeds that impersonate conduct of CPS in a limited scale style is profoundly fundamental for advancement of different network safety advances. In this paper, a crossover digital physical testbed for modern control frameworks is created and different kinds of genuine digital assault situations are infused and carried out. Also, online continuous digital assault identification calculations are proposed to give an exhaustive arrangement to the digital protection of digital actual Industrial Control System (ICS).

In this paper, the hybrid testbed architecture is selected for development of the ICS testbed, where the Tennessee Eastman (TE) plant is simulated inside a PC and the remaining parts are implemented using actual industrial hardware. The TE plant is selected as the industrial process for our developed cyber-security testbed due to the following reasons. First, the TE model is a well-known chemical process that is used in control systems research and its dynamics are well-understood. Second, it should be properly controlled otherwise small disturbances will drive the system towards an unsafe and unstable operation.

Finally, from the anomaly detection perspectives, the cyber attack detection algorithms can be divided into five main categories, namely: linear, proximity-based, probabilistic, outlier ensembles, and neural networks approaches [7]. Therefore, in order to have a comprehensive comparison for cyber attack detection approaches that t the TE process, the following algorithms have been chosen from various categories such as: Principal Component Analysis (PCA), One-Class Support Vector Machines (OCSVM), Local Outlier Factor (LOF) k-Nearest-Neighbors (kNN), and Isolation Forest (IF). Comparative studies are conducted based on the cyber attack detection time and the confusion matrix performance metrics where subsequently, the OCSVM and kNN are demonstrated to yield promising performance for accomplishing the cyber attack detection objective.

II. RELATED WORK

Cyber attacks on TE processes are likewise researched in the writing. In [8], a respectability assault is infused on the controlled variable signs and the relating sensor estimations are seen by connection based grouping calculation. Various examinations have been directed on finding the ideal opportunity to send off the Denial of Administration (DoS) assault on either the sensor or actuator signals in the TE cycle. A few digital assault identification strategies, for example, model-based approaches [12], grouping based approaches [11], Gaussian blend models [10], and RNN-based approaches are created for discovery of various digital assaults on the TE interaction. Notwithstanding, the above work are all in view of the reproduced TE process and digital assaults are for the most part copied inside the simulation file.

Besides, a few ongoing ICS testbeds for exploring network protection are created in the writing and Table 1 presents correlations among these testbeds for different reach of uses that depend on TYPE (reenactment (S), physical (P), genuine ICS (R), and mixture (H)), Process, Data Type (network information (NET) and cycle information (PR)), Detection Technique, Attacks, Attack Type (copying (E) and physical (P)). As displayed in this table, the digital physical testbeds are produced for the actual water framework and different contextual analyses as far as information type, correspondence furthermore, assault infusion/location are introduced. In [1], a model-based location approach is created to recognize three various assaults by utilizing network information. Likewise, a physics based identification approach is introduced in [8] to distinguish subtle weakness by utilizing the cycle information. In [9], an Intrusion Detection System (IDS) approach is created to identify four different assaults by utilizing network information. In [2], various information driven interruption recognition calculations are created utilizing the organization information from the

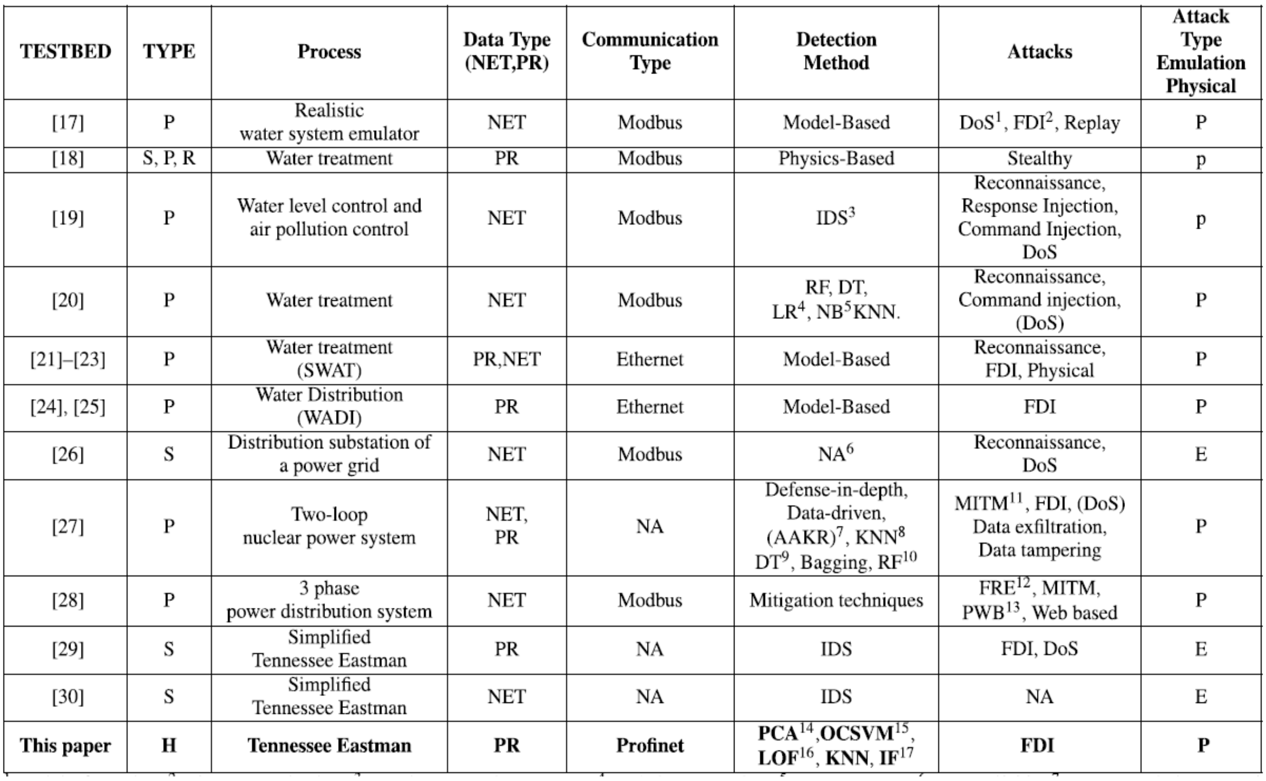
Modbus correspondence convention. The water framework testbeds are created in view of the Ethernet/IP as the correspondence convention.

A reproduction testbed is utilized in [6] and in [7] a physical testbed is created and different assault discovery calculations are created by utilizing both the organization and the interaction information. In [29], [30], a simplified variant of the Tennessee Eastman process is used as the actual plant in the testbed and model-based assault location calculations are proposed for the reenactment based testbeds disregarding any actual equipment in the test system.

III. LITERATURE SURVEY

In this paper, a full version of the nonlinear chemical process of the Tennessee Eastman process is used as the physical process in the developed hybrid testbed. Moreover, based on the structure and features of PROFINET as the industrial field bus that is used in the Siemens distributed I/O, the actual real-time false data injection cyber attack is implemented through the man-in-the-middle (MITM) architecture on the developed testbed. This is achieved by utilizing Address Resolution Protocol such that the cyber hacker acts as the MITM in the closed-loop system and modifies the sensor measurements sent to the PLC or the actuator commands that are sent to the distributed I/O. Furthermore, various real-time online cyber attack detection algorithms are developed and implemented on the testbed and their performance capabilities are compared and evaluated. Consequently, this is the first work in the literature that completely simulates a full-version of the Tennessee Eastman Process using a hybrid testbed.

Table 1. Overview of the existing cyber-security study



TESTBED	TYPE	Process	Data Type (NET,PR)	Communication Type	Detection Method	Attacks	Attack Type Emulation Physical
[17]	P	Realistic water system emulator	NET	Modbus	Model-Based	DoS[1], FDI[2], Replay	P
[18]	S, P, R	Water treatment	PR	Modbus	Physics-Based	Stealthy	p
[19]	P	Water level control and air pollution control	NET	Modbus	IDS[3]	Reconnaissance, Response Injection, Command Injection, DoS	p
[20]	P	Water treatment	NET	Modbus	RF, DT, LR[4], NB[5]KNN.	Reconnaissance, Command injection, (DoS)	P
[21]–[23]	P	Water treatment (SWAT)	PR,NET	Ethernet	Model-Based	Reconnaissance, FDI, Physical	P
[24], [25]	P	Water Distribution (WADI)	PR	Ethernet	Model-Based	FDI	P
[26]	S	Distribution substation of a power grid	NET	Modbus	NA[6]	Reconnaissance, DoS	E
[27]	P	Two-loop nuclear power system	NET, PR	NA	Defense-in-depth, Data-driven, (AAKR)[7], KNN[8] DT[9], Bagging, RF[10]	MITM[11], FDI, (DoS) Data exfiltration, Data tampering	P
[28]	P	3 phase power distribution system	NET	Modbus	Mitigation techniques	FRE[12], MITM, PWB[13], Web based	P
[29]	S	Simplified Tennessee Eastman	PR	NA	IDS	FDI, DoS	E
[30]	S	Simplified Tennessee Eastman	NET	NA	IDS	NA	E
This paper	**H**	**Tennessee Eastman**	**PR**	**Profinet**	**PCA[14],OCSVM[15], LOF[16], KNN, IF[17]**	**FDI**	**P**

As such, this work gives an extensive arrangement for the network protection of ICS empowered with the accompanying primary contributions

1) A cross breed testbed is created by utilizing the mimicked full-rendition of the Tennessee Eastman Process as a nonlinear temperamental cycle and the Siemens field gadgets like PLC and disseminated I/O, though the past work in [29], [30] just thought to be the simplified adaptation
of TE without having any genuine equipment in the testbed.

2) Real-time false data injection cyber attacks are implemented by compromising the PROFINET field-bus protocol for the first time in the literature, where as shown in Table 1, all of the previous works are based on either the Modbus or the Ethernet communication protocols.

3) Several online cyber attack detection methodologies such as PCA, OCSVM, LOF, KNN, and IF are developed and implemented for real-time detection of cyber attacks in the supervisory level of the testbed. In contrast, in most of the previous work in the literature the detection algorithms are implemented off-line after collecting the data from the testbed.

IV. TENNESSEE EASTMAN (TE) PROCESS SIMULATION

The TE process has 12 manipulated variables (XMVs), 41 measured variables (XMEAS), and 20 different process disturbances (IDVs) which can be chosen by the user [6]. The output measurements (XMEAS) of the plant are divided into 22 continuous-time and 19 discrete-time measurements. In the developed testbed in this work, only 9 inputs and 16 continuous-time outputs are used as specified in Tables 2 and 3, respectively. It should be noted that the time unit of the original TE process model was in hours which is not suitable for a real-time simulation. Thus, in order to make the process real-time, the model is modified accordingly by changing the state dynamics of the system and correspondingly the controller gains.

Table 3. Process measurements used in the testbed

Variable name	Variable number	Units
A feed	XMEAS 1 (y_1)	kscmh
D feed	XMEAS 2 (y_2)	kg/h
E feed	XMEAS 3 (y_3)	kg/h
A and C feed	XMEAS 4 (y_4)	kscmh
Reactor pressure	XMEAS 7 (y_7)	kPa gauge
Reactor level	XMEAS 8 (y_8)	%
Reactor temperature	XMEAS 9 (y_9)	C
Purge rate	XMEAS 10 (y_{10})	kscmh
Prod. separator temperature	XMEAS 11 (y_{11})	C
Prod. separator level	XMEAS 12 (y_{12})	%
Prod. separator underflow	XMEAS 14 (y_{14})	m3/h
Stripper level	XMEAS 15 (y_{15})	%
Stripper underflow	XMEAS 17 (y_{17})	m3/h
A Concentration	XMEAS 23 (y_{23})	mol %
C Concentration	XMEAS 25 (y_{25})	mol %
G Concentration	XMEAS 40 (y_{40})	mol %

In the developed ICS testbed, the Siemens S7-1200 PLC CPU and the SIMATIC EP 200SP distributed I/O modules are used. For establishing the interface between the simulated process on the PC, and PLCs and distributed modules, MF644 and MF634 DAQ boards are used mainly due to a high number of analog inputs/outputs and their compatibility with MATLAB/Simulink. Each I/O module contains 4 analog inputs and 2 analog outputs and in order to connect all PLCs with all I/Os, the Siemens CSM 1277 switch modules are used.

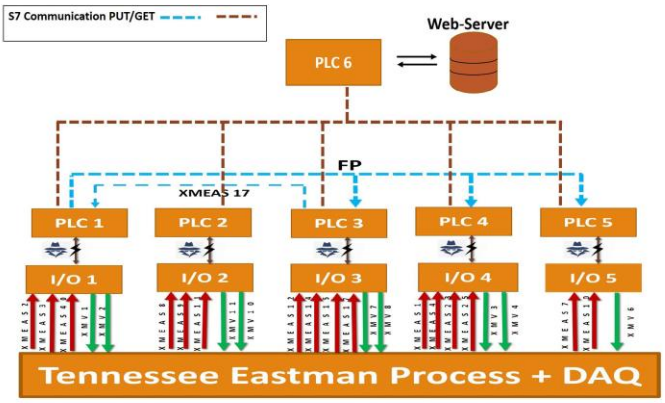


Figure 1. The TE process block diagram.

V. CYBER ATTACK INJECTION

In this section, our methodology for injecting cyber attacks on the developed testbed is presented. Generally, different protocols enable various attack surfaces such as the Data Integrity (DI) attack (e.g. manipulating sensor measurements), and Denial-of-Service (DoS) which causes disruption of communication now among entities. In an ICS architecture, cyber attacks can be categorized into two general types, namely as configuration and operational attacks. In the configuration attack, the malicious hacker targets the configuration protocols of the ICS, and consequently gets access to full control of the system. On the other hand, in the operational attacks, the malicious hacker mainly targets the operational communication protocol such as the PROFINET IO Real-time data, in which critical field data are transferred.

For this cyber attack to take place, it is assumed that (i) The hacker has a field level access to the IO Module and PLCs.(ii) Hacker has knowledge of the physical system, implying that, he/she is aware of what is being transmitted from the sensors and what are being transferred to actuators.

In [4], the authors exploit a vulnerability of the PROFINET Discovery and Basic Configuration Protocol (DCP) to inject DoS attacks through port stealing, against the application relation between the IO Controller and the IO Device. This type of cyber attack is not designed to be stealthy and has a higher probability of detection. An early attempt for false data injection through port stealing is presented in [35] although the developed attacks are not implemented on a real testbed.

In this paper, based on the structure and features of the PROFINET, a false data attack is injected into the PROFINET IO. Real-time data through the man-in-the-middle (MITM) structure is also validated on the developed testbed. This is mainly achieved by utilizing the ARP in which the port of the victim on the shared medium (such as a switch) is stolen and the hacker acts as a Man-in-the-Middle (MITM) in the closed-loop system that can modify the sensor measurements that are sent to the PLC. The PROFINET IO devices do not have any endpoint security functionality [36] which allows cyber attacks feasible once a malicious hacker has a physical access to a device or its network connections. One of the most effective and damaging cyber attacks on the PROFINET IO devices is the MITM cyber attack.

The MITM cyber attack will be implemented in our developed testbed, by utilizing the Port Stealing methodology. In the Port Stealing attack, the switch MAC table is compromised such that the hacker's MAC address is registered in place of the victim. Therefore, the intended port from the I/O module is stolen by the hacker, and consequently he/she can transmit false data to the PLCs. Port Stealing is an active cyber attack which allows a hacker to sniff packets in a switched network as well as modify packets by injecting new packets. This cyber attack targets the Application Relationship between the IO Controllers and the IO devices. Successful Port Stealing requires the hacker to synchronize with the real-time data communication and establish a race condition.

Algorithm: Nearest-Neighbor Algorithm

```
Training:
Input: xi - training data (i 2 f1; 2; 3; : : : ;Ng), k,
Output: Threshold Tr
1: for i D 1; : : : ;N do
2: Compute the k nearest neighbors of xi using the Ball-tree algorithm.
3: Compute the decision score (ascore(xi)) as the largest distance between xi and its nearest neighbors.
4: end
5: Set threshold as Tr D maxi(ascore(xi))
Testing:
Input: D - test data, xi - training data, Tr ,
Output: Test data ag r
1: Compute the k nearest neighbors of D using the Ball-tree algorithm.
2: Compute the decision score (ascore(D)) as the largest distance between D and its nearest neighbors.
3: if ascore(D) > Tr then
4: D is abnormal, r D 1.
5: else
6: D is normal, r D 0.
7: end
```

VI. PERFORMANCE EVALUATION AND ASSESSMENT

In this section, evaluation and validation of our proposed cyber attack detection schemes are provided and demonstrated for the developed TE testbed infrastructure.

DATASET

As previously indicated, the proposed methodologies of this work are demonstrated by using the real datasets that are generated from the implemented ICS testbed. The generated dataset consists of 25 variables such that 16 variables are corresponding to the sensor measurements and 9 variables are corresponding to the actuator signals.

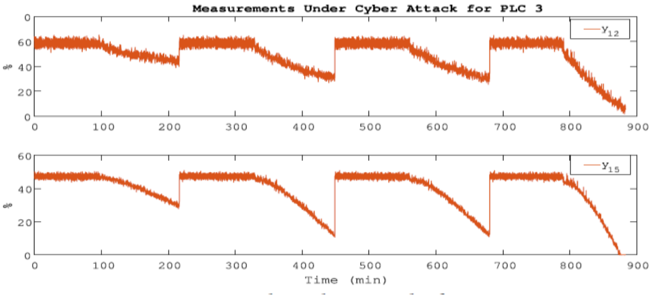


Figure 2. Measurements under cyber attacks for PLC3.

Two types of datasets are generated, where initially the testbed was run for almost 72 hours under the normal condition (that is, cyber attack free) for generating the training set of the size (25 X 96827) (after removing the initial transient behavior), i.e. N D 96827. Subsequently, the testbed was run several times subject to different cyber attack scenarios and different cyber attack gateways and points.

VII. PERFORMANCE EVALUATION METRICS

The confusion matrix is a form of contingency table with two dimensions identified as True and Predicted, and a set of classes corresponding to both dimensions, as presented in Table 5. The following detection and classification performance metrics are derived from the confusion matrix as follows:

Table 1. The confusion matrix.

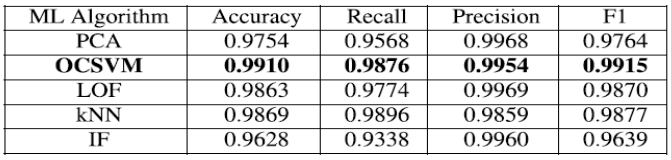
Predicted

	Positive	Negative
Positive	True Positive (TP)	False Negative (FN)
Negative	False Positive (FP)	True Negative (TN)

Accuracy	Accuracy specifies the closeness of measurements to a specific category/class and it is computed as	$Accuracy = \frac{TP + TN}{TP + FP + TN + FN}$
Recall	Recall is the True Positive Rate (TPR) and is computed as	$TPR = \frac{TP}{TP + FN}$
Precision	Precision is the Positive Predictive Value (PPV) and is computed as	$PPV = \frac{TP}{TP + FP}$
F1 Score	F1 Score is the harmonic average of the precision and recall, where it is at its best at a value of 1, implying perfect precision and recall and is computed by	$F1 = 2\frac{PPV * TPR}{PPV + TPR}$

It should be noted that the main aim of this section is to perform a quantitative comparison study of various cyber attack detection schemes is presented using the real-time data generated by the developed testbed.

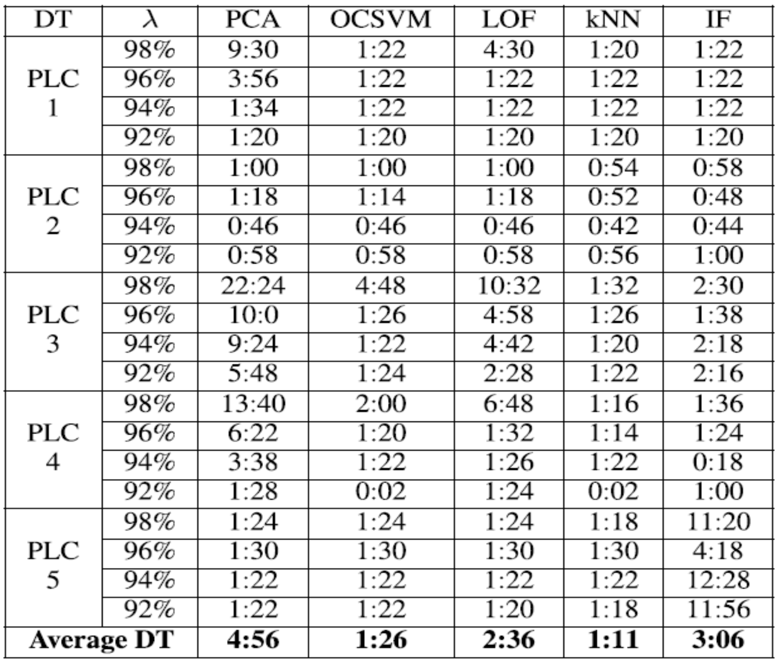
Table 2. Performance of the proposed schemes.



ML Algorithm	Accuracy	Recall	Precision	F1
PCA	0.9754	0.9568	0.9968	0.9764
OCSVM	**0.9910**	**0.9876**	**0.9954**	**0.9915**
LOF	0.9863	0.9774	0.9969	0.9870
kNN	0.9869	0.9896	0.9859	0.9877
IF	0.9628	0.9338	0.9960	0.9639

In this subsection, a quantitative comparison study of various cyber attack detection schemes is presented. As previously indicated, the field data are collected in real-time from the PLC's local cloud. Therefore, by implementing the cyber attack detection schemes on the process data in real time, the status of the data can be determined online. Table 6 provides the efficiency of the proposed schemes. As illustrated is Table 6, the IF has the worst performance over the provided datasets due to high oscillation in the detection signal (high number of false negative alarms), while it has the fastest training time (speed) in comparison with the other techniques. Moreover, the OCSVM scheme has achieved quite promising results as compared to other methods. In general, the training speed is directly proportional to the characteristics of the scheme.

Table 3. The cyber attack detection time (DT).



DT	λ	PCA	OCSVM	LOF	kNN	IF
PLC 1	98%	9:30	1:22	4:30	1:20	1:22
	96%	3:56	1:22	1:22	1:22	1:22
	94%	1:34	1:22	1:22	1:22	1:22
	92%	1:20	1:20	1:20	1:20	1:20
PLC 2	98%	1:00	1:00	1:00	0:54	0:58
	96%	1:18	1:14	1:18	0:52	0:48
	94%	0:46	0:46	0:46	0:42	0:44
	92%	0:58	0:58	0:58	0:56	1:00
PLC 3	98%	22:24	4:48	10:32	1:32	2:30
	96%	10:0	1:26	4:58	1:26	1:38
	94%	9:24	1:22	4:42	1:20	2:18
	92%	5:48	1:24	2:28	1:22	2:16
PLC 4	98%	13:40	2:00	6:48	1:16	1:36
	96%	6:22	1:20	1:32	1:14	1:24
	94%	3:38	1:22	1:26	1:22	0:18
	92%	1:28	0:02	1:24	0:02	1:00
PLC 5	98%	1:24	1:24	1:24	1:18	11:20
	96%	1:30	1:30	1:30	1:30	4:18
	94%	1:22	1:22	1:22	1:22	12:28
	92%	1:22	1:22	1:20	1:18	11:56
Average DT		**4:56**	**1:26**	**2:36**	**1:11**	**3:06**

For instance, the IF infrastructure is based on combination of multiple decision trees (binary) which leads to having a considerably fast training speed. On the other hand, OCSVM scheme calculates the decision boundaries about the data points, and hence its training speed is slow. Table 7 shows the cyber attack detection time (DT) corresponding to various cyber attack scenarios. Overall, as expected from Table 6, the OCSVM and kNN have the fastest detection times and by increasing the cyber attack severity, the cyber attack detection times are generally improved. However, for the IF algorithm, due to high oscillations in the original signal and effects of post processing algorithm, by increasing the detection times are not improved.

VIII. CONCLUSION

In this paper, a hybrid testbed is created and executed for a industrial control systems (ICS) through continuous reenacting the Tennessee Eastman (TE) process as the physical part of the testbed and executing the other layers of the ICS utilizing Siemens modules, like PLC furthermore, circulated I/O. Because of different security parts of ICS, there are numerous imperatives and difficulties in acquiring real field information. Hence, by producing and logging the information from the actual piece of the proposed testbed, a dataset as close as conceivable to the genuine field information is produced. Appropriately, by utilizing this dataset, the effect of different ongoing digital assaults on the framework and the relating proposed online location approaches are considered. The Man-In-The- Center (MITM) digital assaults are straightforwardly carried out on the PROFINET correspondence conventions to such an extent that the pernicious programmer can change the sensor estimations that are shipped off the PLC.

Accordingly, a few digital assault location approaches have been created and carried out in real time. Table 6 shows the general presentation of each digital assault discovery philosophy under different pernicious assault situations. Besides, Table 7 gives the digital assault discovery time for each plan. Albeit, all the assessed plans have had the option to identify the digital assaults previously close bringing down of the plant, notwithstanding, the OCSVM conspire shows the best presentation for this specific application. This review that depends on the proposed testbed can help in deciding the ideal methodology for a specific ICS process that depends on specified limitations (for example the plant closure condition) and prerequisites (for example the plant creation rate). It ought to be stressed that none of the past works in the writing have thought about the full Tennessee Eastman process in their created testbed. Likewise, to the best of the creators' information, none of the past work have worked on the PROFINET convention for infusing constant digital assaults. Besides, in a large portion of the past work, the digital assault recognition calculations are carried out disconnected later gathering the information from the testbed where as in this work, the digital assault recognition plans are executed in with no reservations continuous in the administrative level of the testbed. Thus, in this work the web-based execution for our proposed digital assault discovery plans are shown and given. Future work will include the execution of more complicated multi-point digital assaults on the testbed and assessment of the presentation of digital assault location and alleviation plans progressively on the testbed.

IX. REFERENCES

[1]. Devrim Unala, "Cyber-Security Methodology for a Cyber-Physical Industrial Control System Testbed", VOLUME 9, 2021, IEEE Access.

[2]. Y. Zhao, Z. Nasrullah, and Z. Li, ``PyOD: A Python toolbox for scalable outlier detection,'' J. Mach. Learn. Res., vol. 20, no. 96, pp. 1-7, Jan. 2019.

[3]. A. Winnicki, M. Krotol, and D. Gollmann, ``Cyber-physical system discovery: Reverse engineering physical processes,'' in Proc. 3rd ACM Workshop Cyber-Phys. Syst. Secur., Apr. 2017, pp. 3-14.

[4]. I. Kiss, P. Haller, and A. Bereá, ``Denial of service attack detection in case of tennessee eastman challenge process,'' Procedia Technol., vol. 19, pp. 835-841, Dec. 2015.

[5]. Ravindra Changala, "A Survey1 on Clustering Techniques to Improve Energy Efficient Routing in Wireless Sensor Networks" in International Journal of Applied Engineering Research, 10(58), pp.-1-5,2015.

[6]. G. Bernieri, E. Etchevés Miciolino, F. Pascucci, and R. Setola, ``Monitoring system reaction in cyber-physical testbed under cyber-attacks,''

Comput. Electr. Eng., vol. 59, pp. 86-98, Apr. 2017.

[7]. C.-T. Lin, S.-L. Wu, and M.-L. Lee, ``Cyber attack and defense on industry control systems,'' in Proc. IEEE Conf. Dependable Secure Comput., Aug. 2017, pp. 524-526.

[8]. M. Teixeira, T. Salman, M. Zolanvari, R. Jain, N. Meskin, and M. Samaka, ``SCADA system testbed for cybersecurity research using machine learning approach,'' Future Internet, vol. 10, no. 8, p. 76, Aug. 2018.

[9]. S. Adepu and A. Mathur, ``Distributed attack detection in a water treatment plant: Method and case study,'' IEEE Trans. Dependable Secure Comput., vol. 18, no. 1, pp. 8699, Jan. 2021.

[10]. C. M. Ahmed, V. R. Palleti, and A. P. Mathur, ``Wadi: A water distribution testbed for research in the design of secure cyber physical systems,'' in Proc. 3rd Int. Workshop Cyber-Phys. Syst. Smart Water Netw., 2017, pp. 25-28.

[11]. Ravindra Changala, "Secured Activity Based Authentication System" in " in Journal of innovations in computer science and engineering (JICSE), Volume 6, Issue 1,Pages 1-4, September 2016.ISSN: 2455-3506.

[12]. V. K. Mishra, V. R. Palleti, and A. Mathur, ``A modeling framework for critical infrastructure and its application in detecting cyber-attacks on a water distribution system,'' Int. J. Crit. Infrastruct. Protection, vol. 26, Sep. 2019, Art. no. 100298.

[13]. 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 Trans. Ind. Informat., vol. 15, no. 7, pp. 4362-4369, Jul. 2019.

[14]. X. Li, C. Zhou, Y.-C. Tian, and Y. Qin, "A dynamic decision-making approach for intrusion response in industrial control systems,'' IEEE Trans. Ind. Informat., vol. 15, no. 5, pp. 25442554, May 2019.

[15]. J. J. Downs and E. F. Vogel, "A plant-wide industrial process control problem,'' Comput. Chem. Eng., vol. 17, no. 3, pp. 245-255, Mar. 1993.

[16]. N. L. Ricker and J. H. Lee, ``Nonlinear modeling and state estimation for the tennessee eastman challenge process,'' Comput. Chem. Eng., vol. 19, no. 9, pp. 983-1005, Sep. 1995.

[17]. Ravindra Changala, "Object Tracking in Wireless Sensor networks using Data mining Techniques", in IOSR Journal of Electrical and Electronics Engineering, 2015.

[18]. PROFIBUS & PROFINET International (PI), Karlsruhe, Germany. PROFINET Security Guideline. Accessed: Feb. 14, 2020. [Online]. Available:https://www.probus.com/download/pro/net-security-guideline

[19]. Ravindra Changala, "Online Attendance using PCA Based Image Face Recognition" to publish in "International Journal for Research in Applied Science and Engineering Technology (IJRASET)" with Impact Factor 1.241, ISSN: 2321-9653,Volume 2, Issue XII, December 2014.

[20]. A Sophos Article 04.12v1.dNA, eight trends changing network security by James Lyne. 2.

[21]. Cyber Security: Understanding Cyber Crimes-Sunit Belapure Nina Godbole

[22]. Computer Security Practices in Non Profit Organisations – A NetAction Report by Audrie Krause.

[23]. A Look back on Cyber Security 2012 by Luis corrons – Panda Labs.

[24]. IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013.

[25]. CIO Asia, September 3rd, H1 2013: Cyber security in malasia by Avanthi Kumar.

[26]. https://cltc.berkeley.edu/scenario-back-matter/

[27]. https://www.bitdegree.org/tutorials/what-is-cyber-security/

[28]. M. Elnour, N. Meskin, K. Khan, and R. Jain, ``A dual-isolation-forestsbased attack detection

framework for industrial control systems,'' IEEE Access, vol. 8, pp. 36639-36651, 2020.

[29]. F. Pedregosa, G. Varoquaux, and A. Gramfort, ``Scikit-learn: Machine learning in Python,'' J. Mach. Learn. Res., vol. 12, pp. 28252830, Oct. 2011.

[30]. K. M. Ting, ``Confusion matrix,'' in Encyclopedia Machine Learning, C. Sammut and G. I. Webb, Eds. Boston, MA: Springer, 2010, p. 209.

Cite this article as :

Yagnasri Ashwini, Chetluru Rohini, Kondabathula Durga Charan, Ramakrishna Gandi, "A Novel Study on Design and Implementation of a Cyber Physical Industrial Control System by Using Cyber Security Techniques", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 9 Issue 5, pp. 76-86, September-October 2022. Available at doi : https://doi.org/10.32628/IJSRST229489
Journal URL : https://ijsrst.com/IJSRST229489