RESEARCH PAPER

Attack Detection in Cyber Physical Systems using Machine Learning.

Vasaki Ponnusamy[1], Said Bakhshad[2], Oh Wan Ping[2], Fatima-tuz-Zahra[3], Noaman M. Noaman[4], Azeem Khan[5]

[1] Higher Colleges of Technology, Fujairah Men's Campus, Fujairah, UAE
Email: vasaki.ponnusamy@gmail.com;
[2]Faculty of Information and Communication Technology, Universiti Tunku Abdul Rahman, Malaysia
Email:engg.syedpk@gmail.com, christine16189@1utar.my
[3] School of Computer Science, Taylor's University, Selangor, Malaysia;
Email: fatima.zahra@taylors.edu.my
[4] College of Computer Engineering, University of Technology, Bahrain, Kingdom of Bahrain
Email: nmnoaman@utb.edu.bh
[5] Faculty of Islamic Technology, Universiti Islam Sultan Sharif Ali (UNISSA), Brunei Darussalam,
Email: azeem@unissa.edu.bn

ABSTRACT
In recent years the advancements in the smart infrastructure like smart cities, smart devices and their interconnection with each other as well as with the internet has given rise to deployments of systems called cyber physical systems in both public and private domains. Where this advancement has brought ease and comfort into our life, it has also increased the vulnerability to security attacks. The reason is insecure implementation of such systems and transmission of sensitive data over equally or more insecure networks. As a result, exponential increase in attacks like denial of service, ransomware, and flooding attacks has been observed. The development of security techniques is still in its early stages while at the same time deployment of insecure systems has vastly grown. Due to this reason, it is necessary to focus on the security aspects of cyber physical systems to avoid greater harm, like financial and life loss. Therefore, in an effort to contribute towards the security of cyber physical systems, authors have proposed an anomaly based intrusion detection system for detection of denial of service attack using machine learning. Decision tree classifier has been used to develop the system because it can handle categorical as well numerical data which is compatible with the requirements of a cyber physical system. The proposed approach is evaluated using parameters like accuracy and the paper is then concluded with final remarks on results and future direction of research.

Keywords: cyber physical systems Internet of Things,smart infrastructures,denial of service attack, machine learning
How to cite this article: Ponnusamy V, Bakhshad S, Ping OW, Zahra Ft, Noaman NM, Khan A., Attack Detection in Cyber Physical Systems using Machine Learning. .Int J Drug Deliv Technol. 2026;16(2s): 42-55; DOI: 10.25258/ijddt.16. 42-55
Source of support: Nil.
Conflict of interest: None

INTRODUCTION

Cyber Physical System (CPS) is the integration of computing, networking, and physical processes. Physical processes and feedback loops are monitored through sensors and controlled through actuators via embedded computers and networks. Physical processes reflect their effect on calculations and vice versa. To provide abstractions, modeling, design, and analysis techniques, a cyber-physical system combines computation and physical processes. CPS requires that computing and network technologies include physical dynamics in addition to information. The technology relies on multiple disciplines. For example, computational science, control theory, and communications engineering. Next, the software is embedded in the device and its main task is more than computing. A CPS can be observed to range between comparatively minor systems such as an automotive or airplanes, to wide-scale systems such as the national grid [1].

Beginning in 2006, research project called 'Science of Integration for CPSs' has been funded by the National Science Foundation (NSF). A variety of academic and other institutions have joined this research project, notably among them, UC Berkeley, Vanderbilt, Memphis, Michigan, Notre Dame, Maryland, and General Motors Research and Development Center [2]. Similarly, in 2004 the European Union (EU) launched the Embedded Intelligence and Systems Advanced Research and Technology (ARTEMIS) project to address the research and structural challenges facing the European industry by virtue of the definition and implementation of an agenda for embedded research in embedded computing systems. Additional to these measures, researchers from alternative countries, like China

**Author for Correspondence: noorzaman.jhanjhi@taylors.edu.my*

and South Korea, have begun to display an increased sensitivity to the gravity of CPSs analysis.

The US government named CPS as the latest strategy for development during 2007. Events such as CPS Week and the International Conference on CPS saw researchers from various countries mention the relevant concepts, technologies, applications, and challenges throughout. This caught the attention of researchers who also sought the need for theoretical foundations, design and implementation, practicality, and literacy [3]. Areas such as energy management, network security, data transmission and management, model-based design, control technology, system resource allocation, and applications have been the focus of current advances in research. Overall, despite the progress made in modeling, energy and safety control, and software-based design methods by researchers, research within the domain of CPS is still in its infancy.

Integration of Wireless Sensor Networks (WSN), CPS and the Internet of Things (IoT) with each other has accelerated and in recent years, these emerging fields have also achieved success. These achievements have contributed to the advancements of CPS as well. The purpose of the CPS research program is to deepen the integration of physical and network (computing, communication, and control) designs. CPS differs from the traditional desktop computing, embedded or real-time systems, and WSNs. Nevertheless, they share some defining features, listed as[4-6]:

- Network capabilities in each physical component and resource constraint. Computing and network bandwidth comprises of the coded instructions within every embedded system or physical component, and system resources are typically limited.
- Networking on multiple and extreme scales. CPS, whose network includes wired or wireless networks, Wi-Fi, Bluetooth, and GSM, is a distributed system. In addition, system size and device categories seem to vary widely.
- CPS facilitates convenient human-computer interaction, and advanced feedback control techniques are widely used in these systems. Closed-loop control and high degree of automation. Fig. 1 shows the concept map of cyber physical systems.

1. Literature Review

In this section features of Cyber Physical Systems (CPS), their practical applications, and relationship with IoT is discussed. Some other topics covered in this section include security attacks in CPS and review of existing approaches to overcome these attacks.

1.1. Features of CPS

As shown in Fig. 2, a CPS is a complex system with computation, communication, and control (3C) technology integration [8]. They combine network functions, notably, computing and communication, to physical functions like sensors and actuators. CPS can be observed over a diverse set of technological solutions, including but not limited to medicinal practice, automotive industry, national power grids, urban infrastructure, manufacture, aircraft, and building systems

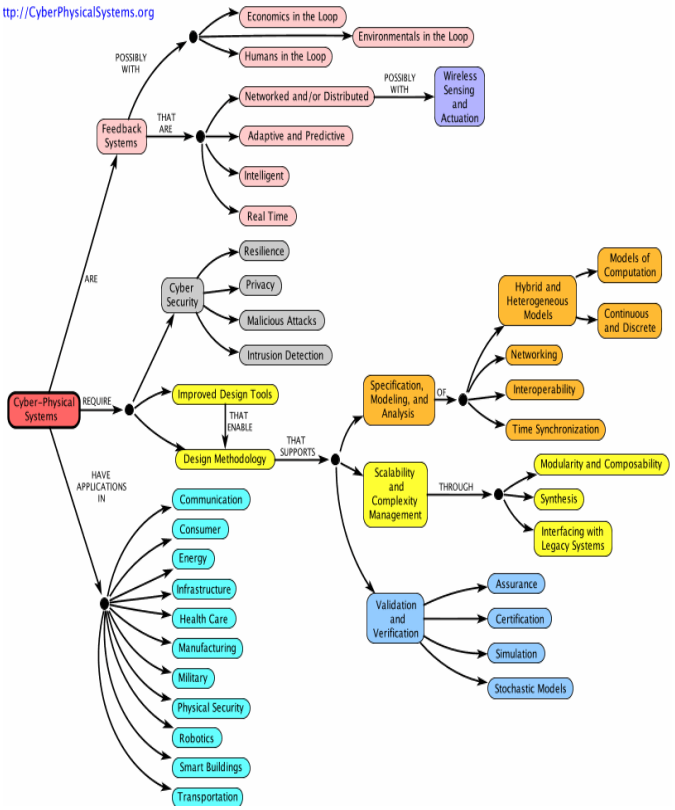

Fig. 1. Concept Map of CPS [7]

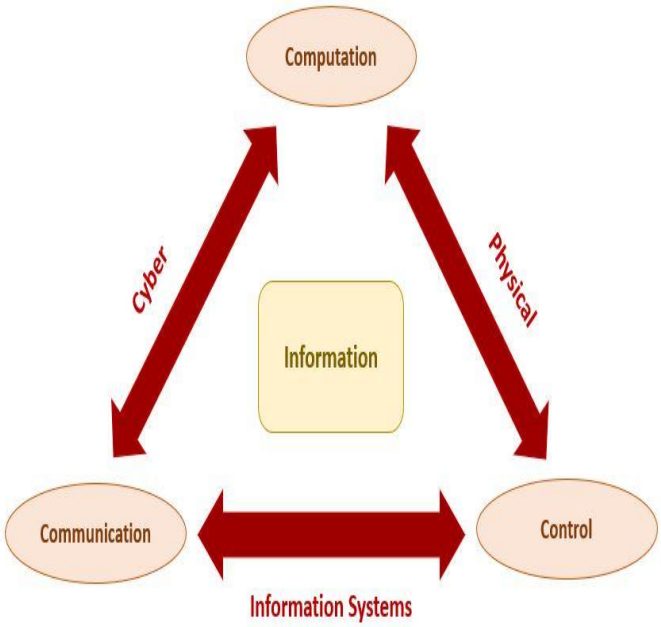

Fig. 2. conception of cyber physical systems

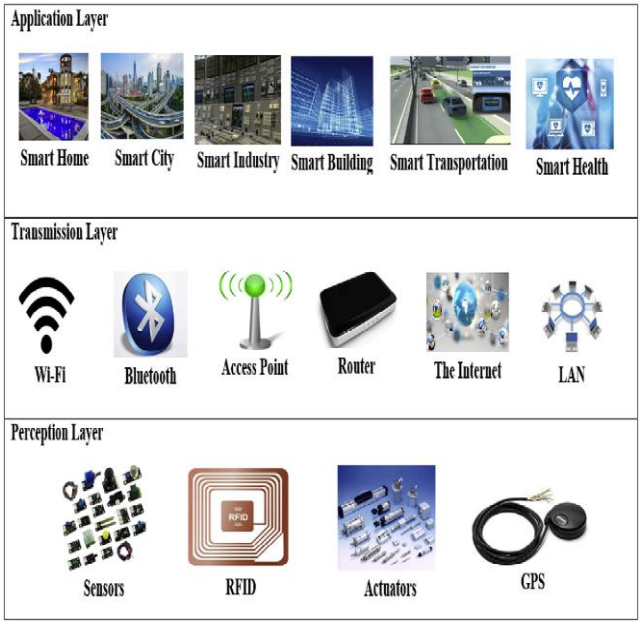

Fig. 3. Three-layered architecture of a cyber physical system [9]

A CPS comprises of three primary components: 1) A physical eco-system, 2) a communication and networking element, and 3) a dispersed cyber system. The CPS design has a set of distributed hardware, software and network components embedded in the physical system and environment. The software plays the vital role of bringing together all the software programs required for information processing, filtering and storage. A CPS engages with the physical systems over the network. Real-time distribution, scalability and reliability are considered to be the main features of a CPS Most CPS support applications drawn upon real-time data, such monitoring, control, and prediction in the real-time.

Generally, the architecture of a Cyber Physical System consists of three layers, notably, Sensing or Perception Layer, Transmission Layer, and finally, the Application Layer [9] as represented in Fig. 3.

Terminal devices which include sensors, actuators, cameras, GPS, RFID tags and readers form the aptly named Sensing (or Perception) Layer. With the capability to collect real-time data, i.e. sound, light, hearing, power or location these devices execute commands from the application layer. The Transmission Layer, also known as the Transport or Network Layer, exchanges and processes data between the Perception and Application Layers. Local Area Network, the Internet, or other communications technologies like Wi-Fi, Bluetooth, ZigBee, and infrared are employed to execute Transmission. The Application Layer, upon processing the information from the Transport Layer, issues commands to the sensors and actuators to execute, with the primary aim of creating a smart environment.

The physical systems of mobile networks are special CPSs with mobility built into it by default. The smartphone platform is the ideal mobile network physical system. Typical examples of mobile network physical systems include applications for detecting traffic accidents [10], measuring traffic, and monitoring heart disease patients.

1.2. Practical applications of CPS

Standard CPS applications are typically autonomous systems, communicating based on sensors. They include smart grids, automated car systems, medicinal monitoring, procedure control systems, distributed robotics, and autonomous avionics. Innovation and competition in industries such as agriculture, production, transportation, energy, architectural design and automation, healthcare and manufacturing are driven by the development of new smart CPSs. Further explanation [11-13] of some of these applications is as follows:

- *Production:* CPS are capable of distributing real-time information between industrial machinery, production supply chain, vendors, business systems, and clientele to improve production procedures. Simultaneously, CPS can improve these processes by virtue of monitoring itself and controlling the entire production process, subsequently adjusting production to meet customer preferences. CPS provides greater visibility and more control over the supply chain, improving product traceability and security.
- *Medicinal setting:* CPS is used to monitor the patient's physical condition in real time and remotely, to prevent patient hospitalization (such as patients with Alzheimer's disease), to improve the disabled and elderly patient medical treatment. In addition, CPS is used for research in the specialty of neuroscience to better the understanding regarding human functions that support the brain-body interface and robots for therapy purposes.
- *Renewable energy:* Exemplary of a Cyber Physical System, a smart grid, in which devices of a sensory and mechanic nature, observe the grid and control it by responding accordingly, thus improving both reliability and energy efficiency.
- *Smart building:* Smart devices engage with the CPS to consume reduced amounts of energy, while increasing safety and residents' comfort. For example, a CPS can be used within a building structure to monitor energy consumption, provide control over usage of the system, which may contribute towards achieving the aim of a zero-energy building. Moreover, a CPS can determine the extent of structural damage to a building in the event of an accident and aid in structural failure prevention.
- *Traffic:* communication between Personal vehicles and infrastructure, real-time traffic information sharing regarding location or problems, provide preventative measures to avoid accidents and blockages, enhance safety, saving time and money in the long run.
- *Agricultural:* the field of agriculture can be modernized and specialized with the help of a CPS. Basic information relating to weather, soil, water and other factors is collected by the CPS to create a more accurate

analytical model to base the agricultural management system on. CPS can continuously detect changes to requisite resources, such as soil fertility, soil and air moisture, plant health and other information, to maintain an ideal environment through sensors.

- *Computer networks:* CPS promotes the network environment to better understand system and user behaviour, helping to improve performance and improve managing resources. It may be used to optimize application to analyse environment and user behaviour, or to monitor the resources available. In addition, social networking sites and e-commerce sites with a large users-base can archive their users' navigation information and their associated web content, analyse the information, and then attempt predicting interesting things, recommend friends, articles, links, pages, events, or products to friends.

1.3. Relationship between CPS and IoT

Becoming increasingly advanced as their capabilities increase, smart devices continue to remain a relatively cost-efficient technology [12]. In addition, the broad penetration of high-speed wireless networks, such as the 4G cellular network, has been the backbone for a number of smart devices. . Each device can obtain information from the ecosystem to utilize it or share it across to another device within the Internet of Things [14]. The Internet of Things is a fluctuating, dispersed environment consisting of a multitude of smart devices equipped with capabilities to sense changes in its environment and take action in such an environment. Because of these devices, people can gather real world information by virtue of monitoring the external environment and create a permeating computing atmosphere that allows communication with other devices within its ecosystem, globally. The Internet of Things is designed to make the Internet permeate further within human life, enabling devices to connect and work together as a single sensor or group of sensors that create larger terminals, acting as an entire system [12].

The synergy between computing components and physical components, especially the use of cyber-physical systems (CPS), facilitates the implementation of the Internet of Things. CPS introduces the cooperation of cyberspace and physical space by integrating computing resources. CPS typically supports real-life processes, providing operational control over IoT objects that allow physical devices to perceive the environment and modify it. The Internet of Things (IoT) is a revolutionary innovation that delivers innovation and significant improvements to the social and business environment. With IoT technology, intelligent applications that adapt to its surrounding and improve resources management, providing systems with enhanced efficiency. The design of the Internet of Things and CPS are geared towards providing support to applications that manage voluminous data and a broad set of data environments. As a result, CPS can aid in further building on the efficiency and efficacy of resource management

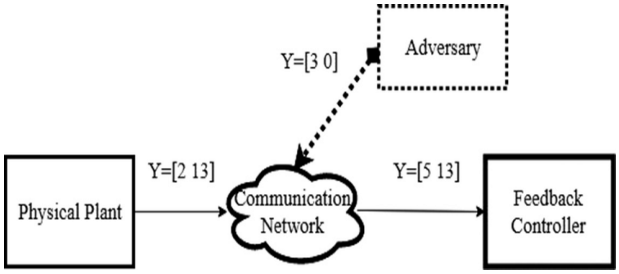

Fig. 4. Denial of service attack [16]

within the smart city vision by virtue of utilizing information and communication technologies [12]. Smart cities aim to reduce expenditures while providing innovative solutions in order to provide quality services for ease of life.

There is a significant overlap between CPS and IoT. The latter is a look into the future, with millions of Internet-connected devices, allowing them to remotely accumulate data about the real world, sharing it with other systems and devices, while IoT places great emphasis on uniquely recognizable devices and embedded systems connected to the Internet, the emphasis of a CPS is on the dynamic between computing and the physical world. For example, between the sophisticated hardware and its associated software characteristics of the system. If a system involves interaction with the physical world through sensors, actuators or both, then such a system can be classified as a cyber physical system. Like any other system or network, cyber physical systems are also vulnerable to security attacks. There are various techniques to detect and mitigate these attacks. In section 2.4 some of the attack detection methods are discussed.

1.4. Security attacks in CPSs

Listed as a primary security attack, Denial of service attacks [15] prevent a system from processing actual, systematic traffic or network resource-usage requirements. In this kind of cyber-attack, a large amount of data is pushed over to the network in order to keep the server (or other systematic resource) engaged, resulting in service interruption and a breakdown of normal procedures. Upon access to the network of physical systems, an attacker's options can be listed as:

- Use the entire sensor network or a traffic flood controller to the point of a system-wide shut down due to systematic overload.
- Service abortion or misbehavior by virtue of the controller or system network being exposed to invalid data.
- Traffic is blocked, causing the system's authorization elements to lose access to network resources.

Fig. 4 shows the schematic diagram of a denial of service attack in CPS. Established communications over the communication network between the physical plant and the

feedback controller is disturbed by the adversary. Therefore, the feedback controller cannot obtain information about the physical plant.

In Lappeenranta, Finland, a DDoS attack [17] occurred in a city of about 60,000 people. The attack was more pronounced within a world closely linked with cyberspace. The attack destroyed the heating and hot water systems of the two residential buildings, locked them in an endless restart loop, shattered the system, forcing residents to leave the building, and leaving the technicians confused over the operational resumption of the system. This incident may be an insulated incident undertaken by an individual, for a petty point of embarrassing the building management or it may be a trial run, precursory or preparatory of a digital attack strategy for a larger attack on life-protective systems in the future. In another incident in October 2016, Western media referred to the massive slowdown on the Internet in most parts of the United States as "down the Internet". This kind of attack that caused Twitter, Spotify, PayPal and other major websites to trace back to the security vulnerabilities of consumer electronics [18] made by a company. Hackers targeted these vulnerabilities and controlled nearly 500,000 DVRs and smart cameras. They used the Internet connectivity capabilities of these devices to launch large-scale distributed denial of service (DDoS) attacks. Although the attack did not cause any kinetic energy, it became an attack that brought the IoT and smart devices' vulnerability to security attacks into the limelight.

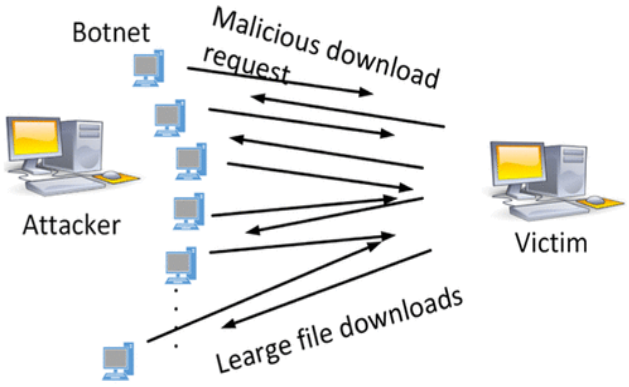

Fig. 5. HTTP flood attack using HTTP GET request

Some of the common DDoS attacks in CPS include HTTP flooding attacks (Fig. 5), TCP SYN attack and SIP flood attack. As another example, HTTP flooding attacks are exemplary of resource exhaustion attacks, whereby application layer protocols are used to attack victims. In such an attack, specifically, HTTP GET and HTTP POST requests are manipulated with malicious intent by an attacker, during the routinely course of communicating with a server or within a particular application. The idea of overwhelmed resources remains the same, i.e. the web server rejects any incoming requests in its entirety, regardless of its legitimate users. Carrying out such an attack, a valid IP address is used to establish a TCP connection. The attacker uses the IP address of his botnet to establish a connection. Fig. 5 visualises an HTTP GET request exploited as part of an example HTTP flood attack, in which the attacker executes an HTTP GET, attempting to request the download of very large files. Using its botnet, multiple requests are sent in this manner, to which the victim responds by performing a series of operations unknowingly, beginning with reading the file from back-end storage, storing it in the random access memory, and ultimately, splitting it into multiple transmissible packets to send back to the botnet. Therefore, the response invoked has involved the victim's resources of memory and processing capability. As a result, these voluminous requests have a burdening effect on the victim's entire resources and makes it impossible to cater to any requests made by legitimate users of the system. Parsed links obtained in response to such attacks can enable an attacker to camouflage his attack by making the attack traffic appear like normal internet traffic.

There have been similar incidents of intrusion and security attacks in real life as well, notable among them, a 2008 Polish attack carried out by a juvenile at 14, in Lodz, during which he used a reprogrammed TV remote for interacting with the urban tram system switch intersections. Then he used the remote control, changing the routes of the tram [19]. His mischief ended in an accidental collision, causing more than a dozen injuries. In another incident a network kinetic attack was triggered in 2000 by an Australian man in Maroochy Shire, Queensland, which caused even greater damage [20]. As a contractor, the person helped in designing and installation of wastewater management systems and wished to secure his finances by securing the services to maintain them. Upon observing this to not be the case, he spent a few months carrying out acts of sabotage, executing system-wide attacks randomly, distributing over 264,000 liters of untreated liquid urban waste throughout the town, damaging the aquatic life and threatening the health of residents before being arrested.

Another type of attack that CPSs are prone to is man-in-the-middle (MITM) attack, which relies on sending false messages to the operator in the terms of false positives or false negatives. The operator assumes normal working conditions, avoiding action as needed. An adverse event can be caused during the course of an operator following a standard routinely procedure and attempting to perform a change in the system. Multiple manifestations in the control-data modification and replay can affect system operation. Once physical plant and feedback controller network communications are acknowledged, the opponent modifies the actual information and injects the wrong data into the target network. This malicious data is forwarded to the feedback controller which erroneously, processes it accordingly.

Eavesdropping is another type of attack through which an attacker intercepts systematic information over a network. It is considered as a passive kind of attack due to non-interference in the system's workload by the attacker, as he can only take observations on operations, causing privacy issues. Analyzing a smart grid associated privacy-related issues overview known to be quite comprehensive,

the author focuses on the opponents who eavesdrop on the information to make inferences to the user [21]. The legal framework seeks to enforce laws and regulations with the intention to further solidify the right to privacy. The primary risk to privacy is monitoring load non-intrusively (the attacker identifies the device being exploited), utilizing its capability to detect patterns (the attacker extracts information regarding activities performed by the device internally, like recognizing TV channels). The author highlights several tips for reducing privacy risks such as using cryptographic approaches, perturbation, and verifiable computation methods

Rushanan (2014) describes the types of opponents that medical devices are subjected to in [22], including the active or passive communication eavesdropping ability. The threat is mainly concentrated on the telemetry interface. The authors also analyzed software managing user accounts, associated hardware, and sensory input interfaces, proposing authentication (such as biometrics, distance boundaries and channels that are out-of-band), as well as the availability or absence of additional devices that can be worn, to establish access denial protocols upon medical devices and mitigate possible attacks on the interface to the medical data telemetry. Additionally, using observations collected to establish safe behavioural patterns in order to seek out unsafe behavior and detect attacks was also discussed during the research..

1.5. Intrusion detection in CPS

Cyber Physical Systems (CPSs) can be observed to be deployed on a wide-scale, centrally controlled, regardless of geographical constraints, varying in nature of devices and their connection, systems that perform sensitive and precise operations of life, composed of a network component, linking mechanical operations performed by actuators, to environmental and peripheral input data from sensors, and control over the said procedures by virtue of data collected manually or otherwise, for e.g., systems employed in environments demanding situational awareness or pervasive medical procedures[23], smart grids, and drone systems. A multitude of control loops, pre-defined time usage of processes and operations, established network traffic patterns, components of a previous technological cycle due to market and supply conditions, with wireless networks possibly in segments are all a feature of such a system. CPS combines networks (networking components with enterprise-grade servers) to the physical (sensory inputs with motion actuator) domains.

An attack on CPS models attacks in both the long and short terms. An opponent without regard, rhyme or reason can establish entry into the network, and straightaway create a disaster by destroying related processes. However, opponents with a higher sophistication level may be careful to avoid normal, systematic, operational disruption in order to create and push forward a distributed attack, at any time. Stuxnet is an example of launching a security attack using such approach. Therefore, detection speed (detection delay) is a particular hurdle to designing a CPS Intrusion Detection System (IDS). CPS IDS design focus is to leverage its distinctive features and detect anomalous behavior as an attack.

CPS IDS implements two core functions:

- Collect data about suspects
- Analyze data

CPS accumulates audit data in the process appropriately named Data collection, resulting in data stored in a variety of formats intended for further human or machine usage, for e.g.collecting rumor reputation scores, keeping archives of the calls to the local node by the system, and archiving the network interface traffic. Utilizing the data collected by the data collection process, the Data Analysis process generates output in binary (bad or good), ternary (bad or good or undefined) or continuous (0 to 100 percent bad probability) data, with data mining, statistical analysis, and pattern matching as notable applications of the concept. Some of the responsibilities of CPS IDS are as follows:

- Monitoring physical processes and network-level user or machine activities and therefore physical laws that control the behavior of physical devices, making certain behaviors easier to see than others.
- Monitoring activities that are often automated and time-driven within a closed-loop environmental setting, introducing a measure of regularity as well as predictability for monitoring behavior.
- Should be able to handle sophisticated attacks such are zero day, rendering detection based on knowledge redundant.
- Should deal with components of a comparatively dated technological cycle, utilizing detection based on behavior effectively due to individually identified physical processes that impact the function of legacy components.

CPSs are usually network-integrated for remote management, reporting, and monitoring. This integration exposes them to the risk of a cyber-attacks sourced at non-trusted networks, such as the open Internet. Some of them include ransomware, denial of service, and flooding attacks. Once an attacker achieves network security breach, he may disrupt the operation of related systems. Therefore, there is an urgent requirement for intrusions detection into CPSs, especially CPSs that perform procedures that may have a critical impact on its intended users or beneficiary. One strategy delivers detection based on specification, which demands a precise definition of system behavior. Due to the complexity and dynamics of CPS along with inaccuracy and missing portions of the documentation at the design or operating levels, it is difficult to obtain similar system behavior. Easy-to-handle formal models are observed to be oversimplified in most instances, which makes them inappropriate for the purposes of a efficient detection.

Another detection uses machine learning (ML) in order to gain insights based on behavior for detecting an intrusion. Given that the methods that use unsupervised ML suffer

inaccurate results vis-à-vis high false-negative or positive rates, using high-fidelity CPS test beds is effective to replicate all major physical and control components, such as those in of modern CPS responsible for facilities to treat water, generating systematic training data to further scrutinized via supervised methods. This way detects the origination of a network attack at the processing level, physically, but also recognizes particular variations of attacks. It has fast detection speed and robustness to noise. In addition, the models adaptability within the system can be swiftly learned to synchronise the workings of CPS and the operating environment within. It is highly accurate with good recollection with a reduced false positive (FP) rate [24].

In papers [25] and [26], authors have also focused on the theme of the CPS intrusion detection system. The first paper mentions the capability of CPS to make autonomous, sentient decisions to maintain, heal, and upgrade, additional to detecting an intrusion. First, the author explains the canvas to vulnerabilities externally and internally exploited by attackers and explains methods of detection. The technique to detect intrusions currently at disposal are classified as mechanisms based on signature, exceptions and state protocol analysis. The researchers suggest five essential features of the functions in place for detecting intrusion in CPS:

- No privacy hindrance.
- Be capable to block unknown and known attacks.
- Runtime data needs to be provided
- Should have a fault-tolerant system
- Needs to be able to run in a distributed topology

Various IDS classifications have been put forth as suggestions by Mitchell, et al. (2014) [26], split into two groups between:

- Detection technology
- Audit material

The former class relates to detection based on knowledge, comprising methods that base on archival data regarding bad behaviour and are capable of determining misbehavior at the system or data stage. Additionally, detection based on behavior is a class, useful in the events of experience an attack like zero day due to its absence of any bias while monitoring. Audit materials, alternatively, can be classed as based on host, paying attention to the analytics logs, and audits around network that monitor network activity such as deep packet inspection to determine node compromise.

Many IDSs audit based on host for log analysis or additional information from file system details maintained by a node to determine if it is under threat. Distributed control is one of the main pros of using host-based auditing. This is lucrative to large-capacity deployments such as smart grids. Next, the ease in specifying or detecting host-level anomalous behavior has major pros when performing host-based auditing, as thorough knowledge specific to the host can be applied to distinguish an intruder. If no analysis is performed, each node must accumulate data to audit, despite the procedural increase. This is a major downside of host-based auditing, especially in resource-constrained applications. The advanced attackers mask their footprint by altering the data to be audited. Furthermore, it maybe particular to either OS or application, as per the specific contents within the log [26].

Some other effective approaches to detect and prevent security attacks in CPSs include using filters, implementing secure overlay services [27][28], lightweight schemes for resource-constrained systems [29][30] honeypots [31][32], and load balancing [33]. This research, a system to detect intrusion based on anomalies is suggested for DoS attack prevention using machine learning. Next section discusses the proposed solution.

2. Methodology

In this section, the proposed solution for detection of DoS attack is discussed along with the methodology used to develop the system.

2.1. Attack Detection using Machine Learning

Machine learning has become one of the evolving methods which is being utilized in growing numbers in cyber physical systems including military drones, robots, and smart cars. Since these networked physical systems can cause harm to humans, the safety component of the machine learning of said systems desires to be checked, for example, feature selection. [34]. Initially engineered for static environments, Machine learning algorithms and techniques assume sourcing training and test data both from the same distribution [35]. Currently, said algorithms are increasingly put to use in the function of an online learner, with continual retraining, to make decisions in a system oriented around security, practically visible in applications to detect fraud, filter spam, to systems that detect intrusions to the network. The listed applications capitalize on the ML model in order to prevent access to unauthorized users. The ML algorithm is vulnerable to both skilled as well as complex opponents during retraining and decision-making. Study into this specialty is called Antagonistic Machine Learning and defined as “machine learning algorithms designed to withstand complex attacks and the capabilities and limitations of attackers” [35]. It shows that this field is widely being researched for developing security solutions such as intrusion detection systems [36] for various domains including IoT, wireless sensor networks and cyber physical systems.

2.2. Workflow

The National Science Foundation (NSF) states that “the Cyber Physical System (CPS) is an engineering system built by the seamless integration of computational algorithms and physical components” while according to Papp et al. [37] embedded systems are “computing systems built into larger

systems designed for specialized functions combined with hardware, software and optional mechanical components" [37]. A CPS can manifest itself in the form of an embedded system. Moreover, since robots are mechanical structures by definition, computer software, actuators, and combinations of sensors that manage and control these devices [38], robots can be observed as an embedded system and a CPS. The CPS and framework workflow considered in this paper is presented in Fig. 6. According to Fig. 6 first, a network topology is created for real world performance. Then, all the devices are configured and made sure that all of them are correctly configured for them to start communicating with each other. Before the attack is launched, normal traffic is collected by using tools such as Wireshark. After that, the attack is launched and attack traffic is collected in real-time. Thereafter, syslog file is created which includes all the normal and abnormal traffic captured during the implementation. After the dataset is created in syslog file, machine learning is performed for attack detection. Then, further network traffic is observed and analyzed. Attacks can be analyzed on different layers such as physical layer, information layer, and application control layer

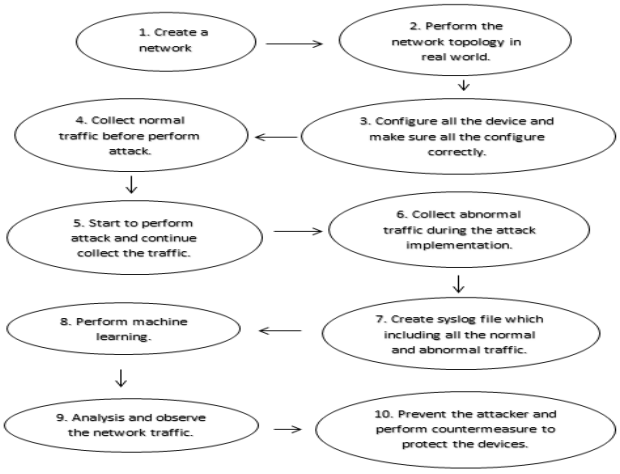

Fig. 6. Framework workflow

2.3. Attack detection

Due to the fact that anomaly detection strategy has the potential to detect new types of attacks, it has always been the focus of many researchers. However, the systematic complexity contributes towards these systems requiring extensive testing, evaluation, and adjustment before deployment, which hinders their adoption in practical applications. Running these systems thoroughly through actual tag network traces, mixed with intrusive and abnormal behavior, is the most ideal test and evaluation method. This is a huge challenge in itself due to the acute shortage of said datasets. On one hand, a large number of these datasets are internal to any organization, and privacy concerns demand restrictions over their sharing. On the other hand, other datasets that are available are primarily anonymous and cannot be representative of the current patterns, or they lack certain statistical features, thus there being no ideal dataset. With the changes in network behavior, patterns and the development of intrusion, moving from static and one-time data sets to dynamically generated datasets is vital. This reflects the network traffic composition and intrusion at the same time but can also be reproducible, modified and expandable.

To overcome aforementioned shortcomings, a systematic method is designed to produce datasets for analysis, testing and evaluating intrusion detection systems, emphasising on anomaly detectors based on the network component. Based on the dataset that is downloaded, the attack scenarios is DDoS. The attack infrastructure includes fifty computers, and the victim organization has five departments, including four hundred and twenty computers and thirty servers. The dataset contains the records of network traffic captured along with system logs of all computers, as well as CICFlowMeter-V3 being used to extract eighty functions from the data analysed.

In the CSE-CIC-IDS2018 dataset, the concept of a configuration file is used to generate a data set in a systematic manner, containing detailed accounts of intrusion and infer dispersal models for applications, protocols, or underlying network objects. Agents or human operators can use these profiles to create network activity. With the all-encompassing nature of the configuration files generated, its effects can be observed after application across various network protocols with differing topologies. Datasets can be created to suit particular needs with the aid of such Profiles Based on the downloaded data set, it constructs two different profile categories

Attack	Tools	Duration	Attacker	Victim
DDoS+PortScan	Low Orbit Ion Canon (LOIC) for UDP, TCP, or HTTP requests	Two days	Kali linux	Windows Vista, 7, 8.1, 10 (32-bit) and 10 (64-bit)

Fig. 7. List and duration of attacks performed

- B-Profile: Use a variety of analytical methods such as machine learning and statistical analysis (including K-means, random forest, SVM and J48) to encapsulate the user's physical behavior. The characteristics of encapsulation are the protocol packet size, packet density per stream, particular payload patterns, payload size and dispersal of the protocol request-time distribution. The test platform environment will simulate the protocols including HTTPS, HTTP, SMTP, POP3, IMAP, SSH and FTP. A high number of them are HTTP and HTTPS judging from the initial traffic observation.
- M-Profile: Try to detail the attack in a clear way. Simply, easily understood instructions can be interpreted by humans and then executed. Ideally,

autonomous agents and compilers will be used to read and perform out these actions. Fig. 7 show the DDoS attack scenario:

i. HTTP denial of service: In such a case, the main tools are named Slowloris and LOIC, and these tools have been known to make it impossible to access the web server with a singular attack machine. Initially, Slowloris establishes a complete TCP connection with a remote server. the connection stays open by virtue of Slowloris periodically transmitting valid but incomplete server HTTP requests, preventing the socket to close. Due to the service connection capability limitation that a web server has, it is only an issue of time till all sockets are exhausted and further connections cannot be established. In addition, HOIC is another well-known application that is capable of exposing websites to DoS attacks to execute against. The effective usage of the infrastructure by the profile is a vital obseration. The test platform will include some interconnected workstations based on Windows and Linux. For Windows computers, different service packs will be used (because each service pack has multiple vulnerabilities already known), while in Linux computers, a distribution that contains vulnerabilities that can be exploited via the Metasploit program will be used, due to its design centering around the lure for new penetration testers.

The implementation and infrastructure of B-Profile: In order to generate good traffic for the background, B-Profile is built to extract the abstract behavior of a human user-group. It attempts to use analytical methods such as machine learning and statistical analysis \to encapsulate user-created network events. The characteristics of encapsulation are the protocol packet size, the stream packets density, particular payload patterns in the, the payload size, and the distribution of request time in the protocol. After arriving at the B configuration file from the user, agents (CIC-Benign Generator) or human operators can utilize them for creating realistic, non-harmful activity on the network. This method can be employed by academic and commercial entities in order to create datasets that are closer to reality. Thus the need for the dataset being anonymous is removed.

Next, the implementation and infrastructure of M-Profile: Fig. 8, visualises the implemented network, a common LAN network topology on the AWS computing platform. In order to make the various machines similar to the actual network, 5 subnets were installed, namely Dep1 for the R & D department, Dep2 for the management department, Dep3 for the technician department, Dep4 for the secretary and operations department, Dep5 for the IT department and the server room. With the exception of IT, varying versions of MS Windows (8.1 and 10) have been installed across all departments, with Ubuntu installed across the IT department. Differing MS Windows servers were selected for implementation across the server room.

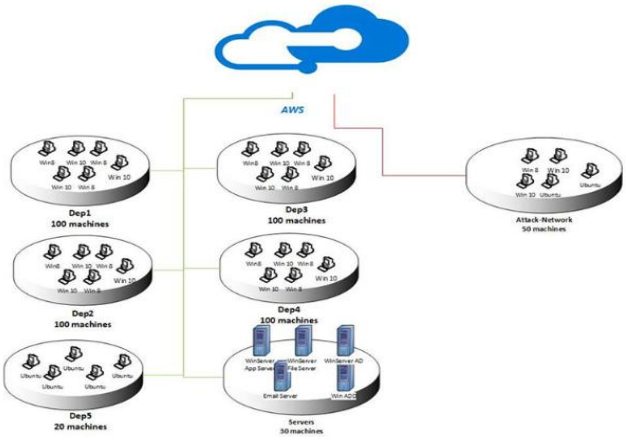

Fig. 8. Network topology

DDoS attack scenarios and tools: The H.O.I.C (High Orbit Ion Cannon), is an open source application written in BASIC, created to perform network stress test and denial of service attacks with the capability to target up to 256 URLs simultaneously, as the successor of the Praetox Technologies developed Low-Orbit Ion Cannon. They utilize the free to use and distribute HOIC tool to perform DDoS attacks by using 4 different computers. The infrastructure is implemented and attack scheme is executed which is based on all selected attacks (DDoS attacks) and the scheme defined in the previous section. Fig. 9. shows the attack list, related attacker and victim IPs, date of the attack, start and end time. Written in Java, CICFlowMeter creates network traffic flow, as it provides greater flexibility in selecting functions to be calculated, adding new functions, and better controlling the timeframe of timeout of the flow. Creating a bidirectional flow (Biflow), with the first packet making the determination on the forward (to destination) and backward (to source) directions, resulting in 83 statistical functions, such as duration, number of packets. Other variables such as the number of nodes, length of the packets, etc. are computed in both the forward and reverse directions.

The application outputs data in the CSV file format. Each stream has six columns of tags, namely FlowID, SourceIP, DestinationIP, SourcePort, DestinationPort, and protocols with more than 80 network traffic functions. Normally, the TCP flow is terminated when the connection is disconnected (via FIN packets), and the UDP flow is terminated when the flow times out. The stream timeout value can be arbitrarily assigned by various schemes. For example. Both TCP and UDP are 600 seconds. Having deducted the function and generated the CSV file, now the data need to be tagged. The attack plan timeline used, as well as the source and target IP and port and protocol names, to mark the data for each flow.

The dataset is organized everyday raw data of each machine is recorded everyday, including network traffic (Pcaps) and event logs (Windows and Ubuntu event logs). While extracting features from raw data, CICFlowMeter-V3 was employed and 80+ features about the network traffic were extracted and committed to storage as CSV files for

each computer. Two type of DDoS attacks have been detected from the dataset which are DDoS attack-LOIC and DDOS attack-HOIC mapped to "DDoS attack-LOIC-UDP" and "DDoS attack-HOIC" to "DDOS". The second mapping is to convert the string to value which is "Begin" to "0" and "DDOS" to "1". The reason is to develop easy management practices and easy-to-understand system. Decision tree classifier has been used to detect the attacks based on its many advantages (Fig. 10). The reason to use this machine learning technique is that it can handle both categorical and numerical data. Furthermore, decision tree classifier can solve the logistics regression problem which occurs when there are more than two dependent variables. It is derived from independent variables, and each node has a characteristic condition. The parent node makes decision for the leaf node to navigate according to the conditions. Once the leaf node is reached, the output can be predicted. The correct order of conditions can verify the tree. Entropy/information gain is used as a criterion for selecting node conditions and greed-based recursive algorithms are used to derive the tree structure. Additionally, the predictivity power of decision tree model is high, and it performs well in terms of interpretability which makes it compatible with the nature of CPS.

The results obtained after decision tree model implementation on DDoS dataset shows 0.9981 accuracy rate which indicates closeness to its true value and presence of the attack in the given dataset. This is important because poor equipment, poor data processing, or human error may cause the accuracy of the results to be inconsistent with the actual situation. Therefore, it is important to test the model on the datasets with known attacks first, and compare them with the accuracy rate of developed model. Accuracy is to ensure that the information is correct while precision is the closeness between a series of measurements of the same thing.

Attacker	Victim	Attack Name	Date	Attack Start Time	Attack Finish Time
18.218.115.60 18.219.9.1 18.219.32.43 18.218.55.126 52.14.136.135 18.219.5.43 18.216.200.189 18.218.229.235 18.218.11.51 18.216.24.42	18.218.83.150- 172.31.69.28	DDOS-LOIC-UDP	Wed-21-02-2018	10:09	10:43
18.218.115.60 18.219.9.1 18.219.32.43 18.218.55.126 52.14.136.135 18.219.5.43 18.216.200.189 18.218.229.235 18.218.11.51 18.216.24.42	18.218.83.150- 172.31.69.28	DDOS-HOIC	Wed-21-02-2018	14:05	15:05

Fig. 9. Daily attack list, machine IP, attack start and end time.

```
In [27]: classifier = DecisionTreeClassifier(criterion = 'entropy', random_state = 0)
         classifier.fit(X_train.iloc[:1000, :3], y_train.iloc[:1000])

Out[27]: DecisionTreeClassifier(class_weight=None, criterion='entropy', max_depth=None,
                                max_features=None, max_leaf_nodes=None,
                                min_impurity_decrease=0.0, min_impurity_split=None,
                                min_samples_leaf=1, min_samples_split=2,
                                min_weight_fraction_leaf=0.0, presort=False, random_state=0,
                                splitter='best')
```

Fig. 10. Decision tree classification

3. Discussion on attack prevention mechanisms in CPS

The domain of attack prevention in cyber physical systems is in early stages. Therefore, it is necessary to perform extensive research to prevent insecure deployments of these systems. Post vulnerability identification, development of defensive measures that can restrict access to malicious agents becomes imperative. The rest of this section will discuss some of the defense mechanisms that have been proposed or implemented for improving the security aspects of CPS. Researchers have proposed encryption methods, route security, and route anonymity to avoid eavesdropping attacks, and scrutinized vital concerns during the design stage of cryptosystems, for e.g. key management, authentication, and encryption or decryption algorithms [39]. The literature shows a number of recommendations for establishing a key agreement to prevent compromised key attacks. The first category of key agreement-related attacks involves a key transfer protocol where an entity-created session key is transmitted to another securely [40]. The other category is a protocol for synchronising keys, which utilizes information from two entities in order to derive shared keys to prevent compromised key attacks [40].

In another paper, an elastic controller is designed for the network physical control system to avoid it from becoming a target of DoS attack [41]. The coupling design framework is incorporated into the IDS network using configuration strategy. The algorithm within the suggested strategy is built on linear matrix inequalities to calculate optimal network security policies and control methods to prevent DoS attacks.

Table 1 shows the summary of security methods to prevent major attacks in CPS [39-44].

Similarly, McLaughlin (2016) presented an eight-step procedure in [45] to assess vulnerability in its full detail, beginning with documentary analysis to final testing, and ICS security implementation. The strategy to addressing the vulnerabilities focuses primarily on the control architecture that customizes its mechanisms based on the domain:

checking control code at runtime, referring to the monitor architecture, providing an architecture for estimating the time to an unsafe state, and architecture with a trusted computing foundation. In another paper authors emphasize on exploiting the systematic physical characteristics to notice attacks (such as physical-based intrusion detection) [46]. The author discusses the need for a clear definition: Statistical test for anomaly detection

Table 1. Summary of security techniques for prevention of attacks in cyber physical systems [39-44].

Attack type	Countermeasure
Denial-of-service attack	Mandatory Access Control (MAC), Access Control Lists (ACL), Role-based access control, Discretionary access control
Compromised-key attack	Key agreement protocols, two party key establishment protocols, cryptography, key transport protocol
Man-in-the-middle attack	Digital signature, biometrics, Mandatory Access Control (MAC), Trusted Platform Module (TPM), Message digest
Eavesdropping	Anonymous routing, cryptosystem (symmetric and asymmetric), secure routing

- Method (indicator) for evaluating the effectiveness of anomaly detectors
- Physical system model
- Trust hypothesis

These above-mentioned four features are also identified in several publications within the field of CPS, including power systems, ICS, control theory, self-driving cars, cameras, power theft, and medical equipment. After discussing the common assumptions and shortcomings of such research, the author draws conclusions and suggests improvements, including the placement of security monitors. They also proposed a new measure for the effectiveness evaluating of intrusion detection models based on physical. The safety and privacy concerns within the Industrial Internet of Things (IIoT) applications have been attended to [47]. As a mitigation measure, the authors have proposed to use techniques involving checking integrity, through software and hardware.

In another paper, the writers have compared the mechanisms for identifying dangerous nodes and harmful data in ITS [48]. The author analyses detecting behavioural error by describing a domain-specific anomalous behaviour classification, which is subject to the anomaly being caused by an inconsistent node or data. Programs that detect attacks were surveyed on the three levels, namely, the local, global, and collaborative levels, and point out the importance of the link between the Airborne Unit (OBU) and the message to identifying bad behaviour and has developed a solution based on the level of available link capabilities. An investigation into the vehicle self-organizing network (VANET) defence mechanism was conducted [49].

The survey focuses on model-based security mechanisms such as mechanical modelling, trust-based modelling, and Markov chain modelling in addition to supervisory-based defence. Additionally, it also provides a comparative study of system infrastructure and attacks that can be defeated by specific technologies. The study also mentions that most defences aim to detect specific levels of misconduct and urge the researchers to study the reliability of links. For example, one of the main challenges in transport system modelling is flexibility. The problem becomes even more serious when developing security features for such systems. Other security issues are related to scalability, lack of clear lines of defence and real-time operations [49]. Differing kinds of possible attacks with the capability to impact privacy are also discussed, and most attacks such as forged GPS information or deployment control commands are analyzed for their ability to cause drone failure [50]. The authors further identify possible solutions such as encryption and IDS to alleviate the effects of said attacks. In another paper, Nguyen (2017), while examining security concerns in CPS [51] and displayed the role of software models in CPS design and validation. The level of abstraction being higher than the code level is one of the key benefits from Model-based strategies. The authors have also created a methodical study of the mapping and discovered different patterns in security analysis based on model. Similarly in [52-57] and [58-61] authors have investigated and reviewed current approaches proposed by researchers to overcome security issues in integrated systems.

In this paper, the importance of developing secure CPSs as well as IoT infrastructures, implementation of security strategies and development of strong monitoring mechanisms has been highlighted. The security attacks discussed in literature review have demonstrated the high level of insecurity present in current cyber physical systems and urgent need of development of security techniques has been presented. This paper is also written in an effort to contribute in this domain by proposing an anomaly detection system using machine learning for DoS attack prevention in cyber physical systems.

4. CONCLUSION

The evolving domain of cyber physical systems and their security features have been explored as a part of this research paper. While their integration with various

technologies like Internet of Things, smart devices and resources-constrained sensors as well as actuators has led to the development of advanced infrastructures like smart cities, the factor of interconnection has also caused increased security and privacy issues. Denial of Service is one of the most common type of attacks, addressed in this paper by proposing a system to detect intrusion based on anomaly analysis. Due to the fact that these systems are usually connected with the internet, it has become very convenient for the attackers to access and target cyber physical systems. Therefore, the aforementioned system is proposed in an effort to contribute towards the improvement in security of these systems. In this paper the DoS attack is addressed using a machine learning technique called decision tree classifier and a dataset with existing DoS attack is used. This approach is used to observe the accuracy rate of attack detection in a dataset in the presence of known attack to improve the model for unknown attacks in similar domain in future. This step is performed to ensure that the model is capable of correctly and precisely identifying the attack However, in future, more security attacks are expected to be addressed for secure cyber physical systems deployment in public and private domains.

REFERENCE

1. F.M. Zhang, K. Szwaykowska, W. Wolf and V. Mooney, “Task Scheduling for Control Oriented Requirements for Cyber-Physical Systems,” in Proc. of 2008 Real-Time Systems Symposium, pp.47-56, 2008.
2. J. Sprinkle, U. Arizona, and S. S. Sastry, “CHESS: Building a Cyber-Physical Agenda on Solid Foundations,” Presentation Report, Apr. 2008.
3. J.Z. Li, H. Gao, B. Yu, “Concepts, Features, Challenges, and Research Progresses of CPSs,” Development Report of China Computer Science in 2009, pp. 1-17, 2009.
4. R. Rajkumar, “CPS briefing,” Carnegie Mellon University, May 2007.
5. B. H. Krogh, “Cyber Physical Systems: The Need for New Models and Design Paradigms,” Presentation Report, 2008.
6. B. X. Huang, “Cyber Physical Systems: A Survey,” Presentation Report, Jun. 2008.
7. L.H. Wang, M. Törngren, and M. Onori, “Current status and advancement of cyber-physical,” Journal of Manufacturing Systems, May 2015.
8. Wan, K. et al., “Investigation on composition mechanisms for cyber physical systems,” International Journal of Design, Analysis and Tools for Circuits and Systems, vol. 2, no. 1, August 2011, pp.30-40
9. Y. Ashibani, and Q.H. Mahmoud, “Cyber physical systems security: analysis, challenges and solutions,” Computer & Security, vol. 68, 2017, pp. 81-97.
10. N.A. Khan, N.Z. Jhanjhi, S.N. Brohi, R.S. A. Usmani, A. Nayyar, “Smart traffic monitoring system using Unmanned Aerial Vehicles (UAVs), Computer Communications”, Volume 157, 2020, Pages 434-443, ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2020.04.049
11. A.Zanni, “Cyber-physical systems and smart cities”, IoT, IBM Developer, 2015. Available at: https://developer.ibm.com/articles/ba-cyber-physical-systems-and-smart-cities-iot/
12. S.K. Khaitan, S. K. and J.D. McCalley, “Design techniques and applications of cyber physical systems: a survey,” IEEE Systems Journal, vol. 9, no. 2, June 2015, pp.350-365.
13. J. Al-Jaroodi, N. Mohamed, I. Jawhar and S. Lazarova-Molnar, "Software Engineering Issues for Cyber-Physical Systems," *2016 IEEE International Conference on Smart Computing (SMARTCOMP)*, St. Louis, MO, 2016, pp. 1-6, doi: 10.1109/SMARTCOMP.2016.7501717.
14. D.K. Alferidah, N.Z. Jhanjhi, “A Review on Security and Privacy Issues and Challenges in Internet of Things”, in International Journal of Computer Science and Network Security IJCSNS, 2020, vol 20, issue 4, pp.263-286
15. Baheti, R, Gill, H. Cyber-physical systems. In: Samad, T, Annaswamy, AM (eds) The impact of control technology, vol. 12. New York: IEEE, 2011, pp.161–166.
16. Y. Maleh, M. Shojafar, A. Darwish, and A. Haqiq. “Cybersecurity and Privacy in Cyber-Physical Systems,” Cybersecurity in Cyber-Physical Systems, May 2019, pp.9-10
17. M. Kumar, “DDoS Attack Takes Down Central Heating System Amidst Winter in Finland”, 2016, http://thehackernews.com/2016/11/heating-system-hacked.html
18. Michael Kan, Chinese Firm Admits Its Hacked DVRs, Cameras Were Behind Friday's Massive DDOS Attack, 2016, http://www.pcworld.com/article/3134039/hacking/chinese-firm admits-its-hacked-products-were-behind-fridays-massive-ddos-attack.html
19. G. Baker, “Schoolboy Hacks into City's Tram System”, 2008, Available: http://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys tram-system.html
20. T. Smith, “Hacker Jailed for Revenge Sewage Attacks”, The Guardian, 2001, Available: http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/
21. Mo, Yilin, and Bruno Sinopoli. “Secure control against replay attacks. In 2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton), pp. 911-918. IEEE, 2009.
22. Rushanan, Michael, Aviel D. Rubin, Denis Foo

Kune, and Colleen M. Swanson. “Sok: Security and privacy in implantable medical devices and body area networks.” In 2014 IEEE Symposium on Security and Privacy (SP), pp. 524–539. IEEE, 2014.

23. M. Humayun, NZ Jhanjhi, M. Z Alamri, “Smart Secure and Energy Efficient Scheme for E-Health Applications using IoT: A Review”, International Journal of Computer Science and Network Security 20 (4), 55-74.

24. K.N. Junejo and J. Goh, “Behaviour-Based Attack Detection and Classification in Cyber Physical Systems Using Machine Learning”, ACM Digital Library, pp. 34–43, May 2016, Available: https://doi.org/10.1145/2899015.2899016

25. Han, Song, Xie, Miao, Chen, Hsiao-Hwa and Ling, Yun, 2014. Intrusion detection in cyber-physical systems: Techniques and challenges. IEEE Systems Journal 8 (4), pp. 1052–1062.

26. R. Mitchell and Ing-Ray Chen, “A survey of intrusion detection techniques for cyber-physical systems”, ACM Comput. Surv. 46, 4, Article 55 (April 2014), 29 pages. DOI:https://doi.org/10.1145/2542049

27. Adkins, D, Lakshminarayanan, K, Perrig, A. Towards a more functional and secure network infrastructure. Technical report no. UCB/CSD-03-1242, 2003. EECS Department, University of California, Berkeley, http://www2.eecs.berkeley.edu/Pubs/TechRpts/2003/6241.html

28. Keromytis, AD, Misra, V, Rubenstein, D. SOS: secure overlay services. ACM SIGCOMM Comp Com 2002; 32(4): 61–72.

29. Almulhim, M., Islam, N., & Zaman, N. (2019). A Lightweight and Secure Authentication Scheme for IoT Based E-Health Applications. International Journal of Computer Science and Network Security, 19(1), 107-120.

30. A. Diro, H. Reda, N. Chilamkurti, A. Mahmood, N. Zaman and Y. Nam, "Lightweight Authenticated-Encryption Scheme for Internet of Things Based on Publish-Subscribe Communication," in IEEE Access, vol. 8, pp. 60539-60551, 2020, http://dx.doi.org/10.1109/ACCESS.2020.2983117 .

31. Krämer, L, Krupp, J, Makita, D. AmpPot: monitoring and defending against amplification DDoS attacks. In: Proceedings of the international workshop on recent advances in intrusion detection, Kyoto, Japan, 2–4 November 2015, pp.615–636.

32. Weiler, N . Honeypots for distributed denial-of-service attacks. In: Proceedings of the 11th IEEE international workshops on enabling technologies:infrastructure for collaborative enterprises, 2002 (WET ICE 2002), Pittsburgh, PA, 12 June 2002, pp.109–114. New York: IEEE.

33. McMullin, M. DNS, load balancing and DDoS attacks, 2016, https://kemptechnologies.com/blog/load-balancing-and-ddos-attacks/ (accessed 5 May 2017).

34. M. Barreno, B. Nelson, A. D. Joseph, and J. D. Tygar, "The security of machine learning," Machine Learning, vol. 81, no. 2, pp. 121-148, 2010.

35. L. Huang, A. D. Joseph, B. Nelson, B. I. P. Rubinstein, and J. D. Tygar, "Adversarial machine learning," in Proceedings of the 4th ACM workshop on Security and artificial intelligence, 2011, pp. 43-58.

36. S.H. Kok, A. Abdullah, NZ. Jhanjhi and M. Supramaniam, “A Review of Intrusion Detection System using Machine Learning Approach”, International Journal of Engineering Research and Technology 12 (1), 2019, 8-15.

37. D. Papp, Z. Ma, and L. Buttyan, "Embedded systems security: Threats, vulnerabilities, and attack taxonomy," in Privacy, Security and Trust (PST), 2015 13th Annual Conference on, pp. 145-152.

38. S. Morante, J. G. Victores, and C. Balaguer, "Cryptobotics: Why robots need cyber safety," Frontiers in Robotics and AI, vol. 2, pp. 23-23, 2015.

39. Kao, Jung-Chun, and Radu Marculescu. “Eavesdropping minimization via transmission power control in ad-hoc wireless networks.” In Sensor and Ad Hoc Communications and Networks, 2006. SECON’06. 2006 3rd Annual IEEE Communications Society on, vol. 2, pp. 707–714. IEEE, 2006.

40. Chalkias, Konstantinos, Foteini Baldimtsi, Dimitrios Hristu-Varsakelis, and George Stephanides. “Two types of key-compromise impersonation attacks against onepass key establishment protocols.” In International Conference on E-Business and Telecommunications, pp. 227–238. Springer, Berlin, Germany, 2007.

41. Yuan, Yuan, Quanyan Zhu, Fuchun Sun, Qinyi Wang, and Tamer Başar. “Resilient control of cyber-physical systems against denial-of-service attacks.” In Resilient Control Systems (ISRCS), 2013 6th International Symposium on, pp. 54–59. IEEE, 2013.

42. Adhikari, Uttam. Event and Intrusion Detection Systems for Cyber-Physical Power Systems. Mississippi State University, 2015.

43. Lyn, Kevin G. “Classification of and resilience to cyber-attacks on cyber-physical systems.” PhD diss., Georgia Institute of Technology, 2015.

44. Saltzman, Roi, and Adi Sharabani. “Active man in the middle attacks.” OWASP AU (2009).

45. McLaughlin, Stephen, Charalambos Konstantinou, Xueyang Wang, Lucas Davi, Ahmad-Reza Sadeghi, Michail Maniatakos, and Ramesh Karri. “The cybersecurity landscape in industrial control systems.” Proceedings of the IEEE 104, no. 5 (2016):1039–1057.

46. Urbina, David I., David I. Urbina, Jairo Giraldo, Alvaro A. Cardenas, Junia Valente, Mustafa Faisal, Nils Ole Tippenhauer, Justin Ruths, Richard Candell, and Henrik Sandberg. Survey and New Directions for Physics-Based Attack Detection in Control Systems. US Department of Commerce, National Institute of Standards and Technology, 2016.

47. Sadeghi, Ahmad-Reza, Christian Wachsmann, and Michael Waidner. "Security and privacy challenges in industrial internet of things." In Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE, pp. 1–6. IEEE, 2015

48. Van der Heijden, Rens W., Stefan Dietzel, Tim Leinmüller, and Frank Kargl. "Survey on misbehavior detection in cooperative intelligent transportation systems." Arxiv preprint arXiv:1610.06810 (2016).

49. Sakiz, Fatih, and Sevil Sen. "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV." Ad Hoc Networks 61 (2017): 33–50.

50. Altawy, Riham, and Amr M. Youssef. "Security, privacy, and safety aspects of civilian drones: A survey." ACM Transactions on Cyber-Physical Systems 1, no. 2 (2017): 7.

51. Nguyen, Phu H., Shaukat Ali, and Tao Yue. "Model-based security engineering for cyberphysical systems: A systematic mapping study." Information and Software Technology 83 (2017): 116–135.

52. Z.A. Almusaylim and N. Zaman, "A review on smart home present state and challenges: linked to context-awareness internet of things (IoT) Wireless Networks", 25 (6), 3193-3204. https://doi.org/10.1007/s11276-018-1712-5

53. L.Seungjin, A. Abdullah and N.Z. Jhanjhi, "A Review on Honeypot-based Botnet Detection Models for Smart Factory" International Journal of Advanced Computer Science and Applications(IJACSA), 11(6), 2020. http://dx.doi.org/10.14569/IJACSA.2020.0110654

54. Khalid Hussain, N.Z. Jhanjhi, H.M. Rahman, Jawad Hussain, Muhammad Hasan Islam, "Using a systematic framework to critically analyze proposed smart card based two factor authentication schemes", Journal of King Saud University - Computer and Information Sciences, 2019, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2019.01.015 .

55. Jhanjhi, N., Humayun, M., Almuayqil, S.N. (2021). Cyber Security and Privacy Issues in Industrial Internet of Things. Computer Systems Science and Engineering, 37(3), 361–380. https://doi.org/10.32604/csse.2021.015206

56. B. Hamid, N. Jhanjhi, M. Humayun, A. Khan and A. Alsayat, "Cyber Security Issues and Challenges for Smart Cities: A survey," 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), Karachi, Pakistan, 2019, pp. 1-7, doi: 10.1109/MACS48846.2019.9024768.

57. Jhanjhi, N., Humayun, M., Almuayqil, S.N. (2021). Cyber Security and Privacy Issues in Industrial Internet of Things. Computer Systems Science and Engineering, 37(3), 361–380. https://doi.org/10.32604/csse.2021.015206

58. Humayun, M., Niazi, M., Jhanjhi, N. et al. Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arab J Sci Eng 45, 3171–3189 (2020). https://doi.org/10.1007/s13369-019-04319-2

59. Humayun, M., Jhanjhi, N.Z., Talib, M.N., Shah, M.H., Suseendran, G. (2021). Cybersecurity for Data Science: Issues, Opportunities, and Challenges. In: Peng, SL., Hsieh, SY., Gopalakrishnan, S., Duraisamy, B. (eds) Intelligent Computing and Innovation on Data Science. Lecture Notes in Networks and Systems, vol 248. Springer, Singapore. https://doi.org/10.1007/978-981-16-3153-5_46

60. Prabakar D, Sundarrajan M, Manikandan R, Jhanjhi NZ, Masud M, Alqhatani A. Energy Analysis-Based Cyber Attack Detection by IoT with Artificial Intelligence in a Sustainable Smart City. Sustainability. 2023; 15(7):6031. https://doi.org/10.3390/su15076031

61. D. K. Alferidah and N. Jhanjhi, "Cybersecurity Impact over Bigdata and IoT Growth," 2020 International Conference on Computational Intelligence (ICCI), Bandar Seri Iskandar, Malaysia, 2020, pp. 103-108, doi: 10.1109/ICCI51257.2020.9247722