Retraction Notice

The Editor-in-Chief and the publisher have retracted this article, which was submitted as part of a guest-edited special section. An investigation uncovered evidence of systematic manipulation of the publication process, including compromised peer review. The Editor and publisher no longer have confidence in the results and conclusions of the article.

AB, KK, HJA, and MK did not agree with the retraction. MDA either did not respond directly or could not be reached.

Secure framework against cyber attacks on cyber-physical robotic systems

Akashdeep Bhardwaj,[a] **Mohammad Dahman Alshehri**,[b] **Keshav Kaushik**,[a] **Hasan J. Alyamani**,[c] **and Manoj Kumar**[a,*]

[a]University of Petroleum and Energy Studies, School of Computer Science, Dehradun, India

[b]Taif University, College of Computers and Information Technology, Department of Computer Science, Taif, Saudi Arabia

[c]King Abdulaziz University, Department of Information Systems, Faculty of Computing and Information Technology in Rabigh, Jeddah, Saudi Arabia

Abstract. Robot-based platforms and processes have integrated the security and efficiency of data into a comprehensive range for domains, such as manufacturing, industrial, logistical, agricultural, healthcare, and internet services. Smart cyberattacks have been on the rise, specifically targeting corporate, industrial robotic systems. These attacks execute once the internet of things, internet, and organization integration is implemented with the industrial units. We implemented security criteria-based indices for cyber-physical systems (CPS) with industrial components and embedded sensors that process the information logs and processes. We proposed an attack tree-based secure framework that does not include every CPS device but takes into consideration the critical exploitable vulnerabilities to execute the attacks. We categorized each physical device and integrated sensors based on logs and information in a sensor indices device library. This research simulated real-time exploitation of vulnerabilities on CPS robotic systems using the proposed framework in form of a two-phased process. This validates the enhanced data security output of the integrated sensor and physical nodes with the intelligent monitor and controller system health monitor during real-time cyberattacks This research simulated common cyberattacks on cyber-physical controller servers based on cross-site scripting and telnet pivoting. The authors gathered known and unknown vulnerabilities and exploited them with a tree-based attack algorithm. The authors calculated the average time for cyberattackers with different skills when trying to compromise CPS devices and systems. © *2022 SPIE and IS&T* [DOI: 10.1117/1.JEI.31.6.061802]

Keywords: cyber-physical; robotic security; robotic platforms; attack framework; cross-site scripting; telnet pivot.

Paper 210644SS received Sep. 22, 2021; accepted for publication Dec. 3, 2021; published online Mar. 10, 2022.

1 Introduction

Given the extent to which digital technologies and physical devices have infiltrated our lives, there is a belief that this closer integration with many other disciplines will only grow to new heights in the near future. The new age of industrial revolution 4.0 is largely concerned with future systems of digital manufacturing. In homes, smart sound, light and heating solutions, housekeeping robots, air conditioning systems connect and integrate with computational systems and devices. The transportation domain includes cars, planes, and electrical bicycles. Healthcare pacemakers, personal assistance robots, insulin pumps, and smart prosthetics provide immense help to patients. These technologies did not exist until recently, yet now they offer the potential to save and improve the quality of life tremendously. Wearable fitness and health monitoring devices offer the potential of a huge positive impact for healthy people as well as those with physical or cognitive disabilities.[1] Industry monitoring and control systems involve the use of sensors,

*Address all correspondence to Manoj Kumar, wss.manojkumar@gmail.com

1017-9909/2022/$28.00 © 2022 SPIE and IS&T

networks to observe large land or marine areas. Examples from the energy sector include smart grids, windmills, and technologies to harvest green energy. It is no exaggeration to imagine the entire planet Earth as a massive cyber-physical (CP) ecosystem. Accidental occurrences occur that seriously cost human life and service provision financially and economically. However, high-sophisticated problems and hazards arise from hostile threats and internet attacks, which include robotic platform malware, hijacks, and remote control.

Smart industrial production systems generate goods using computer-integrated processes, networks for intelligence, cybernetics, and mechatronics.[2] Cyber-physical systems (CPS) integrates physical dynamics, monitoring, and control servers with software application components and networks. This smart production system incorporates real-world physical and computer components, which result in highly monitored and controlled states and parameters for optimum production. These are entwined to operate at temporal and spatial states to monitor and control physical processes and vice versa. Smart grids, industrial control units, driverless cars, automatic pilot avionics, autonomous automobiles, and robotic systems are some common examples of CPS. While CPS shares a relatively similar architecture to the internet of things (IoT) but does not work in a standalone manner. CPS operates in an automated manner with a higher level of coordination and processes, as an interacting combination of computational components and physical devices, such as actuators, robots, embedded sensors, and human machine interfaces in production facilities. Such infrastructures provide technical solutions and promote new efficient human engagement with various domain architecture and abstractions, such as consumer, energy, infrastructure, environmental, health care, manufacturing, military, physical security, smart cities, transportation, and robotic equipment and machinery.

To maximize the use of resources and system performance, CPS combines and collaborates computing and physical processes connected to the internet or internal secure data center. However, cyber threats and attacks through internal networks or internet access jeopardize the security of physical and computational interacting elements. These smart cybersecurity attacks infiltrate CPS via the cyber or the networked component to attack the primarily controllers, industrial servers, computers, programmable logic controllers, robotic systems. Secure connection to external networks has always been a security concern for CPS deployments. CPS controllers suffer irreparable damages when attackers discover new ways to access the control systems to alter their services and configurations. Although cyber mitigations systems, such as end-point security, antivirus shields, or network intrusion detection devices, have emerged as possible solutions for internal attacks, yet the smart cyberattacks and threats have been multiplying and getting sophisticated. CPS suffers badly in this regard, as control and security are solely served by the command-and-control server, and the devices are often secured by no other protection. Smart security attacks on the cyber layer to the CPS systems have an intrinsic causal impact. More recent cyberattacks include the Colonial pipeline attack[3] in May 2021 suffered a ransomware attack that affected the computer systems and equipment managing the pipeline. Company operations were halted even as the colonial pipeline ransomware attack cost 75 bitcoin or US $ 4.4 million. Stuxnet[4] and Aurora[5] attacks raised the need to recognize the high priority requirement of protection of critical physical infrastructures.

In this context, CPS is a fresh field for research for designing and deploying mitigation measures to counter and mitigate smart cyberattacks. Interest in the security of industrial infrastructure has increased for collaborative robotic systems working on vital infrastructures with automatic and semiautomatic assembly processes globally. In recent times, attention to managing and mitigating cyber risks by reducing security gaps posed by automation processes or manual actions has gained huge consideration. Cyber safety and detection solutions are designed for CPS running on collaborative-networked ecosystems.

Highlights of this research include:

- Unique taxonomy of cybersecurity attacks on CPS, the innovative aspect of this classification is to identify smart cybersecurity-related issues for robotic industrial CPS applications. Then research papers and vendor vulnerabilities are categorized based on cyberattack causes, attacks, threat vectors, threats, and risks involved.
- Secure framework to enable safe and secure human-robotic system collaboration in industrial environments. The proposed secure CPS framework can help reduce threats, such as

information breaches, data transfers, or alternations, in device logs from smart cyberattacks on the computational nodes, devices, and interfaces connecting various physical components.

- Algorithms for determining the anomalies in the sensor logs due to smart cyberattacks.
- Detect Denial of Service (DoS) attacks by focusing on the anomaly values due to denial of service attacks on robotic industrial infrastructures. Sensors deployed in such environments face integrity attacks as altered log records. This aids in the reconstruction of errors and anomaly detection for various classes and the difference in infrastructure performance before and after the attack.
- Performed simulated attack-tree assessment to exploit vulnerabilities and insecure conditions in the robotic CPS systems.

This research paper is organized as follows: Sec. 2 presents the selection process of the previously published literature and the most relevant references reviewed by the authors as part of the study. This further facilitates the creation of the unique taxonomy for CPS cyberattack categories in Sec. 3. Based on this classification and knowledge, the authors present the research methodology for the research in Sec. 4 and present the unique secure framework for mitigating smart cyberattacks against robotic CPS. Sections 5 and 6 focus on a specific use case involving an industrial setup with a robotic process having subsystem modules integrating with physical devices, including the experimental results and discussions on the results obtained from this research. Finally, Sec. 7 presents the main conclusions of this research work and the outlook on future research.

2 Literature Survey

The authors reviewed 245 research papers published since 2018 from highly referred journals (IEEE, Elsevier, ACM, IGI-Global, among others). Based on research related to industrial robotics, CPS, and cybersecurity attacks, the authors segregated research that classified or presented new attacks and presented frameworks to secure the integrated computers and physical systems. The authors then classified and shortlisted the research papers using a four-level selection method and shortlisted 39 relevant and closely matching works with this research as shown in Fig. 1.

Based on the 245 papers selected, the authors categorized each paper and using a four-stage selection process and selected the final 39 papers. Table 1 classifies the papers as per CPS, industrial robotics, robotic attacks, robotic platforms, robotic attack taxonomy, and secure robotic framework.

Huang et al.[6] proposed smart robotic vehicle to reconfigure the hardware settings to deliver cryptographic functions and neural network inference with improved system efficiency and adaptability for agricultural CPS. To support its decision-making mechanism, the authors presented a model of crop growth and a detection model for pests and diseases. The industrial

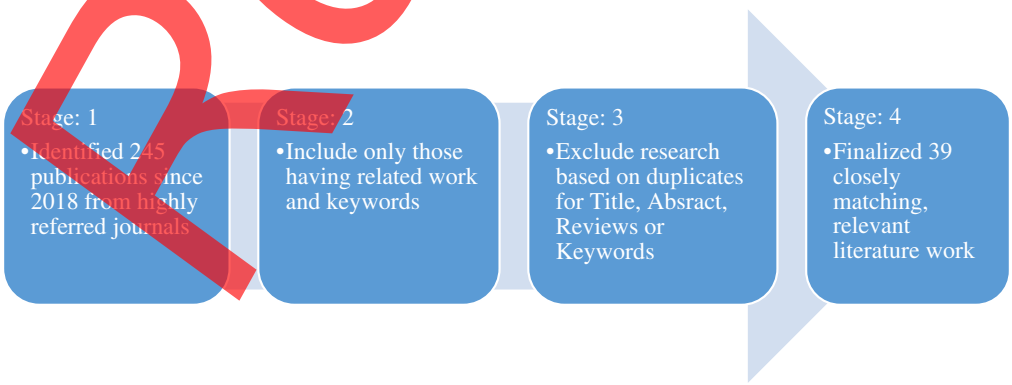

Fig. 1 Research selection methodology.

Table 1 Research papers and subcategories.

Grading classification	Stage: 1	Stage: 2	Stage: 3	Stage: 4	Breakup (%)
CPS	51	38	23	9	22.17
Industrial robotics	49	37	22	8	21.30
Robotic attacks	31	23	14	5	13.48
Robotic platforms	34	26	15	6	14.78
Robotic attack taxonomy	28	21	13	5	12.17
Secure robotic framework	37	28	17	6	16.09
	245	173	104	39	—

robotic assembly process and the working environment are generally described by the contact states.

Zhang et al.[7] classified contact state classifications based on extreme machines for industrial robotic assembly and have extended the network to kernel learning to solve problems of contact state recognition. The code generation system is independent of the training dataset and is used to classify the contact condition of the complex assembly process using kernel-based on the basic classification. The results showed that the proposed classification method can recognize the contact status and that kernel-based machine classification performance is higher than extreme learning machines. This allows the robot that favors the assembly tasks to provide more accurate information on the contact states.

Shih and Lian[8] proposed to connect and synchronize between a physical shop floor and cyberspace to a new frame of a grinding robot system with CPS. The gaps between the real world and simulation nevertheless lead to uncertainty. The object locating method can contribute to the precise position of the grinding machine. The robot trajectory can be generated and automatically modified to satisfy smart production. Two complex workpieces that include six tool paths were completed successfully by the authors. The system's grinding quality is better than that of the robot, and the time of education is reduced by 90%.

Muthusamy[9] examined robotic assistance impedance-based robotic control approaches. By conducting physical human–robot interaction experiments, the authors provided aid and cooperation from each approach. Modern robotic manipulators are equipped with sophisticated manipulation hands. By providing admission or impedance control to the interactive forces of the finger-part, the multiple-finger hand-arm cooperation with a human partner can be improved. The conventional way of using torque/force sensors on the wrist differs both internally and externally, as well as the interaction point.

Jhaveri et al.[10] proposed a mechanism of SDN routing to improve quality of services (QoS) in CP robotic systems requiring real-time. To enable QoS in such late-limited networks, writers use SDN capabilities to dynamically select routings based on current links. An effective industrial topology has also been verified for the proposed approach. Experiments have shown that an existing delay-based routing system significantly outperforms the proposed approach as regards average output, end-to-end delay, and jitter. For industrial applications in CP robotic systems, the proposed solution would be significant. The contact state is described for the robotic assembly environment when vision-based systems for occluded parts fail.

Li et al.[11] developed an assembly process model based on the support of vector regression and particle swarm, which describes the relationship between assembly contact state and robot executive action, to solve the contact state recognition problem. To predict the next robot motion, the established model with parameters optimized by PSO is used. The result shows that the proposed method can model and lay the basis for the improvement of the flexibility and fastness of small assemblies for the complex assembled process of low-voltage appliances.

Butt et al.[12] introduced a new soft robotic actuator design and construction process with pressure and curvature sensing attributes. The pressure-sensitive film consists of five sensitive areas, which are embedded in the soft actuator and are connected to the back of the soft actuator

by a flexible fabric-based curvature sensor. The production and design of the soft actuator are straightforward, cost-effective, and do not affect continuous bending. Both sensors are characterized and the results analyzed. The actuator can provide feedback on the piezo-resistant effect for both the haptic and the curvature. Finally, this feedback is used for a closed-loop grasping experiment, when both actuators are placed in a parallel grip and only pressure feedback is used to present the concept of softened haptic perception.

Ding et al.[13] presented an extensive study on the relationship between robotic perceptions, robot perception, and distributed computing; this study examined the challenges and opportunities offered to distributed computing by intelligent CPS. There are also multiscale distributed hybrid intelligence architecture named music and initial practices for enabling this architecture.

Keung et al.[14] reviewed CPS applications in mobile robotic systems. Four algorithms: a priori, frequent pattern growth, ECLAT, and k-mode algorithms are used to reduce robotic robot conflict and increase RMFS capacity management. The total completion time based on frequently assigned items is lower than on the random allocation of storage. However, conflicts with the docking grid are increasing because the most common items in a specific area are concentrated. Human workers have been replaced with robotic applications in manufacturing environments. However, a few problems persist, such as robotic automation, robot training, not sacrificing safety problems, and adapting the robot to manufacturing changes and uncertainties.

The concept of adult and child robots was proposed by Hong et al.[15] to address these challenges. Role characteristics and task division for guided assembly tasks are identified and analyzed and applied. The solution proposed includes robot navigation, mobile handling, robot learning, and intelligent assembly with controlled strength. There have been experimental platforms, and some preliminary results show that the proposed method is very promising. The methods proposed will make industrial robots smarter.

Huang et al.[6] introduced a collision-free swarm robotic CPS development control strategy using a robust orthogonal firefly algorithm. The proposed fluid-based cyber and cognition levels, using the smart connectivity, data-to-information conversion, and configuration levels, are integrated with the robotic sensors and actuators to design a pragmatic swarm robotic CPS using the system to program chip technology. The distributed control strategy and the potential field of broadcasting are used to address the problem of training swarm robotic CPS with barriers. The embedded central processing unit, operating system, intellectual property networking, and robot-customized IPs are integrated with the proposed swarm robotic CPS into field-programmable gate array chips. The results of the experiment and comparisons with other methods reveal the merits of the proposed swarm robotic control unit for a collision-free control of distributed formation.

The new ecological and intelligent surveillance station design, with environmental factors sensors and robotic monitoring cameras to detect and actively monitor spectrum wildlife utilizing robotic pan-tilt-zoom cameras, was presented by Zhu et al.[17] in the field of vision. This system enables forest activities and life habits, wind speed, and directional sensors, temperature and humidity sensors, and concentration sensors, as defined by this system, to be effectively and constantly monitored through cooperation with several devices, such as robotic pan and zoom cameras. The system also monitors wildlife and forest climate change. The experiments show the feasibility and efficiency.

Wang et al.[18] suggested a strategy based on a nonlinear disturbance observer for a robotic manipulator to manipulate the nonsingular fast terminal sliding modes. A fractional-order, nonsingular fast-end-mode control method, which is designed to track the desired manipulator trajectory accurately, combines the advantages of fractional calculus theory with a sliding-mode control strategy. The Lyapunov function demonstrates the stability of the closed-loop control system. Simulation findings show that the strategy proposed can effectively improve the tracking and control precision of the joints and perform the manipulator's fine operation.

Gautham and Bera[20] presented the trajectory tracking of robotic manipulators. Sliding mode control is an efficient tool for controlling complex nonlinear systems, because of their low sensitivity to uncertainties. In an event-induced strategy, the control signal is only updated when a particular event condition is infringed and thus the regular performance of control tasks is avoided. To illustrate the theoretical forecasts, simulation results are shown.

The use of the RFID to look for items by a set of automated guide vehicles evolving in a two-dimensional grid workspace with a range of static obstacles was described by Hentout et al.[21] The research for objects of interest was used to manage the robots that move within their workspace while spreading and reading pheromones. This indirect mechanism is used. The results of the simulation show the effectiveness of the approach proposed and the reduction in the total number of nodes visited. Systems with enhanced or enhanced resilience properties are needed because the use of CPS continues to increase in human life. Within these systems, the survival feature must be insured in terms of ambient assisted living systems.

Gomez and Matson[22] outlined a scheme for achieving survivable results as a result of the interaction between varieties of agents interacting in the setting of these systems by a multiagent system. Wang et al.[23] focused on developing an intelligent perceptual system that can develop the robot task program to program in industrial assembly tasks by demonstrating. In visually observed demonstrations, the main problem of the system is to understand the semantics of the parts and the abilities. To describe this problem as a common inference of skills actions, the authors presented a probabilistic framework. The findings showed that PBD can be implemented in assembly tasks to achieve the teacher–student scenarios with its proposed perception system and finally verified the effectiveness and feasibility of the system.

Khrueangsakun et al.[24] investigated the CPS trend, highlighting the digital twins' human user interface for monitoring and control to enhance the VR and AR visualization for easier system interpretation. This paper introduced the design of a four-degree-of-freedom (4-DoF) robotic arm system in real-time web-based monitor and control where the robotic arm is a physical and web-based cyber part visualization. The design proposed provided two-way communication, real-time control, and surveillance that could be used for industrial applications.

Drawing robots are designed without human assistance to copy or create drawings. Yu et al.[25] presented an overview of key technologies that showed that the current methods are problematic. These authors proposed faster, more humanized, and more creative trends in robotic drawing in the future. Implementation of CPS physical elements, communication networks, and control systems, including the IoT, the internet, and other systems. The security challenges and various types of attacks, such as jamming and distributed denial of service (DDoS), are many for these systems. CPS attacks are generally much smarter and more dynamic and therefore require defending strategies that can address this intelligence and dynamic level or use machine learning as a basis for a variety of CPS security problems.

Alabadi and Albayrak[26] reported on recent research using the Q-learning algorithm for enabling security and privacy. Various Q-learning approaches are studied in security and defense strategies. Classified and analyzed by attacks, domain, supported techniques, and details of the Q-learning algorithm are the latest in Q-learning and CPS systems. There were also discussions on future research trends for the effective use of Q-learning and profound Q-learning concerning CPS security.

A taxonomy after analyzing the state of CPS security issues was presented by Gawanmeh and Alomari.[27] The authors analyzed safety issues in CPS, as well as applications for safety, such as eHealth and medical, smart grid and power, vehicle technology, industrial control and production, autonomous systems and UAV systems, and finally IoT-related problems. Human actors require special interfaces to integrate with IoT frameworks that provide the right software architectures, data models, protocols, message types, and applications in terms of complexity and multimodality.

Sahinel et al.[28] focused on the requirements and design approaches for integrating human actors within a CPS. The concept and implementation of a full human-integration framework are presented as part of a multiagent IoT middleware after the systematic assessment and taxonomy of related research literature.

The safety and security of CPS are often mutually important. Making sure there are no negative consequences might require a considerable and rigorous effort during CPS development. However, rapid feedback can help security engineers understand how trivial design choices in their field can have unacceptable effects on each other, early in the life cycle. The cyber risk evaluation framework was proposed by Asplund et al.[29] The framework was based on openly available and widely used security and security-domain taxonomies and a unique mapping where data security loss can impact safety-related aspects of data. The authors demonstrated

the framework with real-time examples from various organizations. This was the first time that diverse parts were brought together into a unified framework with a method. The authors demonstrated how the framework may be put to good use using examples from within companies.

Li et al.[30] developed a scheduling method based on time and task thresholds that accomplishes the dynamic randomization of mimic defense from two distinct dimensions. Finally, a dynamic scheduling algorithm based on the multilevel queue is proposed by integrating time and random thresholds. The study found that a dynamic scheduling method based on a multilevel queue can consider both security and reliability, has superior dynamic heterogeneous redundancy features, and effectively prevents attackers from mastering the transformation rule of heterogeneous executors.

Rehman et al.[31] presented a method for identifying and classifying DDOS attacks in the real world. The study used both traditional machine learning classifiers and a deep learning method to assess the efficacy of the proposed model. A comparison of gated recurrent unit, recurrent neural network, and machine learning methods was also provided by the authors. In comparison to others, the gated recurrent unit delivers an efficient detection and identification rate, according to the findings of the experiments.

Shafiq et al.[32] suggested a hybrid feature selection approach based on machine learning that employed two metrics: weighted mutual information and area under the ROC curve. These measurements honed in on the most useful aspects of a traffic flow. The authors presented a robust features selection method to choose robust features from the specified characteristics. The suggested method improves the accuracy of machine learning classifiers and aids in the detection of harmful communications. On the diverse network environment traces datasets, the authors evaluated the study work using 11 well-known ML classifiers. Their algorithms achieved more than 95% flow accuracy in tests, according to the results.

Khan et al.[33] investigated software vendor security risks and obstacles. The authors used a search string inspired by the research questions to perform a comprehensive literature review of pertinent research papers. Using the recommended review, their research identified 15 key security difficulties and 64 standard practices for the critical security challenges. The conclusions of this study revealed similarities and differences in the highlighted security concerns across time, continents, databases, and approaches.

Kaur et al.[34] investigated an offline cloud scenario in which computers are efficiently deployed and scheduled for user processing demands using lion optimization packet optimization of software defined networks. Reduced bandwidth, job execution times and latencies, and increased throughput are all considered when evaluating performance. In a cloud environment, a minimal execution time algorithm is utilized to calculate the completion time of all available resources allotted to the virtual machine, and the lion optimization method is applied to packets. The proposed work has been proved to increase throughput and reduce delay.

CPS, which are widely used in critical infrastructures, are subject to a variety of threats. One of the most serious risks to CPS is data integrity assaults, which distort sensor measurements and cause control systems to fail. To secure CPS, anomaly detection methods are provided. Sensor and process noise were used by Luo et al.[35] to identify data integrity assaults, which represent the intrinsic properties of physical devices and the manufacturing process in CPS. Deep noise discovered that data integrity threats alter noise patterns, which are the root cause of anomalies.

Amin et al.[36] presented a comprehensive overview of cyber-physical (CP) assaults, vulnerabilities, mitigation measures for power electronics, and smart grid security concerns. An overview of power electronics system security on the networked smart grid from a CP perspective was presented, followed by emphases on important CP attack patterns with significant impact on the operation of power electronics components, as well as corresponding defense methods. The authors also highlighted the CPS dangers and mitigation techniques, as well as interactions with smart grid applications.

In the face of a jamming attacker, Alipour-Fanid et al.[37] investigated the security of remote state estimation in wireless CPS where sensors feed measurements to the remote state estimator through a multichannel wireless link. The authors presented an approach that does not require any prior knowledge of the attacker's attack policy or channel state information. This optimizes sensor channel selection and power consumption while also ensuring the asymptotic stability of the estimator. The results show that the approach achieves sublinear learning regret bound in

theory. When compared with solutions that directly apply the baseline solution, the solution improves the regret upper bound.

To enable heterogeneous IoT architecture, Gupta et al.[38] developed an upgraded information-centric networking-based internet of things content caching technique by enabling AI-based collaborative filtering within the edge cloud. This content caching technique based on collaborative filtering would intelligently cache material on edge nodes for cloud database traffic control. In comparison to the best-considered LCD, the evaluations conducted to check the performance of the proposed strategy over various benchmark strategies revealed better performance with an average gain of 15% in the cache hit ratio, a 12% reduction in content retrieval delay, and a 28% reduction in average hop count.

For the packet dropout problem induced by jamming assaults, Xu et al.[39] developed a simpler tree-based model predictive control solution based on attack detection. This approach efficiently represents all scenarios along the prediction horizon in the form of a binary tree, allowing it to deal with probabilistic packet dropouts. A combined system that considers all situations can be obtained by merging all probable attacks in the prediction horizon. The controller is then designed using an attack detection approach, which dramatically minimizes the number of possibilities anticipated at each time step. Finally, the simulation results show that using the attack detection method reduces the running time significantly without compromising control performance. The findings of this study can help to increase the control efficiency of CPSs that have been assaulted.

From the literature survey, the authors identified four specific security-related gaps and issues focusing on four CPS applications. Table 2 illustrates the assessment and classification of previous papers based on CPS security aspects and attack levels, and this is followed by a unique taxonomy of CPS cyberattacks based on the cause, attack vectors, threats, and risks involved.

3 Taxonomy of Cybersecurity Robotic Challenges

Cyberattacks targeting critical industrial robotic systems and business applications have increased and become sophisticated to detect and mitigate even as the threat surface area has increased due to the integration of physical devices with internet network access, process, and IoT components. This primarily gives rise to attacks targeting both the robotics systems and the privacy of the data generated. The authors performed an assessment using confidentiality, integrity, availability, authentication, and privacy (CIAAP) traits of various vulnerabilities in industrial robotic implementations. This involved robotic vendors as per common vulnerabilities and exploits (CVE) and presents the top gaps in Table 3. Mitigation of these vulnerabilities is a potential future research domain. Typically, these vulnerabilities exploit:

- Confidentiality causes data and process code to be revealed with total information disclosure or with integrated human-robotic scenarios involving IoT devices and cloud-enabled networked robots;
- Integrity violation results in complete loss of system logs, OS, and app modules leading to the entire infrastructure being compromised;
- Availability issues lead to the total shutdown of the impacted resources, due to unauthorized access resulting in hang or frequently repeatable crashes or even complete DoS.
- Authentication issues (improper validation or default values) allow bypassing the client authentication certificates on critical backend database or upstreams systems. Attackers send unprotected server name indications to the HTTP host header and backend specifying a protected backend.
- Privacy issues due to attacks on robotic devices lead to, increased access, direct surveillance, and social profile tracking of users as well as industrial systems. Robots have embedded sophisticated IoT processors and sensors that magnify capacity to observe and analyze as compared to humans.

This results in various vulnerabilities scan and attacks being targeted toward the robotics data and system security influencing the CIAAP. This taxonomy classifies smart attacks targeting both the robots and the systems in the setup as shown in Fig. 2. The taxonomy highlights cause, threat vectors, and impact of the attacks on robotic CPS environments.

Table 2 CPS security and attack levels.

	Robotic CPS security				Robotic attack levels			
Research references	Design	Detection	Mitigation	Response	Apps	Firmware	Network	Process
Huang et al.[6]	√	√	—	—	√	—	—	√
Zhang et al.[7]	—	—	√	√	√	—	√	—
Shih and Lian[8]	—	√	√	—	—	√	—	—
Muthusamy[9]	√	—	√	—	√	√	—	√
Jhaveri et al.[10]	—	√	—	√	—	√	—	—
Li et al.[11]	√	√	√	—	√	√	—	—
Butt et al.[12]	—	√	—	√	—	—	√	√
Ding et al.[13]	—	√	√	—	√	—	√	—
Keung et al.[14]	—	√	—	√	—	√	—	—
Hong et al.[15]	√	√	—	—	√	—	—	√
Xu et al.[16]	—	√	√	—	—	—	√	
Zhu et al.[17]		—	√	√	—	√	—	—
Wang et al.[18]	√	—	√	√	√	—	—	√
Bhardwaj et al.[19]	—	√	√	—	—	—	√	—
Gautham and Bera[20]	√	√	—	—	—	—	√	—
Hentout et al.[21]	—	√	√	—	√	—	—	√
Gomez and matson[22]	—	√	—	—	—	—	—	—
Wang et al.[23]	—	√	—	—	—	—	√	—
Khrueangsakun et al.[24]	—	—	√	√	—	√	—	—
Yu and Chen[25]	—	—	√	√	—	—	—	√
Alabadi and Albayrak[26]	√	—	√	—	√	—	—	—
Gawanmeh and Alomari[27]	—	√	√	—	√	—	√	—
Sahinel et al.[28]	√	—	—	√	—	—	√	—
Asplund et al.[29]	√	—	—	—	—	√	√	—
Alshukri et al.[40]	√	√	—	√	—	√	—	—
Tanjim et al.[41]	√	√	—	—	—	—	√	—
Uddin et al.[42]	—	√	√	—	—	—	√	—
Zhang et al.[43]	—	√	—	√	—	—	√	√
Haus et al.[44]	—	√	√	—	√	—	√	—

4 Research Methodology

The authors designed security criteria-based indices for CPS collaboration. Security levels are defined as indices based on the CPS components and embedded sensors that process the information logs and processes. The authors categorized each physical device and integrated sensors based on logs and information in a sensor indices device library. After the initial set of sensors

Table 3 CIAAP CPS vulnerabilities.[45]

Vendor	CVE	Vulnerability type
Citrix	CVE 2021 22914	Bypass of Citrix cloud connectors, lead to sensitive information storage access via command line and client parameters
	CV 2021 22907	Remote code execution allows improper access control to unauthenticated malicious users
	CVE 2020 13998	Gain local admin access using 2FA by privilege escalation for unauthenticated users.
	CVE 2020 8246	Citrix ADC, gateway, and net scalar against denial of service attacks originating from management network systems
Oracle	CVE 2021 22883	Too many database connection attempts from unknown protocols lead to the leaking of file descriptors, which leads to excessive memory loss on the system
	CVE 2021 2219	PeopleSoft SQR tools allow low privilege attacks via HTTP on the database leading to unauthorized update, delete, and table modification
	CVE 2021 2057	Oracle retail app is exploitable for partial denial of service attacks and unauthorized management access
Epsom	CVE 2020 9453	EMP_MPAU.sys driver does not validate local user input values, leading to a denial of service attacks on Epsom iProjection units
	CVE 2020 9014	EMP_NSAU.sys leads to denial of services for input to the virtual audio controller via IOCTL 0x9C402402 iProjection systems
Robotis	CVE 2019 15786	Dynamixel SDK app is vulnerable to buffer overflow attacks when receiving large RX-Packets as input from physical units
Rockwell	CVE 2021 22665	Automation driver tools (SPv5.1 and AOPv4.1) allow the local user to attack physical devices with limited access and exploit system processes
	CVE 2020 27267	Kepserver v6.8 and ThinkWorx industrial server have heap-based buffer overflow, causing servers to crash and leak sensitive data
	CVE 2020 13573	Denial of service vulnerability exists causing Ethernet packets to be recrafted to send malicious commands and trigger DoS attacks.

is selected, an optimal solution is reached between the sensors, specifications, and collaborating physical devices from the library. The authors implemented an optimization algorithm to match vendor-specific needs and requirements for any smart secure CPS. Based on the vendor's needs, the solutions are presented. The sensor device library categorized and tabulates the sensor and embedded devices, physical systems as per the logs generated from critically located sensors. Inbound and outbound traffic configurations are utilized as a part of the data threshold. These are applied during the "design" and "device selection" phase and can be customized as per vendor or client requirements as shown in Fig. 3.

Apart from assigning priority to the components in the CPS device library, the research methodology includes a customized selection of CPS NIST standard features. Again, these are selected in real-time as per the design inputs by the client for the industrial scenario integrating with robotic and physical devices working with human workers for monitoring and control. Once the optimized and secure CPS architecture meets the client requirements, the security tests are performed. The authors simulated a modern-day CPS robotic system associated with solar power generation and water desalination against cyber risks and attacks. The attack graphs included three stages: input generator, scan for conditions to determine vulnerabilities, and then exploit. The sensors and IoT devices have a prerequisite as per four conditions.

- Access level in the infrastructure setup;
- Privilege assigned for accessing previous exploit vulnerability;

Fig. 2 CPS security taxonomy.

- Service delivered by the device integrating with physical units;
- Network connections to other devices.

While exploiting a specific vulnerability, attacks focus on gaining unauthorized access to the sensor and IoT device logs as well as apps and the embedded controllers to control the system. Firewalls and any intrusion detection agents are disabled once the intruder accesses the authentication server. Then commands are sent to close, open, or stop the circuits through the edge firewall and then the intruder exploits the web application firewall. This model takes into account the exploit level and the vulnerability type to select the priority. The authors designed the architecture to withstand cyberattacks against the critical vulnerabilities; this is shown in Fig. 4 for robotic CPS systems with the following assumptions:

- Edge firewall is a hardware device, similar to Cisco ASA at the network edge, this simulates and offers standard network port and packet filtering.
- Security systems such as VPN servers with dual 2FA authentication with endpoint enterprise security and an IDS provide further network-level security.
- As a third level, the web app firewall inside the infrastructure provides application security at layer 4 level for final access to the application and database servers. These act as log aggregators and controllers from the sensors, IoT, and physical devices.

5 Proposed Secure Smart Cybersecurity Framework

Advanced, unknown attacks are inbound via the edge firewall and compromise the authentication servers and security systems to impact the application control modules. Any new security system such as endpoint security or IPS offering similar security mitigation solutions can also be

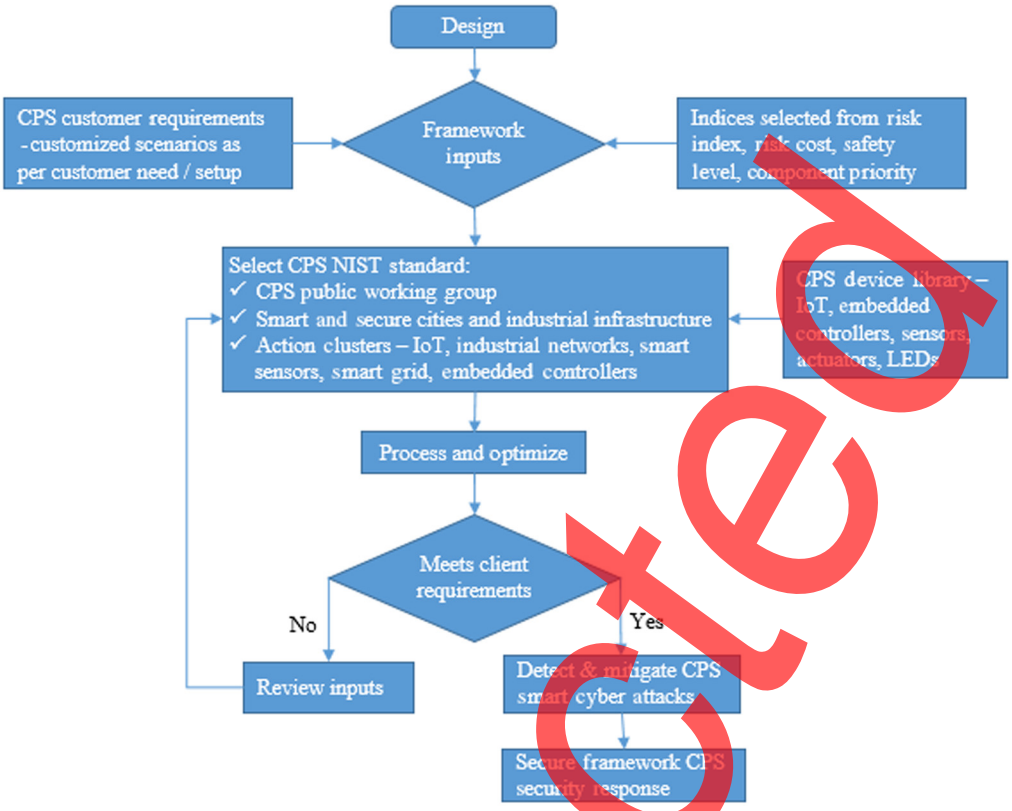

Fig. 3 CPS and security collaboration process.

Fig. 4 CPS infrastructure with dual firewalls and security systems.

compromised. Redundant and dual-control server to validate any control command is proposed as a backup CPS controller. However, manual or automatic switching to such a mechanism is difficult to implement given the critical real-time sensor and robotic systems involved. One option is comparing the real-time sensor readings and logs against the prestored threshold after taking into account the integrated physical devices with the sensors and IoT.

The authors proposed an attack tree-based secure framework as shown in Fig. 5 that does not include every CPS device; however, it takes into consideration the critical exploitable vulnerabilities to execute the attacks. Assuming there are two exploits on the edge firewall: zero-day or unknown exploits denoted by (Exp1, 0, 1), that is, identified by attackers but not known publicly, and known exploit denoted by (Exp2, 0, 1) available on red team attack tools such as Metasploit. To exploit these, attackers need to have services available remotely as Exp(1) and Exp(2) along with user privilege access Usr0 connecting the application and database server as (0,1). When privilege access vulnerability is exploited, the intruder gains unauthorized access as Usr(1) on the authentication system. Assuming the web app firewall has few zero-day exploits denoted by (Exp 3, 1, 2), the intruder can exploit this with privilege access to gain remote access to the app and database servers.

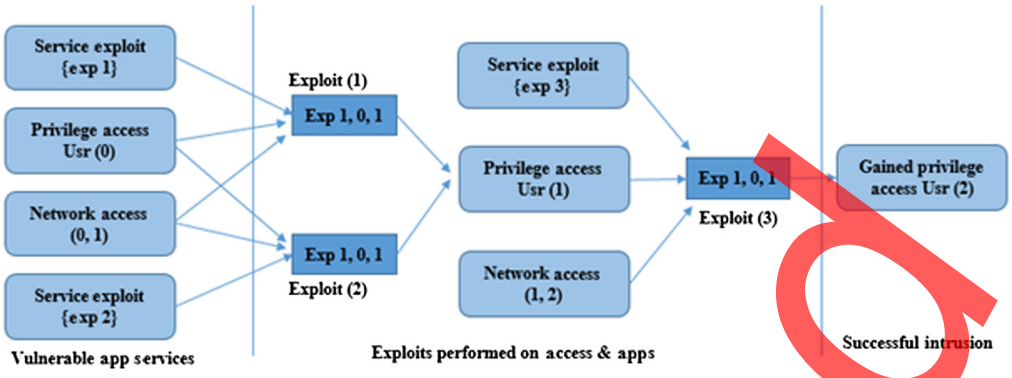

Fig. 5 Proposed attack tree framework for known and unknown exploits.

Changes in the output efficiency are easily monitored against an optimum threshold value and alerts are generated. Human involvement and control provide the intelligent decision-making step. However, slight deviations resulting in previously unknown unusual behavioral response of the physical devices is difficult to monitor. These can be due to a smart, sophisticated cyberattack or hardware or app malfunctions, or protocol issues in the device sensor, embedded chips, or the IOS itself a machine due to some malfunction. The pseudocode for the exploit is presented for reference below (Algorithm 1).

Algorithm 1 Algorithm for Exploit.

```
for i in range(0, a.slot+1):
    a.y_real_arr.append(a.yreal)
    # sensor attack here
    a.score.append(a.s)
    pid. SetPoint = a.ref[i]
    pid.update(feedback_value=a.ymeasure, current_time=i * a. Ts)
    a_cin = pid.output
    # print(a.ymeasure,i,a_cin,xout)
    if a_cin > 10:
       a_cin= 10
    elif a_cin< -10:
       a_cin = -10
    else:
       a_cin = a.cin
    control_inputs.append(a.cin)
    if i>a.place:
       if (a.score[-1] == a.thres):
          a.att = a.drift
       else:
          a.att = a.thres+a.drift-a.score[-1]
```

```
Attack part: (I is position for malicious data)

I = np.array([9520, 9312, 3214, 4324, 4143, 4143, 7323, 8023, 4565, 234,
3123, 2524, 5324, 45, 3234, 4452, 977, 4040, 3567, 1234, 2345, 7454, 1890,
5789, 3432])mid2 = 0.6

mid = 0

m = np.array([])

for i in I:

  tsz=d[i+50000]

  tsz[mid]=tsz[mid]+mid2

  att=np.array([tsz])

  if mid < 13:

    mid = mid+1

  else:

    mid = mid-13

    mid2 = 0.8

  loss = autoencoder.evaluate(att,att)

  print(loss)

  m = np.append(m,loss[0])
```

Figure 6(a) shows the register reading and its value to observe anomalies or any abnormal behavior by the computational components or the physical devices at high values thresholds or if the system stabilizes after measuring against the predetermined optimum values to deliver consistent value output. The authors also tested the framework for a use case involving CPS monitoring and controlling IoT Wet sensors. Simulated attacks were executed to gather the response and the readings as shown in Fig. 6(b) for the plot between the wet sensor register v/s value.

Reconstruction error for different attack classes for anomaly detection in the CPS robotic setup. The below graph plots the reconstruction error and the data point index. After observing the normal values in Fig. 7(a), different anomalies are plotted in Fig. 7(b). The reconstruction error for anomalies of different sensors is plotted against the time series. It has been observed that different anomalies have reacted differently depending upon the type of input, and they are shown with a different color in the above figure for better differentiation.

Figures 8(a)–8(c) show the plot between the difference in the speed, rotational angle, and altitude, respectively, for before and after attack scenarios.

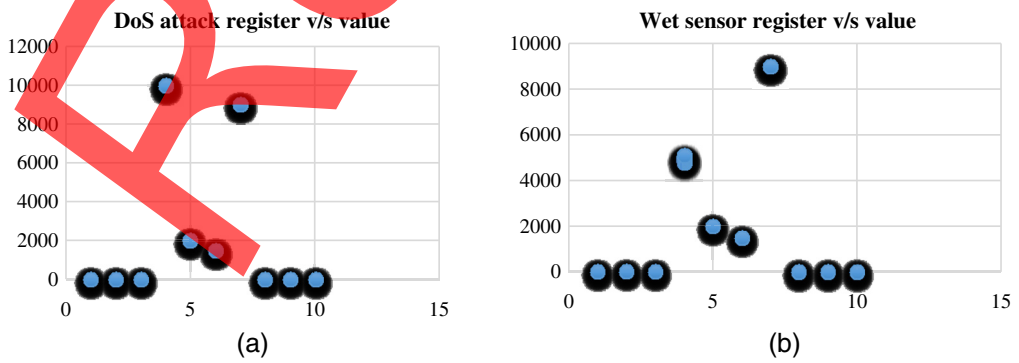

Fig. 6 (a) DoS attack register v/s value and (b) wet sensor register v/s value.

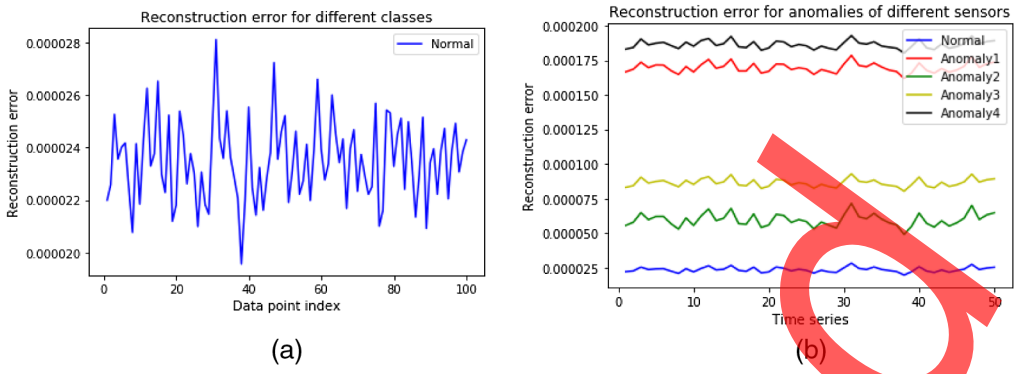

Fig. 7 (a) Reconstruction error (different classes) and (b) reconstruction error (different sensors).

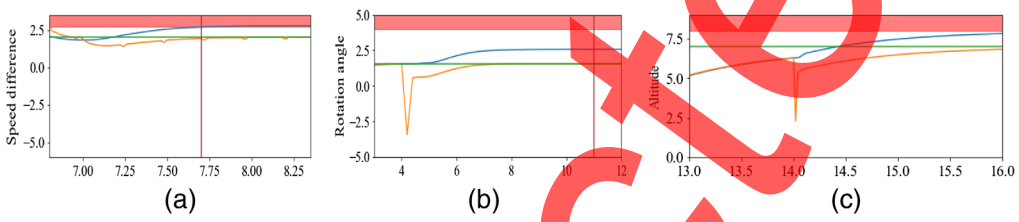

Fig. 8 (a) Speed difference, (b) rotational angle difference, and (c) altitude difference before and after an attack.

6 Experimental Results

This research simulates real-time exploitation of vulnerabilities on CPS robotic systems using the proposed framework in the form of a two-phased process. This validates the enhanced data security output of the integrated sensor and physical nodes with the intelligent monitor and controller system health monitor during real-time cyberattacks. The assumption is taken for a small- to medium-intensity cyberattack to exploit the known and unknown zero-day vulnerabilities. This research also assumes that the intruder can successfully breach the firewall security and embeds abnormal network traffic data flow, which results in congesting the CPS network. This further impacts the CPS robotic working significantly and results in partial to complete loss of access and severely impacts the QoS of the CPS infrastructure. This research validates the security framework for an IoT sensor-physical integrated CPS to simulate real industrial scenarios and apply to complex infrastructures. The authors first executed cross-site scripting (XSS) attack with malicious scripts being injected into the CPS server controller site and apps to run on the user system as shown in Fig. 9. The scripts change the user input with invalidated and sanitized inputs to alter the output for physical components.

This redirected the human access to robotic CPS to the intruder's malicious site as presented in pseudocode below XSS redirection on CPS (Algorithm 2).

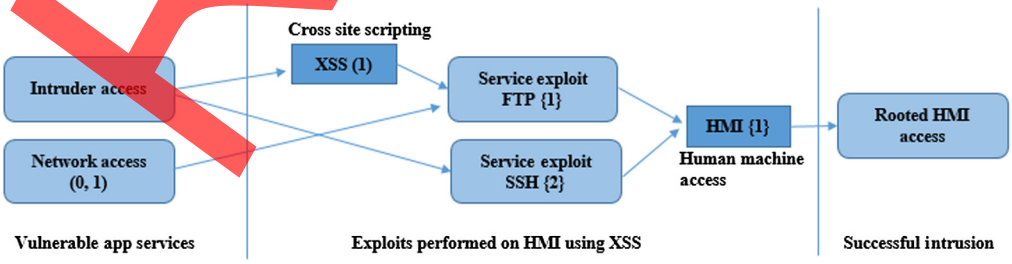

Fig. 9 Cross-site scripting attack.

Algorithm 2 Algorithm for XSS redirection on CPS.

```
Redirecting to...
http://var buffer = []; var attacker = '/Akash/Lab/Keylogger/?c='
Document.on-keypass = function [e] { var timetamp = Now. Date() / -;
var stroke = {k:e.key, t:timestamp}; buffer.push{stroke}; }
window.set.interval(function()
{
if (buffer.length > 0)
{ var data = encodeURIComponent(JSON.stringify(buffer));
new Image().sra = attacker + data;
buffer = [];
}, 200);
```

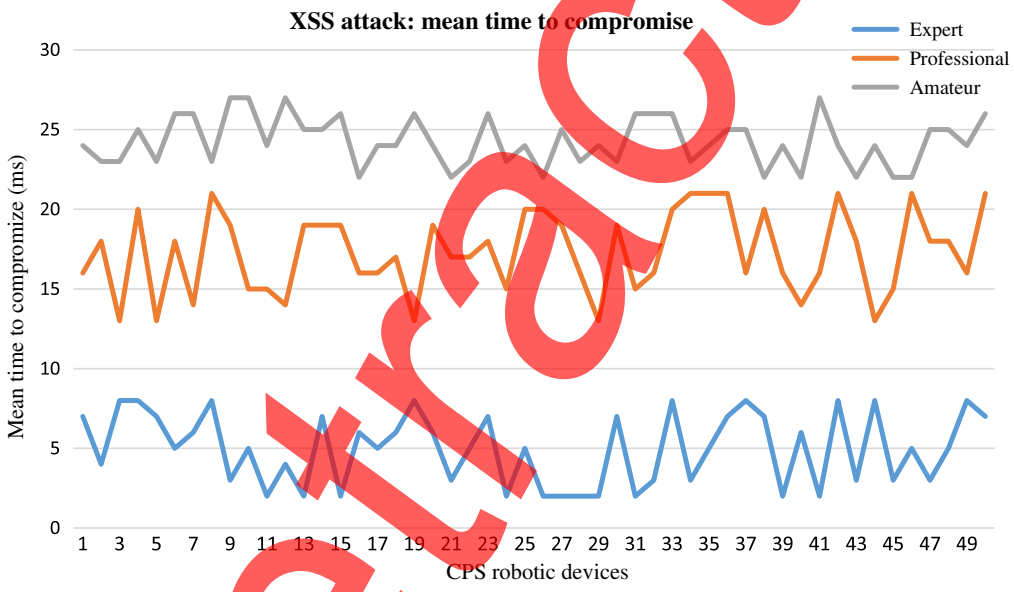

Fig. 10 XSS attack.

The authors calculated the time required to find vulnerabilities and used them to exploit the robotic devices and components being monitored and controlled by the CPS app and database servers. This was performed by three different levels of intruders, including expert cyber hackers, professionals, and amateurs on the CPS architecture as shown in Fig. 10.

The authors then executed a Telnet anonymous attack, as shown in Fig. 11, on one of the robotic CPS log aggregator service controller servers and exploited it successfully.

Telnet access further provided a remote shell through which the intruder can access the processes running on the server as shown in Fig. 12.

The intruder is easily able to hide their malicious process behind a legitimate process, the authors selected Explorer.exe because it is a process that runs at startup, and it is always present on CPS Windows servers. To execute this the command: "migrate PID number" is run to migrate the process from one to another, as shown in Fig. 13, with the intruder installing the backdoor, type run metsvc, and now accessed ports that were created and the directory where the malicious script files are being uploaded before the attack.

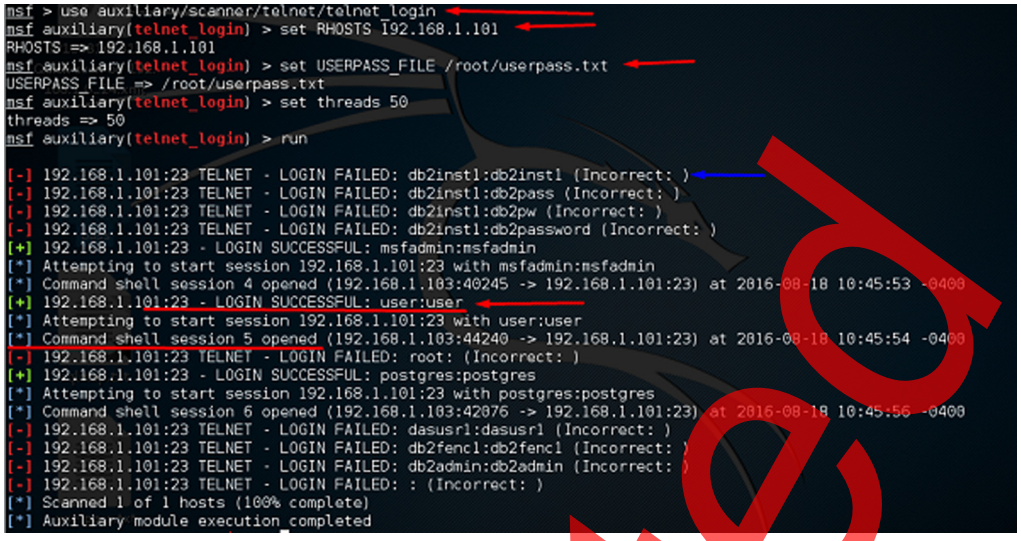

Fig. 11 Telnet remote exploit on robotic CPS.

Fig. 12 Successfully accessed process list.

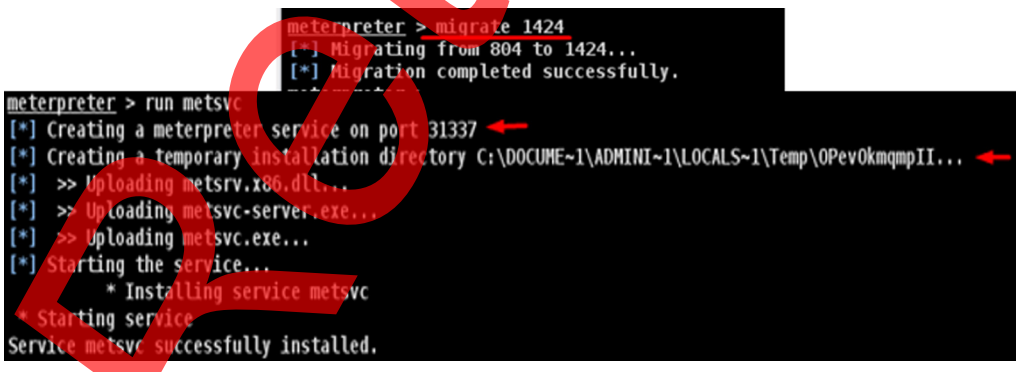

Fig. 13 Migrate legitimate process to malicious and exploit CPS server.

The authors also calculated the time required to compromise the Telnet service and get a remote shell on the CPS controller server to access the processes. Then, one legitimate process was migrated to execute another malicious process, which opened a port and aided in further exploiting the robotic devices and components on the CPS architecture as shown in Fig. 14.

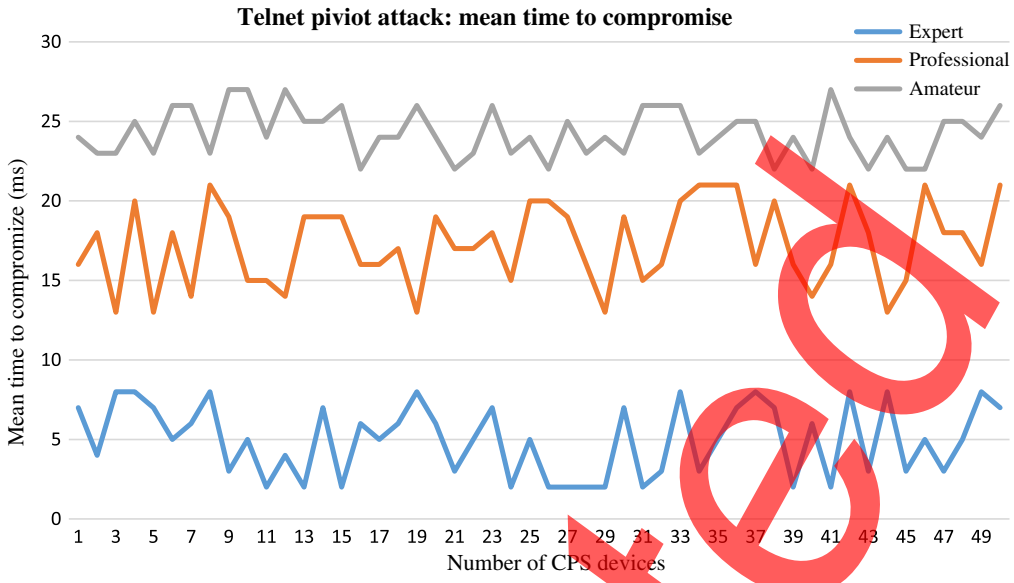

Fig. 14 Telnet pivot attack.

CPS device logs reveal internal information that helps determine vulnerabilities as well as scan results. For each vulnerability, the output log (cpi_.txt) is generated under the resultant directory and provides the mission and inputs that trigger the finding vulnerability as well as the simulation outputs for cyber components and physical devices (Algorithm 3).

The output and graphs for mean time to compromise displayed the trend that expert-level cyber attackers stood out and easily hacked the CPS app and services as compared to professional and amateur hackers, who were slow but still successful.

Algorithm 3 Simulation outputs for cyber components and physical devices.

 # cpi_20210722_101319_g0_s1.txt

[MISSION]

QGC WPL 110

0 0 0 16 0 0 0 0 -37.343262 145.152364 584.080017 1

1 1 3 22 0 0 0 0 -37.343262 145.152375 43.7768741 1

2 0 3 19 0 0 0 0 -37.343294 145.150958 30.4509854 1

3 0 3 19 0 0 0 0 -37.343341 145.152229 33.3352852 1

4 0 3 19 0 0 0 0 -37.343349 145.153908 34.7347567 1

5 0 3 19 0 0 0 0 -37.343069 145.154233 46.0866376 1

6 0 3 21 0 0 0 0 -37.343069 145.154238 0 1

[INPUTS]

[['log_id', '20200520_101319_g0_s1', 'tunnel', '0 0 0 0', 'timeout', 0, 'battcap', 0, 'nums', 3, 3, 10], ['static', 'false', 'mass', '36.0', 'ixx', '28.0', 'iyy', '10.0', 'izz', '15.0', 'size', '3 3 10'], ['windGustDirection', '164.0 6.0 81.0', 'windGustDuration', '6.0', 'windGustDuration', '6.0', 'mag_field', '6e-07 2.3e-21 -4.2e-47', 'temperature', '298.15', 'pressure', '101325.29', 'temperature_gradient', '-0.0066']]

[OUTPUT]

(5, [9.6103, 1.8497, 1.239], [3.7014, 9.8052, 0.3639])

7 Conclusion

Robotic CPS need to be secure at all times with the highest level of security; however, ever-increasing smart cyberattack constantly target the CPS infrastructure. This research focused on presenting a new unique comprehensive taxonomy. Defining the exact critical category of the CPS devices is challenging to estimate, so the authors used a customized digital library as input for the proposed secure CPS framework for the CPS robotic architectures of interconnected computational and physical devices in the architecture. The authors simulated two common cyberattacks on CPS controller servers: cross-site or XSS attacks got executed in an average time of 4.54 s by an expert attacker, 16.84 s by a professional attacker, and 24.44 s by amateurs. Telnet pivoting attacks also displayed a similar trend as illustrated in the graphs above. This research also gathered the known and unknown vulnerabilities using a tree-based attack algorithm and exploited them to determine the meantime to compromise 50 devices and systems as per three different levels of cyber intruders.

Acknowledgments

This work was carried out under Taif University Researchers Supporting Project Number: TURSP-2020/126, Taif University, Taif, Saudi Arabia.

References

1. "Cyber-physical systems," NIST, 2019, https://www.nist.gov/el/cyber-physical-systems.
2. "Robotics and cyber-physical systems | computer science research at Max Planck Institutes," CIS Robotics, 2019, https://www.cis.mpg.de/robotics/.
3. S. Morrison, "The Colonial pipeline ransomware cyberattack: how a major oil pipeline got held for ransom," Vox, 2021, https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices.
4. M. Pfefferle, "What is Stuxnet? Verve industrial," 2021, https://verveindustrial.com/resources/blog/what-is-stuxnet/.
5. Exabeam, "Operation Aurora—2010's major breach by Chinese hackers," 2019, https://www.exabeam.com/information-security/operation-aurora/.
6. C. Huang et al., "Design of an intelligent robotic vehicle for agricultural cyber physical systems," in *IEEE Int. Conf. Consum. Electron.*, pp. 1–2 (2020).
7. S. Zhang et al., "Contact state classification in industrial robotic assembly tasks based on extreme learning machine," in *IEEE 8th Annu. Int. Conf. CYBER Technol. Autom., Control, and Intell. Syst.*, pp. 617–622 (2018).
8. C. Shih and F. Lian, "Grinding complex workpiece surface based on cyber-physical robotic systems," in *IEEE Int. Conf. Ind. Cyber Phys. Syst.*, pp. 461–466 (2019).
9. R. Muthusamy, "Investigation and design of robotic assistance control system for co-operative manipulation," in *IEEE 9th Annu. Int. Conf. CYBER Technol. Autom., Control, and Intell. Syst.*, pp. 889–895 (2019).
10. R. Jhaveri, R. Tan, and S. Ramani, "Real-time QoS-aware routing scheme in SDN-based robotic cyber-physical systems," in *IEEE 5th Int. Conf. Mechatron. Syst. and Rob.*, pp. 18–23 (2019).
11. F. Li et al., "Modeling contact state of industrial robotic assembly using support vector regression," in *IEEE 8th Annu. Int. Conf. CYBER Technol. Autom., Control, and Intell. Syst.*, pp. 646–651 (2018).
12. J. Butt, H. Wang, and R. Pathan, "Design, fabrication, and analysis of a sensorized soft robotic gripper," in *IEEE 8th Annu. Int. Conf. CYBER Technol. Autom., Control, and Intell. Syst.*, pp. 169–174 (2018).
13. B. Ding et al., "Invited paper: distributed computing in cyber-physical intelligence: robotic perception as an example," in *IEEE Int. Conf. Service-Oriented Syst. Eng.*, pp. 1–17 (2019).
14. L. Keung et al., "Cloud-based cyber-physical robotic mobile fulfillment systems considering order correlation pattern," in *IEEE Int. Conf. Ind. Eng. and Eng. Manage.*, pp. 113–117 (2020).

15. Q. Hong et al., "Robot teaching and learning based on 'adult' and 'child' robot concept," in *IEEE 8th Annu. Int. Conf. CYBER Technol. Autom., Control, and Intell. Syst.*, pp. 181–186 (2018).
16. S. Xu et al., "Collision-free fuzzy formation control of swarm robotic cyber-physical systems using a robust orthogonal firefly algorithm," *IEEE Access* **7**, 9205–9214 (2019).
17. J. Zhu et al., "Smart surveillance: a nature ecological intelligent surveillance system with robotic observation cameras and environment factors sensors," in *IEEE 8th Annu. Int. Conf. CYBER Technol. Autom., Control, and Intell. Syst.*, pp. 451–456 (2018).
18. H. Wang, L. Fang, and J. Xu, "Fractional-order nonsingular fast terminal sliding mode control for a robotic manipulator with NDOB," in *IEEE 9th Annu. Int. Conf. CYBER Technol. Autom., Control, and Intell. Syst.*, pp. 1240–1244 (2019).
19. A. Bhardwaj, V. Avasthi, and S. Goundar, "Cyber security attacks on robotic platforms," *Netw. Secur.* **2019**(10), 13–19 (2019).
20. V. Gautham and M. Bera, "Event-triggered sliding mode control based trajectory tracking of robotic manipulators in a cyber-robotic space," in *IEEE Region 10 Conf.*, pp. 2657–2662 (2019).
21. A. Hentout et al., "Virtual pheromone-based approach for objects searching in RFID-based cyber-physical robotic systems," in *Int. Conf. Appl. Smart Syst.*, pp. 1–7 (2018).
22. M. Gomez and E. Matson, "Survivability of MAS through collective intelligence," in *Second IEEE Int. Conf. Rob. Comput.*, pp. 319–323 (2018).
23. Y. Wang et al., "Perception of demonstration for automatic programing of robotic assembly: framework, algorithm, and validation," *IEEE/ASME Trans. Mechatron.* **23**(3), 1059–1070 (2018).
24. S. Khrueangsakun, S. Nuratch, and P. Boonpramuk, "Design and development of cyber physical system for real-time web-based visualization and control of robot arm," in *5th Int. Conf. Control and Rob. Eng.*, pp. 11–14 (2020).
25. D. Yu and H. Chen, "A review of robotic drawing," in *IEEE 8th Annu. Int. Conf. CYBER Technol. Autom., Control, and Intell. Syst.*, pp. 334–338 (2018).
26. M. Alabadi and Z. Albayrak, "Q-learning for securing cyber-physical systems: a survey," in *Int. Congr. Hum.-Comput. Interaction, Optim. and Rob. Appl.*, pp. 1–13 (2020).
27. A. Gawanmeh and A. Alomari, "Taxonomy analysis of security aspects in cyber physical systems applications," in *IEEE Int. Conf. Commun. Workshops*, pp. 1–6 (2018).
28. D. Sahinel et al., "Integration of human actors in IoT and CPS landscape," in *IEEE 5th World Forum Internet Things*, pp. 485–490 (2019).
29. F. Asplund et al., "Rapid integration of CPS security and safety," *IEEE Embedded Sys. Lett.* **11**(4), 111–114 (2019).
30. Q. Li et al., "Dynamic scheduling algorithm in cyber mimic defense architecture of volunteer computing," *ACM Trans. Internet Technol.* **21**(3), 1–33 (2021).
31. S. Rehman et al., "DIDDOS: an approach for detection and identification of distributed denial of service (DDoS) cyberattacks using gated recurrent units (GRU)," *Future Gener. Comput. Syst.* **118**, 453–466 (2021).
32. M. Shafiq et al., "A machine learning approach for feature selection traffic classification using security analysis," *J. Supercomput.* **74**, 4867–4892 (2018).
33. W. Khan et al., "Analyzing and evaluating critical challenges and practices for software vendor organizations to secure big data on cloud computing: an AHP-based systematic approach," *IEEE Access* **9**, 107309–107332 (2021).
34. J. Kaur et al., "Packet optimization of software defined network using lion optimization," *Comput. Mater. Continua* **69**(2), 2617–2633 (2021).
35. Y. Luo et al., "Deepnoise: learning sensor and process noise to detect data integrity attacks in CPS," *China Commun.* **18**(9), 192–209 (2021).
36. M. Amin et al., "CPS attacks mitigation approaches on power electronic systems with security challenges for smart grid applications: a review," *IEEE Access* **9**, 38571–38601 (2021).
37. A. Alipour-Fanid et al., "Online-learning-based defense against jamming attacks in multi-channel wireless CPS," *IEEE Internet Things J.* **8**(17), 13278–13290 (2021).

38. D. Gupta et al., "Edge caching based on collaborative filtering for heterogeneous ICN-IoT applications," *Sensors* **21**, 5491 (2021).
39. Y. Xu et al., "Simplified tree-based MPC for the cyber-physical system with jamming attacks," in *4th IEEE Int. Conf. Ind. Cyber-Phys. Syst.*, pp. 891–897 (2021).
40. D. Alshukri et al., "Intelligent border security intrusion detection using IoT and embedded systems," in *4th IEEE MEC Int. Conf. Big Data and Smart City*, Muscat, Oman (2019).
41. M. Tanjim et al., "A flight control system for a vehicle," in *IEEE Int. Conf. Rob., Electr. and Signal Process. Tech.*, Dhaka, Bangladesh (2019).
42. S. Uddin et al., "Unmanned aerial vehicle for cleaning the high rise buildings," in *IEEE Int. Conf. Rob., Electr. and Signal Process. Tech.*, Dhaka, Bangladesh (2019).
43. U. Zhang et al., "Emotion-aware multimedia systems security," *IEEE Trans. Multimedia* **21**(3), 617–624 (2019).
44. T. Haus et al., "Centroid vectoring for attitude control of floating base robots: from maritime to aerial applications," *IEEE Access* **7**, 16021–16031 (2019).
45. "CVE security vulnerability database. Security vulnerabilities, exploits, references and more," 2021, CVE Details, https://www.cvedetails.com/vulnerability-list/.

Biographies of the authors are not available.