Threats in Software CPS and Potential Security Solutions

[1]Iheanyi Emeka Ukamaka and [2]Agada Martina
[1,2]University of Nigeria, Nsukka, Nigeria.
[1]ukamaka3221@hotmail.com

ArticleInfo
Journal of Machine and Computing (http://anapub.co.ke/journals/jmc/jmc.html)
Doi : https://doi.org/10.53759/7669/jmc202202007
Received 25 December 2021; Revised form 15 February 2022; Accepted 03 March 2022.
Available online 05 April 2022.

Abstract – The concept of cybernetics, microelectronics, design, and process science are all intertwined in CPS. Embedded systems are often used to describe process control. While a strong connection between the physical and computational aspects is still important in certain embedded systems, it is less so in those systems as a whole. However, although sharing a fundamental architectural framework with the Internet of Things (IoT), there is more integration and coordination between CPS's physical and computational components in IoT. Data security and assurance refers to the protection of an asset, which might be a person, an organisation, or a system. A system's assets might be material or intangible, but they all have a real worth. Assets for Computer and Communications Security (CCS) are included in modern CPS, but so are assets produced from the features of CCS. With ever-increasing problems, integration concerns and limitations in current solutions, such as lack of safety, confidentiality and precision, maintaining a safe CPS ecosystem is not a simple process. Cryptographic and non-cryptographic methods may both help to reduce this problem.

Keywords – Cyber-Physical System (CPS), Internet of Things (IoT), Computer and Communications Security (CCS)

I. INTRODUCTION

To define an intelligent system or a Cyber Physical System (CPS), it is vital to think of it as a computer-based algorithm that manages or controls a physical mechanism. System components in cyber-physical systems may function on a variety of timescales and scales, display a variety of diverse behavioural modalities, and interact dynamically depending on the situation. Smart grid, self-driving car systems, health monitoring, control systems and robots are all examples of CPS. The aerospace, automobile, chemical, public infrastructure, power, medicine, production, transportation, multimedia, and consumer appliance industries all have predecessors to cyber-physical network represented in **Fig. 1** below. Most full-fledged CPS systems are not built as independent devices but rather as a system of connected parts with mechanical input and output. The idea is strongly linked to robotics and sensor networks, with computational intelligence processes leading the way.

Breakthroughs in engineering and science have made it possible to combine computational and physical components by methods of intelligent processes, enhancing the flexibility of the system to changes in the environment. For example, collision avoidance, robotic surgery, and nano-level production will all benefit from this. Other applications include rescue operations, disaster response, and deep-water exploration, as well as air traffic management, warfighting, effectiveness, and the enhancement of human capacity through the use of cyber-physical processes in a variety of ways. And finally, the development of zero-net energy buildings and the construction of zero-energy buildings will all benefit human capacity enhancement through the use of human brains in various ways (such as; in healthcare management and delivery).

Sensor-based communication-enabled autonomous robots are a common use for CPS. In many wireless sensors networking, for instance, the analyzed data is sent to a central node. This is just a partial list; there are other CPS such as smart grid, autonomous vehicle, process controller system, redistributed robotics, and autonomous pilot avionic. Actual-life use cases of these systems incorporate MIT's globalized robotic garden [2], whereby a group of roboticists tends a plantation to tomato. The scheme incorporates redistributed sensors (wherein every plant is integrated with a sensor networking tracker), wireless networks, manipulation systems and navigation tools. More emphasis is placed on the components of the control system in CPS, which permeate infrastructural facilities in the research activities of the Idaho National Laboratories and its colleagues. This endeavor offers a comprehensive approach to next century design and takes into account the resilient factors that are not clearly quantifiable, like cyber defense, human contact and intricate inter – dependencies.

As a further instance, MIT's continuing CarTel program uses taxis to gather real-time traffic statistics for Boston. Combined with previous information, this data is utilized to determine the most efficient routes at a particular time of day. Also in the smart grid paradigm, CPS are employed in power grids to conduct enhanced control in order to integrate distributed renewable power more effectively. Special corrective action strategies are required when wind farm power

exceeds the grid's capacity. For these kinds of problems, distributed CPS are essential. Industry 4.0 [3] was made possible through the IMC-AESOP project, a European Commission collaboration with companies like Schneider Electricity, SAP, Honeywell, Microsoft, and others via the use of cloud-enabled cyber-physical networks.

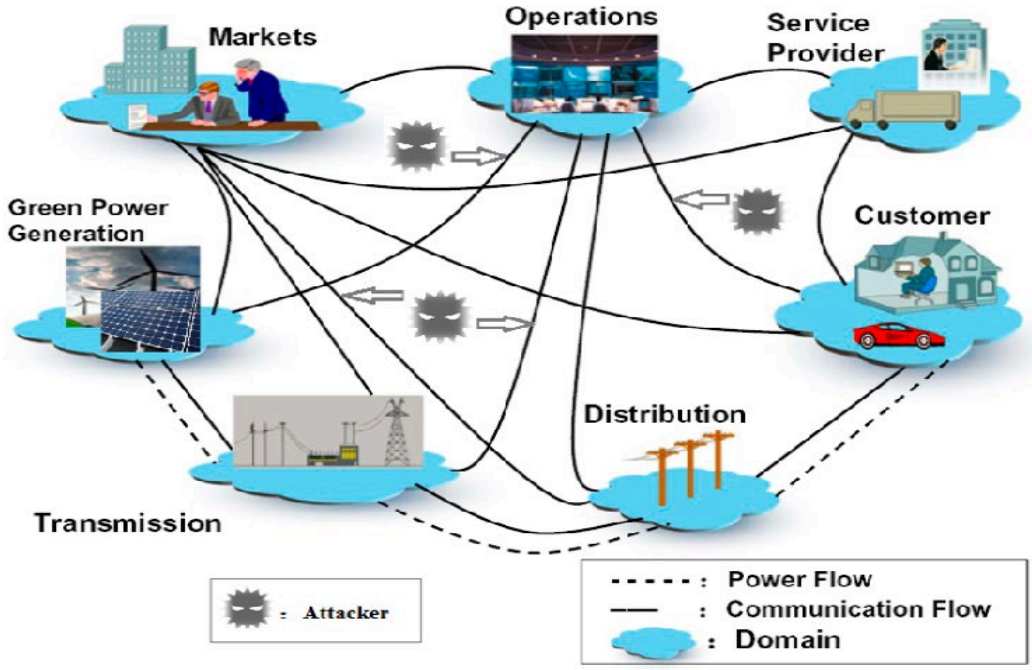

Fig. 1: Cyber-physical network

In developing embedding systems and CPS, huge differences in the design approach between software and structural design may be a barrier. CPAs in several disciplines do not share a "language" of design practice, which is a significant drawback. Software and physical aspects of a system must be allocated tasks and trade-offs must be analyzed in the context of today's economy, where quick invention is considered crucial. When disciplines are coupled via co-simulation, new tools and design methodologies are not required, according to [4]. Co-simulation is possible, according to findings from the MODELISAR project, which proposed a new standard in the form of a Functional Mock-up Interfaces for this purpose.

This paper has been organized as follows: Section II critically analyses the paper; whereby threats in CPS have been discussion, and analysis of CPS security solutions has been done. In the solution section, two solutions have been considered (i) Cryptographic-based solutions; and (ii) non-Cryptographic-based solutions. The final Section III draws conclusions to the research.

II. CRITICAL ANALYSIS

Threats in CPS

The term "asset" is used in the field of data assurances and safety to refer to the resources that are being safeguarded from being harmed either intentionally or by accident. A system's assets might be physical or immaterial, depending on the context in which they exist. The assets of Computer and Communications Security (CCS) are still part of modern CPS, but so are the assets developed from their features that it is now called modern CPS. Users' contentment (the system's capacity to interact effectively with them), major system malfunctions (like power grid failure), reduced physical system efficiency, and damages to equipment are all examples of the unique assets that CPS has (as in the Stuxnet incident).

CPS assets are protected by a wide range of security measures, including reliability, honesty, confidentiality, authentication, and non-repudiation. For the most part, the primary purpose of safety is to ensure that the integrity of a system's assets is maintained and that they are not at risk from outside threats. The term "threat" refers to anything or anybody that can harm an asset. Human error, equipment malfunctions and natural disasters are all examples of non-malicious threats that may arise from a range of sources, from hostile governments to terrorist groups to dissatisfied employees. System flaws may be exploited to acquire control, hurt or extort critical data. a system is at risk if a danger can launch a successful attack on the system. In the following examples, certain CPS assets and threats will be provided from different markets.

Everyone wants access to medical care, and should be as easy and simple as possible for everybody. With Cyber Physiological Networks accounting for the bulk of these innovations, this goal may be achieved in many ways throughout the health business. Another emerging role of CPS within the healthcare sector is to provide timely medical aid, integrating

monitoring and diagnosis of patients outside customary medical facilities such as in-home monitoring and diagnosis systems. This is based on other features such as image evaluation and drug redistribution. As vital as these approaches are in enhancing the users' lives in the globe, it is fundamental to ensure that resources included in this process are safe. We place a high value on the well-being and safety of our employees. It is important to protect the privacy and clinical findings of patients. Patient data must be protected under the HIPAA (Health Insurance Portability and Accountability Act). More use cases of clinical network devices are for drug dispensing, medical scanning and picture storage as well as remote diagnostics. There are a number of special hazards associated with the CPS system that might affect these assets. For the collection, exchange, storage, and management of electronic health data, CPS in healthcare systems is heavily reliant on present communication and computer technology standards. Regular computer systems face the same dangers as medical systems.

Most of these threats integrate: (i) unpermitted accessibility to medical data; (ii) alteration of medical data, amounting to incorrect treatment, diagnosis, and definitely fatalities; (iii) generation of incorrect alarms or suppressions or actual alerts presented by the systems in case of emergency cases; (iv) software threats (malware attacks); and (v) hardware malfunctioning or failures amounting to incorrect application of treatment or diagnoses.

Healthcare facilities, anesthetic systems, and the profession of medicine are all high-risk mechanisms today, not only nuclear power plants. It is essential to do a thorough risk analysis and control research before installing cyber physical processes in this business due to the obvious high valuation of the assets. It's vital to take a systemic approach to evaluating the safety of these systems. For instance, just checking each piece of machinery and pronouncing the system safe is not enough. Also crucial is the larger communication infrastructure, which includes the many components. It's possible, for example, that a hospital tracking system may interact with a home-based patient 's healthcare monitoring equipment over many channels, such as the Website, and that a hospital tracking system can interact with interior healthcare crew or emergency staff. Data originating from the tracking devices could be manipulated or intercepted within the transit even before it enters the healthcare system. Healthcare experts could overlook the real problem, denying effective therapy to patients who have already suffered health and immune harm as a result of their health condition and maybe their therapy. In order to make sure that systems function in a trustworthy and safe way, constant cooperation is needed between device and integrated system engineers, as well as security and network specialists.

Important infrastructure includes everything from utilities to transportation. CI systems are essential to the smooth operation of the country's economy. Examples include electrical energy generating and transmission, and also oil and gas production. There are considerable interactions amount the natural domain and physical processes in the activities of these businesses Numerous consequences flow from the vulnerability of these systems. An invasion on Iran's nuclear amenities in 2010-11 showed how valuable devices can be, but it also showed how equipment can communicate directly with the natural environment, posing ecological disaster risks. Lastly, affected facilities can have a pessimistic effect on the health of tens of thousands to countless thousands of individuals worldwide. On the national and global level, the repercussions of compromising these structures are dire. Power disruptions are expected to cost anywhere from $25 to $180 billion a year, as per the Ministry of Power. Power outages may cost firms in the chart below a lot of money.

CPS Security Solutions

Due to the ever-increasing obstacles, compatibility concerns, and limitations of the available solutions, sustaining a safe CPS systems type (see **Table 1**) is not a simple effort. Cryptographic and non-cryptographic methods may be used to minimize this problem in the physical and cyber environment of CPS (see **Fig. 2**).

Table 1: The division of CPS framework with respect to the criticality

Type	Description
Safety criticality	A threat of this sort might result in the death of people or the onset of chronic illnesses that are lethal over time, as well as substantial environmental damage like fires, flooding, and radiation accidents.
Mission criticality	This form of CPS is vulnerable to both deadly and non-fatal attacks, as well as entire and partial CPS failures.
Security criticality	An assault on a CPS of this sort may result in significant fiscal and commercial losses, a tarnished image, and the departure of CPS subcontractors and customers.
Security criticality	There are several ways to compromise the integrity of a CPS using this form of CPS, including the use of security flaws like backdoors and rootkits.

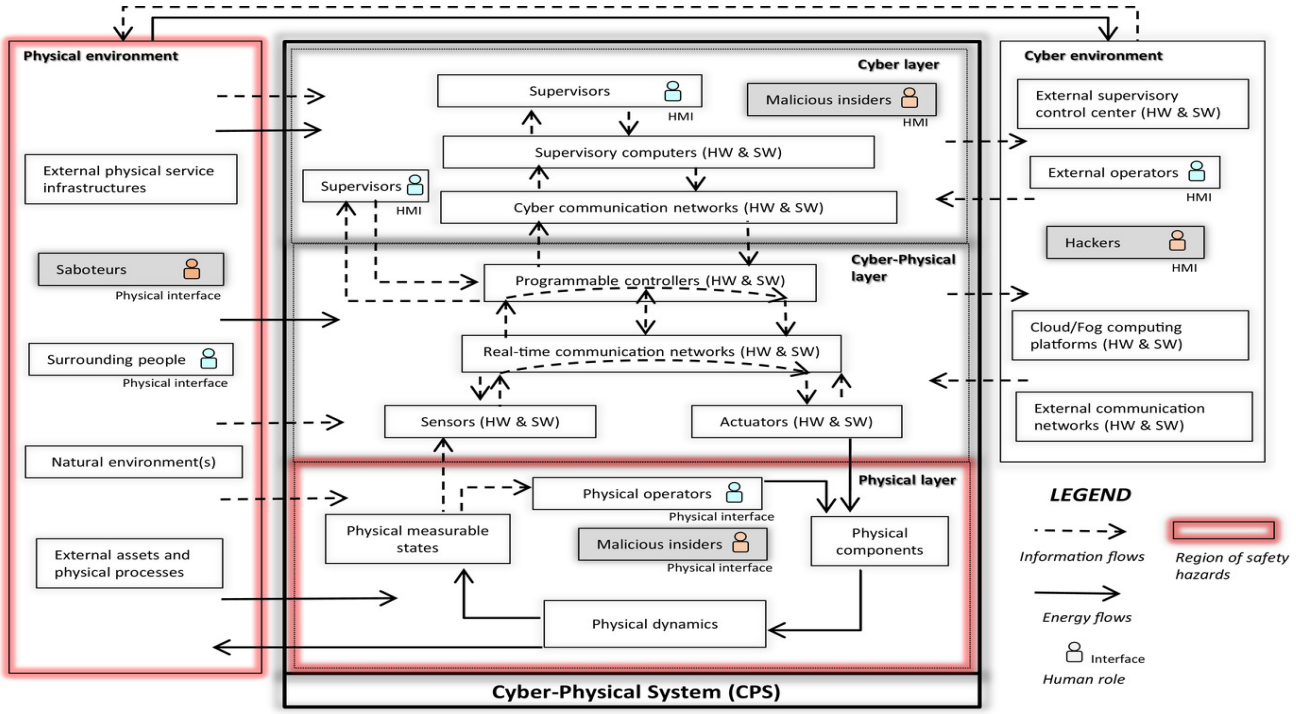

Fig. 2: CPS layers & environments network

Cryptographic-based solutions

In SCADA systems, in particular, cryptographic techniques are primarily used to protect the communication link from active/passive assaults as well as any unwanted access and detection. Traditional encryption methods based on ciphers and hashing algorithms cannot be used by CPS, including IoCPT, because of the system's power and size limitations. As a consequence, instead of focusing just on data security, the emphasis should be on maintaining and ensuring the whole process performance. As a result, several options were put forward. According to a study done by academics in the year (23) on the topic of safe data storage and exchange using standard and developing encryption techniques, Cryptographic identification and encryption techniques for Distributed Energy Resources (DER) programs were studied and addressed by Zhang, Cho, and Mago in [5]. They provided advice on how to use cryptography to DER systems. [6] provided a summary of recent improvements in industrial CPS security control and threat detection, particularly against denial-of service, replay, and deceptive assaults. A lesson on the effectiveness of communications secrecy, user authentication, information protection, and the accessibility of services, as well as assaults and new threats and remedies, may be found in [7].

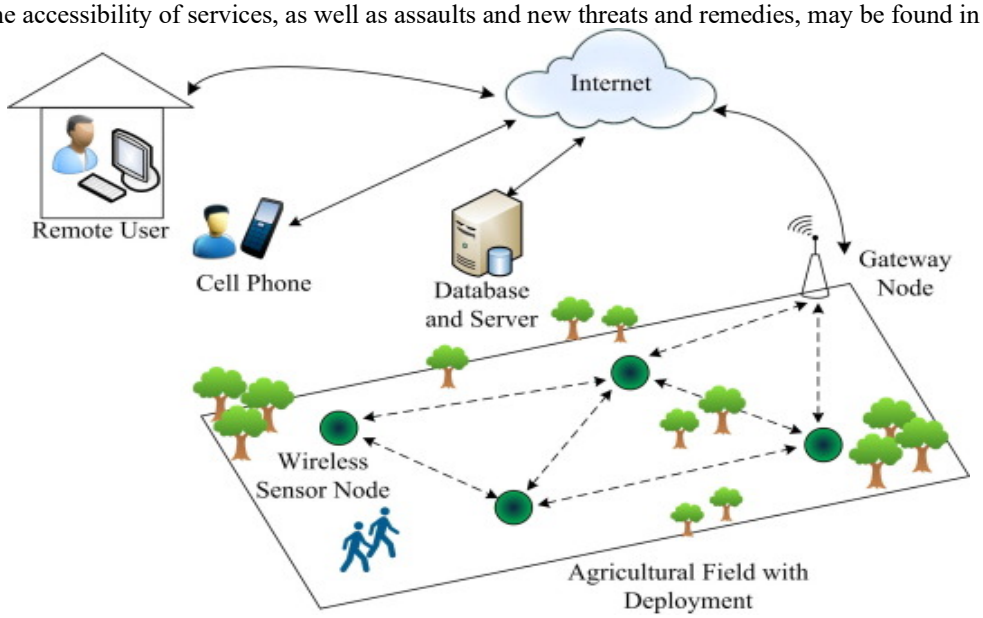

Fig. 3: Wireless sensor network

In order to meet the primary security objectives of the CPS, many alternatives were put up. In [8], Lamba introduced a new paradigm for analyzing cyber-attacks and CPS threats. Using their paradigm, researchers may analyze all of the attack aspects, including the offender, his goals, cyber enslavement, control-theoretic and physical model features, in order to assure a full analysis of CPS attack elements. On the other hand, in [9], Zhou et al. published comprehensive guidelines for the security of Industrial Control Systems (ICS) that include technological controls such as intrusion detection systems and access restrictions as well as operational procedures like training and understanding. Security professionals at [10] used phishing and social control tactics in a simulation operation to acquire access to workers' information owing to their ignorance and lack of skills. An analysis of the keywords used in [11] by Younis et al. reveals a preference for operational controls or simply technical ones. "Multi-level NSES (Network Security Evaluation System)" alludes to 5 different security dimensions and degrees. When it comes to Wireless Sensor Networks (WSN) (see **Fig. 3**) safety for IoCPT/CPS/IoT applications, NSES presents a more comprehensive picture.

NSES provides guidance to network operators in the early stages of system design to ensure that the appropriate security requirements are met. A classification of these methods is made in accordance with one of the below security objectives:

Confidentiality

It is critical to protect CPS communications links. This led to the presentation of a variety of cryptographic mechanisms Prior to encryption, compression methods may be used to reduce the size of data. Their approach cuts costs and alleviates the issue. There have been several lightweight block ciphers, such as an ultra-lightweight ciphertext by scientists and a low-latency cryptosystem that may be used for ubiquitous computing scenarios. Aside from their ability to provide cryptographic blocks for any capacity-restricted device, they were also inexpensive and quick to produce. Modbus transmissions that are not encrypted should be protected by encryption-decryption systems at both ends, according to Agarwal, Pareek, and Agarwal in [12]. So, converting tacit knowledge into explicit knowledge and the other way around takes longer and needs more work than usual. "Bumps-in-wire" encryption solutions for CPS have been offered by the AGA (American Gas Association) at a significant delay cost. Agarwal, Pareek, and Agarwal's research describes an ElGamal algorithm-based hierarchical cryptosystem technique for safeguarding CPS interactions. There have been a number of obstacles in decryption that have been addressed by the WSO2 Complex Event Processor (WSO2-CEP). A safe and trustworthy CPS environment can be ensured by the findings of this investigation.

Maan and Chaba in [13] introduced a unique lightweight encrypted technique for actual-time necessities in CPS, integrating VANET (Vehicular ad hoc Network) as shown in **Fig. 4**. Observations have shown that this strategy is safe and dependable, as well as effective. LABE (Lightweight Attribute Based Encryption System) for mobile cloud-aided CPSwas introduced in the study. With minimal overhead and fine-grained network access, LABE has been shown to be safe and reliable in protecting users' data. Blockchain technology was used to develop a new structure named Secure Pub-Sub (SPS) by Maan and Chaba. Hybrid cryptography was employed to keep data safe from prying eyes. Hybrid For these reasons it is important to ensure data security and trustworthiness, while preserving anonymity and financial fairness among subscribers and authors. Public key cryptography (PKC) employing classical Elliptic-Curves (ECC) was proposed by Maan and Chaba as a possible post-quantum enhancement to Datagram Transport Layer Security (DTLS).

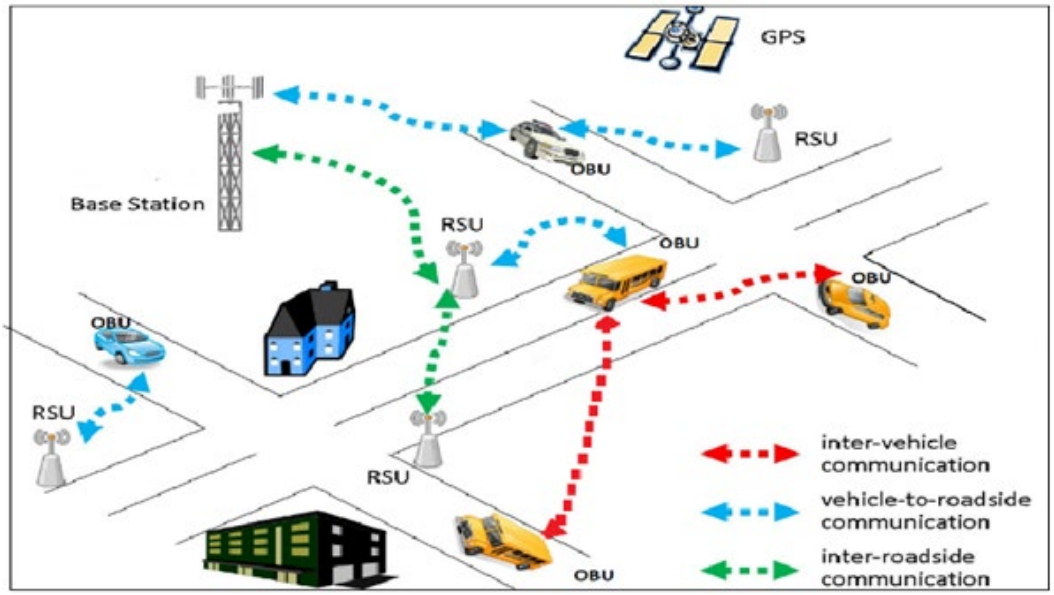

Fig. 4: Vehicular ad hoc network

Integrity

All actual data getting in and going out must be protected from any logical or physical manipulation. Various options are therefore put forward. ICS software rearrangement and network threats were addressed in [4] by Lyn et al. who described a method they had developed dubbed the TAIGA (Trusted Autonomous Interfaces Guardian Architectures) (TAIGA). TAIGA safeguards hazards from both the plant management and supervision nodes, while incorporating trustworthy safety-preserving backup controllers. To safeguard SCADA systems, the authors developed the Shadow Safety Unit ("SSU"), a low-cost gadget that may be utilized in relation to RTU (Remote Terminal Units) and PLC. SSU complements current SIEM designs, and it may invisibly capture its communications control channel in collaboration with physiological processing output/input connections to progressively review the operational and safety status of RTU and PLC.

The use of hardware-based cipher models and a degree of encryption for transmitted packets was also proposed in the research to counteract MITM, replay, and command modifications assaults. The authors suggested a tiered technique to securing sensitive data. In addition to a lightweight key administration system, their methods used hash chains to offer layered protections for both high- and low-level security zones. The greater the security level, the more difficult it is for an attacker to get a hold of the information. Because of this, ICS application providers should concentrate on producing compatible editions of programmes to assure that the operators of ICS never turn to initial OS's versions.

Availability

Making sure that CPS devices are always on call is an absolute need. Various approaches to reducing and resolving concerns with accessibility are thus put forward. The TEPCS (Tennessee Eastman Process Control System) approach was employed to evaluate the DoS risks and integrity degree owing the research by authors in [15]. DoS assaults are unsuccessful against sensor nodes, according to this model's results after being put through their paces Because of their efficacy in defeating denial-of-service (DoS) assaults solely, we ask that security defenses against fidelity attacks be given precedence. As described in the research, the network ICS testbeds oriented on physical computations and simulations, and virtualization was developed and provided by the authors as a control unit for business and the SCADA system simulations using PLCs, RTUs and DCS controller interactivity. The authors used a free software PLC and an IPS based on computer training to safeguard and protect the OpenPLC version from a variety of assaults. DoS threats, injection, and interception were shown to be ineffectual, and the OpenPLC project was able to defeat the man-in-the-middle threats by data encryption without affecting individual properties of time.

Authentication

As the initial line of protection, it is critical that authenticity be well-built, planned, and managed. Resultly, in [16], scientists introduced an authentication system based on public key-exchange to keep out unwanted visitors. Wireless systems are used as a source of energy instead of batteries in these devices. There are wearable gadgets that employ out-of-band authentication to authenticate users through extra channels such as audio and visual. An alternative approach would be to produce basis or key of encrypting and protecting the sensor networks connection using Medical CPS (MCPS) characteristics, which would primarily include heart rate and blood pressure measurements. Pre-equalization is used in Ankarali et alphysical 's layer authentication approach in the study. Safety, confidentiality, and usefulness are all included in research, a study that examines user authentication without the need of a device.

Authenticated Identity-Oriented Cryptography with no Key Escrow (AIOCwnKE) technique was described in the research to safeguard consumer privacy and valuables against unlawful assaults on M2M interactions. Creating a safe and secure environment for mobile devices to communicate. The vulnerability of password-based procedures has been shown in latest editions of PLCs - 2016. PLC memory passwords may be intercepted and broken, according to the authors. They can then conduct more complex assaults, including replay and memory corruption. Consequently, this allows them to conduct more advanced attacks. ICS-specific key handling was provided in the study with no latencies by a team of researchers.

Privacy

It is not a simple undertaking to maintain the confidentiality of consumers' huge data. Differential confidentiality and homomorphic encryption are only two of the privacy-preserving approaches that have been proposed as a consequence of this problem.

Differential Privacy – Confidential real-time huge information and data while transmission is protected from disclosure Investigators used ICA (Independent Component Analysis) onto massive energy CPS dataset to examine the features minimization role along different degrees of privacy preservation in [17]. The outcomes showed that ICA is much safer without compromising personal data and provides a higher safety protection and dataset usefulness. The researchers developed a lightweight confidentiality higher-order Bi-Lanczos approach within an integrated cloud-fog-edge infrastructure for big data analysis. Tensor protocols are used to offload computations that would otherwise take place in the user's private space. The study introduced a safe and effective Differential Privacy (DP) outsourcing system to tackle data providers' difficulties with being exposed to privacy threats. It was shown in the study that elliptic curve cryptography

could ensure storing correctness while also guaranteeing proxy-oriented confidentiality in an identity-based proxy-oriented outsource scheme in cloud-based MCPS.

Homomorphic Encryption – Cryptography encryption methods were used to improve data security and privacy protections. Secure Estimations based on Kalman Filtering (SEboKF) was developed utilizing a multiplicative cryptography encryption approach with custom decryption approach to limit networking costs and increase data security. Fully homomorphic encryption (FHE) is a sophisticated cryptographic technique that may directly perform mathematical procedures on encrypted parameters without the need for decryption. Additionally, a tree-based calculation of consecutive mathematical operations is implemented in order to slow down its aging process. In [18], Tamilarasi, Gandhi, and Palanisamy introduced parallel homomorphic encryption approach, which endorses floating point value to effectively generate ciphertext procedure with no decryption. Homomorphic encryption in cloud computer systems has been shown to be possible while limiting application difficulties.

Non-cryptographic-based solutions

Numerous non-cryptographic selections had been put out in an effort to lessen the impact of any conceivable cyber-attack or malevolent occurrence. Intrusion Detection Systems (IDS), firewalls, and honeypots were used to do this. Thus, other writers' answers are referred to and debated in this article.

Intrusion Detection Systems

Due to the variety of network setups, many IDS approach types are available. When it concerns identification, setup, cost, and network location, each IDS solution has benefits and disadvantages unique to it. Robinson and Cybenko [19] reported doing several types of study in an effort to identify assaults on the CPS. There are two basic types of assault here. Anomaly detection is used to define regular CPS operations in this physics-based paradigm. As described in the study, this cyber-based model is utilized to identify prospective threats. Many of the currently used methods are focused on detecting threats to a narrow range of use cases e.g., unmanned vehicles, production control frameworks, and micro grids. In an attempt to identify malicious software injection assaults in CPS, the authors took use of the potential of a worst-case implementation time by acquiring information via static application analysis. To use IDS in Medical CPS, researchers studied a behavior-rule specification-based method in the study. A state machine that can identify any departure from a health device's behavior definition was also given by the authors in the study.

Intrusion Detection System Placement

Any particular IoT network's boundary router, one or more hosts, or any physical device may be equipped with an IDS to guarantee the needed detection of threats. As a result of the IDS's capacity to often query the network status, there may be a communications latency among the LLN (Low Current Lossy Networking) and the border router. IDS placement techniques have been presented by Chen et al. [20].

Distributed IDS

LLN objects utilise D-IDSs, which are optimized for each resource-constrained node, while being used across the network. As a result, a small, distributed IDS was proposed in this paper. A method for matching attack signatures and packet payloads was discovered by P in [21], and researchers also suggested a variety of more efficient approaches. By allocating nodes to observe their neighbors in the dispersed placement, researchers came up with a light-weight approach for monitoring a node's energy use. The term "watchdogs" refers to nodes like this. For the identification and mitigation of sinkhole attacks, the researcher proposed a method dubbed "Intrusion discovery of sinkhole intrusion onto IPv6 over 6LoWPAN for IoTs that merges the ideas of image and loyalty with watchdog nodes. When a network is redesigned or an attacking event occurs, the node's role may change.

Centralized IDS

The majority of C-IDS deployments are in centralized systems. This permits the LLN to collect and transfer all data over the border to the Internet. A centralised IDS may thus monitor all of the communications between the Internet and LDN. However, detecting assaults using just LLN nodes is insufficient since it is impossible to keep track of every node at the same time that an attack is taking place. Le et al. [22] provided a solution based on the analysis of all packets that travel throughout the border router among the network and application domains. A botnet assault is, however, the primary focus of the project. The IDS communication system would be unaffected in the event of DoS attacks, where researchers installed a central location that allowed them to examine the potential of defeating DoS assaults. When it comes to physical assaults, the authors used their centralized strategy that was installed in the border router.

Hybrid IDS

Balancing the benefits of central and dispersed locations, as well as mitigating the downsides of each, is the goal of H-IDS. Prior to actually taking on further responsibilities for observing other nodes, the primary node in each cluster may host an IDS example, allowing it to organize the network into clusters. Because of this, hybrid IDS locations may be designed to demand more capabilities than a dispersed IDS installation.

Salameh, Shayanfar, and Barkhordari in [23] used a hybrid arrangement with a limited number of "watch dogs" nodes to cover the system in the same manner. As a result of this, they were able to see whether any of their neighbors were infected or not by listening in on their communications. thereby cutting down on comms costs. The authors were able to divide the system into minor clusters, wherein each has cluster heads, while still utilizing similar collection of gadgets. Single IDS cases could be integrate in every source node, with every element of cluster generating its essential data as well as that of its neighbors, allowing for centralized monitoring of the whole cluster. As an alternative, IDS modules were installed in the edge node and other networking devices with a central element. Using the Signaling Protocols low-enegy and lossy device system datasets, the authors recommended their IDS, SVELTE that trusts the routing hosts with the obligation to digest more intensified IDS modules and to discover attempts to system intrusion. Based on the authors' findings, network nodes were liable for any noticeable changes in their neighborhood. It is the border router's primary role to store and analyze the data, but the networking node is obliged to deliver data concerning immediate neighbours within a centralized unit, which is integrated in the bordering routers. Rendering it simpler to sense and identify intrusions as well as early phases of an assault. At the border of the router, as well as on the networking nodes, the authors offer an IDS. As a result, the IDS module monitors the neighboring nodes, identifying any intrusion attempts, and notifying the other IDS modules of this activity.

Intrusion Detection Methods

Hybrid-based, behavior-based, anomaly-based, and Signature-based, are the four basic IDS methodologies. While these methodologies and testing procedures were discussed by Blair, Debenham, and Edwards [24], the detection mechanisms used to classify them into the five major groups were also discussed.

Signature Based

Quick and simple to set up, this kind of detection is ideal for large areas. Nevertheless, it is only useful for identifying known dangers. To put it another way, this shows that it has a high vulnerability to unknown threats such polymorphic malware and encrypting services. Signature-based IDS, despite its restricted capabilities, is very accurate and successful in automatically detecting threats, with a simple method to explain the process. There's a problem with this strategy, though, since it doesn't work for new or variant assaults, because their matching fingerprints remain a mystery and the signature patch is continually being updated. Attack fingerprints and packet payloads were compared as part of the study by Santos et al. [25]. It was shown in the study that an IDS signature-based on an "Artificial Immune System" (AIS) could categorize every datagram as harmful or non-malicious based on matching signatures, thanks to the use of detectors patterned after immune cells. The capacity to adapt to new situations in new locations that are being watched may be a result of this kind of approach. DoS attacks on 6LoWPAN networks were detected by the authors by integrating an IDS with a signature-based approach. The primary goal of this IDS was to reduce the false alarm rate by adapting "Suricata4" for 6LoWPAN networks. As an expansion of the method described by previous scholars, the researchers developed a signature-based strategy.

Behaviour Based

Networking devices, such as nodes and protocols, behave in predictable ways when they are subject to a set of regulations and thresholds known as "behaviour based." An intrusion may be detected using this method if the network behavior deviates from the expected one. It is similar to anomaly-based detection in that it relies on human expertise to establish each specified rule, but it differs somewhat from specification-based systems. It is therefore more accurate than anomaly detection in terms of false positives. As a result, because they are put to work immediately, no training is required. However, this method is unsuitable for application in all contexts and might be prone to errors or be time-consuming. DDoS assaults on the IoT middleware may be prevented by sending an alarm if the number of requests exceeds the threshold line, according to Vijayakumar and Ganapathy in [26]. Using system security and malicious activity detection, researchers in the study proposed a new specification-based technique to identify RPL assaults.

Extensions to Vijayakumar and Ganapathy's work were made by Darabkh, Al-Akhras, and Khalifeh [27]. According to the study, their experiments had a high true-positive and low false-positive rates compared to standard RPL network, but they also used more energy. When it comes to network security, network administrators have the power to develop and maintain their own policies. Rule violations are sent to the Event Management System (EMS) [28] as soon as they occur, so that these alerts may be correlated throughout the network's nodes. The network administrator's competence and combined experiences and abilities were critical to the success of researchers' techniques. This means that the network's security may be in danger if any incorrect specifications are used, resulting in an extremely high false-positive frequency or a highest accuracy rate.

Anomaly Based

In the event of a divergence from the system's regular behavior, this form of monitoring may issue an alarm. However, there is a significant risk of false positives with this detection approach. By calculating an average for every of the three metrics that compose the typical behavior profile, researchers in [29] provided a technique for detecting botnets. Prior to the system monitoring network traffic and raising an alarm anytime a measure deviates from the previously established

estimated averages, this was accomplished by manual intervention. For the purpose of creating a normal profile, the researchers employed Computer Intelligence techniques to design their own wireless IDS architecture. Additionally, each IP address allocated will have a separate usual behavior profile. Nodes' behavior may be studied by taking energy consumption into account as a parameter, according to the study. So, for each mesh-under and route-over routing method, creating a regular power consumption paradigm is necessary, in which each node monitors its own usage. Maliciousness is detected if the node is found to be deviating from the set parameters.

It was reported by Gethoffer in [30] that a bit-pattern matching strategy that conducts a characteristic selection was effectively used by researchers to construct a deep-packet anomaly-based solution to reduce the run-on resource restricted IoT devices. They tested four major kinds of attacks (including SQLi, worms, etc.) on internet-enabled gadgets, and the findings showed minimal false-positive percentages. There was a breakthrough in IoT global internal anomaly discovery in the study, when the researchers successfully established a method to monitor node information rate and packet capacity. They also demonstrated an IDS that is especially built to identify wormhole attacks in IoT nodes in Ogasahara [31], as well as three primary methods to detect system abnormalities. When evaluated for wormhole detection, they found that the system had a prediction accuracy of 94% while only identifying the attack and the attacker with an accuracy rate of 87%. Scientists from K developed the Spiking One Class Anomaly Detection Framework (SOCCADF) algorithm, which was presented in the research. This technique employs a single class categorization methodology in a novel and practical manner since it was trained on data describing conventional ICS activities, rather than data from other sources. To add to the difficulty of detecting APT hazards, this system can identify any deviations in behavior and irregularities. They claim that SOCCADF is particularly well-suited to complex issues and applications involving large amounts of dataset according to the author. In Ogasahara's analysis, it was noted that the algorithm had a high level of efficiency, reliability and accuracy compared to other algorithms studied.

Radio-Frequency Based

A Radio frequency-based anomaly identification methodology for critical establishment of programmed logic controller was proposed by Stone and Temple in [32]. The findings of their experiments show that a single waveform response may be used to distinguish between abnormal and regular operating situations. However, their performance suffers dramatically when combined with a multi-time domain waveform reaction. In order to address this issue, the authors introduced an anomaly detection approach that relies on RF fingerprint features obtained from the waveform amplitudes, phases, and frequencies to distinguish between anomalous and normal working situations. It was also reported in the study that the researchers have developed an improved approach for detecting aberrant programmable reasoning controller actions using the emission from RF. At SNR (Signal Power Ration) equal or more than 0 dB, CBAD (Cincinnati Bell-Any Distance) approach attained TADR (Threat Agent Detection and Response) identification performance of more than 90%. In spite of these findings, this method is susceptible to RF noise, channel deterioration, and coding loops. Researchers in the study provided a timing-based attack detection assessment approach to assist controller model drivers in detecting firmware and ladder reasoning program modification to the programme logic controller. Whenever the field devices have been deployed, it could be a baseline fingerprint, which is been established. To detect or communicate with the operator of inadvertent or purposeful alterations within programmable reasoning controller, different device fingerprints are contrasted and acquired within the baseline.

Hybrid Based

To effectively optimize their advantages whereas controlling drawbacks, specification-oriented methodologies of anomaly-based and signature-based detection are employed. A hybrid IDS termed as SVELTE was described in [33] by researchers who found a good balance between the memory and computational costs of signature-based and anomaly-based techniques. The researchers used the IDS assessment methodology they offered to evaluate their anomalous and signature-based IDS. Their findings showed that none of the approaches were successful in identifying specific assaults on their own. They integrated these methods in order to detect and cover a larger area of assault. An anomaly-based strategy that assures packet interaction between these nodes was provided in the study in order to identify and isolate sinkhole assaults by integrating the Intrusion Detection of SiNkhole Attacks on 6LoWPAN for the Internet of Things (INTI). The assessment node was extracted based on trust and popularity utilizing the specification-based technique. However, the researchers created a situation where INTI-IDS detected sinkholes with a 92 percent success rate when compared to SVELTE. The percentage has only exceeded 75% in the event of a predetermined situation, though. Although it has shown a lower percentage of false-positive results than SVELTE, it does not have as many false-negative results.

Firewalls

Due to the progress of IDS and AI technologies, firewalls were seldom used in the CPS sector. Because of this, a few firewall-based options were offered. Pairing Firewalls among corporate and production zones to improve server cyber security was discussed by Guterres and Ashari in [34]. Because of the high level of security and the distinct management responsibilities, they decided on a pair of firewalls. The authors described a new approach for inspecting and filtering SCADA protocol communications using iptables as an efficient and strong open-source network-level firewall. A structure called Argus was proposed in the researchers who wanted to protect a public resource against cyber-physical assaults.

During testing, it was shown to be successful in identifying both simple and complicated multi-component deception attempts. Event data may be used to anticipate the failure of network devices such as load balancing and firewalls in real time. They were primarily interested in the raw device records that were being collected. As a result, there was a low attrition rate of devices, with a 76% accuracy rate and a recalling of a particular system failure forecast rate of approximately 66% being achieved. A new security architecture described in the study quickly locates a cyber-attack and restores the compromised cyber-physical system's functioning. Only system availability assaults were shown to be successful, according to the results.

Honeypots & Deception Techniques

CPS relies heavily on decoys to mask and secure their system from intruders. Using honeypots is the primary method for doing this. However, there are other deceiving options. There is a wide variety of deception strategies that honeypots might deploy; ICS honeypots may be created using high-interaction, virtualized and server-oriented ICS honey traps to generate maintained and cost-effective honeypot, which possibly analyses and records an attacker's actions. In this case, the goal is to attack ICS honeypots that use Ethernet/IP as a communication medium. Using HoneyPhy, researchers have developed a physics-aware paradigm for complicated CPS honeypots that keeps track of both the behavior that originates from the CPS operation and the gadget that drives the CPS itself. It has been shown that HoneyPhy might be utilized to shape the actions in an actual-time manner. This model was utilized to effectively develop HoneyBot, which is the first software hybrid honeypot established for robotics connected through a network. HoneyBot can trick attackers into thinking their attacks have worked, according to simulations.

Using telnet and SSH, many researchers placed a medium-interaction honeypot in order to collect data from assaults. In order to classify attacker kinds and activities, this information was analyzed. CPS security was improved by presenting a honeypot game approach with both high/low options of interaction Results from simulations show that the best deployment of human resources and defense strategy may be achieved. In order to make their solution compatible with CPS data security "Conceal," a novel deceit as a service concept is efficient and accessible. A combination of the methods m-mutation and k-anonymity, as well as l-diversity for configuration diversification, was used to achieve this goal of anonymizing addresses, fingerprints, and configurations. As many as 90% of the time, Conceal's proxies are able to rescue. Tripicchio and D'Avella [35] proposed the Deep Detection Architecture (DDA) to protect industrial management systems from cyber-physical threats. In addition, a cyber-physical simulation approach was devised and put to use to examine the security mechanisms in various attack scenarios. To make matters worse, it is expected that DDA would be widely employed in the next ICS version and in the industries v4.0 architecture. The authors devised a misleading signalling system to counter sophisticated CPS adversaries. An adversary's conduct may be influenced by knowledge that is strategically available.

III. CONCLUSION

This study examines the dangers to CPS and suggests possible remedies. However, although sharing a fundamental architectural framework with the Internet of Things (IoT), there is more integration and synchronization between CPS's computing and communication components in IoT. Data security and assurance refers to the protection of an asset, which might be a person, an organisation, or a system. A system's assets might be physical or immaterial, depending on the context in which they exist. Assets for CCS are included in modern CPS, as well as assets produced from their features. As the hurdles, integration concerns, and limitations of current solutions continue to grow, it is becoming more difficult to maintain a safe CPS ecosystem. Aside from cryptographic and non-cryptographic methods, this issue may be addressed in a variety of ways. The uniqueness and demands of CPS mean that many of the security measures used to protect standard IT networks are ineffective or simply not applicable. Because of the nature of their activities and their degree of complexity, ICS is the biggest CPS user of CCS security technology. Even with their high degree of complexity, certain security systems are difficult to apply.

References

[1]. R. Johari, A. Kaur, M. Hashim, P. K. Rai, and K. Gupta, "SEVA: Secure E-voting application in cyber physical system," Cyber-phys. syst., vol. 8, no. 1, pp. 1–31, 2022.

[2]. K. Takemoto, H. Yokoyama, T. Okuno, A. A. Moe, and G. Lee, "Tilling depth control of compact plowing robot toward Home Gardens," in 2020 IEEE 9th Global Conference on Consumer Electronics (GCCE), 2020.

[3]. Z. Liu et al., "The architectural design and implementation of a digital platform for Industry 4.0 SME collaboration," Comput. Ind., vol. 138, no. 103623, p. 103623, 2022.

[4]. R. Ponzini, R. Da Vià, S. Bnà, C. Cottini, and A. Benassi, "Coupled CFD-DEM model for dry powder inhalers simulation: Validation and sensitivity analysis for the main model parameters," Powder Technol., vol. 385, pp. 199–226, 2021.

[5]. J. Zhang, H. Cho, and P. Mago, "Design and optimization of integrated distributed energy systems for off-grid buildings," J. Energy Resour. Technol., pp. 1–27, 2021.

[6]. J. Gardiner, A. Eiffert, P. Garraghan, N. Race, S. Nagaraja, and A. Rashid, "Controller-in-the-middle: Attacks on software defined networks in industrial control systems," in Proceedings of the 2th Workshop on CPS&IoT Security and Privacy, 2021.

[7]. S. Soloviov, State Research Testing Institute of Problems of Technical Protection of Information, Federal Service on Technical and Export Control of Russia, Y. Yazov, and State Research Testing Institute of Problems of Technical Protection of Information, Federal Service on Technical and Export Control of Russia, "Information support of the activity for technical protection of information," Vopr. kiberbezopasnosti, no. 1(41), pp. 69–79, 2021.

[8]. A. Lamba, "A through analysis on protecting cyber threats and attacks on cps embedded subsystems," SSRN Electron. J., 2020.

[9]. S. Zhou, Y. Hua, X. Dong, Q. Li, and Z. Ren, "Predefined containment control for general linear multiagent systems with time-varying delays and switching topologies: Containment control multiagent systems," Advanced Control for Applications: Engineering and Industrial Systems, vol. 2, no. 2, p. e26, 2020.

[10]. D. J. Brooks, M. Coole, and P. Haskell-Dowland, "Intelligent building systems: security and facility professionals' understanding of system threats, vulnerabilities and mitigation practice," Secur. J., vol. 33, no. 2, pp. 244–265, 2020.

[11]. M. Younis, O. Farrag, S. Lee, and W. D'Amico, "Optimized packet formation in multi-level security wireless data acquisition networks," Secur. Commun. Netw., vol. 4, no. 12, pp. 1420–1439, 2011.

[12]. V. Agarwal, P. Pareek, and M. Agarwal, "Ultrafast optical message encryption-decryption system using semiconductor optical amplifier based XOR logic gate," in 2018 International Conference on Numerical Simulation of Optoelectronic Devices (NUSOD), 2018.

[13]. U. Maan and Y. Chaba, "Deep Q-network based fog node offloading strategy for 5 G vehicular Adhoc Network," Ad Hoc Netw., vol. 120, no. 102565, p. 102565, 2021.

[14]. K. G. Lyn, L. W. Lerner, C. J. McCarty, and C. D. Patterson, "The trustworthy autonomic interface guardian architecture for cyber-physical systems," in 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, 2015.

[15]. R. Ettiane, A. Chaoub, and R. Elkouch, "Toward securing the control plane of 5G mobile networks against DoS threats: Attack scenarios and promising solutions," J. Inf. Secur. Appl., vol. 61, no. 102943, p. 102943, 2021.

[16]. "Fog computing with IoT device's data security management using density control weighted election and extensible authentication protocol," Int. j. intell. eng. syst., vol. 15, no. 1, 2022.

[17]. J. de J. N. Ayón, J. L. G. Sánchez, E. S. B. Cabral, J. S. Castañón, and M. J. R. Roblero, "An independent component analysis approach for wide-area monitoring of power system disturbances," Electr. Power Compon. Syst., vol. 48, no. 6–7, pp. 615–627, 2020.

[18]. Tamilarasi, R. Gandhi, and Palanisamy, "Privacy preserving partially homomorphic encryption with optimal key generation technique for VANETs," Research Square, 2021.

[19]. D. Robinson and G. Cybenko, "A cyber-based behavioral model," J. Def. Model. Simul. Appl. Methodol. Technol., vol. 9, no. 3, pp. 195–203, 2012.

[20]. H. Chen, J. A. Clark, S. A. Shaikh, H. Chivers, and P. Nobles, "Optimising IDS Sensor Placement," in 2010 International Conference on Availability, Reliability and Security, 2010.

[21]. D. P. Et.al, "A novel technique for IDS in distributed data environment using Merkel based security mechanism for secure user allocation," Turk. J. Comput. Math. Educ. (TURCOMAT), vol. 12, no. 3, pp. 4284–4297, 2021.

[22]. A. Le, J. Loo, A. Lasebae, M. Aiash, and Y. Luo, "6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach: IOT, 6LOWPAN, RPL, QOS SECURITY THREATS, IDS," Int. J. Commun. Syst., vol. 25, no. 9, pp. 1189–1212, 2012.

[23]. M. Salameh, M. Shayanfar, and M. Barkhordari, "Seismic performance of a hybrid coupled wall system using different coupling beam arrangements," Tek. dergi, 2022.

[24]. A. Blair, J. Debenham, and J. Edwards, "A comparative study of methodologies for designing IDSSs," Eur. J. Oper. Res., vol. 103, no. 2, pp. 277–295, 1997.

[25]. L. I. Santos et al., "Decision tree and artificial immune systems for stroke prediction in imbalanced data," Expert Syst. Appl., vol. 191, no. 116221, p. 116221, 2022.

[26]. D. S. Vijayakumar and S. Ganapathy, "Show-based logical profound learning demonstrates utilizing ECM fuzzy deduction rules in DDoS assaults for WLAN 802.11," in Advances in Intelligent Systems and Computing, Singapore: Springer Singapore, 2021, pp. 189–208.

[27]. K. A. Darabkh, M. Al-Akhras, and A. Khalifeh, "Improving routing protocol for low-power and lossy networks over IoT enviroment," in 2021 30th Wireless and Optical Communications Conference (WOCC), 2021.

[28]. E. Kim and G. Cuskelly, "A systematic quantitative review of volunteer management in events," Event manag., vol. 21, no. 1, pp. 83–100, 2017.

[29]. T. A. Tuan, H. V. Long, and D. Taniar, "On detecting and classifying DGA botnets and their families," Comput. Secur., vol. 113, no. 102549, p. 102549, 2022.

[30]. H. Gethoffer, "Polar plane blockquantization of speech signals using bit-pattern matching techniques," in ICASSP '77. IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005.

[31]. Y. Ogasahara, K. Kuribara, K. Oshima, Z. Qin, and T. Sato, "Yield and leakage current of organic thin-film transistor logic gates toward reliable and low-power operation of large-scale logic circuits for IoT nodes," Jpn. J. Appl. Phys. (2008), vol. 61, no. SC, p. SC1044, 2022.

[32]. S. Stone and M. Temple, "Radio-frequency-based anomaly detection for programmable logic controllers in the critical infrastructure," Int. J. Crit. Infrastruct. Prot., vol. 5, no. 2, pp. 66–73, 2012.

[33]. "IDS working paper research summary 332: Hybrid activism: Paths of globalisation in the Brazilian environmental movement," IDS Work. Pap., vol. 2009, no. 332, pp. i–ii, 2009.

[34]. L. E. J. Guterres and A. Ashari, "The analysis of web server security for multiple attacks in the tic Timor ip network," IJCCS, vol. 14, no. 1, p. 103, 2020.

[35]. P. Tripicchio and S. D'Avella, "Welding defect detection with deep learning architectures," in Welding Principles and Application [Working Title], IntechOpen, 2022.