Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 7s (2025)

Security Protection of Industrial Cyber Security with IIoT Through Zone Function Modeling Algorithm

[1]Basi Reddy.A, [2]Dr.R.Yogesh Rajkumar

[1]Research Scholar,Department of Computer Science and Engineering,,Bharath Institute of Higher Education and Research,Selaiyur, Tambaram, Chennai, India 600073

[2]Assistant Professor, Department of Information Technology,,Bharath Institute of Higher Education and Research,Selaiyur, Tambaram, Chennai, India-600073

Email ID: basireddy.a@gmail.com ,yogeshrajkumar.it@bharathuniv.ac.in

Article History:

Received: *24-10-2024*

Revised: *10-12-2024*

Accepted: *18-12-2024*

Abstract:

The convergence of cyber and physical domains is a burgeoning phenomenon inside conventional industrial systems, with the objective of augmenting adaptability and effectiveness in the realms of surveillance, management, and regulation. The integration of industrial cyber-physical systems (ICPSs) on a large scale is associated with an increased susceptibility to security vulnerabilities. The identification of attacks is an essential element of the initial protective barrier and carries substantial significance within the wider framework of security safeguarding. Currently, there is a lack of a data-driven approach to evaluate the risk of SCADA software for IIoT devices, despite the clear need to understand the cyber threat to urban critical infrastructure. Statistical models are developed with the purpose of determining risk metrics for SCADA systems, which may be employed to evaluate the probability of exploiting vulnerabilities connected with SCADA. We have developed a customizable schema for ranking SCADA hazards based on our study findings. The security community may employ this schema to improve their understanding of hazards particular to SCADA. In order to ascertain the effectiveness of the proposed approach, a laboratory apparatus is ultimately developed. The results suggest that the suggested approach provides a solution characterized by a notable degree of precision, while also demonstrating efficient performance in real-time situations.

Keywords: Industrial cyber physical systems (ICPSs), security protection, cyber security

Overview:

The rapid growth of computer technology has prompted traditional industrial automation systems to strive for a smoother integration between the real world and cyberspace, hence increasing their vulnerabilities and triggering a range of cyber security concerns [3]. The prevalence of incidents related to security inside industrial control systems and Power Plants (ICPSs) has been consistently increasing each year, as evidenced by the reports released by the Manufacturing Control Systems Computer Emergency Readiness Team [4]. Considering the crucial role of ICPSs in the nation's economy, any malicious infiltration might have significant consequences for the welfare of persons, the environment, and resources [5], [6].

In the realm of security, intrusion detection plays a pivotal role by serving as an essential element that acts as an exterior protective barrier. There are two primary classifications for this phenomenon:

signature-based and anomaly-based [7]. Signature-based approaches utilize a database or pre-established signatures to identify and categorize attacks, often exhibiting effectiveness when confronted with documented intrusion attempts. However, the intrinsic qualities of these entities make them inadequate in detecting new or unexpected attacks. This research paper provides a thorough examination of the risks associated with flaws and abuses in vital infrastructure SCADA systems, utilizing statistical approaches. Furthermore, the paper offers recommendations on the architecture of SCADA IIoT systems in order to mitigate the risk of potential system exploitation in the future.

Evaluating the risk of IIoT vulnerabilities is a challenging endeavor the framework's slow adoption can be linked to the substantial time and cost required for its deployment, despite being deemed the best-in-class [4]. The recognition of cyber risk can be facilitated by the utilization of pre-existing taxonomy for Hmi and essential infrastructure vulnerabilities [5]–[7]. While it is possible that these taxonomies might be useful, their results are not firmly based on data-driven, empirical study. This raises questions about their appropriateness for evaluating cyber hazards in the field. Introduction to SCADA IIoT

System Control and Data Acquisition (SCADA) systems are a type of device in the Industrial Internet of Thing (also known as II that provide a supervisory software controlling layer for many controllers with programmable logic (PLCs). SCADA systems are purposefully designed to cater to extended distances, such as the transportation of water or power. Due to the greater distances, there is usually less supervision on the networks that make use of them. 80% of companies in the US employ SCADA systems [8]. SCADA systems are dependent on telephone communication or other third-party networks for their functioning, which leads to a reduction in the speed, and frequency, and overall level of communications [9]. The reason for this is because SCADA systems frequently function in an event-driven fashion, whereby data is exclusively communicated from gadgets to the program when there is a change in its value [9]. In order to provide oversight of additional Industrial Internet of Things (IIoT) gadgets, SCADA systems require an operator interface or a human-computer interface (HMI) to supervise, provide instructions to, and oversee the devices connected to the system [10].

SCADA systems often run on commercially accessible Windows personal PCs, making them susceptible to several operating system and Window-based assaults [12]. A prominent challenge arises from the increasing requirement to incorporate SCADA-based IIoT systems into IT networks. The employment of TCP/IP-based attacks can facilitate illegal entry into SCADA programs whose may be vulnerable.

The process of identifying and categorizing vulnerabilities

Several categories and categorizations of attacks and vulnerabilities in critical infrastructure have been identified [6]. Two previous studies have focused on different areas of vulnerability in critical infrastructure. The utilization of these typologies demonstrates significant benefits in understanding the vast critical infrastructure environment. Nevertheless, their use in providing practical counsel to executives, managers, and policy makers is hindered by their lack of clarity, hence limiting their power to give significant insights for security experts and researchers. Moreover, both studies fail to

explicitly assess the safety of the SCADA systems, which play a vital role in the operation of urban infrastructure.

Pak (6) provided a comprehensive list of many types of generic attacks that he considers very relevant to the domain of cybersecurity. These categorizations encompass denial of service assaults bugs, and Trojan horses. In a comprehensive manner, Pak (2016) put up a number of organizational proposals. These recommendations included improving the sharing of information in vulnerable critical infrastructure sectors, publicly announcing vulnerabilities to facilitate corrective actions, and promoting collaboration between the public and private sectors to strengthen security through training and education initiatives. Furthermore, he advocates for the continuous monitoring of susceptible ports that are susceptible to attacks [6]. The solutions put up by Pak (6) lack explicitness due to the broad scope of the conventional definition of critical infrastructure, which comprises many cyber systems, including those found in industries such as banking and energy.

Li et al. [7] developed a classification that is especially tailored for cyber assaults against SCADA infrastructure. Additionally, they included specific suggestions on the hardware and software weaknesses that SCADA networks may be prone to. SCADA is susceptible to several critical vulnerabilities, including the lack of separate privileges in embedded OSes, buffer overflow, and injection of SQL [7]. The study undertaken by Zhu et al. [7] did not offer clarity on how control engineers judged the relevance of these assaults and vulnerabilities for SCADA, despite their active efforts to discover and solve them.

Moreover, it is crucial to do an inquiry into the association between the vulnerability risk metrics of First.org and the amount of attacks related to the program subclass of systems for SCADA. Furthermore, there is a need for a tailored data-driven vulnerability prioritization framework for SCADA that corresponds to the unique business attributes of an enterprise. Incorporating this schema into NIST's comprehensive ICS digital safety framework represents a significant enhancement.

Communications and Information Process Systems (ICPSs) encompass the integration of technology, communication, and physical systems, exhibiting a robust interdependence among the cyberspace and physical domains [19]. Attacks on security in ICPSs have the potential to impact not just the digital sphere but also the physical environment [20]. Therefore, it is crucial to broaden the range of detection of anomalies in Industrial Control and Power Systems (ICPSs) beyond the area of cyber threats and also take into account abnormalities in physical systems.A. Detection of anomalies in ICPSs1) Providing a comprehensive description of all industrial procedures is difficult due to their extensive scope and complex characteristics. Hence, the resolution of the problems pertaining to false negatives and false positive presents considerable obstacles [7].

The major aim of assaults is to disturb physical processes, and hence, the atypical actions may not be evident in the realm of cyberspace.

The genesis of the attacks cannot be exclusively ascribed to a cyber-system, but can also come from susceptible media, like Stuxnet, which used portable storage devices to enter Siemens systems [24]. Under the most dire circumstances, intentionally undermining anatomical structures might result in a cataclysmic catastrophe. The theoretical approach proposed by Pasqualetti and colleagues [27] employs geometrical control theory in order to tackle the complexities associated with digital and

physical systems and the detection of attacks. This framework is especially designed to address attacks that are undetected and cannot be identified.

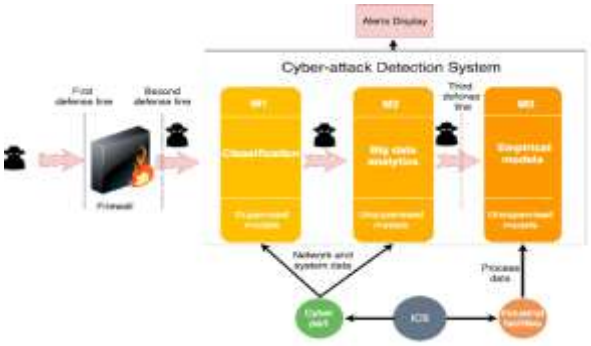

Figure 1: Industrial Control System based Cyber Attacks Timeline

The Implementation of Zone Partitioning for Enhancing Security Protection
The implementation of zone partitioning in IEC62443 [13] serves as an effective measure to prevent system failure. This is because attacks are unlikely to penetrate multiple isolated zones simultaneously. Additionally, zone partitioning aids in conducting thorough risk assessments, identifying security measures, and safeguarding system safety [14]. The design of industrial systems was considered by Genge et al. In their study, Jin et al. (2017) conducted a partitioning of the business subsystems inside a military information system (MIS) into distinct secure domains. They subsequently introduced a MIS access control technique that relies on a security domain oriented administrative role based management model. This approach aims to effectively manage and regulate the secure domains. Jee et al. [18] implemented a secure intrusion response solution by implementing network control center communication control. This approach effectively prevented the propagation of malicious assaults and invasions to other subsystems by dividing and isolating the affected subsystems. However, these research just examined isolation protection techniques and mostly concentrated on information technology systems. The physical system of ICPSs was not addressed by any of the aforementioned studies [29-30].

Zone partition is a very efficient and dependable method that may be employed for the purpose of safeguarding security and conducting anomaly investigation. In conclusion, the criteria and procedures for anomaly analysis are described in accordance with the estimated zone functions.

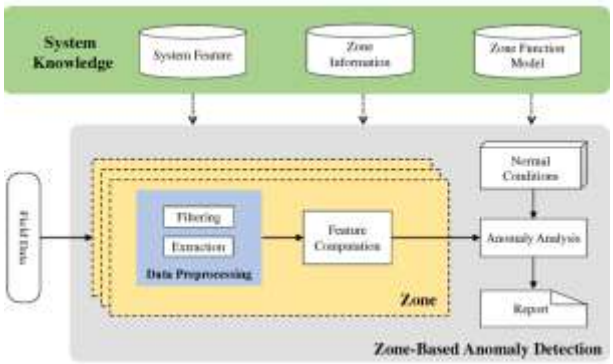

Figure 2: Architecture of the zone-based anomaly detection for ICPSs

Experimental Procedure Zone Partition Method

The primary objective of zone partitioning in this study is to effectively segregate the aforementioned variables into distinct zones, hence ensuring that any anomalies present may be accurately represented within the remaining zones. Based on the qualitative description of the causal model, it is evident that the state may be viewed in isolation, as well as in relation to all the elements within complex system (cs) and each individual element inside es.
The cause set for s is denoted as cs = cis |i °F [1,m], whereas the effect set is denoted as es = eis |i °F [1, n]. The number of members in these two sets is m. A detectable set is defined for the set s, where Ds is defined as the sum of cs *h*e1s *o*e2s *o*… °Fens *o*s.
The notation "i" is used to indicate that each set in the expression is considered as a mutually independent element. For example, d1s = cs, d2s = e1s, and dn+2s = s.
The detectable set for the entire system, including target nodes, may be expressed as d = dj si | i = 1 tol ; j = 1 to a(i), where a(i) represents the size of dsi. Given the division of each element in dsi into distinct zones, it can be inferred that the states would be seen inside these zones. The zone information is described as a 3-tuple, denoted as z = (v, s, b).

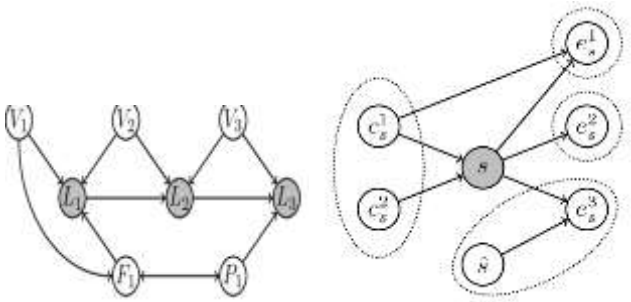

Figure 3: Structure of causal model for the target node s. (a) Basic structure. (b) Two typical situations

Let v represent the variables in z, s represent the states that may be inferred from v, and b represent whether v is enough for seeing each state in s. Within set b, a value of 1 signifies adequacy, whereas a value of 0 signifies inadequacy. In addition, it is necessary to couple s with b. For instance, let z be defined as (n1, n2, s1 π s2, 1 ℃ 0), where n1 and n2 represent the variables inside z. It demonstrates that z can accurately deduce s1 based on n1 and n2, but not for s2.
The algorithm alone achieves the partitioning of each critical state, however there may exist some crossovers and inconsistencies among the zones pertaining to other physical states. Furthermore, the scale of the zone magnitude will be substantial for a complicated system. A unique technique has been developed to tackle these issues, as depicted in the technique. In this algorithm, the set κ is utilized to document the zones that intersect with a certain zone.

Algorithm: Zone Partition Algorithm

Input: *Observed sensor value from Industrial IoT*
Output: *Partition of regions with a time Interval*

Begin

1. *Initialize boundary value, sub_region, distance*
2. *Partition the region with the time period*
3. *Each region is again divided into k sub_regions with boundary value*
4. *Compute the distance between first and last records in each sub_region*
5. *If the last value of sub_region n and the initial value of sub_region n+1 is similar,*
   then
   a. *Enhance the sub_region n with inclusion of similar values from sub_region n+1*
   b. Retrench the sub_region n+1 with no. of values passed to sub_region n
   else
   a. Repeat the step from 4 to 7 until all the regions are sorted.
6. *End*

RESULTS AND DISCUSSION

The vulnerability analysis in this work was extended to the CWE level. The initial step was the calculation of the vulnerability density for each CWE. The aforementioned calculation used the division of the aggregate count of CVEs per CWE by the overall count of vulnerabilities. As an illustration, the CWE "buffer overflow" had a total of 202 CVEs. The CWE density of 24.40% was calculated by dividing this by the total number of SCADA vulnerabilities, which is 828. The frequency of SCADA CWEs serves as an indicator of the frequency with which various vulnerability categories are encountered in SCADA critical infrastructure, and is crucial for the establishment of a priority schema.

Due to this circumstance, the primary concern for SCADA operators and security staff may not be the density of CWE. The density of CWE exploits can offer a more accurate evaluation of operational risk, given that these flaws are easily accessible for attackers to use. The identical formula was utilized for the exploits in accordance with CWE. As an illustration, the CWE "out-of-bounds read" has 32 vulnerabilities linked to CVEs. The table presents the five most prominent CWEs in terms of exploit density.

Table 1: Cyber Weakness Classes

Rank	Cyber Weakness Classes	Density
1	Buffer Overflow	0.344
2	Information Exposure	0.205
3	Improper Input Validation	0.200
4	Cross SitenSeripting	0.063
5	Path Traversal	0.061

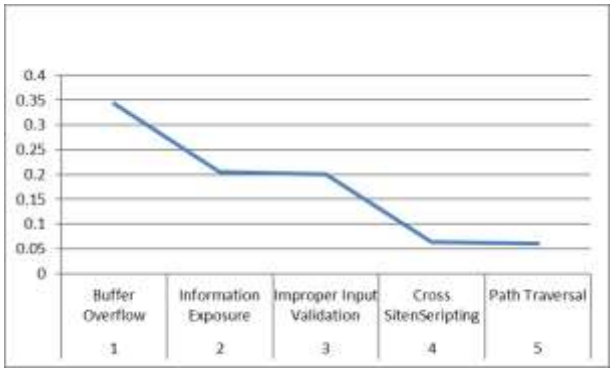

Figure 4: Density Level of Cyber weakness Classes

Operator Implications

This article, albeit focused on a specific subsector of IIoT, can have a significant influence on the security of urban critical infrastructure. The results of our study suggest a significant correlation between the risk metrics of First.org and the density of exploits, particularly in the context of SCADA systems. This knowledge can be valued by three distinct cohorts of professionals specializing in critical urban infrastructure security:

Activities inside an organization typically bear the challenging task of creating and overseeing programs to ensure the firm's security on a large scale. Based on our research, Chief Information Security Officers (CISOs) may optimize their initiatives to protect SCADA systems. Instead of implementing initiatives aimed at developing metrics for evaluating the danger of different Industrial Internet of Things (IIoT) systems, Chief Information Security Officers (CISOs) might opt to utilize

Our findings can also be advantageous for SOC analysts, who are a distinct set of security specialists. The primary responsibility of SOC analysts frequently include the monitoring and remediation of security vulnerabilities in real-time. Rather of adopting a reactive approach to identify security risks, our risk prioritization schema aims to assist analysts in proactively identifying the IIoT systems that are susceptible to attacks. The prioritized device list of SOC analysts may be determined by cross-referencing IIoT devices with the most exploited CVEs and CWEs that have been detected.

The design and development of future SCADA IIoT systems should emphasize the elimination of the vulnerabilities identified in this article. By prioritizing vulnerabilities during the design process, it is possible to mitigate the occurrence of future attacks targeting this particular class of Industrial Internet of Things (IIoT). Drawing upon the advice pertaining to the three most prominent vulnerabilities, namely buffer overflows, inappropriate input validation, and information disclosure, it is possible to put forth technical design methods aimed at mitigating these vulnerabilities.

Buffer overflows are a common occurrence in operating systems that are implemented using the C programming language. The programming language facilitates direct memory access, hence contributing to the mitigation of energy consumption in the device. The cost efficiency of SCADA systems is significantly influenced by energy efficiency, particularly due to their widely spread nature in areas with limited resource availability. In addition, C exhibits high memory efficiency, making it particularly advantageous for compact devices necessary for urban vital infrastructure. Notwithstanding the advantages associated with C, the presence of buffer overflow risks arising from

coding errors represents a significant drawback. The aforementioned risk can be mitigated with the implementation of a memory-safe programming language during the development of forthcoming SCADA systems. Rust, a memory-efficient language, is recognized as a memory-safe programming language [28]. If future Industrial Internet of Things (IIoT) systems can be implemented using the Rust programming language, the problem of buffer overflows will be eliminated, hence eliminating this vulnerability for IIoT SCADA systems.

Table 2: SCADA Exploits versus CWE Frequency, Impact Score and Exploitability Score

	Estimate	**Std.Error**	**t-Value**	**Pr(>|t|)**
Intercept	-21.490	6.225	-2.113	0.015
Frequency	0.267	0.025	10.424	2.12
Impact Score	0.542	0.465	1.13	0.188
Exploitability Score	1.417	1.023	1.561	0.135

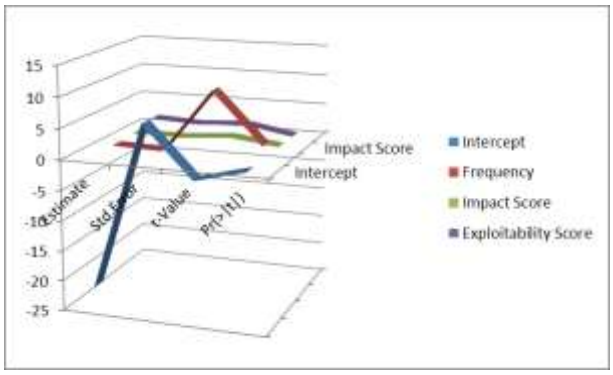

Figure 5: Supervisory control and data acquisition (SCADA) systems in IIOT

The findings of this study were unexpected, as they suggest that there exists a distinct characteristic in the association between SCADA CWE frequency and exploitability, as well as the impact scores, and exploit density. This finding contradicts the findings of Allodi and Massacci [2], who saw a similar relationship in IT systems. Additionally, this suggests that the intricate equation employed by First.org, which transforms impact and exploitability ratings into CVSS scores, does not account for the association between them.

The term "DA" refers to the level of accuracy in identifying all observed outliers. It is calculated by dividing the total number of anomalous instances in the testing dataset by the number of discovered outliers [7]. While the FNR measure is consistently low, the FPR metric exhibits significant variation.

Specifically, false alarms often occur during regular operation when BP-NN is trained with inadequate data. This issue may be mitigated by increasing the size of the training set. However, given that the training error has already been satisfied, there are only a limited number of enhancements that can be made when the dataset size exceeds 1600. Specifically, there are two supplementary approaches to enhance the training efficacy inside this system: Take into account a wide range of operational settings and ensure that the training set does not contain a large amount of comparable data.

Table 3: PERFORMANCE ON DIFFERENT TRAINING SETS

Dataset	Normal	Anomaly	FP	FN	FPR	FNR	DA
400	432	607	355	54	82.21%	8.73%	63.43%
800	432	607	175	3	40.14%	0.33%	78.82%
1200	432	607	38	1	8.58%	1%	95.25%
1600	432	607	10	0	2.09%	0%	98.54%
2000	432	607	6	0	1.16%	0%	99.18%

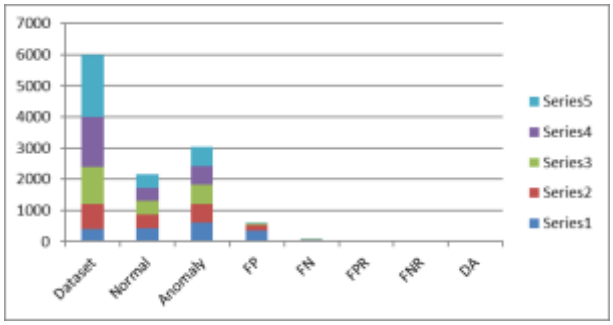

Figure 6: PERFORMANCE ON DIFFERENT TRAINING SETS

Based on the findings of the experiment, three distinct conclusions may be drawn regarding our strategy.

1) The detection of attacks is possible when their objectives include the interception or destruction of the physical process.

The capacity to detect abnormalities is present in every zone. The suggested method's properties are examined by a comparative analysis with other established techniques, and the findings are presented in Table. It is evident that the majority of other approaches, which just concentrate on physical states, are unable to identify the anomaly resulting from the spoofing assault examined in this study. Furthermore, only a limited number of the current solutions has all the features of the strategy outlined in this article.

Conclusion

The study also reveals strong correlations between vulnerability risk indicators of First.org and the frequency of SCADA attacks. Security experts should reconsider their claims that exploitability and impact ratings are not reliable indicators of the likelihood of exploitation, based on these findings. Given the distinctive demands of SCADA systems and the accompanying difficulties in addressing vulnerability patching, it is imperative to explore alternate security solutions pertaining to priority vulnerabilities. The prioritizing structure offered may be tailored to meet the specific needs and parameters of an organization. Urban operators of critical infrastructure can utilize prioritization with NIST's complete cybersecurity framework to get insight into the risk associated with their SCADA system.

Due to its reliance on empirical and data-driven conclusions, the SCADA priority schema need ongoing updates in response to the publication of new vulnerabilities. The priority model will become obsolete if a sequence of novel SCADA exploits is introduced, specifically targeting a

certain vulnerability class. Future research might incorporate the examination of supplementary attributes of vulnerabilities as variables in order to ascertain their correlation with the likelihood of exploitation. The comprehensive consideration of physical domain elements is necessary in any anomaly detection system due to the inherent characteristics of ICPSs.

REFERENCES

[1] Z. Asad, M. A. R. Chaudhry, and D. Kundur, "On the use of matroid theory for distributed cyber-physical-constrained generator scheduling in smart grid," IEEE Trans. Ind. Electron., vol. 62, no. 1, pp. 299–309, Jan. 2015.

[2] P.-Y. Chen, S. Yang, and J. A. McCann, "Distributed real-time anomaly detection in networked industrial sensing systems," IEEE Trans. Ind. Elec- tron., vol. 62, no. 6, pp. 3832–3842, Jun. 2015.

[3] K. Stouffer, J. Falco, and K. Scarfone, "Guide to industrial control systems (ICS) security," NIST Special Publ., vol. 800, no. 82, pp. 16–16, 2011.

[4] U.S. Dept. Homeland Security, "ICS-CERT year in review 2015," U.S. Dept. Homeland Security, Washington, DC, USA, 2015.

[5] T. Novak and A. Gerstinger, "Safety-and security-critical services in build- ing automation and control systems," IEEE Trans. Ind. Electron., vol. 57, no. 11, pp. 3614–3621, Nov. 2010.

[6] B. Karabacak, S. O. Yildirim, and N. Baykal, "Regulatory approaches for cyber security of critical infrastructures: The case of turkey," Comput. Law Security Rev., vol. 32, no. 3, pp. 526–539, Jun. 2016.

[7] C. Zhou et al., "Design and analysis of multimodel-based anomaly in- trusion detection systems in industrial process automation," IEEE Trans. Syst., Man, Cybern., Syst., vol. 45, no. 10, pp. 1345–1360, Oct. 2015.

[8] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia´-Ferna´ndez, and E. Va´zquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," Comput. Security., vol. 28, no. 1, pp. 18–28, Feb./Mar. 2009.

[9] Z.-H. Pang, G.-P. Liu, D. Zhou, F. Hou, and D. Sun, "Two-channel false data injection attacks against output tracking control of networked sys- tems," IEEE Trans. Ind. Electron., vol. 63, no. 5, pp. 3242–3251, May 2016.

[10] A. A. Ca´rdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry, "Attacks against process control systems: Risk assessment, detection, and response," in Proc. ACM Symp. Inf., Comput. Commun. Security, Mar. 2011, pp. 355–366.

[11] G. Sabaliauskaite and A. P. Mathur, "Countermeasures to enhance cyber- physical system security and safety," in Proc. IEEE 38th Int. Comput. Softw. Appl. Conf. Workshops, Jul. 2014, pp. 13–18.

[12] Y. Park, S. H. Baek, S.-H. Kim, and K.-L. Tsui, "Statistical process control- based intrusion detection and monitoring," Qual. Rel. Eng. Int., vol. 30, no. 2, pp. 257–273, 2014.

[13] Int. Soc. of Automation (ISA) Std., Security for industrial automation and control systems 727 Part 3-2: security risk assessment and system design, ISA-62443-3-2, 2013.

[14] Y. Hashimoto et al., "Safety securing approach against cyber-attacks for process control system," Comput. Chem. Eng., vol. 57, pp. 181–186, Oct. 2013.

[15] T. Morita et al., "Detection of cyber-attacks with zone dividing and PCA," Procedia Comput. Sci., vol. 22, pp. 727–736, 2013.

[16] B. Genge, P. Haller, and I. Kiss, "Cyber-security-aware network design of industrial control systems," IEEE Syst. J., vol. 11, no. 3, pp. 1373–1384, Sep. 2017.

[17] Y. Jin, H. Liu, L. Sun, and J. Song, "Study on security domain-oriented military information systems access control model," in Proc. Intell. Syst. Knowl. Eng., 2014, pp. 849–856.

[18] J. Jee, J. Jang, I. Jo, and Y. Shin, “A network partition scheme to protect secure zone for malicious code,” in Proc. Int. Conf. Inf. Netw., 2013, pp. 476–480.

[19] S.-H. Choi, I.-B. Jeong, J.-H. Kim, and J. J. Lee, “Context generator and behavior translator in a multilayer architecture for a modular development process of cyber-physical robot systems,” IEEE Trans. Ind. Electron., vol. 61, no. 2, pp. 882–892, Feb. 2014.

[20] M. Pajic, I. Lee, and G. J. Pappas, “Attack-resilient state estimation for noisy dynamical systems,” IEEE Trans. Control Netw. Syst., vol. 4, no. 1, pp. 82–92, Mar. 2017.

[21] I. N. Fovino, A. Coletta, A. Carcano, and M. Masera, “Critical state-based filtering system for securing SCADA network protocols,” IEEE Trans. Ind. Electron., vol. 59, no. 10, pp. 3943–3950, Oct. 2012.

[22] J. Kim and S. Jung, “Implementation of the RBF neural chip with the backpropagation algorithm for on-line learning,” Appl. Soft Comput., vol. 29, pp. 233–244, Apr. 2015.

[23] J. Luo and E. E. Konofagou, “A fast normalized cross-correlation calculation method for motion estimation,” IEEE Trans. Ultrason., Ferroelect., Freq. Control., vol. 57, no. 6, pp. 1347–1357, Jun. 2010.

[24] R.Senthamil Selvan “INTEGRATING THE BIGDATA ANALYTICS AND DEEP LEARNING analysis human movement to improve the sports” by 2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS), ISSN:0018-9219,E-ISSN:1558-2256,December 2023. 10.1109/AECE59614.2023.10428236.

[25] R.Senthamil Selvan “MULTI OBJECTIVES EVALUATOR MODEL DEVELOPMENT FOR ANALYZE THE CUSTOMER BEHAVIOUS” by 2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS), ISSN:0018-9219,E-ISSN:1558-2256,December 2023. 10.1109/AECE59614.2023.10428189.

[26] R.Senthamil Selvan “Cloud Computing Based Medical Activity Supporting System” by 2024 2nd International Conference on Disruptive Technologies (ICDT) on 15th and 16th March 2024, 10.1109/ICDT61202.2024.10489245, ISSN:0018-9219,E-ISSN:1558-2256,11 April 2024

[27] W. Li, L. Xie, Z. Deng, and Z. Wang, “False sequential logic attack on SCADA system and its physical impact analysis,” Comput. Security, vol. 58, pp. 149–159, May 2016.

[28] Z. Asad, M. A. R. Chaudhry, and D. Kundur, “On the use of matroid theory for distributed cyber-physical-constrained generator scheduling in smart grid,” IEEE Trans. Ind. Electron., vol. 62, no. 1, pp. 299–309, Jan. 2015.

[29] P.-Y. Chen, S. Yang, and J. A. McCann, “Distributed real-time anomaly detection in networked industrial sensing systems,” IEEE Trans. Ind. Electron., vol. 62, no. 6, pp. 3832–3842, Jun. 2015.