A Survey on DDoS Attacks on Network and Application Layer in IoT

Chapter · January 2022

DOI: 10.1007/978-3-030-96040-7_19

2 authors, including:

Pramod Kumar Mishra
Banaras Hindu University
40 PUBLICATIONS **1,161** CITATIONS

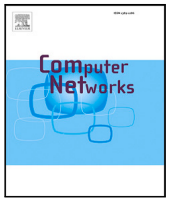
SEE PROFILE

Computer Networks 236 (2023) 110015

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet



Review article

DDoS attacks in Industrial IoT: A survey

Shubhankar Chaudhary, Pramod Kumar Mishra *

Department of Computer Science, Institute of Science, BHU, India

ARTICLE INFO

Keywords:
IoT
IIoT
SDN
DDoS
IIoT architecture
Security

ABSTRACT

As the IoT expands its influence, its effect is becoming macroscopic and pervasive. One of the most discernible effects is in the industries where it is known as Industrial IoT (IIoT). IIoT provides automated, comprehensive, regressive and easy-to-use methods to look over its components. Along with the benefits, it also brings concerns that spawn from the IoT itself. Moreover, the challenges in the industries also add up because they have their own set of requirements and procedures to perform. Among those challenges, one of the prominent is DDoS attacks. So, through this paper, the DDoS attacks in IIoT is studied. This paper has culminated the work done in the domain involving IoT and IIoT. With this different forms of attacks involved in DDoS, the tools involved in generating the attacks and the overall traffic generators is also discussed. To elucidate, IIoT architecture and various layers involved in communication is discussed to correlate the threat of DDoS attacks in IIoT. Further, the studies made in various categories such as machine learning, deep learning, federated learning and transfer learning is elaborated. Finally, the challenges present in IIoT and the security requirements needed to overcome challenges in IIoT is explained.

1. Introduction

Internet of Things (IoT) is an interconnection of trillion of devices over the Internet which can sense, communicate and actuate in the environment and among themselves. The term IoT is coined by Kevin Aston in 1999. According to an estimate, there are around 20.4 billion IoT devices till 2022 [1,2]. Extension to it, Industrial IoT(IIoT) is an intricate system of the IoT devices. To say it more precisely, it is an application of IoT in manufacturing industries [3,4]. These devices form an operational network that logically communicates with each other; accumulate, process and collaborate data and operations in real time. This helps in making intelligent production decisions, providing services and implement operational tasks [5,6]. One of the salient features of IIoT is also that they can do plain jobs like quality assessment, component assembly and connection of devices easily [1,7].

It is cardinal to bear in mind the importance of IoT when IIoT is addressed. IoT is a broad domain composed of various domains such as Health IoT, Industrial IoT, Commercial IoT and Defense IoT. IIoT is the application of IoT in industries and holds common security goals such as confidentiality, integrity and availability [8–10]. On the other side, it disassociates itself in matters pertinent to stringent requirements when different perspectives such as focus, failure implication, reaction to threat, management, deployment condition and lifespan is considered [11,12]. But still, inherently it holds some of the implicit property of IoT. This is explained by the evidence when IIoT is implemented in real-life scenarios the challenges faced by the IIoT are somehow similar to IoT and it is very common to have an IIoT device akin to an IoT device.

One of the implicit properties is known as resource constraint[13]. Some of the examples where IoT faces the resource constraint is in medical application and agriculture. The same effect is also visible in IIoT. The problem faced by these IoT devices due to resource constraints also occurs in IIoT devices. Hence, it is very important to have a grasp of IoT devices, especially characteristics, vulnerabilities and properties to develop a good understanding of IIoT devices. The loopholes that occur in IoT, might occur in the IIoT also. The methods implemented in IoT give a notion of techniques that can also be implemented in IIoT. In the same way, tools may also be utilized in IIoT. So, it is imperative to be aware of IoT together with IIoT.

Although IIoT is a part of IoT, few characteristics still make it different [11]. IoT focuses on personal asset and data protection whereas IIoT focuses on safety and prevention from an interruption in the industrial domain. A simple IoT device failure may not be harmful, but failure in an IIoT device causes production halt, discontinuation of a process and even physical threat. IoT device, in an instance of a threat, shut down itself and adopts a remediation strategy, but IIoT device do not have the leisure to do so. Instead, IIoT device only have the option of maintenance.

Further, IoT device upgrade happen during runtime where as IIoT device upgrade is scheduled during runtime only. IoT device upgrade is

* Corresponding author.
E-mail addresses: chaudharyshubhankar@gmail.com (S. Chaudhary), mishra@bhu.ac.in (P.K. Mishra).

https://doi.org/10.1016/j.comnet.2023.110015
Received 6 June 2023; Received in revised form 12 August 2023; Accepted 5 September 2023
Available online 14 September 2023

Acronyms

IoT	Internet of Things
IIoT	Industrial Internet of Things
DoS	Denial of Service
DDoS	Distributed Denial of Service
SDN	Software Defined Network
SQL	Structured Query Language
DNS	Domain Name System
IP	Internet Protocol
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
NFV	Network Functions Virtualization
ML	Machine Learning
DL	Deep Learning
IDE	Integrated Development Environment
SVM	Support Vector Machine
HTTP	Hypertext Transfer Protocol
AODV	Ad-hoc On-demand Distance Vector
RPL	Routing Protocol for Low Power and Lossy Networks
DBSCAN	Density-Based Spatial Clustering of Applications with Noise
MLP	Multi-layer Perceptron
ICMP	Internet Control Message Protocol
UDP	User Datagram Protocol
KNN	K-Nearest Neighbour
LSTM	Long Short Time Memory
PCA	Principle Component Analysis
TCP	Transmission Control Protocol
SCADA	Supervisory Control And Data Acquisition
ANN	Artificial Neural Network
AE	Auto-Encoder
RNN	Recurrent Neural Network
NTP	Network Time Protocol
GUI	Graphical User Interface
SMTP	Simple Mail Transfer Protocol
XML	Extensible Markup Language
FTP	File Transfer Protocol
TELNET	Teletype Network Protocol
FTPS	File Transfer Protocol Secure
SFTP	Secure File Transfer Protocol
SSL	Secure Socket Layer
SCTP	Stream Control Transmission Protocol
IT	Information Technology
OT	Operational Technology
BMS	Building Management System
CMMS	Computer Maintenance Management System
HMI	Human Machine Interface
LDDoS	Low rate DDoS
CNN	Convolution Neural Network
GRU	Grated Recurrent Unit
DPNN	Deep Progressive Neural Network
FL	Federated Learning
ROC	Receiver Operating Characteristic
AUC	Area under the ROC Curve
FPR	False Positive Ratio
TL	Transfer Learning
ICS	Industrial Control Systems
PLC	Programmable Logic Controller
TLS	Transport Layer Security
WSN	Wireless Sensor Network
TSN	Time Sensitive Networking
ZTN	Zero Trust Networking
DNP	Distributed Network Protocol
API	Application Programming Interface
MQTT	Message Queuing Telemetry Transport

also quick where as IIoT device take a considerable amount of time so it is scheduled for a particular moment. One of the advantages of IIoT devices are that they usually have a long lifetime about 10–15 years but IoT devices are frequently replaced when compared to IIoT devices. The reason behind this is industries want the manufacturing cost to be lower and less-time consuming where as frequently changing devices will cost more and consume time which they do not want. So they are built to last long. It is also made sure that the IIoT devices are built for harsh conditions, whereas IoT devices do not have such a necessity.

The nuanced difference in the characteristic of IIoT from IoT pushes for more stringent security requirements for IIoT. Despite this, security solutions still overlap as few of the security requirements of both overlap. This is owed to the challenges arising due to resource constraints and key distribution overlap. So it is evident that any challenges found in IoT also covers the purview of IIoT.

Notwithstanding the benefits, IIoT devices are vulnerable because of their limited storing and computational capacity [14–16]. This makes IIoT devices prone to various kinds of attacks. These attacks include malware, authentication attacks, phishing attacks, SQL injections, DNS spoofing, web application attacks and reverse engineering. Apart from the threat to the authentication, authorization and privacy of data, the threat to availability is still a major apprehension, as IoT devices substantially exacerbate the loopholes in the system with the help of Denial of Service attacks [17–19].

Denial of service means forcing a system or its resources ephemerally or everlastingly unavailable. It targets an important aspect of achieving the security goal of information security – known as "availability". Denial of service (DoS) attacks occur from a single source. Single-source DoS usually has a masqueraded IP address which floods the service with requests. A more adversarial form is Distributed Denial of Service (DDoS), in which the attacker uses various IoT devices known as "zombie machines" to flood the service with unwanted requests. "Zombie machine" is the machine recruited as a botnet during a DDoS attack. These botnets are nothing but compromised machines during DDoS attacks.

DDoS attack happens in three phases: *recruitment, code transfer* and *execution*[20]. The target of the attack depends on the motive. The motive can be financial, ideological or intellectual. It can be the result of personal antagonism or collective enmity. The target may vary from user to government. Banks, commercial organizations, e-commerce sites and gambling sites are the target of financial motives. Cyber warfare is also a motive behind DDoS attacks. These consume a significant amount of resource and time.

DDoS attacks occur on a device with the help of data packets and data packet form in most of the devices are synonymous. So, both the IoT and IIoT face the brunt of DDoS attacks regularly. Given, some implicit properties of both devices are common, the method involved in defending against a DDoS attack may also remain the same.

So, from the above discussion, it is established that security issues in IIoT are an important aspect, one of them is DDoS. This article discusses the DDoS security issue in IIoT. Here is the main contribution of this work:

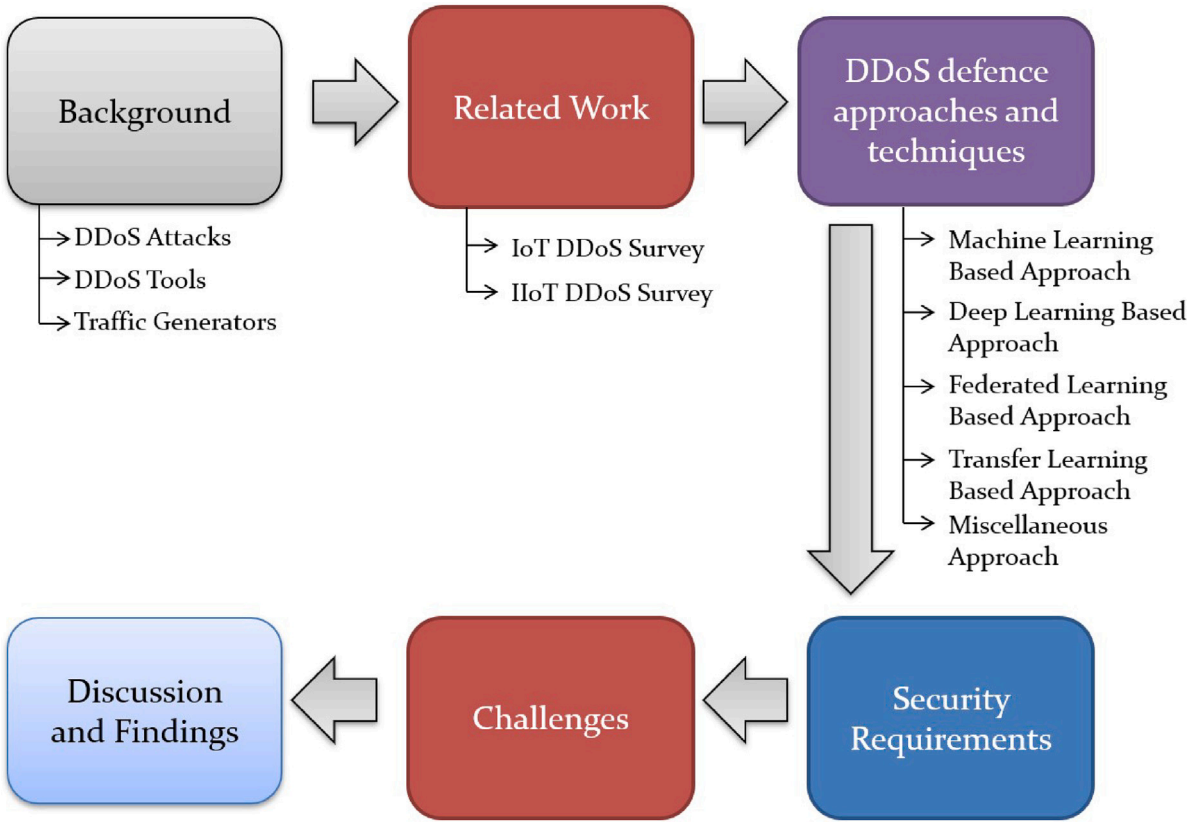


Fig. 1. Workflow of the paper.

- Different types of DDoS attacks, attack tools and traffic generators is given for the background.
- The comparative study of all the papers in tabular form(as well as in summary) is provided to give us an overview of the existing scenario of DDoS attacks and their defense apparatus in IoT and IIoT.
- The Industrial IoT architecture and the layers it encompasses is thoroughly discussed. The vulnerabilities at each layer of the architecture is pointed out.
- In this survey, the security issues in Industrial IoT and the challenges they bring with them is also illustrated.

This paper is organized as follows. In Section 1.1, motivation of the study is explained. Different category of DDoS attacks, traffic generators, attack generation tools are discussed in Section 2. Previous studies analogous to DDoS attacks are discussed in Section 3. IIoT architecture, datasets and network simulators are discussed in Section 4. Studies related to DDoS defense approaches and techniques are discussed in Section 5. The security requirements for Industrial IoT are discussed in Section 6. The challenges deriving from IIoT are discussed in Section 7. Finally, discussions and findings of the study are concluded in Section 8 (see Fig. 1).

1.1. Motivation

The erstwhile papers which studied IIoT security have covered the topic in a generalized way. Their work towards a specialized type of attack is perfunctory. Initial studies merely focused on IIoT layers, the possible attacks, its taxonomy and thus the security requirements of IIoT [3,8,24]. Then the focus shifted to the challenges propping up from it [21,22]. Thereafter, the focus was the classification of the attacks happening in contemporary networks [17]. But still, not every attacks were meticulously studied such as DDoS attacks (see Table 1). Though the DDoS attack was underlined to be one of the concern in IIoT, it was discussed just apparently in previous studies. So, there is a need to understand the DDoS attack in the IIoT whole hog.

Given the state of research in the field of DDoS attacks, much attention is also needed in IIoT domain. Medical applications, smart grids and networking field have explored about the DDoS attacks. But the IIoT domain has largely remained untouched. Given the significance of industries in the economy and its kinship to the development of the society, this domain requires more serious attention and direction[25].

Also, it is necessary to understand the behaviour of the system and threats in IIoT to prevent the industrial components from any affliction caused by the DDoS attacks. Therefore, in order to fill these voids, this article explains DDoS attacks categorically, to detail its effect and consequences in preceding studies and also to derive the essential security requirements and challenges in contemporary circumstances.

Through this article, the researchers who intend to pursue their research in this emerging field can find an in-depth insight about IIoT, its components and the gap present in the preceding studies. This article highlights various propositions combined in a single place that other articles forget to mention or discuss at segregated places. Hence, this article acts as a harbour to get future reference to the research area. Overall, this article provides a glimpse of the necessary knowledge obligatory of DDoS security in IIoT. This article also helps disseminate chronological progress made in this field from the beginning and fathom the shortcomings in the methods implemented till now so as to provide better results in the future.

2. Background

This section gives brief knowledge about the kind of DDoS attacks occurring and various kinds of tools needed in generating these attacks. We have also discussed the traffic generators in this section.

Table 1
Comparative studies with different IIoT surveys.

Reference	Year	DDoS attacks	Challenges	Security Requirement	Classification	Interoperability
Panchal et al. [3]	2018	No	No	Yes	No	No
Yu et al. [21]	2019	No	Yes	No	No	No
Shah et al. [17]	2020	No	No	No	Yes	No
Tange et al. [8]	2020	No	No	Yes	No	No
Sengupta et al. [22]	2020	No	Yes	No	Yes	No
Hazra et al. [23]	2021	No	No	No	No	Yes
Our paper	NA	Yes	Yes	Yes	Yes	No

2.1. DDoS attacks

In this section, the different ranks of DDoS attacks prevalent in the IoT and IIoT environment are explained.

2.1.1. UDP attack

In this kind of attack, the victim server is overwhelmed by the UDP datagrams. First, the server checks the port for which the sender has requested. If the requested port is empty, the request is granted. But the application program for the requested port turns out to be empty so an error occurs. Subsequently, the server sends an error ICMP packet to the sender. But the sender is generally a botnet, the IP addresses are spoofed. Hence, the response is never received by the sender. When these kinds of requests are granted enough, the resources of the server get consumed and the genuine request is declined [26].

2.1.2. ICMP flooding attack

In this attack, the victim device is targeted through the ICMP requests. The victim's device bandwidth is consumed by the illegitimate requests of attackers. The victim's device is not able to service the genuine request as it remains busy reporting the error and management control messages of illegitimate requests [27].

2.1.3. TCP SYN flooding attack

In this attack, the TCP three-way handshake method is used. TCP is a connection-oriented protocol. So it seeks to establish a connection before carrying out any data transfer. The sender sends a SYN connection request to which the victim server responds with a SYN-ACK message. But the IP address is spoofed so the connection establishment ACK message is not received back from the sender. Hence, the resource gets consumed. With this kind of attack done at frequent intervals of time, all the server resources get consumed making the service unavailable [28].

2.1.4. Ping of the death

Ping of the death is a kind of DDoS attack in which the sender sends a packet that is larger than the size of the target victim's processing capability. This makes the processing ability of the victim ineffective and the victim technically crashes or freezes. While in transmission the size of the IP packet remains within the defined limit but after getting received and getting combined in a particular process, the size of the packet exceeds the limit [29].

2.1.5. HTTP flood attack

This is a kind of resource depletion attack applied to the application layer. In this attack, botnets are used to send HTTP GET requests to the victim server. On receiving a request, the server processes the request, checks the back-end, intra-transfers the data and then transfers it to the botnet via the same link. When these requests are sent in large amounts, it depletes the resource on the server. And the server becomes unresponsive to the genuine requests. More generally, the attacker manipulates the HTTP GET and HTTP POST messages for DDoS attack [30].

2.1.6. NTP amplification attack

It is an amplification attack in bandwidth depletion attack. The NTP server is used to synchronize the clock of the machines connected to the server. The attacker spoofs the IP address of the MON_GETLIST command. The response of this command is 600 previous queries to the server which are significantly larger than the query itself. Multiple requests of this query cause amplified response subsequently causing the bandwidth to be consumed [31].

2.1.7. Smurf attack

In this kind of attack, an ICMP echo request is sent to the network with the spoofed IP address of the victim by the cybercriminals. The IP message is broadcasted to every device on the network. Every device of the network, on receiving the echo request, replies with an echo reply message to the spoofed IP address. All the reply is directed towards the victim's IP, consuming all the resources of the victim. Hence, causing the DDoS attack [32].

2.1.8. TCP reset attack

In a TCP reset attack, the attacker forces two communicating nodes to terminate the connection by sending a forget TCP reset packet. It kills the linkage between the two victims. This attack occurs using a single packet of data. The attacker sends a TCP reset segment. Although it is tough, the attacker creates the right spoof segment and tricks the victim to accept it as valid. Later, it is used to disconnect the communication between victims [33].

2.2. Ddos tools

DDoS attack tools are used to set up the attack traffic in the network. Attack generation is a necessary phenomenon required for any kind of testing, training or validation. So it is discussed below. In conjunction with this, the comparative study has also been explained in Table 2.

2.2.1. Stacheldraht

It is a command-line agent-based mechanism implemented in C language. It was created by the Austrian group TESO in 1999. It is used in Linux and Solaris operating systems (OS) and uses ICMP and UDP traffic for DDoS attacks. It involves compromised machines known as Botnets to direct ICMP flood, SYN flood, UDP flood and smurf attacks towards a victim. Both kinds of bandwidth, as well as resource depletion attacks, can be done using this tool [34].

2.2.2. Trinoo

This tool also has an agent-handler-based model. It has a master–slave concept in which the master instructs the slaves to attack the victim. In this, slaves are the ones who broadcast the attack to the victim as per the instruction received by the master. It uses UDP, TCP and HTTP packets in Linux and Solaris. It has a command line interface. With this kind of tool, only bandwidth can be targeted. It was written in C by a teenager [35].

Table 2
Comparative study of DDoS Tools.

DDoS Tools	Affects	Advantage	Disadvantage	Type of traffic	Data concealing?
Stacheldraht	Bandwidth, Resource	Detects source address forgery.	Cannot replicate itself. Manual distribution required.	ICMP, UDP	Yes
Trinoo	Bandwidth	Self replicating.	Some encrypted passwords, prompts and return strings are easily identified.	UDP,TCP, HTTP	Yes
Tribe Flood Network	Bandwidth, Resource	Automated deployments of TFN daemons and leverages different bandwidths.	Needs intruder-supplied list.	TCP, UDP, ICMP	No
Trinity	Bandwidth, Resource	High rate of compromising hosts	The attacker data is not encrypted.	TCP, UDP	No
Mstream	Bandwidth	Effective with few agents also.	Primitive and incomplete feature set.	TCP, UDP, ICMP	No
Shaft	Bandwidth, Resource	Uses handler and different communication protocols between components.	Belongs to same family of above tools.	TCP, UDP, ICMP	No
Kaiten	Bandwidth, Resource	Uses random source address.	Works in windows operating system only.	TCP, UDP	No
Knight	Bandwidth, Resource	Lightweight, powerful, automatic updater.	Works in windows operating system only, data is also not encrypted.	TCP, UDP	No
Black Energy	Bandwidth, Resource	Uses runtime encrypter to avoid antivirus.	Initial versions were dependent on external tools.	TCP, UDP, ICMP, HTTP	No
Hgod	Bandwidth, Resource	Handling is easy.	Works in windows operating system only.	TCP, UDP, ICMP	No
RefRef	Resource	Uses features included in MySQL.	Works in windows operating system only.	–	No
LOIC	Resource	Easy to use and recruit new fellows.	Well scripted firewalls can stop it.	TCP, UDP, ICMP	No
DDoSim	Resource	Uses random IPs with full TCP connection.	The attacker data is not encrypted.	TCP, UDP, SMTP, HTTP	No
TOR's hammer	Bandwidth, Resource	DDoS attacks of anonymized nature can also be done.	Works in TOR network.	HTTP	No
Davoset	Resource	Bypasses protection of web applications.	Only used for linux.	HTTP	No
Pyloris	Resource	Exhausts all the connections.	The attacker data is not encrypted.	TCP, UDP, IMAP, SMTP, HTTP, FTP, TELNET	No
XOIC	Resource	Can target selected IP, port and protocol.	Works in windows operating system only.	TCP, UDP, ICMP	No
Aldi Botnet	Resource	Low cost.	Works in windows operating system only.	HTTP, TCP.	No
R-U-DEAD-YET	Resource	Uses random time intervals.	Works slow.	HTTP	No
HOIC	Resource	Hides geolocation and attack traffic is scatered.	Works in windows operating system only.	HTTP	No
Hulk	Resource	Takes down a server in a minute.	Uses single device for attack.	HTTP	No
Silent ddoser	Bandwidth, Resource	Runs at startup and can update all the bots in one go.	Works in graphical user interface only.	TCP, UDP, HTTP	Yes
SEER	Resource	Generates many variation of same traffic	Works in graphical user interface only.	TCP, UDP, ICMP	No

2.2.3. Tribe flood network

It is a command-line-based handler-agent-based tool implemented in C language. It can also create a series of attacks such as ICMP, SYN, UDP flood and smurf attack in Windows and Linux OS. It was written by a Germany-based security professional named Mixter. It can target the victim's bandwidth as well as resource [36].

2.2.4. Trinity

It is an Internet Relay Chat (IRC) architecture-based tool. It is also command-line based but only for Linux-based platforms. It impacts both bandwidth as well as resource depletion attacks using TCP and UDP traffic. It involves multiple bots. It launches TCP, SYN and RST attacks [34].

2.2.5. Mstream

It is a command line interface-based DDoS apparatus build in C language. It is a point-to-point attack tool. It uses botnets to perform DDoS attacks. It works on Linux and Windows both and creates UDP, TCP and ICMP traffic. It uses a spoofed IP address to create TCP ACK and TCP RST flood towards the victim device. It can also consume the victim's bandwidth as well as resource [37].

2.2.6. Shaft

It is also a command line-based DDoS attack in Unix and Linux environments. It has an agent-handler architecture. It uses botnets to create UDP, TCP and ICMP floods for DDoS attacks. These floods observes the status of the victim machine and reports to the attacker. It is derivative of Trinoo [37].

2.2.7. Kaiten

Kaiten is an IRC architecture-based DDoS attack model. It uses UDP, TCP, SYN and PUSH+SYN flood to perform a DDoS attack. It uses a spoofed IP address It is a command-based attack and works in Windows only [34].

2.2.8. Knight

It is also a Windows-based DDoS tool. The attack model is IRC based. It is made in C and can attack both bandwidths as well as resources of the victim. It uses UDP, TCP and urgent pointer flood. It is a command line-based attack [37].

2.2.9. Black energy

It is a command line-based tool based on the IRC model. It uses TCP, UDP, ICMP and HTTP flood methods to implement the DDoS tool. It is a Linux-based model and has the capacity to choke bandwidth as well as resources. It uses multiple botnets to perform DDoS attacks [34].

2.2.10. Hgod

It is a Windows-based DDoS attack tool. It creates multiple botnets for DDoS attacks. It uses TCP, UDP and ICMP floods for depleting the bandwidth and resources of the victim. It has an IRC-based model. It uses the command line interface and spoofs the IP address [34].

2.2.11. RefRef

It is a window-based DDoS tool that is used to consume the resource of the victim. It has an IRC based model and uses a command line interface. It is written in PERL language. The main aim of this tool is to exploit the pre-existing SQL injection vulnerabilities. It manipulates the victim with SQL queries which make the victim exploit its resources [34].

2.2.12. LOIC

LOIC stands for Low Orbit Ion Cannon. It is a GUI-based resource depletion DDoS tool. It works mostly on all operating systems such as Windows, Mac, Linux and even Android. It is an open-source tool and written in C#. It was initially launched by Praetox Technologies. It uses TCP, UDP, ICMP and HTTP packets to target the server with DDoS attacks. It can be used by multiple individuals [38].

2.2.13. DDoSim

This is also a resource depletion attack tool, but it is only compatible with the Linux operating system. It has a command line interface and is written in C++. It uses TCP, SMTP, HTTP and UDP packets for DDoS attacks and uses multiple devices to perform it [38].

2.2.14. TOR's hammer

It is an agent-based model and has a command-line interface. It spoofs the IP address with random IP to make the trace of the source machine difficult. It works through the TOR network and is built on Python. It targets both the bandwidth and resources. It uses HTTP flood from multiple devices for the attack on Unix, Linux and Mac operating systems [37].

2.2.15. Davoset

It is a DDoS attack tool that utilizes XML and its functionality vulnerabilities. It uses a command line for attack and is built using the PERL language. It requires multiple machines to perform a DDoS attack. It only targets resource depletion of the victim machine and is used in Linux operating system only [37].

2.2.16. Pyloris

It is an IRC-based model built in Python language. It uses the inherent functionalities of the Solaris operating system and is used to check the readiness of the server. It is used for resource depletion attacks. It tests the service level vulnerability of a particular type of DDoS attack only. It uses TCP, IMAP, UDP, SMTP, HTTP, FTP and TELNET for flooding. It works in Linux, Windows and Mac OS and has a command line interface [38].

2.2.17. XOIC

XOIC is a C# sharp-based DDoS attack tool. It includes a graphical user interface (GUI) and is an IRC-based model. It uses TCP, HTTP, UDP and ICMP packets for attack. It works in Windows only. It is used for resource depletion attacks in which multiple devices are required. It is more powerful than LOIC as it can perform DDoS attacks with specific IP addresses and user-selected ports and protocol [38].

2.2.18. Aldi Botnet

Aldi Botnet is GUI based and Web-based tool for DDoS attacks. It is used for the resource depletion of any victim. It is a Windows-based tool that utilizes HTTP and TCP packets using multiple elements [39].

2.2.19. R-U-DEAD-YET

RUDY is the acronym used for the R-U-DEAD-YET tool. It is a Python-based tool and a single device is required. It uses a command line interface in Linux and only targets the resource of a victim. It uses HTTP packets for DDoS attacks. It is a slow tool to crash the victim [37].

2.2.20. HOIC

HOIC stands for High Orbit Ion Cannon. HOIC is a graphical user interface attack tool developed in BASIC specifically for Windows. It is a multi-thread and high-speed attack tool. Multi-threading allows it to communicate or flood it with 256 devices in a single instance. It uses HTTP GET and POST packets to flood the devices. It basically targets the resource of the victims [38].

2.2.21. Hulk

Hulk is a Python-based command line interface tool that uses HTTP packets for DDoS attacks in Linux and Windows. It involves a single device for the attack. It targets the resource of the victim. This tool is very effective in taking down a victim in a minute as it undeviatingly targets the victims. It uses TCP SYN, HTTP GET flood requests. It sends a variety of packets that hides the true personality of the attacker [37].

2.2.22. Silent ddoser

It is a DDoS attack tool that uses UDP, TCP and HTTP flood to deplete the resource and bandwidth of the victim. It is carried out by multiple devices and uses botnets also. This tool is built in Visual Basic and has a graphical user interface. It has an IRC-based model [39].

2.2.23. SEER

This DDoS attack tool targets the resource of the victim. It uses ICMP, TCP and UDP flood from various devices to perform the attack. It creates bots also. It is built in the Java programming language and has a graphical user interface. It uses two tools FLOODER tool and the Cleo tool. First was developed by SPARTA and the other was developed by UCLA. In this method, the traffic movement is also visible [39].

2.3. Traffic generators

Traffic generators are those components that can generate legitimate(normal) as well as illegitimate(attack) traffic. These have been discussed below and their comparative study has been discussed in Table 3.

2.3.1. D-ITG

It is a C++ based HTTP, TCP/IP generator. It uses a command line interface and is supported by Linux, Windows and BSD operating systems. It uses the inter-departure time and packet size as input parameters to precisely generate the traffic. It is proficient in bringing forth traffic at the network, transport and application layer. This generator effectively generates IPv4, and IPv6 traffic [40].

2.3.2. Pylot

Pylot is a graphical user interface-based application layer traffic generator. It generates HTTP and HTTPS traffic in Windows, Ubuntu and MAC OS for analysis purposes. It generates traffic on the basis of request intervals, number of agents, ramp-up time and test duration. It has the capacity to use generate traffic through multiple devices and get observations such as real-time status, results and reports with graph [39].

2.3.3. RUDE

RUDE stands for Real Time UDP Data Emitter. It generates the traffic for the transport layer and provides a graphical user interface. It is developed in C and is made for Linux only. It considers servers, clients and protocol as input parameters for creating traffic. It generates real-time UDP data which can be verified, logged and collected at receiving side known as CRUDE [38].

2.3.4. Geist

It is a window-based traffic generator that is implemented in C and holds the ability to generate HTTP traffic of the application layer. It is a command line-based tool whose scope is limited to HTTP requests only [41].

2.3.5. Bit-Twist

Bit-Twist is a command line-based traffic generator that is used in Linux, Windows and Mac OS. It generates TCP, UDP, IP and ARP packets which are generally the traffic of the network and transport layer. It keeps the traffic packets in a trace file and sends them according to the requirement in size and speed. It is a very powerful ethernet packet generator [38].

2.3.6. Curl loader

It is a C programming language-based traffic generator. It uses a command line interface and works on Linux only. It generates HTTP, HTTPS, FTPS and FTP traffic. It can test load also. It considers the client, IP address range and interface for generating traffic. It generates transport and application layer traffic [38].

2.3.7. LAN Forge Fire

LAN Forge Fire is a graphical user interface traffic generator built on Java. It works in Linux, Windows, and Solaris. It can generate HTTP, HTTPS, FTP, TELNET, SFTP and TFTP traffic in the application layer. It uses client, source and packet information for generating traffic. It requires a TCP connection and provides effects such as latency and jitter [39].

2.3.8. Byte-blower

It is a TCL-based traffic generator that has the capacity to generate IP and TCP packets. It basically checks the stability and performance of IP networks. It uses protocols and latency as input parameters in Windows, Linux and MAC operating systems. Traffic is generated for data link, network and transport layer [42].

2.3.9. Netperf

It is a command line-based tool built in C language. It is used to build BSD, UDP, SCTP and IP traffic in the network and transport layer. It is used to test the end-to-end latency and only unidirectional throughput [43].

2.3.10. Harpoon

Harpoon traffic generator generates HTTP, UDP, TCP and IP traffic in the data link, network and transport layer. It works in a Unix environment. It considers the following parameters for traffic generation: Number of nodes in the network, file size, server session, server port, session, thinking time and file size [39].

2.3.11. HTTP-Perf

It is a command line interface traffic generating tool. It is used to check the performance of the server. It is used in Linux and Unix and generates HTTP and SSL packets. It requires traffic parameters such as the number of headers, number of clients, timeouts and maximum number of connections. It checks the server's performance and generates HTTP-GET request [38].

2.3.12. Tmix

This traffic generator generates realistic transport layer traffic in the Linux operating system. It is a Network Simulator(NS-2) based TCP and IP traffic generator. It is used only in transport layer traffic generation [39].

2.3.13. Trafgen

It is a C-based traffic generator that is used to generate HTTP traffic in Linux. It is a command line-based tool used to generate application layer traffic. It is a multi-threaded network traffic generator having fuzzy testing potential capacity. This generates traffic faster to debug and to do performance evaluation [39].

2.3.14. Webstone

Webstone is implemented in C language. It is a command line-based HTTP traffic generator which works in Windows, Solaris and Unix operating systems. It generates traffic on the basis of the number of minimum clients, time per run and iterations. It is also used to measure the performance of hardware and software products [39].

2.3.15. Seagull

It is a very strong traffic generator made in C++ programming language. It provides a command line interface and provides all the new protocol support such as TCP, UDP, IP and HTTP. It can create all these traffic within two hours without any prior programming knowledge. It works in the network, transport and application layer. It provides a variety of functional, stress, load, endurance and performance tests in dynamic scenarios also [38].

2.3.16. Packmine

Packmine is a network simulator-based tool that was developed by a research group of Bell Labs. It generates the HTTP traffic for the transport and application layer in the Linux operating system. Its capabilities include identifying bottleneck links, loss rate and simulating different round trip times. While generating traffic, the generator considers request size, request rate and client parameters [44].

2.3.17. KUTE

The implementation of this tool is done in C and it is a kernel-based traffic engine. It generates UDP traffic in the transport layer. It has KUTE-REC and KUTE-SEC. KUTE-REC takes the input parameters such as received packets, inter-arrival time and can measure high packet rates. KUTE-SEC has the ability to generate a high packet rate [45].

Table 3
Comparative study of Traffic Generators.

Traffic Generators	Implementation Language	Advantage	Disadvantage	Type of traffic
D-ITG	C++	Generated both IPv4 and IPv6 traffic.	Works only for transport and application layer.	HTTP, TCP/IP
Pylot	Python	Utilizes multiple devices to ramp-up traffic.	Operates only for application layer.	HTTP, HTTPS
RUDE	Linux	Real time traffic is verifiable at receiver end.	Works in linux only and used for transport layer traffic.	UDP
Geist	C	Handles cookies and generates dynamic GET parameters.	Generates only HTTP traffic and runs on Windows only.	HTTP
Bit-Twist	–	Powerful in generating ethernet packets with high speed.	Generates traffic for network and transport layer.	TCP, UDP, IP, ARP
Curl Loader	C	Adjustable tool. Can test the load also.	Linux based, only for transport and application layer traffic.	HTTP, HTTPS, FTP, FTPS
LAN Forge Fire	Java	Supports jitter, lantency, packet and bandwidth loss.	Only for application layer traffic.	HTTP, HTTPS, FTP, TELNET, SFTP, TFTP
Byte-blower	TCL	Provides real-time view for traffic.	Written in TCL.	IP, TCP
Netperf	C	Good for unidirectional throughput and end-to-end latency.	Only for network and transport layer.	TCP, UDP, SCTP, IP.
Harpoon	–	Runs over HTTP and application layer	Works in unix environment.	HTTP, UDP, TCP, IP
HTTP-perf	–	Robust, extendable and supports different protocol.	Works for application layer only.	HTTP, SSL.
Tmix	NS-2	Embedded and works on network simulator(NS-2)	Used in transport layer traffic only.	TCP, IP.
Trafgen	C	Tests fuzzy system also.	Only linux based.	HTTP
Webstone	C	Measure the performance of hardwares and softwares.	Only generates HTTP traffic.	HTTP
Seagull	C++	Generates traffic in two hours without prior traffic knowledge.	Doesnot work in Windows.	TCP, UDP, IP, HTTP
Packmine	NS	Can find bottleneck links and loss rate.	Used only in linux.	HTTP
KUTE	C	Kernel based traffic engine	Generated only transport layer UDP packet.	UDP
SEER	Java	Script writing, experimentation and visualization of traffic.	Scalling up ,high speed traffic generation is not possible.	TCP, UDP, HTTP, ICMP
TCP replay	C/C++	Generates network layer traffic by embedding in Deter testbed.	Works in Unix and Win32.	TCP/IP
Surge	HTTP	Performs distribution of files	Works only on application layer.	–
Ostinato	Python	Cross-platform traffic generator.	Cannot generate application layer traffic.	HTTP, HTTPS
M-GEN	NS-2, TCL	Can be used in NS-2 and OPNET.	Doesnot support application layer traffic.	TCP, UDP, IP
Iperf	Java	Used for maximum achievable bandwidth in IP.	Not for application layer traffic.	TCP, UDP, SCTP

2.3.18. SEER

SEER stands for Security Experimentation Environment. It is a java based graphical user interface tool which can spawn TCP, UDP, HTTP and ICMP traffic. SEER is supported in Windows, Linux and Unix. It takes server IP and client IP as input parameters and can generate legitimate traffic and DDoS traffic. It can visualize the traffic also [39].

2.3.19. TCP replay

It is a command line-based tool, best suitable for intrusion detection and prevention system, is also used as a network layer traffic generator. It is built in C and IP traffic generator. It is based on command line interface for the Unix operating system. It is embedded in Deter testbed. It considers server and client port numbers and IP addresses

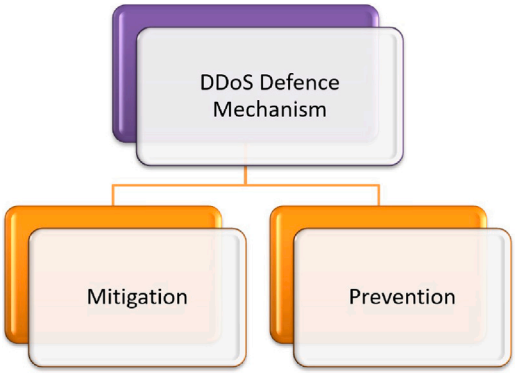


Fig. 2. DDoS defence mechanism.

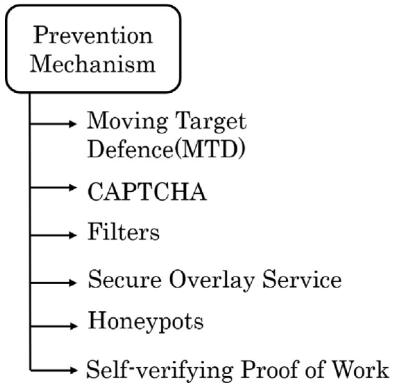


Fig. 3. Prevention mechanism.

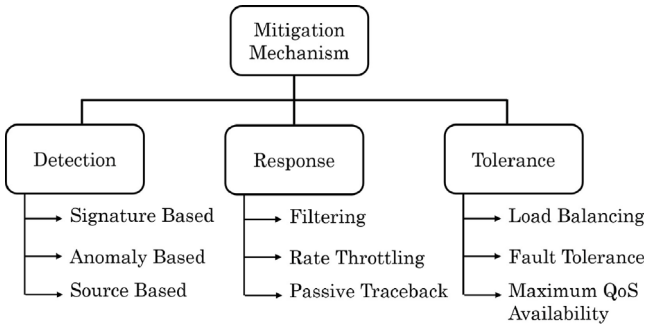


Fig. 4. Mitigation mechanism.

for generating traffic. It is a very reliable tool for testing network components such as firewalls, routers and switches [39].

2.3.20. Surge

Surge is an application layer traffic generator that generates and uses HTTP traffic in the application layer to do various distribution jobs such as request size distribution and file size distribution. It can perform reference matching and find file popularity and embedded file Refs. [46].

2.3.21. Ostinato

Ostinato is a Python-based traffic generator. It is capable of generating TCP, ICMP and UDP traffic. It works on Windows, Linux and Mac operating systems and provides a graphical user interface. It generates traffic for the network and transport layer. It has certain advantages as well, for example, it is a cross-platform traffic generator which means it can create different flows of protocols and at different speeds as well [47].

2.3.22. M-GEN

M-GEN is a TCL-based traffic generator which is used in Unix, MACOSX and Win32. It generates TCP, UDP and IP traffic. It provides a command line interface and generates traffic for the network and transport layer. It can be used in NS-2 and OPNET. It supports IPv6 networking, statistical patterns, transport patterns, message count, payload enhancement and TCP messaging [39].

2.3.23. Iperf

Iperf is a java based traffic generation tool. It works in Windows, Linux, MacOS, BSD and can generate TCP, UDP, SCTP traffic. It generates traffic for the network and application layer. It is a multi-thread generator and utilizes multiple connections for client–server. It is used for testing the maximum achievable bandwidth in the traffic [48].

3. Related work

To secure our devices from DDoS, the defence mechanism used conventionally is basically of two types: prevention and mitigation (see Fig. 2). Prevention of an attack is done before an attack has happened whereas mitigation of an attack is done after the attack has happened, with the help of detection, response and tolerance.

Prevention is a proactive defence technique whose task is to contain and phase out the ramification of DDoS attack. One of the most intermittently used prevention methods is Moving Target Defence (MTD) which uses the concept of dynamic surface. This method makes the attack surface dynamic such that the location of the device is not discoverable, if a vulnerability is already discovered. Dynamic attack surface can be hidden proxies, dynamically changing port numbers and IP addresses [49]. Other prevalently used methods are Completely Automated Public Turing Test (CAPTCHA), EDoS-Shield mitigation which uses the challenge response method [50], Self-verifying Proof of Work (SPoW), DNS based technique, filters [51], secure overlay service [52] and honeypots [53] (see Fig. 3).

Detection of an attack is labelling a malign traffic without unsettling and incorrectly classifying the permissible traffic. The labelling is done by identifying a signature [54], an anomaly [55] and the source of the traffic [56]. Response, on the other hand, is the method adopted after detection of an attack. In this method, we clog the malicious traffic. This method aims to find the malicious traffic source, but this task is difficult in practice. Hence, methods such as filtering [57], rate throttling and passive traceback is used in the traffic. Tolerance is another method used to diminish an attack repercussion. It is used when other methods cease to mitigate the effect of the attack. This method uses load balancing [58], fault tolerance [59] and maximum QoS availability to mitigate the DDoS attack (see Fig. 4).

Since, the IoT and IIoT are highly interrelated and IIoT is an extension of IoT, the discussion of the Distributed Denial of Service(DDoS) attacks and their defense mechanisms in both scenarios is discussed below.

3.1. Internet of things

Internet of Things(IoT) is an interconnection of trillion of devices over the Internet which can sense, communicate and actuate in the environment and among themselves [60]. They are light weight. Due to storage and processing constraints, they have certain vulnerabilities. Hence, DDoS-related studies in IoT is discussed below.

3.1.1. IoT DDoS survey

Prevention in IoT Papers studied in relation to IoT prevention are discussed below and compared in Table 4.

Table 4
Prevention in IoT.

Reference	Year	Topic Discussed	Merit	Demerit	Proposed Method	Tools	Output	Approach
Rambabu et al.[61]	2021	Preventing DDoS attack in IoT network	Incremental classification strategy	Feature optimization method and classification method is not used to improve DDoS attack detection accuracy	Ensemble Classification of traffic flow metric	IDE	Has more defence accuracy and less false alarm.	ML-based.
Huang et al.[62]	2021	Preventing DDoS in IoT using data mining technology.	Predeter-mines the attack. Predicts the timing of the attack.	Parameters are not adjusted and optimized.	SVM algorithm	IDE and IP tracking technology such as Wireshark, etc.	71%accuracy with traffic indicator and remodelling makes it 82% accuracy.	ML-based.
Haque et al.[63]	2021	Discusses the single point SDN infrastructure failure problem to prevent DDoS.	Multiple SDN smart backup controllers.	Does not discusses about information pillage, network hindrance properly.	RTZLK-DAASCP smart controller algorithm.	AMPL programming language, IBM ILOG CPLEX system	Overall cost is very less.	Algorithm based.

Rambabu et al. [8] discussed prevention of the IoT devices from DDoS attacks. Since the attack is not stable because of variable rates, signature-based detection mechanism is unfeasible. So, the attainable solution is the anomaly-based detection method. But the optimal solution is approachable when attack behaviour with respect to time is considered combined with anomaly-based detection. Due to this, short-term estimates replace long-term analysis.

Huang et al. [62] discusses DDoS attacks in IoT devices. First, the author suggests IDS and IPS for detecting and blocking scores of attacks in the databases. This is called traffic cleaning and filtering. Also, a defence strategy in IDS and IPS is used to monitor and track traffic. In order to provide further control, SDN insulates the control layer and data layer. Further, SDN can incorporate NFV to separate network functions from network equipment. But in order to prevent DDoS attacks in real time data mining technology is used to classify and correct the result in real-time. Prediction model – construction module is for classification and the prediction defence module is for correct results in real-time.

Haque et al. [63] discusses DDoS attacks in the SDN environment. As the controller in the SDN is the brain of the network, any attack on the controller can have serious consequences. The author gives various examples of the challenges deriving from the controller of the SDN such as network hindering, switch information pillage and management classification. So, the assurance of SDN networks working properly is essential. So, the author proposes an algorithm that calculates the number of additional controllers required to deploy SDN when DDoS occurs.

Mitigation in IoT Papers studied in relation to IoT mitigation is discussed below and compared in Table 5.

Critic et al. [64] implements machine learning and deep learning algorithms to analyse the DoS and DDoS attacks in IoT devices. It is concluded that deep learning algorithms are preferred over machine learning algorithms while detecting DDoS. Machine learning algorithms are good in relatively less data traffic whereas deep learning algorithms are the best choice when abundant resources and huge data transfer platform are present. They are good for security-related jobs.

Huraj et al. [65] discusses an anomaly detection model to detect the DDoS traffic generated. For this, the author uses the class affiliation process. Network traffic is said to be suspicious if it does not follow the usual traffic. Usual traffic classes are generated that conform to already generated traffic features. Features are selected carefully that are supposed to be stable. An appropriate traffic profile of a class is created by IoT devices initially associated with that class. This profile is used to compose a model that increases the efficiency of machine learning methods.

Kumar et al. [66] checks the defiance of IoT sensors against the DDoS in the smart home environment. But this has been done in the opposite way. It is observed how the sensors behave when they come under a DDoS attack. IoT devices are tested under SYN flood attack and HTTP Get flood attack under three different scenarios. And it is found that communication of IoT sensors through smart-home assistants is the safest way as it resists most DDoS attacks. It further states that their nature needs to be studied in the cloud computing environment.

Doshi et al. [67] discusses a stealthy DDoS attack named Mongolian DDoS which is the result of scattered nature and modest size of each source. The author also tells us about the vulnerabilities in internet services and cyber–physical systems. So, he proposes an emerging threat model for hierarchical IoT networks to give an anomaly-based Intrusion Detection System which detects and mitigate the emerging type of DDoS attack.

Mohapatro et al. [68] studied the DDoS and sinkhole attack on IoT environment, especially in the healthcare environment. The author suggested that these attacks make huge information loss and make the network vulnerable. These attacks are considered under the context of AODV and RPL protocols under which wireless IoT healthcare applications work. In this, different network models are analysed and how their network parameters are impacted. Different detection strategies are suggested based on channel and energy consumption.

Lee et al. [69] studies the vulnerabilities of wireless IoT devices, particularly through the Simple Service Discovery Protocol (SSDP). This protocol is used to search IoT devices. The author uses the vulnerability in the communication protocol of the respective IoT device. The author performs a test and directs the traffic using a reflection attack to block the web services. The author also tests the level of threat. Finally, the author proposes a method to dislodge IoT vulnerabilities in DDoS attacks which is cardinal for the exertion of a multi-level defence system.

Aljuhani et al. [70] discusses how DDoS defence systems are transformed into intelligent and smart systems by using machine learning techniques. The author studied a single or hybrid ML approach in

Table 5
Mitigation in IoT.

Reference	Year	Topic Discussed	Merit	Demerit	Proposed Method	Tools	Output	Approach
Critic et al.[64]	2021	Novel method of detecting IoT generated DDoS.	Novel approach to detect DDoS supporting advanced devices other than just the conventional ones.	Does not focuses the traffic features on time stability of send and receive data ratio feature over time	Conceptual network traffic anomaly detection model	Network Simulator, Gateway	Boosts machine learning method to determine traffic deviation due to DDoS attacks.	ML-Based
Huraj et al. [65]	2020	IoT sensors in smart home environment under DDoS attack.	Gives various comparative analysis of different communicating components.	It is the reverse point of view, how the sensors behave when an DDoS attack occurs.	Flooding the communication between IoT device and IoT sensors with DDoS attacks	Ansible real-time attack environment, Controller and Sensors.	IoT with smart home assistants are the safest to resist DDoS.	Not Applicable.
Kumar et al. [66]	2022	Analysis of DDoS attack in IoT.	Comparison of DL and ML methods in detecting DDoS.	No cloud support yet.	Various learning algorithm KNN, stacking algorithm, Random Forrest, etc.	ARGUS software, Testbed with 20 devices.	Attack classification DL - 99.9, ML – 99.5	Both ML and DL based.
Doshi et al. [67]	2021	Mitigation of Stealthy DDoS in IoT.	Supports distributed and stealth attacks	Less robust to attacks, IDS is trained only once and packet size does not represents real characteristics of network.	Emerging threat model for hierarchical IoT networks	IoT Devices, Python Programming Language	Anomaly based Intrusion Detection System.	Algorithm based.
Mohapatro et al. [68]	2021	DDoS in IoT based healthcare.	Reviews various network parameters and also suggests detection strategies of DDoS on the basis of those.	IoT Healthcare applications are assumed under AODV and RPL protocols only.	Simulating different network models through NetSim.	NetSim simulator environment, Static sensors, Base Stations.	Detection strategies based on channel and energy consumption.	Observation based.
Lee et al. [69]	2021	Methods against large scale reflection DDoS attack in IoT	Includes a method involving DDoS blocking pattern that is used in removing IoT vulnerabilities	It is a countermeasure, not a predefined method.	UPnP function , Large scale traffic control, Destination address control, Web program attack control.	Simple Service Discovery Protocol (SSDP), L2 and L7 protocol.	Multilevel defence system for communication protocol.	Protocol Based.
Aljuhani et al. [70]	2021	Machine Learning method of combating DDoS in IoT.	Includes virtualised environment such as cloud, SDN and network function virtualisation	Lightweight, Delay in detection, Attackers mimicking normal user's behaviour can know the threshold of detection model.	Machine learning and deep learning algorithms.	Single or hybrid ML approach. Transforming DDoS defence systems into intelligent and smart systems	Comparison of DDoS defence system in cloud, SDN and NFV environment.	ML- based.
Trajanovski et al. [71]	2022	Automated Behaviour- Clustering of IoT Botnets	Helps in automatic identification IoT variants with new capabilities	Clustering algorithm shows 90% of the samples collected shows generic IoT botnet behaviour and does not support android malicious codes.	DBSCAN algorithm.	Behaviour Profiles, Sandbox, Python	It keeps pace with growing risks and helps researchers enormously.	ML-based.
Wang et al. [72]	2021	DDoS in SDN based IoT network using secure control and data plane algorithm	SDN-based IoT resists DDoS attacks better than traditional networks	Works under reactive mode only	SECOD (Secure Control and Data Plane) algorithm	Mininet simulator, Testbed-Raspberry Pie 3, Switch and Controllers.	Controller halt – 10%, Switch unresponsiveness – 40%	Algorithm based.
Liu et al. [73]	2022	AI-enabled DDoS in Blockchain Based Smart Transportation System	Automated feature extraction and classification. Protection from unauthorized modification	Does not includes network intrusion, malware and ransom ware attacks.	Autoencode with multilayer perceptron.	Block chain with deep learning.	Attack classification for three datasets : 95%, Very high F1-score rates.	DL-based.
Fan et al. [74]	2022	Detection of DDoS in SDN	Rapid attack detection and change in entropy value	Low-rate DDoS attacks cannot be detected.	Fusion entropy method	SDN controller	Detection of DDoS is 91% higher than normal scenario.	ML-based.
Wang et al. [75]	2021	DDoS detection scheme in SDN-IoT based environment	Maximum detection accuracy.	Neural network structure is not optimized.	Improved firefly algorithm	SDN-WISE-CONTIKI, Mininet.	99% DDoS behaviour and detection accuracy.	DL-based.
Najafimehr et al. [76]	2021	Hybrid approach to detect the DDoS attack	Uses both supervised and well as unsupervised machine learning algorithms.	Structure is not optimized, hence time consuming.	DBSCAN algorithm and classification model.	Python programming language and Linux operating system	198% more effective than conventional ML algorithm.	ML-based.
Ibrahim et al. [77]	2021	Detecting IoT application fitness from DDoS.	DDoS attack can be detected at the origin itself.	Does not involve botnet and botnet controller.	Block-chain enabled protocol.	Self-exposing nodes and SDN controller node.	Blocks the flooding traffic and makes the machine fit.	ML and blockchain based.
Sharma et al. [78]	2021	DDoS detection in IoT networks based on fog computing.	Attacks are detected at the lowest levels.	Fast statistical algorithm instead of deep learning algorithm.	CRPS algorithm	Wireshark.	Model captures more traffic and is more robust.	Statistical based.

(*continued on next page*)

contemporary networking environments to detect DDoS attacks. This also study the ML techniques in virtualized environments which include cloud computing, software-defined networks and network function virtualization environment. Finally, the paper discusses the DDoS attacks in IoT environment.

Trajanovski et al. [71] discusses the automatic identification of IoT botnet variants with the help of automated behaviour-based clustering. Behaviour profiles are developed using the behaviour of botnet samples captured in the sandbox. Then these profiles are clustered using the DBSCAN algorithm after being vectorized using TF-IDF. This method

Table 5 (*continued*).

Reference	Year	Topic Discussed	Merit	Demerit	Proposed Method	Tools	Output	Approach
Cvitić et al. [79]	2021	DDoS detection in traffic detection model	Supports diverse IoT devices with diverse behaviour.	Legitimate traffic profile is created based on predefined classes.	Boosted method of logistic model trees.	Smart home testbed, Wireshark	High performance i.e. accuracy, TPR, FPR.	ML-based. .
Yin et al. [80]	2021	Improvement of performance of LDDoS detection in SDN-IoT.	Helps in selecting optimal low dimension feature set to improve performance.	Only good in stealth attacks.	DIAMOND algorithm.	RYU controller, Mini-net wifi.	Improved detection precision and response time of algorithm.	ML-based.
Ashraf et al. [81]	2021	Botnet detection framework for protecting smart cities network.	Capture behaviour of IoT networks using statistical learning method	SDN not used, explainable AI can also be involved	Beta Mixture Model (BMM) and Correntropy Model.	IDE	99.2% more effective than compelling IDS.	Statistical Learning Based.
Mishra et al. [82]	2021	Detection of amplified DDoS attacks using new identification mechanism.	Detects multiple server attacks.	ML algorithms can be used at the application level to eliminate suspicious data which is not used.	Architectural change in memcached model.	Virtual Machine.	Low latency and high throughput.	Architecture Based.
Zeeshan et al. [83]	2021	Detection of DoS/DDoS using deep intrusion architecture.	Covered two benchmark datsets and reduced the features half	–NA–	LSTM model	Python 3	96.3% accuracy in detecting DDoS attacks.	DL-based.
Yousuf et al.[84]	2022	Detection of DDoS in live traffic IoT network.	Captures live traffic and provides centralized control.	Can be improved in detecting different DDoS attacks.	DALCNN	SDN, Mininet, Wireshark,OpenDayLight	Better than other existing algo in terms of performance parameters.	DL-based.
Zheng et al. [85]	2018	Detection of DDoS in ephemeral traffic using novel technique.	Captures sophisticated attacks	Delays can be further dealt.	RADAR (Reinforcing Anti-DDoS actions in real-time) method.	COTS and SDN switches	Acceptable overhead with acceptable delays.	Algorithm based.
Du et al. [86]	2021	Preventing new attacks in SDN-IIoT.	Optimal equilibrium between legitimate user and attacker	Does not discusses about information pillage, network hindrance properly.	Pseudo-honeypot game strategy.	Openflow network	Effective against DDoS attacks with lower energy consumption.	Architecture based.
Jing et al. [87]	2022	Detecting DDoS attack using Clustering and Graph Structures.	Unsupervised learning is used.	Vertex property is not covered, partition is chosen manually	PCA-FCM model	MATLAB,Python	Detection of DDoS is improved.	Algorithm based.

identified variants with new capabilities effectively and proved that the DBSCAN algorithm is more effective than Mean-Shift and the agglomerative hierarchical clustering algorithm.

Wang et al. [72] studied the latest DDoS attacks in the SDN-based IoT environment. The author uses the SECOD algorithm to resist a DDoS attack in a real SDN-based IoT testbed. This paper concludes that this SDN-based IoT network is more effective in detecting DDoS attacks than traditional networks.

Liu et al. [73] discuss the novel approach which combines deep learning and blockchain technology to protect the smart transportation system. Smart Transportation is the need of the day today and blockchain helps us against unauthorized access whereas the deep learning approach includes an auto-encoder and MLP (multi-layer perceptron) to effectively detect DDoS attacks. The method is implemented on three different datasets and is found that the deep learning model is more than 95% of F1-score.

Fan et al. [74] proposes a method of fusion entropy to detect DDoS attacks in Software Defined Networks. SDNs are the most commonly used architectures nowadays which foresee the higher-level control and administration of networks. Only entropy-based detection methods are slow in detecting and consequently have poor effects. Fusion entropy measures the fickleness of network events and thus has the advantage of expedited attack detection and palpable downfall in entropy value. The entropy value is decreased by 91.25%.

Wang et al. [75] talks about the DDoS attack detection scheme in SDN-IoT-based environment. The method involves an algorithm that specializes in traffic processing to detect DDoS attacks. After that, a firefly algorithm is also used to optimize the neural network structure. This helps in reducing the convergence time and increasing accuracy. Finally, it is suggested that the IFCANN model is better in performance than traditional machine learning models.

Najafimehr et al. [76] describes a hybrid approach to detect DDoS attacks in unknown malicious traffic. The hybrid approach institutes supervised as well as unsupervised Machine Learning (ML) algorithms. The approach uses the DBSCAN algorithm in the unsupervised phase and the classification algorithm in the supervised phase. DBSCAN algorithm is used as a clustering algorithm to cluster the traffic then classification is used to extract the DDoS traffic. The results suggest the advised method is 198% more effective than the best conventional ML algorithm.

Ibrahim et al. [77] proposes a novel method to secure fitness of IoT applications from DoS/DDoS by amalgamating Blockchain-enabled protocol (BEP) approach with self-exposing nodes (SEN). DoS attacks flood victim machines by flooding data packets and making the machine resources unavailable. SEN provides feature entropies of entering and exiting traffic to BEP in the structure of transaction blocks. BEP transacts these mined blocks to the SDN controller node on the basis of which it decides whether there is a DoS attack or not. SDN blocks the flooding traffic and makes the machine fit. In this way, DoS attack can be detected at the origin itself and can be further extended with the help of a botnet and botnet controller.

Sharma et al. [78] discusses anomaly-based detection algorithms for the IoT networks based on fog computing to detect DDoS attacks. The algorithm detects TCP-SYN, ICMP and UDP attacks. It uses a fast statistical algorithm in place of deep learning which is not feasible in a fog environment. The algorithm works on protocol-based attacks whereas fog computing helps in monitoring the local network traffic for the detection of various attacks. The author extracts multiple features from the network and uses CRPS algorithm.

Cvitić et al. [79] talks about the DDoS traffic detection model which utilizes boosted method of logistic model trees for distinct IoT device classes. This is done so because every new device has its own distinctive characteristics which require its own re-learning and re-development. And it is a complex job, especially in dynamic IoT environment traffic. So, the focus is on the device classes. Legitimate profiles are made with the help of the machine learning method. The profiles are based on legitimate traffic flow characteristics which help in understanding whether the device of the class behaves in legitimate limit or not.

Table 6
Prevention in IIoT.

Reference	Year	Topic Discussed	Merit	Demerit	Proposed Method	Tools	Output	Approach
Yang et al.[88]	2021	Securing Industrial IoT from DDoS.	Prevention from external threats, man-in-the-middle attack, replay and impersonation attack.	SCADA installation cost is high and the system is complex.	Encrypted token identification.	Supervisory Control and Data Acquisition (SCADA) network.	Prevents the DDoS effectively in real system.	Algorithm based.
Horak et al.[89]	2021	Vulnerabilities in Industrial IoT under DDoS attack.	Helps in mitigating DDoS in industrial IoT.	The environment is not highly scaled and observations can change on scaling significantly	Various scenarios attack within the network is made and the observation is done.	Bridge, Linux OS.	DDoS attack is mitigated by integrated industrial IoT.	Architecture based.

Yin et al. [80] introduces the DIAMOND algorithm which is a structured co-evolution feature optimization method that helps in choosing optimal features to elevate the detection performance of Low-rate Distributed Denial of Service (LDDoS). This algorithm uses a reachable count sorting clustering algorithm, a group structuring method, a communication strategy and a co-crossover strategy. The SDN-IoT network features are analysed with the optimal solution to give different subpopulation and then structural trees are generated. This tells us to select the most favourable low-dimension feature set and promote the detection precision and response time of the algorithm.

Ashraf et al. [81] advices a new statistical learning-based-botnet detection framework known as IoTBoT-IDS to safeguard the IoT networks in the smart cities against DDoS attacks. It is important to discover such attacks to attain sustainability in smart cities. This framework includes Correntropy models using Beta Mixture Models (BMM). The traffic is captured and normal behaviour is classified. Any anomalous behaviour leads to the detection of botnet activity. It is validated on three benchmark datasets and found to be 99.2% accurate and 2%–5% more effective than compelling intrusion detection methods. Future works include combining AI and SDN techniques in networks of smart cities.

Mishra et al. [82] discusses the innovative identification pattern mechanism which uses a threshold scheme for detecting amplification-based DDoS attacks. It is a pre-emptive method to detect attacks, decrease latency and increase throughput. The paper suggests architectural changes to the memcached server to detect single-server attacks and multiple-server attacks altogether using the SYN request. This context-aware method also increases flexibility.

Zeeshan et al. [83] has proposed a Protocol based Deep Intrusion Detection (PB-DID) architecture in which standard properties of flow and TCP category of two IoT traffic dataset (UNSW-NB 15 and Bot-IoT) is used in creating a dataset of packets. The dataset is balanced and is not over-fitted. Anomaly, DoS and DDoS traffic is classified using the DL technique. The accuracy is 96.3% for binary and multi-class classification. The suggested job lessens half the number of attributes to identify malicious traffic.

Yousuf et al. [84] introduces a fresh algorithm named DALCNN (Detecting Attack using Live Capture Neural Network) whose task is to unmask DDoS attack in IoT using recurrent neural networks. The author uses the SDN network with the OpenDayLight platform. After that three-tier architecture is also recommended to distinguish and spot the DDoS attack. The author uses Mininet and Wireshark to generate and detect various kinds of DDoS attacks. The proposed algorithm calculates the benchmark parameters and performance interpretation of diversified open-source controllers. The designed algorithm efficiency is extended and is more than the existing algorithm.

Zheng et al. [85] has proposed the RADAR (Reinforcing Anti-DDoS Actions in Real-time) method to recognize and shield against DDoS attacks developed from low-rate and ephemeral traffic. The method uses COTS (Commercial Off-The-Shelf) and SDN (Software Defined Network) switches to establish the prototype using adaptive correlation analysis. This method detects link-flood attacks, SYN flooding and UDP amplification attacks without making any change in the switch. The performance is measured using many real hardware test beds. This method detects and defends DDoS attacks with small delays.

Du et al. [86] reveals new attacks in the SDN network and optimal strategies to carry out the best attack. Then the author also proposes a pseudo-honeypot game strategy that uses several Bayesian-Nash Equilibrium (BNE) groups to achieve dynamic protection from the new attack and obtain equilibrium between legitimate users and attackers. The strategy is implemented on test beds to show the proposed method is effective against DDoS attacks with lower energy consumption.

Jing et al. [87] uses the PCA-FCM model to ascertain DDoS attacks. First, the traffic data is extracted using edges and vertices in the graph theory and eight characteristics are used. Further PCA (Principle Component Analysis) is used to further dwindle the count of characteristics for extraction of DDoS and normal traffic. This FCM(Fuzzy C-Means) clustering is used to identify the DDoS traffic. The traffic is verified on CICIDS-2017 traffic. The result shows that detection reliability is better than other methods.

3.2. Industrial internet of things

IIoT is an extension of IoT in industries. Modern-day industries use these devices to enhance their productivity. Like IoT, IIoT devices are also vulnerable due to their devices. DDoS-related studies in IIoT have been discussed below.

3.2.1. IIoT DDoS survey

Prevention in IIoT Papers studied in relation to IIoT prevention is discussed below and compared in Table 6.

Yang et al. [88] proposed a module based on encrypted token identification to prevent the IIoT from DDoS attacks. The two-step identification process involves tokens, devices and remote control of the

Table 7
Mitigation in IIoT.

Reference	Year	Topic Discussed	Merit	Demerit	Proposed Method	Tools	Output	Approach
Borgiani et al. [90]	2020	DDoS attack detection in large scale IIoT networks.	Addresses congestion, low bandwidth	Resources are not optimized, lack of dynamic threshold detection.	Distributed congestion control by Duty-cycle Restriction(D-ConCReCT)	Contiki OS	100% effective upto 500 nodes.	Algorithm based.
Huang et al. [91]	2022	DDoS detection using multipoint collaborative mechanism in IIoT	Reduced time sharing delay.	–NA–	Gossip model using blockchain and block group propagation	MEC Server, Virtual Machine, Pytorch and Matlab.	Reduced propagation delay and effective response.	Blockchain and ML.
Jaylaxmi et al. [92]	2019	Detection of botnets in IIoT.	Performs better than other existing neural network model.	Large dataset training is required	CFS ,CFBPNN and NARX	Python	Accuracy Training-100%,Testing-97.3%	DL-based.
Ahmed et al. [93]	2020	Detection of botnet attack using deep learning model.	Does not requires external tools.	Method was not applied on DDoS attacks.	ANN , Adams optimization problem.	Python, Keras.	Accuracy is 99.6% more than SVM, Naïve Bayes, etc.	DL-based.
Shi et al. [94]	2020	Detection of botnet using network behaviour.	Overcomes rules based detection shortcomings	Consumes a lot of memory resource.	Hybrid model of LSTM and RNN.	Keras	Hybrid model is better than individual model.	DL-based.
Yazdinejad et al. [95]	2022	Detection of threats in IIoT.	Works in complex environment as well	–NA–	LSTM and AE	Keras	Higher accuracy compared to conventional model.	DL-based.

server. It helps not only in preventing external threats, but also from man-in-the-middle, replay and impersonation attacks. This method was applied to Smart Green Energy Science City in southern Taiwan and it was concluded that the mechanism effectively improves security in real systems.

Horak et al.[89] shows the vulnerabilities in production lines by performing DDoS attacks on Industrial IoT systems. Specially two kinds of attacks are performed - direct DDoS flood attack and DDoS reflective attack – on the automated production line. The attacks made the production line dysfunctional and put the entire system in danger. Finally, the solution to it was suggested using integrated industrial IoT devices.

Mitigation in IIoT Few papers studied in relation to IIoT mitigation is discussed below and compared in Table 7.

Borgiani et al. [90] recommends a dispersed congestion control Duty-cycle Restriction(D-ConCReCT) technique to uncover and weaken DoS attacks in IIoT. The essential challenge in IoT devices is congestion in channel transmission. So, this method checks the DDoS detection and mitigation feasibility in large-scale networks. It is deduced that the mitigation of DoS is 100% effective under attack from 500 nodes.

Huang et al. [91] proposes a multipoint collaborative defence mechanism against DDoS attacks for IIoT. Traditional mechanisms cannot be directly used in IIoT as different devices are easily compromised when the budget is limited. The multipoint defence collaborative shares defence information securely through blockchain. Also, a fast defence-sharing mechanism provides safety and reduces delays in sharing information. At a single point EdgeDefence mechanism is created to detect, identify, classify and mitigate DDoS attacks. The author says EdgeDefence is more powerful in terms of performance and classification than the baseline models.

Jaylaxmi et al. [92] uses DeBot, a deep learning model for the disclosure of bots in industrial IoT. The author combines Correlation-based Feature Selection (CFS) technique for selecting the right feature with the recent Cascade Forward Back Propagation Neural Network (CFBPNN) model. It uses a correlation-based subset evaluator to select the best subset of features. Later Nonlinear Auto-regressive Network with exogenous inputs (NARX) technique is used to select the best performance for subsets. Later, the author compares the method with pre-existing models and concludes the introduced mechanism is better in terms of precision, recall and F1 score.

Ahmed et al. [93] introduces us to a deep learning model for the revelation of zero-day botnet attack since botnets are rapidly evolving. First, the author evaluates the efficiency and accuracy of the algorithm using a feed-forward backtracking ANN algorithm and then implemented the algorithm on CTU-13 datasets for testing it. Further, the author uses Adam's optimization algorithm for attaining maximum accuracy of 99.6%, which is more than SVM, Naive Bayes, back propagation and decision tree.

Shi et al. [94] proposes a botnet detection mechanism utilizing the behaviour of the network traffic. This method overcomes the shortcoming of dynamically changing features since the network traffic is inspected and their behaviour is extracted. Further, this time-based input is fed to the LSTM, RNN and a hybrid model of the LSTM and RNN model. The author asserts that the hybrid model is better than the LSTM model followed by RNN.

Yazdinejad et al. [95] proposed a deep learning-based model using LSTM and Auto Encoder (AE) to detect threats and anomalous data in IIoT. First, the balanced dataset is extracted from the imbalanced dataset. Later dataset is fed to LSTM and AE to learn normal data traffic, reduce data dimension and detect anomalies. Two real datasets of Gas Pipeline and Secure Water Treatment are used. The author says the proposed method has higher accuracy when compared to conventional and advanced machine learning models.

Panchal et al. [3] tells about the various security issues in industries which are in the process of adopting Industrial IoT and gives an overview of the layers of IIoT where the attack is possible. The paper gives a taxonomy of IIoT attacks and suggests thorough penetration testing should be done after any modification in IIoT architecture. The author also gives countermeasures to the attacks.

Yu et al. [21] discusses the similarity and challenges deriving out of IoT and IIoT. The challenges in IIoT are more critical due to its attachment to industrial control systems. The author has separately identified challenges in IoT and IIoT because both are applicable to IIoT. Previous work and the work addressing the challenges have been clearly identified.

Nazir et al. [96] talk about SCADA systems. It is stated that SCADA systems are used in a crucial framework such as power generation, water supply, etc. And its connectivity online lays bare global cyber threats. So approaches such as simulation and modelling are used to achieve the desired result against cyber threats. But the current situation of evolving threats suggests to use penetration testing. This helps to find vulnerabilities in systems and real-time threat.

Shitharth et al. [97] compares two techniques for detecting DDoS attacks in SCADA systems. The first method uses the PMD technique and the second method uses Wireshark and TCPDUMP for sniffing DDoS attacks. The author emphasizes the use of SCADA in Smart Grids. The SCADA systems do not have a defined protocol hence the compatibility of the tools used in making SCADA software always remains a reason for worry. Hence, by comparing the two methods, the author concludes that the PMD technique is more efficient in detecting DDoS.

Markovic et al. [98] discusses the vulnerabilities in modern control systems. It is said that the network architecture and the protocols used are vulnerable hence making the control system vulnerable. In particular, the author talks about the SCADA system which is being extensively used in the power generation sector. The author uses simulation models to analyse the performance under a DDoS attack. The author concludes the performance of hydropower plants decreases under DDoS attacks.

4. Industrial IoT(IIoT) architecture

From the above discussion, it can be stated that IIoT architecture comprises of two layers [3]. They are Information Technology (IT) layer and Operational Technology (OT) layer (see Fig. 5). A simple IoT device contains only an IT layer; an OT layer is added to the IIoT. Though IIoT is a part of IoT, the defense in IIoT mostly focused on operational technology [8]. This segment includes smart logistical processes, smart manufacturing techniques and smart cities. IIoT is supervised and oversighted through cyber–physical systems such as Integrated Control Systems (ICS).

The ICS system monitors and administers the critical infrastructure of any industry. These critical infrastructures include a component such as Supervisory Control and Data Acquisition (SCADA), Manufacturing Execution System (MES), Building Management System (BMS) and Computer Maintenance Management System (CMMS) [21]. With this, it is observed that the prime task of IIoT is good management of resources, intelligently monitoring the devices within, checking the health of the machine, modifying, manufacturing the product and taking note of the timeline of the maintenance [99].

The IT and OT layers are separated by the Demilitarized Zone(DMZ). The layer components are explained below:

- **Layer 1:** This is the lowest layer in the architecture and belongs to the OT layer which deals with the physical processing in the industry. They have transmitters, actuators, sensors and embedded devices.
- **Layer 2:** The second layer has the devices such as Distributed Control System (DCS), Programmable Logic Control (PLC) and Gateways which are used for communication with the physical layer .
- **Layer 3:** In this layer, devices such as SCADA, HMI, Control Rooms and Operation Stations are used whose task is to collect and share the data incoming from the bottom layers i.e. Layer 1 and Layer 2. This is the topmost layer of OT.
- **Layer 4:** This is the bottom IT layer. It collects the data incoming and stores it at remote data centres. This layer supports office applications, intranet, mail and web services.
- **Layer 5:** This is a top IT layer. From this place, the company executives handle the data. This supports business planning with the help of cloud computing, data analytics and smart devices.

These layers are exposed to various types of attacks. Layer 1 is exposed to reverse engineering, brute force, eavesdropping and malware. Layer 2 is susceptible to replay attacks, man-in-the-middle attacks, brute force attacks and sniffing. Layer 3 gets hit by IP spoofing, data sniffing, data manipulation and malware. At data centres as in Layer 4, phishing, SQL injection, malware, DNS poisoning and brute force attack are common. And at the topmost level DoS attack, malware, password, side channel attack and man-in-the-middle attack occurs.

In this section, different types of simulators along with datasets used for IIoT is also described in tabular form in Tables 8 and 9.

5. DDoS defense approaches and techniques

This section divides the DDoS defence based on methods such as machine learning, deep learning, federated learning, transfer learning and the rest in miscellaneous approaches.

5.1. Machine learning based approaches

DDoS attack in SCADA system is discovered using machine learning algorithms such as J48, Naive Bayes and Random Forest on different datasets. The accuracy of the random forest classifier is more than J48 followed by Naive Bayes in machine learning algorithms [104].

One of the machine learning approach is the feature selection algorithm FGOA-kNN based on a hybrid filter and wrapper class selection approach. It is used to detect multiclass attacks. This selects the most important features using clustering and then applies the Grasshopper algorithm (GOA) to further reduce them. After getting the important features, the IHHO algorithm is implemented to select and set the hyperparameters of the neural network to finally identify the attack. Chaotic map is used for population diversity and the non-linear formula is used in escape energy to ward off local minima and maintain the trade-off between exploration and exploitation. This method uses a supervised, unsupervised and clustering approach [105].

Intrusion detection schemes for SCADA are also developed using a modified decision tree-fused chi-square feature selection method. Three processes are used in this method namely *data preprocessing, feature selection* and *attack classification*. The main gist of the method is to find the most relevant features after preprocessing, training and classification. This method is reliable as the performance is very stable when it is compared to other methods. Different datasets and Cohen's Kappa

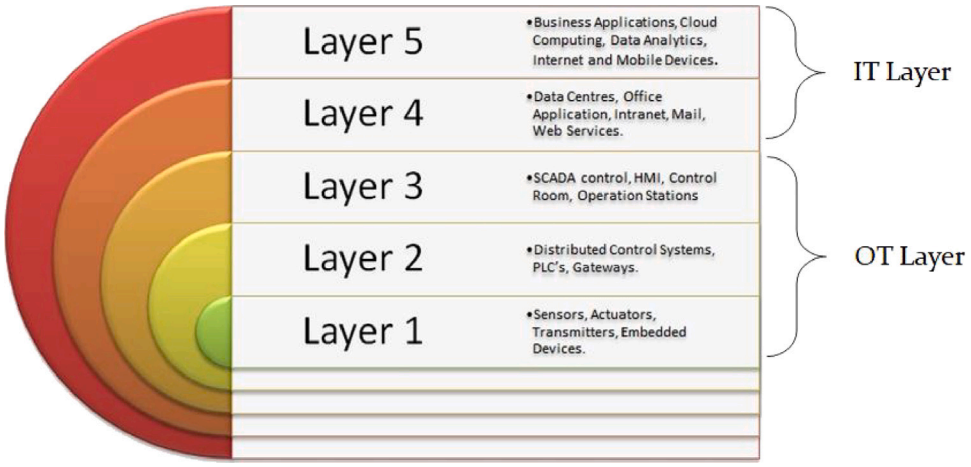


Fig. 5. IIoT architecture.

Table 8
Different IIoT datasets.

Dataset	Size	Attributes	Type of attacks
Edge-IIoT Dataset [100]	2 GB	Distance, flame_sensors, heart_rate, etc.	TTP, ICMP, TCP_SYN, UDP
WUSTL-IIoT-2021 Dataset [101]	2.7 GB	Mean flow, Source Port, Destination Port, Source Packets, etc.	SYN, HTTP
X-IIoTID Dataset [102]	115 MB	Timestamp. Source IP, Destination IP, Source Port, Destination port,etc.	Modbus, WebSocket, CoAP, MQTT, TCP, ARP, HTTP, SSH, DNS, ICMP, SMTP and UDP.
WUSTL-IIOT-2018 Dataset [103]	627 MB	Source port, total packets, total bytes, source packets, destination packets, and source bytes.	Port scanners, address scan attacks, device identification attacks and exploit attacks.

Table 9
Different network simulators.

Network simulators	Operating system	CLI	Programmable	Programing language	Key features
Mininet	Linux	Yes	Yes	Python	Supports SDN, OpenFlow, Complex Topology.
Network Simulator	Unix	Yes	Yes	C++, Python	Supports wired and wireless networks.
OMNeT++	Windows	No	Yes	C++	Supports fixed, mobile nodes and graphics.

coefficient also validate the method. Usually, the IDS is expensive also so a good feature selection ML method is very useful. This method uses WUSTL-IIoT-2018 Dataset [106].

WUSTL-IIOT-2018 dataset WUSTL-IIOT-2018 dataset was created by Teixeira. In this dataset, the SCADA system testbed was used in the water storage tank of the water treatment and distribution system. The testbed gives us a real-world replica. Different kinds of attacks were made on the testbed such as port scanners, address scan attacks, device identification attacks and exploit attacks. The data was captured for 25 h with a total data size of 627MB in which 7,049,989 observations were made. Out of which normal traffic and attack traffic was observed as 93.93% and 6.07% respectively. The data was cleaned and was reduced to 7,037,983 and the following features were observed which vary during the attack and normal traffic: source port, total packets, total bytes, source packets, destination packets, and source bytes.

To detect and mitigate constantly updated DDoS attacks, an adaptive DDoS mitigation method is preferred. One way is to use information entropy and unsupervised anomaly detection method. This can dynamically classify sceptical features and can naturally diagnose the current state. It does not require additional devices with SDN and uses the pipeline method to precisely drop the suspected traffic. It has substantial average mitigation accuracy [107].

One method to detect attacks is through Intrusion Detection Model. In this model, machine learning with feature engineering is utilized. It combines Isolation Forest(IF) and Pearson Correlation Coefficient(PCC).

Table 10
Machine learning approaches.

Reference & Year	Objective	Approach	Performance measure
Alhaidari et al. [104] & 2019	Detection of DDoS attack in SCADA.	J48, Naive Bayes and Random Forest is applied on different dataset	Accuracy
Taher et al. [105] & 2023	Detection of DDoS attack.	FGOA-kNN with IHHO algorithm.	Recall, Precision, F1-score and Accuracy.
Ahakonye et al. [106] & 2023	Anomaly Detection and Classification.	IDS with fused feature selection(FS) and Modified Decision Tree(MDT)	False Positive Ratio(FRP) and Mathews Correlation Coefficient(MCC).
Cai et al.[107] & 2023	Detect and mitigate adaptive DDoS attacks.	Dynamic Classification of suspected features.	Average mitigation accuracy .
Mohy-Eddine et al.[108] & 2023	Detect attacks using IDS.	Isolation Forest(IF) and Pearson Correlation Coefficient(PCC)	Accuracy, Precision, Recall, F1-score, False Positive Ratio.

IF is used to detect and remove outliers and PCC is used to detect to choose the most appropriate features. It has less prediction time and less computational cost [108].

The comparative study of machine learning approaches is done in Table 10.

5.2. Deep learning based approaches

There is a lot of emphasis on high-rate DDoS detection recently in the past when considering SDN networks. To consider the Low rate DDoS (LDDoS) detection, deep learning-based model comprising LSTM can be used. LSTM works as an activation function that helps in investigating various LDDoS attacks and ordinary traffic. Through this detection accuracy of the system can be improved. In this method, the Edge-IIoT dataset was used [109].

Edge-IIoT dataset Edge-IIoT Dataset was created by Mohamed Amine Ferrag for use in a machine learning-based Intrusion Detection System in the centralized and federated mode of IIoT. In this dataset, there are three files: Normal traffic file, Attack traffic file and selected dataset for Machine Learning and Deep Learning. The normal traffic file is captured using different IoT devices, sensors, protocols and cloud configurations. It uses features such as distance, flame_sensors, heart_rate, IR_receiver, Modbus, phValue, soil_moisture,sound_sensor, temperature_and_humidity and water_level. The author also identifies and analyses the DDoS attack to create the attack traffic file. The attack file includes attacks such as Backdoor, HTTP, ICMP, TCP_SYN, UDP attacks and so on. The third file tells us about the two CSV dataset files. The first CSV file is used in a deep learning-based intrusion detection system known as DNN-EdgeIIoT-dataset.csv and the second file is used machine learning-based intrusion detection system known as ML-EdgeIIoT-dataset.csv.

The centralized controller in the SDN-based IIoT is a tempting target for attackers. Importantly, evolving DDoS attacks raise a significant challenge to the controller. So, a hybrid model comprising CNN and LSTM gives admissible data features to identify the DDoS attacks. The method has high-performance accuracy, low complexity and less time cost. This method is also called as Extreme Gradient Boosting (XGBoost) method [110].

Recurrent neural networks (RNN) are being used such as Long Short Term Memory (LSTM) to identify the normal data patterns in time series data, along with Auto Encoder (AE) which is an Artificial Neural Network (ANN) used to reduce the data dimensionality. The combined method is called LSTMAE. Later, with the help of a decision tree, the anomalous data and threat is identified [95]. It works effectively in Gas Pipeline (GP) and Secure Water Treatment (SWT) datasets.

One less complicated way of finding an anomaly and abnormal behaviour in any traffic is through deep-autoencoders. Deep-autoencoders are trained on normal datasets and network flow features. Fifteen network flow features can be easily derived from the dataset with minimum data processing. Even data logs are not required as they are difficult to obtain. This method is practically implementable also as every process involved can be easily implemented across networks without interfering with any processing device and is cost-effective in nature [111].

The hybrid deep learning method is also used to handle the reliability of communication protocol. The communication protocols are very much vulnerable to DDoS attacks. Hence, compromises its availability. So, the hybrid method which focuses on DDoS attacks is used. Initially, the data can be normalized using supervised ML. Then dataset is applied to a hybrid algorithm comprising of the Convolution Neural Network (CNN) and Grated Recurrent Unit (GRU). This procedure gives a better detection rate and accuracy when applied to Smart Grids [112].

Deep learning combined with transfer learning improves efficiency and reliability. A deep learning progressive algorithm (DPNN) that combines progressive learning and deep neural network identifies the attack accurately with 94% compared to 69.7% in the KNN model. This model uses previous knowledge by remembering old insights through transfer learning and lateral connections. The major advantage of this method is that it has low misclassification [113].

For wireless sensing cases in IIoT, a method known as the NIDS-CNNLSTM method is developed to successfully identify and segregate the traffic and operational data of the devices of IIoT. This helps in verifying the malicious data, hence ensuring the security of the IIoT. It is trained on KDDCUP99, NSL_KDD and UNSW_NB15 datasets. It uses CNN and LSTM technique which shows high detection rate and classification accuracy when compared with previous models [114].

A hybrid model of CNN and LSTM was compared to CNN and LSTM individually to detect the abnormal traffic in IIoT. The datasets used were UNSW-NB15 and X-IIoTID. It was observed that the hybrid model thus obtained had a greater detection accuracy for binary as well as multi-class classification of intrusion detection [115].

X-IIoTID dataset X-IIoTID dataset was generated by Munnah Al-Hawawreh. They used Industrial Internet Reference Architecture (IIRA) model for data generation. They divided the model into three tiers: left, middle and right tier. The leftmost tier is known as the edge level. It consists of an IIoT testbed and the basic requirements of the IIoT systems. The middle tier, also known as the platform level, constitutes the operations required for constructing the dataset. The right tier, called the enterprise tier provides the final dataset using exploratory data and analysis tools. This dataset handles the co-existing

Table 11
Deep learning approaches.

Reference & Year	Objective	Approach	Performance Measure
Alashhab et al. [109] & 2022	Detection of low-rate DDoS attack.	LSTM.	Accuracy, Loss-rate, Precision, Recall, F1-score.
Zainudin et al. [110] & 2022	To find important features for DDoS detection.	Extreme Gradient Boosting (Combining CNN & LSTM).	Precision, Recall and F1-score.
Yazdinejad et al. [95] & 2022	To identify anomalous data and attack.	LSTM-AE.	Accuracy, Precision, F1-score, Recall.
Ortega-Fernandez et al. [111] & 2023	Finding anomaly and abnormal traffic.	Deep Auto-encoder.	True False Positive(TPR), False Negative Rate(FNR), AUC-ROC, AUC-PR.
Diaba et al. [112] & 2023	Detecting DDoS attack in Smart grid.	CNN and GRU.	Accuracy, Precision, Recall and F1-score.
Sharma et al. [113] & 2023	To detect and classify attacks in IIoT.	DPNN(Deep Learning Progressive Network)	Confusion Matrix.
Du et al.[114] & 2023	To detect and classify the malicious data in IIoT	NIDS-CNNLSTM	Accuracy, Detection Rate, False Positive Ratio.
Altunay et al.[115] & 2023	To identify the intrusion in IIoT.	Hybrid model of CNN and LSTM	Accuracy, Recall, Precision and F1-score.

real-life heterogeneity, interoperability of IIoT devices and behaviour of different protocols very well and includes various scenarios of attacks.

The comparative study of deep learning approaches is done in Table 11.

5.3. Federated learning based approaches

Federated Learning Empowered Architecture to Mitigate DDoS attack(FLEAM) model is used along with the IMA-GRU protocol to contest harmful DDoS scripts. IMA-GRU protocol is used to maximize the segregated values in edge devices. Above this FLEAM protocol is used, which helps by taking the mitigation intelligence to the edge devices (distributed end) from the centralized end. This gives the model more flexibility, scalability and adjustability. This model has more accuracy and less response time [116].

Federated Learning Intrusion Detection System (IDS) is used to mitigate the DDoS attack on any device. It is also used to secure the critical infrastructure in the marine SCADA system. It is fit for application in the maritime industry provided constraints of complexity and privacy in the marine devices. The basic method of this federated learning is based on building models. The initial model is stored on the server and provided to the available client to train the model on the available dataset. The new models, thus generated, are aggregated at the server side to build a new global and enhanced model. This model is further made available to clients for training purposes. This method is fit for marine devices because evaluated performance such as accuracy, precision, recall and AUC points out significantly towards applicability in the maritime domain [118].

Federated Learning(FL) also ensures privacy preservation when used by SDN servers. FL-based multi-layer perceptron (MLP) model is also a good DDoS classifier with higher accuracy [119].

Federated Learning is also used to classify the DDoS attacks in SDN-enabled IIoT. It is a decentralized DDoS identification method that uses independent clients to train the data. For feature selection, Pearson Correlation Coefficient (PCC) is used. In order to reduce complexity, the classification mechanism can involve CNN combined with MLP. CNN is used to extract features using residual connection with less complexity. MLP is used for the classification of an attack. This method has better performance than existing approaches [120].

It is often the case in IoT devices, labelled data is scarcely obtainable and unlabelled data is available in huge amount. This is because the labelling of data is frustratingly time consuming and dearer. This makes the identification of attacks even more complicated. So, to handle such instances federated semi-supervised learning is utilized in IIoT. Federated learning provides the system with the opportunity to train the model with both labelled and unlabelled data sets. Initially, the unlabelled or the private dataset is trained on an autoencoder (AE) present at each local device for gaining knowledge about relatively less dimensional and holistic data features. Then, these models are aggregated on the cloud server to form global AE and supervised training with the labelled data is performed. In this way, the attacks are classified. It is seen that the method still works with a scarce amount of data and has low communication overhead. It has high classification performance [121].

The devices which are prone to malicious attacks and data privacy concerns in IoT cannot run under a centralized environment due to enormous data and the contemporary distribution of data over devices. So, the approach is a decentralized federated learning method. In this, the local devices send the parameters to the centralized controller which sends them the improved model or the algorithm. Each device receives its own model and trains them to a local dataset. In this way, the process gets repeated and the model gets updated from the global server. This helps in keeping individual device privacy. The reliability and accuracy of the decentralized model are similar to that of the centralized model [122].

In the distributed IIoT environment, detecting anomalies is a tedious task due to the fast-growing landscape, network overhead, uncontrolled environment and data isolation occurring in large-scale and heterogenous cloud and edge environment. So, to solve this tediousness, the federated learning method is integrated with an unsupervised device clustering algorithm. This allows to train an anomaly as well as IDS models and work with unlabelled data, as happens in real scenarios. This method has a small false detection rate and decent detection accuracy [123].

FL has also been used in detecting anomalies in Long Range (LoRa) based IIoT. LoRa is very energy efficient and has more range in the distance but still has inefficient detection rates due to impersonation and a wide variety of devices. So, a distributed anomaly detection approach named Hawk can also be used. This method uses the Carrier

Table 12
Federated learning approaches.

Reference & Year	Objective	Approach	Performance Measure
Li et al.[116] & 2021	To mitigate DDoS attack in IIoT.	FLEAM model and IMA-GRU.	System Accuracy, individual mitigation accuracy and joint mitigation accuracy.
Mothukuri et al. [117] & 2021	Anomaly Detection in IoT devices.	Federated Learning with GRU.	Accuracy, Precision, Recall, F1-score.
Ahakonye et al. [118] & 2022	To mitigate DDoS attack in Marine-SCADA system.	FED-MARINE.	Accuracy, Precision, Recall, AUC.
Zainuddin et al. [119] & 2022	Classifying DDoS attack in IIoT.	Multilayer Perceptron(MLP) model.	Accuracy, Loss and Time-Cost.
Zainuddin et al. [120] & 2022	Classify DDoS attack in SDN-based IIoT.	Pearson Correlation Coefficient, CNN, MLP.	Accuracy, Loss, Time-Cost and Average ROC Score.
Aouedi et al. [121] & 2022	To detect attacks in semi-labelled dataset in IIoT	Federated semi-supervised Learning	Accuracy, Precision, Recall, F1-score
Rashid et al. [122] & 2023	Improving intrusion detection in IIoT.	Decentralized federated learning method	Accuracy, Precision, Recall, F1-score, True Positive Rate(TPR), False Positive Rate(FPR).
Camara et al. [123] & 2023	To detect anomaly in large and heterogeneous IoT environment	Fedearted learning with unsupervised clustering algorithm.	False detection rate(FDR), Accuracy.
Halder et al. [124] & 2023	To detect anomaly in LoRa-based IIoT.	Federated learning based approach Hawk	Accuracy, Precision and Storage space.
Friha et al. [125] & 2023	To identify attacks against IIoT.	2DF-IDS	Precision, Recall and Accuracy.

Frequency Offset (CFO) of the radio signature used in communications of LoRa. Signatures are later used to identify the dubious behaviour of devices. This method is able to catch known and unknown attacks with better accuracy and less storage space [124].

A centralized detection approach for anomaly detection adds privacy and user data concerns. Hence federated learning provides a good alternative to the centralized approach. Shared computational power in federated learning is used in providing better training and Grated Recurrent Units (GRU) are used for better accuracy of classification. Accuracy is further improved by ensembling the results from different GRU's. This approach gives better results than the non-federated learning approach, secures the data and gives optimal accuracy rate [117].

Another method to have the safety of the processes and the data involved in the communication of entities of IIoT is suggested in [125]. The author suggests having a method named 2DF-IDS which is a decentralized, differentially private federated learning method and identifies many cyber-attacks in the smart industry ecosystem. This method comprises of the key exchange protocol, a differential private gradient exchange scheme and a decentralized federated learning method. It has better performance than just a federated learning approach with higher precision, recall and F1-score.

The comparative study of federated learning approaches is done in Table 12.

5.4. Transfer learning based approaches

Transfer Learning can be used to detect attacks using the Deep Transfer Learning(DTL) method consisting of autoencoders (AE). The benefit of DTL is that it learns from the data which is unlabelled also. The first autoencoder is trained in a supervised mode using the labelled information of source data and the second autoencoder is trained in unsupervised mode on target data which is not labelled to classify it as an attack or normal traffic. Multi-Maximum Mean Discrepancy (MMD) metric is utilized to transfer knowledge from the first AE to the second AE. It can be used at any layer of the encoder effectively increasing the learning process. But the drawback is that it increases the training time also. This method increases the attack detection by increasing Area Under the ROC Curve (AUC) [126].

Transfer Learning is also used when the environment of the IoT systems changes and there is a need for an automatic attack-identifying method. Machine Learning techniques solve the problem of complex systems but still they consume time and in the dynamic environment this creates a major hurdle as creating a model from scratch multiple times is not feasible. So, transfer learning is used. It facilitates the knowledge transfer from one instance and applies it to another instance to identify the attack. It is used in two ways. The first way is to transfer the knowledge to create an algorithm for attack detection and the second is to transfer the knowledge to directly detect the attack. Both methods enhance performance than old methods as they have less training time for the detection of new attacks. This method is well tested on resource-constrained wireless network [127].

Transfer learning presents a proven model for a two-class classification problem for attack detection in Industrial Control System (ICS). It is not a multi-class classification model. In this, one-dimension ICS dataflow is converted into two dimensional images. The method of deep residual Convolution Neural Network (CNN) is applied to build an eight-layer residual network and then fine-tuning is performed for transfer learning. The results show that this technique of residual CNN has the potential and secures gradient disappearance and explosion. It also provides reliable predictions for both known and unknown attacks and distributed irregular data just by using short-transfer learning. It also outclasses many algorithms, solves the problem of training time in deep learning models and satisfies the demand of ICS systems [128].

Table 13
Transfer learning approaches.

Reference & Year	Objective	Approach	Performance Measure
Vu et al. [126] & 2020	Detection of attack in IoT	Deep Transfer Learning with Auto-encoder.	AUC score.
Yilmaz et al. [127] & 2021	Automatic attack identification in dynamic changing environment.	Transfer learning using knowledge of one instance in another.	Accuracy, FPR, Detection Rate.
Wang et al. [128] & 2021	Detection of anomaly in ICS.	Deep Residual CNN.	Precision, Recall, FPR, F1-score, Accuracy.
Polat et al. [129] & 2022	Detecting DDoS attack in SDN based SCADA system.	LSTM, GRU, SVM	Accuracy, Sensitivity, Specificity, Precision, F1-score.
Shafiq et al. [130] & 2022	Detecting anomaly in DDoS producing IoT devices.	Auto-encoder neural networks	Accuracy, Average time.
Rodriguez et al. [131] & 2022	To efficiently detect the zero-day attacks in IoT.	Transfer learning, Knowledge transfer, Model refinement.	Accuracy, Precision, Recall, False Positive Ratio, F1-score.

SCADA systems are used with SDN to tackle the scalability and manageability issues in ICS. Still, it needs to be protected from cyber attacks such as DDoS attacks. So, RNN technique Long Short Term Memory(LSTM) and Grated Recurrent Unit(GRU) are used parallel to train the training dataset to extract features and classify it using the SVM technique. Then, with the help of transfer learning concept, the validation data set is used to develop the feature again on the previously trained data model and classify it by SVM. Transfer learning method improves the performance significantly [129].

Transfer learning is also used with autoencoder neural networks for the detection of DDoS. Since training on every IoT device is unfeasible and the machine learning-based method has long training and validation cycles, transfer learning is one of the new ways. It is assumed that similar characteristics are represented by outer layers whereas evident changes are presented by inner layers. Middle layers are retrained on new data gathered from different devices data obtained. In this method, the model is tested before and after transfer learning on Mirai and Bashlite. Hence, giving the best performance [130].

Deep Learning tools require large labelled and balanced datasets for attack detection, but in most scenarios, these parameters are not available sufficiently. In these cases, Transfer Learning (TL) can be a good solution. It is combined with knowledge transfer and model refinement to give more accurate results in known and new attacks. And in zero-day attacks, TL together with network-fine tuning is used for better accuracy and low false positive ratio. In this TL is based on the Convolution Neural Network(CNN) and has a better ratio than DL based Intrusion Detection Systems [131].

The comparative study of transfer learning approaches is done in Table 13.

5.5. Miscellaneous approaches

Honeypots are also used to secure the industrial system. There are several features that can be utilized in the honeypots to prevent SCADA systems. Still, there is no such system that uses all the features, so it is a good conviction to implement a honeypot [132]. The features include dynamically generated executable files, high fidelity, automated shell code analysis, secure malware storage, high interaction obfuscation, search engine web service emulation, USB emulation, full architecture emulation, retard or stop hostile scan, Wireless Access Point obfuscation and dynamic traffic redirection.

The data on a network can be routed through Promiscuous Mode Detection (PMD) technique in packet sniffers before reaching the intended controller. After that, the data is labelled as well. This method gives better results than IDS tools such as Wireshark and Tcpdump, especially in SCADA network [97].

MODBUS protocol is used to secure IIoT as it is imperative to Industrial Control Systems (ICS). It is a standard communication protocol to communicate between IIoT devices. Since it was implemented in 1979, it is vulnerable to various attacks including DoS attacks. It can be prevented by using a timestamp or cookie in the Modbus Protocol Data Unit (PDU) to shed the packets which are tampered. Another way is to implement a firewall before Modbus master to obstruct the virulent IPs [133]. Segregation of access devices based on the role and multi-factor authentication is also implemented in some cases. Prevention can also happen by lowering the priority of Modbus requests below the PLC logic. Any Modbus request is queued in a temporary buffer until the PLC internally writes its tables. Thus, this becomes an arbitrary block between the network layer and PLC hence providing authentication before communication [134]. The connection can also be stopped which sends the packet faster than the threshold. The Modbus protocol is also looked after by the covert channels. Authentication message is hidden in the protocol field or time-based channels are used to observe the inter-arrival time of the packets [135].

Distributed AI (DAI) technique is also considered when IIoT anomaly detection is concerned. To handle the enormous and accelerated data, the ADDAI method is used. This method takes advantage of distributed computing in edge cloud infrastructure and creates less overhead as it is spread geographically and has proximity to the sensors. Distributed nature provides good speed from various devices involved, protection against single point failure and the arrangements required for scalability. Since this method is used on the devices, the communication at the higher level is through the latent variables so the privacy is maintained and practical proof tells it has less communication cost [136].

Another method is the token verification approach [88]. In this method, Transport Layer Security (TLS) protocol with an encrypted token identification approach is used at every node to authenticate every entity before entering the network. So, it becomes a two-way identification procedure. It helps in warding off DDoS, man-in-the-middle, replay and impersonation attacks. It is practically proven and implemented in energy management systems.

The comparative study of miscellaneous approaches is done in Table 14.

6. Security requirements of industrial IIoT

From the above discussion, it can be deduced that few security requirements are indispensable for IIoT devices if smooth and consistent functioning of the industrial system is required. Some have been discussed below (see Fig. 6):

Table 14
Miscellaneous approaches.

Reference & Year	Objective	Approach	Performance measure
Disso et al. [132] & 2013	Securing SCADA using honeypot strategy.	Several honeypot studies.	Latency, Network traffic counter, Background Traffic, System calls, Hiden modules, UML,VMware characteristics.
Shitharth et al. [97] & 2015	Detecting DDoS in SCADA network.	Promisuous Mode Detection(PMD) technique.	Average Computation Time.
Chen et al. [133] & 2015	To understand the vulnerabilities in communication protocols of power systems.	Real Time Digital Simulator with LabVIEW and PXI.	Root Mean Square Error, Packets per second, Time Difference.
Alves et al. [134] & 2018	To detect DDoS attack against SCADA systems.	Lowering the priority of MODBUS request below the PLC.	Scan time test, PLC ladder logic execution test, SCADA connectivity test, Modbus injection attack test.
Bernieri et al. [135] & 2020	To detect attacks with high statistical confidence.	Blocking the connection which sends the packet faster than threshold.	Timing and storage based covert channel.
Zolanvari et al. [136] & 2021	Anomaly detection in IIoT	Distributed AI(DAI)	Matthews Correlation Coefficient(MCC), Accuracy and Undetected Rate(UR).
Yang et al. [88] & 2022	To secure SCADA system under DDoS attack.	Token Verification Approach	CPU idle time.

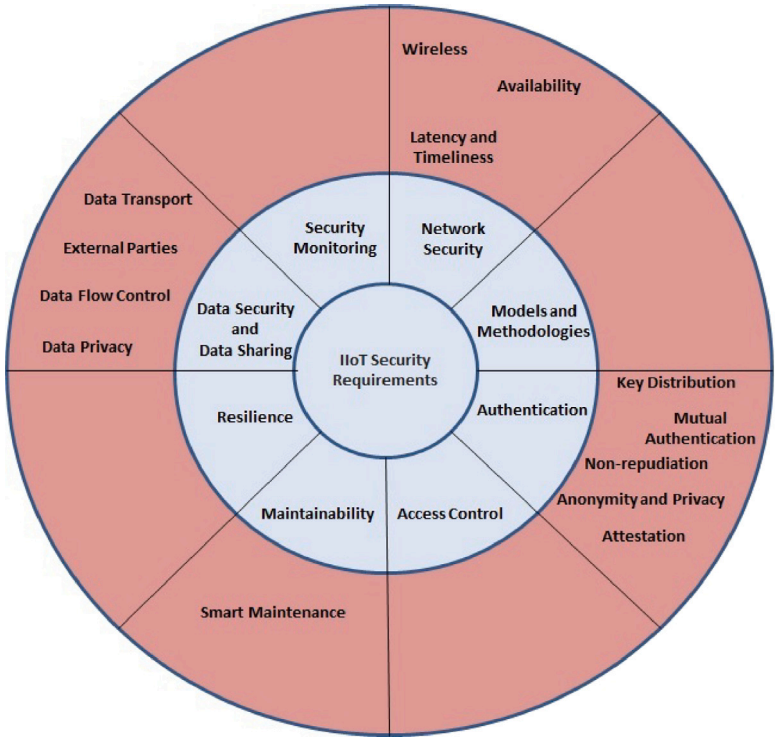


Fig. 6. Security requirements in IIoT [8].

- *Authentication*: Authentication exists in many forms. One of the well-known form is entity authentication. Another is data authentication. Authentication points out various other necessary aspects which need to be considered such as *Key Distribution, Mutual Authentication, Non-repudiation, Anonymity, Privacy* and *Attestation*. These aspects cannot be abandoned while providing authentication to an entity or data.
- *Data Safety*: An early view of the data security being linked to just data confidentiality was replaced by data availability and integrity also. But these properties are barely enough to define data security as connected devices and internet connectivity challenge them. Apart from documentation, notification, identification and prevention, data loss mitigation is also a requirement for cloud providers. Data security involves the smart use of the data internally and among the devices. For example, usage matrix can be used to have smart maintenance and critical information. A few important things which must be taken into account while considering data security are: *Data-Flow Control, External Parties, Data Transport* and *Data Privacy*.
- *Flexibility*: Resilience is a property by which a system is able to persist in an adversarial situation, rejuvenate its capabilities and complete its assigned task. IIoT systems also need to do the same. In order to provide this *continued* operation, the resource can be diversified, created redundancy or can be solved by hardening [137]. Few instances of resilience problems are loss of history due to intermittent connection and compromised device driver. Wireless Sensor Networks (WSN) in SCADA systems face issues related to communication resilience because of their interaction with proprietary SCADA protocols [138]. These issues can be resolved using automated standard compliance.
- *Network Security*: The major problem in the IIoT is the scalability and performance of a network. For *e.g.* bandwidth and latency arising due to complex and large networks [139]. Another problem is the systems used in communication, configuration and security which are propriety software and are not adjustable enough. Software Defined Networks(SDN) and Network Function Virtualization(NFV) is used to handle this challenge. They handle the management and overhead challenge, which means to dynamically reconfiguring the network and administer security policy. They also manage latency, timeliness and availability well [140]. Time Sensitive Networking(TSN) standard is used in hard time application sytems [141]. Apart from this, this is also well understood that legacy systems will continue for some time eventually before getting replaced; hence they should be secluded prudently so as to not provide superabundant overhead.
- *Supervision*: IIoT systems require monitoring, detecting and responding to familiar and unfamiliar risks because there are legacy systems that still require continuous monitoring and legacy systems lag the patches to do so [142]. This is done by Intrusion Detection Systems (IDS). Modbus and MQTT are good examples of this. IIoT systems should also monitor latency in response time and imbalanced datasets also [143,144]. The issue of predictability also affects IIoT due to intermittent and unfluctuating traffic routes. This leads to stealth injection attacks and honeypot attacks. Till now, statistical analysis and logs of the connected devices have been used, but they are not sufficient enough given the challenge of WSN and sparse lightweight environments are not enough. There should be less overhead to monitoring also [145]. Machine Learning tools have high false positive rates which should matter [146]. Adversarial samples are also not new, so robustness through monitoring is important. Threat response is also carried out through monitoring, this should also be an integral part. In an Edge-Cloud-based system resource overheads for small devices should be the least [145]. The network policies being followed should be carefully supervised and monitoring of the network should be eagerly done [147].
- *Models and their approach*: Models used in IIoT have complex and rather abstruse security needs, hence they are mostly observed as recommendations for improving security. Studies suggest that the design of IIoT systems should be carefully designed [148]. Discrete component identification and communication identifiers for every data transfer should be used. Every level of the architecture should be considered for security at development time and required steps should be taken. To have these functions security-by-design method should be used [149]. The self-adapting systems provide more flexibility to the security and business performance tradeoff with the help of self-adapting models and meta-models [150]. Security controls are provided by the security control assignment matrices. It should also be a practice to make specialized models other than generic ones. While making models, it should be carefully noted that the contemporary arrangement is the combination of both old and new technologies as the industry security is not sufficed by merely using one of them. The cliche requirement of the CIA, key management, prevention and scrutiny should also be taken care of. The concept of the cyber-range is being widely used as they inspect each other using attack and their response. After a thorough review, they are used in the industry [151]. Another factor is risk assessment. Proper risk assessment with sufficient parameters is also necessary. It is widely accepted that systems with inadequate risk assessment have a greater susceptibility to vulnerabilities [137]. Models can be built precisely using formal security analysis [152].
- *Managing Power*: IIoT systems must have the ability to reform and protect themselves from unknown vulnerabilities. This property is called maintainability. This can be done by updating firewalls and software patches. So, the system must be able to maintain itself [153]. Risk mitigation strategies for the vulnerable devices should be used in order to update them or they should be prioritized in the patch updation list. Updation should not bother any pre-existing service provided by any devices. Since the IIoT device updates are difficult to track they can be streamlined and can be made available in a decentralized marketplace to keep track and maintain transparency [154]. Maintenance frequency should also be high as it indicates safety. Important devices should remain less exposed to the internet.
- *Access Control*: IIoT devices must have an elementary form of Access Control (AC) mechanism for administrator and user access. It is important to have the clear privilege distinction in SCADA systems [155]. AC methods use authentication methods to verify the identity of the devices. AC is directly related to resource consumption and its availability. While combined with the cloud, fine-grained authorization control is required combined with the usual CIA and non-repudiation requirement [156]. AC protocols should also be able to handle availability, single point failure challenge in distributed environment [157]. It should also work in the federation whenever needed. Blockchain can also be used to provide dynamic access control [158]. The scheme should be scalable and transparent. The identity management in the AC mechanism should be compatible with legacy devices also [159]. Risk assessment of the AC protocols should be done and Zero Trust Networking(ZTN) protocols should be made [160].

7. Challenges in IIoT

In the section below, the challenges emanating from the IIoT are elucidated. These challenges should be meticulously considered while using any IIoT devices as ignoring these will not accomplish the desired objective which user of the device intends to achieve.

- *Legacy Systems*: From the studies, it is understood that the IIoT component is costly and usually made for a long-term life span. With the durability in the life span of the components, their

vulnerability also gets exacerbated. Their operational life becomes sensitive to evolving software and communication protocols. These software and communication protocols are used in components of the IIoT, hence they are critical to any industry. Hence, the challenge with long-term components is a major issue [161].

- *Communication Protocols*: Communication in simple plain text presents its own set of challenges due to a lack of security mechanisms. Specialized protocols exist in IIoT communication such as Modbus and Distributed Network Protocol (DNP3). Modbus challenges include exploitation of vendor method in implementing the protocol, change in protocol specification and attacks on the infrastructure which supports the protocol [162]. DNP3 protocol, on the other hand, is vulnerable to buffer flooding problems for an event [163]. It is observed, usually, the application and data link layer of protocols are vulnerable and hence need to be taken care of.
- *Multiple Access Points*: IIoT devices are disseminated from user devices to sensors and control systems. The servers can be protected at the core, but the field devices due to the limitation of storage capacity and bandwidth cannot be protected. The varying position of field devices also makes it tedious to provide any security mechanism. These devices use wireless, bluetooth, cellular and remote access to the network making them more vulnerable. Sniffing, spoofing, modification and loss of commands and data are common precedents. Tools such as Aircrack-NG are readily available.
- *Forensic Challenge*: In order to investigate any matter of concern in the industrial system or to find a vulnerability or an attack, analysts use various techniques. But challenges affect their method and devices also. These include the problem of live forensics in which the volatile data is very quickly lost. So, the data must be quickly acquired. Additionally, occasionally the response required by these systems also needs to be quick. The volatility of the data is caused due to rapid replacement of the data in the temporary memory [164]. Any delay in the acquisition of data will affect the response also. The response at any instance will be according to the data acquired. Another major problem with the IIoT system is that the system remains live for a long time and volatile memory changing the data affects the hash value at a particular instance, making the auditor's job more difficult to review the validity and integrity of the data. Apart from this, effective and updated logging system is also necessary for the investigators. Tools specific to IIoT devices such as SCADA are also required. It is also important to take into account the order of volatility as more volatile data such as cache and register must be captured early than other components.
- *Backdoors*: Backdoors are a major challenge to the IIoT as they help adversaries to take control of the IIoT system by circumventing the mandatory security mechanisms. There are very well-known previous precedents as well. The Stuxnet worm is a very acknowledged program that infiltrated the Iranian nuclear program PLC in 2010. It was remotely accessed using the backdoor available to the administrator. Though aware of the worm, still the use of hard code is in use which leads to more vulnerabilities.
- *Interaction challenge*: IIoT components such as SCADA and PLC interact in real time because the activity performed by them determines how the product is going to be developed. Hence, the devices have constraints to perform the task in a specified time frame. Time is a paramount logical resource. It determines the deviation process should occur as suggested. It also helps in the decision-making of the control system. The interaction among devices is also complex since the desired activity requires the synchronization of various operational components. It is important to understand severe operational requirements make the system more vulnerable. Past anecdotes show the complete shutdown of a diesel-electric generator costing $1 million [165] and automatic cessation of a nuclear power plant [161]. So, interaction among devices should be very carefully done as even a small mistake can lead to undefined and unwanted consequences.
- *Operating System*: SCADA system can easily get overwhelmed when an updated and evolved attack occurs. This is due to the patches which SCADA operating systems use. The operating system brings security and stability to the system and old patches lead to vulnerabilities remaining open. Hence, it should be our prime concern to keep the operating system up-to-date with the latest patch. But the challenges remain as the patches usually are not available on time. Apart from this, the absence of incentives also plays an important role. Most consumers do not update their system as the benefit of the updates remains obscure.
- *Security Protocol*: IIoT components such as SCADA and PLC lack security protocols. Moreover, the software used is commercial-off-the-shelf, which is not proprietary. So, it remains a point of challenge.
- *Priority Trade-off and Insider Attacks*: Often the updates in the IIoT system are not taken seriously since it stalls the ongoing operation and bring the system to a halt. But continuously working devices are a necessity in IIoT, so thoughtful consideration must be given to the trade-off before opting for updates. Also, there should be awareness of an insider attack. An insider attack may be unintentional or deliberate. In 2000, an annoyed employee attacked the sewage control system in Australia, flooding million litres of sewage [166].

8. Discussions and findings

Through this paper, it can be concluded that IIoT perhaps has vulnerabilities derived from IoT devices which acts as its soul. This brings challenges to IIoT despite bringing various benefits. It is visible that IIoT and IoT are highly correlated to each other and differ in only a few aspects. The difference arises due to the special constraints that IIoT possesses to process its products and the financial risks it involves. Financial impact captivates more interest as financial constraints are more prevalent. DDoS attack is one of the challenges addressed in this paper. To address this, the existing DDoS defense techniques, the merits, demerits, tools and the approach in IoT and IIoT is tabulated. Different types of attacks, tools involved in generating attacks and different types of traffic generators are discussed. To enhance it, the IIoT architecture and the levels that constitute the IIoT architecture is presented for understanding the vulnerabilities at different levels.

Further, the classification of the DDoS defence mechanism based on the approach they adopt such as machine learning, deep learning, transfer learning and federated learning approach is demonstrated. Even our survey is compared with preceding surveys that show our survey covers more aspects than any other paper comprising challenges, security requirement, classification and interoperability.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgements

Both the authors gratefully acknowledge the valuable contribution of comments from the reviewers for improving the quality of the paper. First author shows sincere gratitude to the University Grant Commission, Government of India, for supporting with a Junior Research Fellowship. The corresponding author greatly acknowledges the IoE grant of Banaras Hindu University and Ministry of Education.

References

[1] Himanshu Jaidka, Nikhil Sharma, Rajinder Singh, Evolution of IoT to IIoT: Applications & challenges, in: Proceedings of the International Conference on Innovative Computing & Communications, ICICC, 2020.

[2] Shrutika Mishra, Asha Ram Tripathi, Ai business model: an integrative business approach, Journal of Innovation and Entrepreneurship 10 (1) (2021) 18.

[3] Abhijeet C. Panchal, Vijay M. Khadse, Parikshit N. Mahalle, Security issues in IIoT: A comprehensive survey of attacks on IIoT and its countermeasures, in: 2018 IEEE Global Conference on Wireless Computing and Networking, GCWCN, IEEE, 2018, pp. 124–130.

[4] Shrutika Mishra, AR Tripathi, Literature review on business prototypes for digital platform, Journal of Innovation and Entrepreneurship 9 (1) (2020) 1–19.

[5] Ahmed Banafa, The industrial Internet of Things (IIoT): Challenges, Requirements and Benefits, River Publishers, 2018.

[6] Shrutika Mishra, Financial management and forecasting using business intelligence and big data analytic tools, International Journal of Financial Engineering 5 (02) (2018) 1850011.

[7] Shrutika Mishra, AR Tripathi, Platform business model on state-of-the-art business learning use case, International Journal of Financial Engineering 7 (02) (2020) 2050015.

[8] Koen Tange, Michele De Donno, Xenofon Fafoutis, Nicola Dragoni, A systematic survey of industrial Internet of Things security: Requirements and fog computing opportunities, IEEE Commun. Surv. Tutor. 22 (4) (2020) 2489–2520, http://dx.doi.org/10.1109/COMST.2020.3011208.

[9] Shrutika Mishra, AR Tripathi, Iot platform business model for innovative management systems, International Journal of Financial Engineering 7 (03) (2020) 2050030.

[10] Shrutika Mishra, AR Triptahi, Platforms oriented business and data analytics in digital ecosystem, International Journal of Financial Engineering 6 (04) (2019) 1950036.

[11] M. ENISA, Good Practices for Security of Internet of Things in the Context of Smart Manufacturing, European Union Agency for Network and Information Security (ENISA), 2018.

[12] S Mishra, Performance analysis of women in central bank monetary system using business intelligence, Global Journal of Management and Business Research 19 (3) (2019) 1–28.

[13] Shrutika Mishra, AR Tripathi, RS Singh, Priyanshu Mishra, Design and implementation of internet of everything's business platform ecosystem, 2021.

[14] Pei-Yih Ting, Jia-Lun Tsai, Tzong-Sun Wu, Signcryption method suitable for low-power IoT devices in a wireless sensor network, IEEE Syst. J. 12 (3) (2017) 2385–2394.

[15] Shrutika Mishra, Priyanshu Mishra, Analysis of platform business and secure business intelligence, International Journal of Financial Engineering 9 (03) (2022) 2250002.

[16] Shrutika Mishra, Priyanshu Mishra, AI business models: A strategic business dynamics, 2022.

[17] Yash Shah, Shamik Sengupta, A survey on classification of cyber-attacks on IoT and IIoT devices, in: 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference, UEMCON, IEEE, 2020, pp. 0406–0413.

[18] Shrutika Mishra, Priyanshu Mishra, An analytical analysis of alphabet and google platform business models, International Journal of Financial Engineering 10 (01) (2023) 2250029.

[19] Shrutika Mishra, Priyanshu Mishra, Ai business models and its impact on business strategic framework, International Journal of Financial Engineering 10 (02) (2023) 2350001.

[20] Tasnuva Mahjabin, Yang Xiao, Guang Sun, Wangdong Jiang, A survey of distributed denial-of-service attack, prevention, and mitigation techniques, Int. J. Distrib. Sens. Netw. 13 (12) (2017) 1550147717741463.

[21] Xingjie Yu, Huaqun Guo, A survey on IIoT security, in: 2019 IEEE VTS Asia Pacific Wireless Communications Symposium, APWCS, IEEE, 2019, pp. 1–5.

[22] Jayasree Sengupta, Sushmita Ruj, Sipra Das Bit, A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT, J. Netw. Comput. Appl. 149 (2020) 102481.

[23] Abhishek Hazra, Mainak Adhikari, Tarachand Amgoth, Satish Narayana Srirama, A comprehensive survey on interoperability for IIoT: Taxonomy, standards, and future directions, ACM Comput. Surv. 55 (1) (2021) 1–35.

[24] Shrutika Mishra, AR Tripathi, RS Singh, Priyanshu Mishra, Comparative analysis of digital business models, Journal of the Knowledge Economy (2023) 1–40.

[25] Shrutika Mishra, AI enabled platform business models and data analytics, Varanasi.

[26] Christos Douligeris, Aikaterini Mitrokotsa, DDoS attacks and defense mechanisms: Classification and state-of-the-art, Comput. Netw. 44 (5) (2004) 643–666.

[27] Tao Peng, Christopher Leckie, Kotagiri Ramamohanarao, Survey of network-based defense mechanisms countering the DoS and DDoS problems, ACM Comput. Surv. 39 (1) (2007) 3–es.

[28] Dakshil Shah, Varshali Kumar, TCP SYN cookie vulnerability, 2018, arXiv preprint arXiv:1807.08026.

[29] Khaled M. Elleithy, Drazen Blagovic, Wang K. Cheng, Paul Sideleau, Denial of service attack techniques: Analysis, implementation and comparison, 2005.

[30] Junho Choi, Chang Choi, Byeongkyu Ko, Pankoo Kim, A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment, Soft Comput. 18 (2014) 1697–1703.

[31] Jakub Czyz, Michael Kallitsis, Manaf Gharaibeh, Christos Papadopoulos, Michael Bailey, Manish Karir, Taming the 800 pound gorilla: The rise and decline of NTP DDoS attacks, in: Proceedings of the 2014 Conference on Internet Measurement Conference, 2014, pp. 435–448.

[32] Sanjeev Kumar, Smurf-based distributed denial of service (DDoS) attack amplification in internet, in: Second International Conference on Internet Monitoring and Protection, ICIMP 2007, IEEE, 2007, p. 25.

[33] Paul Watson, Slipping in the window: TCP reset attacks, 2004, Presentation at.

[34] Nazrul Hoque, Monowar H. Bhuyan, Ram Charan Baishya, Dhruba K. Bhattacharyya, Jugal K. Kalita, Network attacks: Taxonomy, tools and systems, J. Netw. Comput. Appl. 40 (2014) 307–324.

[35] David Dittrich, The DoS project's 'trinoo'distributed denial of service attack tool, 1999.

[36] Paul J. Criscuolo, Distributed Denial of Service: Trin00, Tribe Flood Network, Tribe Flood Network 2000, and Stacheldraht Ciac-2319, Technical Report, California Univ Livermore Radiation Lab, 2000.

[37] Packet Storm, https://packetstormsecurity.com/.

[38] DDoS attack tools, https://sourceforge.net/directory/?q=ddos+attack+tools.

[39] Sunny Behal, Krishan Kumar, Characterization and comparison of DDoS attack tools and traffic generators: A review, Int. J. Netw. Secur. 19 (3) (2017) 383–393.

[40] Stefano Avallone, Antonio Pescape, Giorgio Ventre, Distributed internet traffic generator (D-ITG): analysis and experimentation over heterogeneous networks, in: Poster at International Conference on Network Protocols, ICNP, 2003.

[41] Krishna Kant, Vijay Tewari, Ravishankar Iyer, Geist: A web traffic generation tool, in: Computer Performance Evaluation: Modelling Techniques and Tools: 12th International Conference, TOOLS 2002 London, UK, April 14–17, 2002 Proceedings 12, Springer, 2002, pp. 227–232.

[42] ByteBlower, 2014, https://www.excentis.com/blog/.

[43] Netperf, 2015, https://hewlettpackard.github.io/netperf/.

[44] Internet traffic research group, packmine, 2005, https://www.isi.edu/nsnam/ns/doc/node555.html.

[45] KUTE- kernel-based traffic engine, 2007, http://caia.swin.edu.au/genius/tools/kute/.

[46] ICIT, traffic generators internet traffic, 2010, http://www.icir.org/models/trafficgenerators.html.

[47] Ostinato Traffic Generator for Network Engineers — ostinato.org, 2010, https://ostinato.org/.

[48] iPerf-, https://iperf.fr/iperf-download.php.

[49] Vaishali Kansal, Mayank Dave, DDoS attack isolation using moving target defense, in: 2017 International Conference on Computing, Communication and Automation, ICCCA, IEEE, 2017, pp. 511–514.

[50] Mohammed H. Sqalli, Fahd Al-Haidari, Khaled Salah, Edos-shield-a two-steps mitigation technique against edos attacks in cloud computing, in: 2011 Fourth IEEE International Conference on Utility and Cloud Computing, IEEE, 2011, pp. 49–56.

[51] Kihong Park, Heejo Lee, On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets, ACM SIGCOMM Comput. Commun. Rev. 31 (4) (2001) 15–26.

[52] Angelos D. Keromytis, Vishal Misra, Dan Rubenstein, SOS: Secure overlay services, ACM SIGCOMM Comput. Commun. Rev. 32 (4) (2002) 61–72.

[53] Lukas Krämer, Johannes Krupp, Daisuke Makita, Tomomi Nishizoe, Takashi Koide, Katsunari Yoshioka, Christian Rossow, Amppot: Monitoring and defending against amplification DDoS attacks, in: Research in Attacks, Intrusions, and Defenses: 18th International Symposium, RAID 2015, Kyoto, Japan, November 2-4, 2015. Proceedings 18, Springer, 2015, pp. 615–636.

[54] Bo Sun, Lawrence Osborne, Yang Xiao, Sghaier Guizani, Intrusion detection techniques in mobile ad hoc and wireless sensor networks, IEEE Wirel. Commun. 14 (5) (2007) 56–63.

[55] Julius Jow, Yang Xiao, Wenlin Han, A survey of intrusion detection systems in smart grid, Int. J. Sensor Netw. 23 (3) (2017) 170–186.

[56] Alireza Izaddoost, Mohamed Othman, Mohd Fadlee A. Rasid, Accurate ICMP traceback model under DoS/DDoS attack, in: 15th International Conference on Advanced Computing and Communications, ADCOM 2007, IEEE, 2007, pp. 441–446.

[57] Xin Liu, Xiaowei Yang, Yanbin Lu, To filter or to authorize: Network-layer DoS defense against multimillion-node botnets, in: Proceedings of the ACM SIGCOMM 2008 Conference on Data Communication, 2008, pp. 195–206.

[58] Xin Liu, Xiaowei Yang, Yong Xia, Netfence: Preventing internet denial of service from inside out, ACM SIGCOMM Comput. Commun. Rev. 40 (4) (2010) 255–266.

[59] Michael Menth, Rüdiger Martin, Joachim Charzinski, Capacity overprovisioning for networks with resilience requirements, ACM SIGCOMM Comput. Commun. Rev. 36 (4) (2006) 87–98.

[60] Qusay F. Hassan, Introduction to the Internet of Things, in: Internet of Things a to Z: Technologies and Applications, 2018, pp. 1–50, http://dx.doi.org/10.1002/9781119456735.ch1.

[61] Kalathiripi Rambabu, N. Venkatram, Ensemble classification using traffic flow metrics to predict distributed denial of service scope in the Internet of Things (IoT) networks, Comput. Electr. Eng. 96 (2021) 107444.

[62] Lingfeng Huang, Design of an IoT DDoS attack prediction system based on data mining technology, J. Supercomput. 78 (4) (2022) 4601–4623.

[63] Muhammad Reazul Haque, Saw Chin Tan, Zulfadzli Yusoff, Kashif Nisar, Rizaludin Kaspin, Iram Haider, Sana Nisar, Joel J.P.C. Rodrigues, Bhawani Shankar Chowdhry, Muhammad Aslam Uqaili, et al., Unprecedented smart algorithm for uninterrupted SDN services during DDoS attack, Comput. Mater. Continua 70 (1) (2022) 875–894.

[64] Ivan Cvitić, Dragan Peraković, Marko Periša, Mate Botica, Novel approach for detection of IoT generated DDoS traffic, Wirel. Netw. 27 (3) (2021) 1573–1586.

[65] Ladislav Huraj, Marek Šimon, Tibor Horák, Resistance of IoT sensors against DDoS attack in smart home environment, Sensors 20 (18) (2020) 5298.

[66] Prahlad Kumar, Harnoor Bagga, Bhuneshwar Singh Netam, Venkanna Uduthalapally, Sad-IoT: Security analysis of DDoS attacks in IoT networks, Wirel. Pers. Commun. 122 (1) (2022) 87–108.

[67] Keval Doshi, Yasin Yilmaz, Suleyman Uludag, Timely detection and mitigation of stealthy DDoS attacks via IoT networks, IEEE Trans. Dependable Secure Comput. 18 (5) (2021) 2164–2176.

[68] Manorama Mohapatro, Itu Snigdh, An experimental study of distributed denial of service and sink hole attacks on IoT based healthcare applications, Wirel. Pers. Commun. 121 (1) (2021) 707–724.

[69] Yong-joon Lee, Hwa-sung Chae, Keun-wang Lee, Countermeasures against large-scale reflection DDoS attacks using exploit IoT devices, Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije 62 (1) (2021) 127–136.

[70] Ahamed Aljuhani, Machine learning approaches for combating distributed denial of service attacks in modern networking environments, IEEE Access 9 (2021) 42236–42264.

[71] Tolijan Trajanovski, Ning Zhang, An automated behaviour-based clustering of IoT botnets, Future Internet 14 (1) (2021) 6.

[72] Song Wang, Karina Gomez, Kandeepan Sithamparanathan, Muhammad Rizwan Asghar, Giovanni Russello, Paul Zanna, Mitigating DDoS attacks in sdn-based IoT networks leveraging secure control and data plane algorithm, Appl. Sci. 11 (3) (2021) 929.

[73] Tong Liu, Fariza Sabrina, Julian Jang-Jaccard, Wen Xu, Yuanyuan Wei, Artificial intelligence-enabled DDoS detection for blockchain-based smart transport systems, Sensors 22 (1) (2021) 32.

[74] Cong Fan, Nitheesh Murugan Kaliyamurthy, Shi Chen, He Jiang, Yiwen Zhou, Carlene Campbell, Detection of DDoS attacks in software defined networking using entropy, Appl. Sci. 12 (1) (2021) 370.

[75] Jiushuang Wang, Ying Liu, Huifen Feng, IFACNN: Efficient DDoS attack detection based on improved firefly algorithm to optimize convolutional neural networks, Math. Biosci. Eng. 19 (2) (2022) 1280–1303.

[76] Mohammad Najafimehr, Sajjad Zarifzadeh, Seyedakbar Mostafavi, A hybrid machine learning approach for detecting unprecedented DDoS attacks, J. Supercomput. 78 (6) (2022) 8106–8136.

[77] Muhammad Ibrahim, Muhammad Hanif, Shabir Ahmad, Faisal Jamil, Tayyaba Sehar, YunJung Lee, DoHyeun Kim, SDN Based DDoS Mitigating Approach Using Traffic Entropy for IoT Network.

[78] Deepak Kumar Sharma, Tarun Dhankhar, Gaurav Agrawal, Satish Kumar Singh, Deepak Gupta, Jamel Nebhen, Imran Razzak, Anomaly detection framework to prevent DDoS attack in fog empowered IoT networks, Ad Hoc Netw. 121 (2021) 102603.

[79] Ivan Cvitić, Dragan Perakovic, Brij B. Gupta, Kim-Kwang Raymond Choo, Boosting-based DDoS detection in Internet of Things systems, IEEE Internet Things J. 9 (3) (2021) 2109–2123.

[80] Wencheng Yin, Yunhe Cui, Qing Qian, Guowei Shen, Chun Guo, Saifei Li, DIAMOND: A structured coevolution feature optimization method for lddos detection in SDN-IoT, Wirel. Commun. Mob. Comput. 2021 (2021).

[81] Javed Ashraf, Marwa Keshk, Nour Moustafa, Mohamed Abdel-Basset, Hasnat Khurshid, Asim D. Bakhshi, Reham R. Mostafa, IoTBoT-IDS: A novel statistical learning-enabled botnet detection framework for protecting networks of smart cities, Sustainable Cities Soc. 72 (2021) 103041.

[82] Nivedita Mishra, Sharnil Pandya, Chirag Patel, Nagaraj Cholli, Kirit Modi, Pooja Shah, Madhuri Chopade, Sudha Patel, Ketan Kotecha, Memcached: An experimental study of DDoS attacks for the wellbeing of IoT applications, Sensors 21 (23) (2021) 8071.

[83] Muhammad Zeeshan, Qaiser Riaz, Muhammad Ahmad Bilal, Muhammad K. Shahzad, Hajira Jabeen, Syed Ali Haider, Azizur Rahim, Protocol-based deep intrusion detection for DoS and DDoS attacks using UNSW-NB15 and bot-IoT data-sets, IEEE Access 10 (2021) 2269–2283.

[84] Omerah Yousuf, Roohie Naaz Mir, DDoS attack detection in Internet of Things using recurrent neural network, Comput. Electr. Eng. 101 (2022) 108034.

[85] Jing Zheng, Qi Li, Guofei Gu, Jiahao Cao, David K.Y. Yau, Jianping Wu, Realtime DDoS defense using COTS SDN switches via adaptive correlation analysis, IEEE Trans. Inf. Forensics Secur. 13 (7) (2018) 1838–1853.

[86] Miao Du, Kun Wang, An SDN-enabled pseudo-honeypot strategy for distributed denial of service attacks in industrial Internet of Things, IEEE Trans. Ind. Inform. 16 (1) (2019) 648–657.

[87] Hengchang Jing, Jian Wang, Detection of DDoS attack within industrial IoT devices based on clustering and graph structure features, Secur. Commun. Netw. 2022 (2022).

[88] Yu-Sheng Yang, Shih-Hsiung Lee, Wei-Che Chen, Chu-Sing Yang, Yuen-Min Huang, Ting-Wei Hou, Securing SCADA energy management system under DDoS attacks using token verification approach, Appl. Sci. 12 (1) (2022) 530.

[89] Tibor Horak, Peter Strelec, Ladislav Huraj, Pavol Tanuska, Andrea Vaclavova, Michal Kebisek, The vulnerability of the production line using industrial IoT systems under DDoS attack, Electronics 10 (4) (2021) 381.

[90] Vladimir Borgiani, Patrick Moratori, Juliano F. Kazienko, Emilio R.R. Tubino, Silvio E. Quincozes, Toward a distributed approach for detection and mitigation of denial-of-service attacks within industrial Internet of Things, IEEE Internet Things J. 8 (6) (2020) 4569–4578.

[91] Hongcheng Huang, Peixin Ye, Min Hu, Jun Wu, A multi-point collaborative DDoS defense mechanism for IIoT environment, Digit. Commun. Netw. (2022).

[92] P.L.S. Jayalaxmi, Gulshan Kumar, Rahul Saha, Mauro Conti, Tai-hoon Kim, Reji Thomas, DeBot: A deep learning-based model for bot detection in industrial Internet-of-Things, Comput. Electr. Eng. 102 (2022) 108214.

[93] Abdulghani Ali Ahmed, Waheb A. Jabbar, Ali Safaa Sadiq, Hiran Patel, Deep learning-based classification model for botnet attack detection, J. Ambient Intell. Humaniz. Comput. (2020) 1–10.

[94] Wan-Chen Shi, Hung-Min Sun, DeepBot: A time-based botnet detection with deep learning, Soft Comput. 24 (21) (2020) 16605–16616.

[95] Abbas Yazdinejad, Mostafa Kazemi, Reza M. Parizi, Ali Dehghantanha, Hadis Karimipour, An ensemble deep learning model for cyber threat hunting in industrial Internet of Things, Digit. Commun. Netw. (2022).

[96] Sajid Nazir, Shushma Patel, Dilip Patel, Assessing and augmenting SCADA cyber security: A survey of techniques, Comput. Secur. 70 (2017) 436–454.

[97] S. Shitharth, D. Prince Winston, A comparative analysis between two counter-measure techniques to detect DDoS with sniffers in a SCADA network, Proc. Technol. 21 (2015) 179–186.

[98] Jasna D. Markovic-Petrovic, Mirjana D. Stojanovic, Analysis of SCADA system vulnerabilities to DDoS attacks, in: 2013 11th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services (Telsiks), Vol. 2, IEEE, 2013, pp. 591–594.

[99] Wazir Zada Khan, M.H. Rehman, Hussein Mohammed Zangoti, Muhammad Khalil Afzal, Nasrullah Armi, Khaled Salah, Industrial Internet of Things: Recent advances, enabling technologies and open challenges, Comput. Electr. Eng. 81 (2020) 106522.

[100] Mohamed Amine Ferrag, Othmane Friha, Djallel Hamouda, Leandros Maglaras, Helge Janicke, Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning, IEEE Access 10 (2022) 40281–40306.

[101] Maede Zolanvari, Marcio A. Teixeira, Lav Gupta, Khaled M. Khan, Raj Jain, Machine learning-based network vulnerability analysis of industrial Internet of Things, IEEE Internet Things J. 6 (4) (2019) 6822–6834.

[102] Muna Al-Hawawreh, Elena Sitnikova, Neda Aboutorab, X-IIoTid: A connectivity-agnostic and device-agnostic intrusion data set for industrial Internet of Things, IEEE Internet Things J. 9 (5) (2021) 3962–3977.

[103] Marcio Andrey Teixeira, Tara Salman, Maede Zolanvari, Raj Jain, Nader Meskin, Mohammed Samaka, SCADA system testbed for cybersecurity research using machine learning approach, Future Internet 10 (8) (2018) 76.

[104] Fahd A. Alhaidari, Ezaz Mohammed AL-Dahasi, New approach to determine DDoS attack patterns on SCADA system using machine learning, in: 2019 International Conference on Computer and Information Sciences, ICCIS, IEEE, 2019, pp. 1–6.

[105] Fatma Taher, Mahmoud Abdel-salam, Mohamed Elhoseny, Ibrahim M. Elhasnony, Reliable machine learning model for IIoT botnet detection, IEEE Access (2023).

[106] Love Allen Chijioke Ahakonye, Cosmas Ifeanyi Nwakanma, Jae-Min Lee, Dong-Seong Kim, SCADA intrusion detection scheme exploiting the fusion of modified decision tree and Chi-square feature selection, Internet Things 21 (2023) 100676.

[107] Tianyang Cai, Tao Jia, Sridhar Adepu, Yuqi Li, Zheng Yang, ADAM: An adaptive DDoS attack mitigation scheme in software-defined cyber-physical system, IEEE Trans. Ind. Inform. (2023).

[108] Mouaad Mohy-Eddine, Azidine Guezzaz, Said Benkirane, Mourade Azrour, Yousef Farhaoui, An ensemble learning based intrusion detection model for industrial IoT security, Big Data Min. Anal. 6 (3) (2023) 273–287.

[109] Abdussalam Ahmed Alashhab, Mohd Soperi Mohd Zahid, Amgad Muneer, Mujaheed Abdullahi, Low-rate DDoS attack detection using deep learning for SDN-enabled IoT networks, Int. J. Adv. Comput. Sci. Appl. 13 (11) (2022).

[110] Ahmad Zainudin, Love Allen Chijioke Ahakonye, Rubina Akter, Dong-Seong Kim, Jae-Min Lee, An efficient hybrid-dnn for DDoS detection and classification in software-defined IIoT networks, IEEE Internet Things J. (2022).

[111] Ines Ortega-Fernandez, Marta Sestelo, Juan C Burguillo, Camilo Piñón-Blanco, Network intrusion detection system for DDoS attacks in ICS using deep autoencoders, Wirel. Netw. (2023) 1–17.

[112] Sayawu Yakubu Diaba, Mohammed Elmusrati, Proposed algorithm for smart grid DDoS detection based on deep learning, Neural Netw. 159 (2023) 175–184.

[113] Mehul Sharma, Shrid Pant, Priety Yadav, Deepak Kumar Sharma, Nitin Gupta, Gautam Srivastava, Advancing security in the industrial Internet of Things using deep progressive neural networks, Mob. Netw. Appl. (2023) 1–13.

[114] Jiawei Du, Kai Yang, Yanjing Hu, Lingjie Jiang, NIDS-CNNLSTM: Network intrusion detection classification model based on deep learning, IEEE Access 11 (2023) 24808–24821.

[115] Hakan Can Altunay, Zafer Albayrak, A hybrid CNN+ LSTMbased intrusion detection system for industrial IoT networks, Eng. Sci. Technol. Int. J. 38 (2023) 101322.

[116] Jianhua Li, Lingjuan Lyu, Ximeng Liu, Xuyun Zhang, Xixiang Lyu, FLEAM: A federated learning empowered architecture to mitigate DDoS in industrial IoT, IEEE Trans. Ind. Inform. 18 (6) (2021) 4059–4068.

[117] Viraaji Mothukuri, Prachi Khare, Reza M. Parizi, Seyedamin Pouriyeh, Ali Dehghantanha, Gautam Srivastava, Federated-learning-based anomaly detection for IoT security attacks, IEEE Internet Things J. 9 (4) (2021) 2545–2554.

[118] Love Allen Chijioke Ahakonye, Cosmas Ifeanyi Nwakanma, Jae Min Lee, Dong-Seong Kim, FED-MARINE: Federated Learning Framework for DDoS Detection and Mitigation in Maritime-SCADA Network.

[119] Ahmad Zainudin, Rubina Akter, Dong-Seong Kim, Jae-Min Lee, Privacy-preserving federated learning-based DDoS classification for IIoT networks, 2022, pp. 504–505.

[120] Ahmad Zainudin, Rubina Akter, Dong-Seong Kim, Jae-Min Lee, FedDDoS: An efficient federated learning-based DDoS attacks classification in SDN-enabled IIoT networks, in: 2022 13th International Conference on Information and Communication Technology Convergence, ICTC, IEEE, 2022, pp. 1279–1283.

[121] Ons Aouedi, Kandaraj Piamrat, Guillaume Muller, Kamal Singh, Federated semisupervised learning for attack detection in industrial Internet of Things, IEEE Trans. Ind. Inform. 19 (1) (2022) 286–295.

[122] Md Mamunur Rashid, Shahriar Usman Khan, Fariha Eusufzai, Md Azharuddin Redwan, Saifur Rahman Sabuj, Mahmoud Elsharief, A federated learning-based approach for improving intrusion detection in industrial Internet of Things networks, Network 3 (1) (2023) 158–179.

[123] Xabier Sáez-de Cámara, Jose Luis Flores, Cristóbal Arellano, Aitor Urbieta, Urko Zurutuza, Clustered federated learning architecture for network anomaly detection in large scale heterogeneous IoT networks, 2023, arXiv preprint arXiv:2303.15986.

[124] Subir Halder, Thomas Newe, Radio fingerprinting for anomaly detection using federated learning in LoRa-enabled industrial Internet of Things, Future Gener. Comput. Syst. 143 (2023) 322–336.

[125] Othmane Friha, Mohamed Amine Ferrag, Mohamed Benbouzid, Tarek Berghout, Burak Kantarci, Kim-Kwang Raymond Choo, 2DF-IDS: Decentralized and differentially private federated learning-based intrusion detection system for industrial IoT, Comput. Secur. (2023) 103097.

[126] Ly Vu, Quang Uy Nguyen, Diep N. Nguyen, Dinh Thai Hoang, Eryk Dutkiewicz, Deep transfer learning for IoT attack detection, IEEE Access 8 (2020) 107335–107344.

[127] Selim Yılmaz, Emre Aydogan, Sevil Sen, A transfer learning approach for securing resource-constrained IoT devices, IEEE Trans. Inf. Forensics Secur. 16 (2021) 4405–4418.

[128] Weiping Wang, Zhaorong Wang, Zhanfan Zhou, Haixia Deng, Weiliang Zhao, Chunyang Wang, Yongzhen Guo, Anomaly detection of industrial control systems based on transfer learning, Tsinghua Sci. Technol. 26 (6) (2021) 821–832.

[129] Hüseyin Polat, Muammer Türkoğlu, Onur Polat, Abdülkadir Şengür, A novel approach for accurate detection of the DDoS attacks in SDN-based SCADA systems based on deep recurrent neural networks, Expert Syst. Appl. 197 (2022) 116748.

[130] Unsub Shafiq, Muhammad Khuram Shahzad, Muhammad Anwar, Qaisar Shaheen, Muhammad Shiraz, Abdullah Gani, Transfer learning auto-encoder neural networks for anomaly detection of DDoS generating IoT devices, Secur. Commun. Netw. 2022 (2022).

[131] Eva Rodríguez, Pol Valls, Beatriz Otero, Juan José Costa, Javier Verdú, Manuel Alejandro Pajuelo, Ramon Canal, Transfer-learning-based intrusion detection framework in IoT networks, Sensors 22 (15) (2022) 5621.

[132] Jules Pagna Disso, Kevin Jones, Steven Bailey, A plausible solution to SCADA security honeypot systems, in: 2013 Eighth International Conference on Broadband and Wireless Computing, Communication and Applications, IEEE, 2013, pp. 443–448.

[133] Bo Chen, Nishant Pattanaik, Ana Goulart, Karen L. Butler-Purry, Deepa Kundur, Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed, in: 2015 IEEE International Workshop Technical Committee on Communications Quality and Reliability, CQR, IEEE, 2015, pp. 1–6.

[134] Thiago Alves, Thomas Morris, OpenPLC: An IEC 61,131–3 compliant open source industrial controller for cyber security research, Comput. Secur. 78 (2018) 364–379.

[135] Giuseppe Bernieri, Stefano Cecconello, Mauro Conti, Gianluca Lain, TAMBUS: A novel authentication method through covert channels for securing industrial networks, Comput. Netw. 183 (2020) 107583.

[136] Maede Zolanvari, Ali Ghubaish, Raj Jain, Addai: Anomaly detection using distributed ai, in: 2021 IEEE International Conference on Networking, Sensing and Control, Vol. 1, ICNSC, IEEE, 2021, pp. 1–6.

[137] Aron Laszka, Waseem Abbas, Yevgeniy Vorobeychik, Xenofon Koutsoukos, Synergistic security for the industrial Internet of Things: Integrating redundancy, diversity, and hardening, in: 2018 IEEE International Conference on Industrial Internet, ICII, IEEE, 2018, pp. 153–158.

[138] Fábio Januário, Carolina Carvalho, Alberto Cardoso, Paulo Gil, Security challenges in SCADA systems over wireless sensor and actuator networks, in: 2016 8th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops, ICUMT, IEEE, 2016, pp. 363–368.

[139] Petr Kadera, Petr Novák, Performance modeling extension of directory facilitator for enhancing communication in FIPA-compliant multiagent systems, IEEE Trans. Ind. Inform. 13 (2) (2016) 688–695.

[140] Manuel Cheminod, Luca Durante, Lucia Seno, Fulvio Valenza, Adriano Valenzano, Claudio Zunino, Leveraging SDN to improve security in industrial networks, in: 2017 IEEE 13th International Workshop on Factory Communication Systems, WFCS, IEEE, 2017, pp. 1–7.

[141] Thomas Kobzan, Sebastian Schriegel, Simon Althoff, Alexander Boschmann, Jens Otto, Jürgen Jasperneite, Secure and time-sensitive communication for remote process control and monitoring, in: 2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation, Vol. 1, ETFA, IEEE, 2018, pp. 1105–1108.

[142] Ekhi Zugasti, Mikel Iturbe, Iñaki Garitano, Urko Zurutuza, Null is not always empty: Monitoring the null space for field-level anomaly detection in industrial IoT environments, in: 2018 Global Internet of Things Summit, GIoTS, IEEE, 2018, pp. 1–6.

[143] Md Mahmud Hasan, Hussein T. Mouftah, Cloud-centric collaborative security service placement for advanced metering infrastructures, IEEE Trans. Smart Grid 10 (2) (2017) 1339–1348.

[144] Maede Zolanvari, Marcio A. Teixeira, Raj Jain, Effect of imbalanced datasets on security of industrial IoT using machine learning, in: 2018 IEEE International Conference on Intelligence and Security Informatics, ISI, IEEE, 2018, pp. 112–117.

[145] Qiao Yan, Wenyao Huang, Xupeng Luo, Qingxiang Gong, F. Richard Yu, A multi-level DDoS mitigation framework for the industrial internet of things, IEEE Commun. Mag. 56 (2) (2018) 30–36.

[146] Salwa Alem, David Espes, Eric Martin, Laurent Nana, Florent De Lamotte, A hybrid intrusion detection system in industry 4.0 based on ISA95 standard, in: 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications, AICCSA, IEEE, 2019, pp. 1–8.

[147] Andrea Melis, Davide Berardi, Chiara Contoli, Franco Callegati, Flavio Esposito, Marco Prandini, A policy checker approach for secure industrial SDN, in: 2018 2nd Cyber Security in Networking Conference, CSNet, IEEE, 2018, pp. 1–7.

[148] Ghaidaa Shaabany, Reiner Anderl, Security by design as an approach to design a secure industry 4.0-capable machine enabling online-trading of technology data, in: 2018 International Conference on System Science and Engineering, ICSSE, IEEE, 2018, pp. 1–5.

[149] Amin Hassanzadeh, Shimon Modi, Shaan Mulchandani, Towards effective security control assignment in the industrial Internet of Things, in: 2015 IEEE 2nd World Forum on Internet of Things, WF-IoT, IEEE, 2015, pp. 795–800.

[150] Silia Maksuti, Ani Bicaku, Markus Tauber, Silke Palkovits-Rauter, Sarah Haas, Jerker Delsing, Towards flexible and secure end-to-end communication in industry 4.0, in: 2017 IEEE 15th International Conference on Industrial Informatics, INDIN, IEEE, 2017, pp. 883–888.

[151] Adrien Becue, Yannick Fourastier, Isabel Praça, Alexandre Savarit, Claude Baron, Baptiste Gradussofs, Etienne Pouille, Carsten Thomas, CyberFactory# 1—Securing the industry 4.0 with cyber-ranges and digital twins, in: 2018 14th IEEE International Workshop on Factory Communication Systems, WFCS, IEEE, 2018, pp. 1–4.

[152] Haralambos Mouratidis, Vasiliki Diamantopoulou, A security analysis method for industrial Internet of Things, IEEE Trans. Ind. Inform. 14 (9) (2018) 4093–4100.

[153] Luying Zhou, Huaqun Guo, Anomaly detection methods for IIoT networks, in: 2018 IEEE International Conference on Service Operations and Logistics, and Informatics, SOLI, IEEE, 2018, pp. 214–219.

[154] Andreas Seitz, Dominic Henze, Daniel Miehle, Bernd Bruegge, Jochen Nickles, Markus Sauer, Fog computing as enabler for blockchain-based IIoT app marketplaces-A case study, in: 2018 Fifth International Conference on Internet of Things: Systems, Management and Security, IEEE, 2018, pp. 182–188.

[155] Gregory Falco, Carlos Caldera, Howard Shrobe, IIoT cybersecurity risk modeling for SCADA systems, IEEE Internet Things J. 5 (6) (2018) 4486–4495.

[156] Fagen Li, Jiaojiao Hong, Anyembe Andrew Omala, Efficient certificateless access control for industrial Internet of Things, Future Gener. Comput. Syst. 76 (2017) 285–292.

[157] Chao Lin, Debiao He, Xinyi Huang, Kim-Kwang Raymond Choo, Athanasios V. Vasilakos, BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0, J. Netw. Comput. Appl. 116 (2018) 42–52.

[158] Asma Lahbib, Khalifa Toumi, Anis Laouiti, Steven Martin, DRMF: A distributed resource management framework for industry 4.0 environments, in: 2019 IEEE 18th International Symposium on Network Computing and Applications, NCA, IEEE, 2019, pp. 1–9.
[159] Davy Preuveneers, Wouter Joosen, Elisabeth Ilie-Zudor, Identity management for cyber-physical production workflows and individualized manufacturing in industry 4.0, in: Proceedings of the Symposium on Applied Computing, 2017, pp. 1452–1455.
[160] Romans Vanickis, Paul Jacob, Sohelia Dehghanzadeh, Brian Lee, Access control policy enforcement for zero-trust-networking, in: 2018 29th Irish Signals and Systems Conference, ISSC, IEEE, 2018, pp. 1–6.
[161] Brent Kesler, The vulnerability of nuclear facilities to cyber attack; strategic insights: Spring 2010, in: Strategic Insights, Spring 2011, Monterey, California. Naval Postgraduate School, 2011.
[162] Peter Huitsing, Rodrigo Chandia, Mauricio Papa, Sujeet Shenoi, Attack taxonomies for the Modbus protocols, Int. J. Crit. Infrastruct. Prot. 1 (2008) 37–44.
[163] Dong Jin, David M. Nicol, Guanhua Yan, An event buffer flooding attack in DNP3 controlled SCADA systems, in: Proceedings of the 2011 Winter Simulation Conference, WSC, IEEE, 2011, pp. 2614–2626.
[164] Peter Eden, Andrew Blyth, Kevin Jones, Hugh Soulsby, Pete Burnap, Yulia Cherdantseva, Kristan Stoddart, SCADA system forensic analysis within IIoT, in: Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing, Springer, 2017, pp. 73–101.
[165] Anurag Srivastava, Thomas Morris, Timothy Ernster, Ceeman Vellaithurai, Shengyi Pan, Uttam Adhikari, Modeling cyber-physical vulnerability of the smart grid with incomplete information, IEEE Trans. Smart Grid 4 (1) (2013) 235–244.
[166] Jill Slay, Michael Miller, Lessons Learned from the Maroochy Water Breach, Springer, 2008.

Shubhankar Chaudhary is a research scholar under the supervision of Prof. P.K Mishra in Department of Computer Science, Institute of Science, Banaras Hindu University, Varanasi (India). His research interest includes Network Security, Machine Learning and Internet of Things.
EMAIL ID: chaudharyshubhankar@gmail.com

P.K. Mishra is Professor at Department of Computer Science, Institute of Science, Banaras Hindu University, India. He is also a Principal Investigator of the research projects at DST Centre for Interdisciplinary Mathematical Sciences, Banaras Hindu University. He is a senior member of IEEE. His research interests include Computational Complexity, Data Mining, IoT, High Performance Computing and VLSI Algorithms.
EMAIL ID: mishra@bhu.ac.in