SAMQUEST-Journal of Emerging Innovations
E-ISSN 3108-1207
Vol.1,Issue 2,pp.145-160 , July- Dec 25
Available online at : https://www.samglobaluniversity.ac.in/archives/

Review

Enhancing Cyber security in Cyber-Physical Systems and IoT Networks: A Comprehensive Review of Recent Advances and Challenges

Mohit Jain[1] , Dr Saurabh Mandloi[2]
Saurabh Mandloi[2] School of computer Sciences. SAM Global University Bhopal
Corresponding Email:- **bmctmohitcs@gmail.com**

Received:12/July/2025; **Accepted**:15/July/2025 ;**Published**:7/Feb/2026

Abstract-The Internet of Things (IoT) has revolutionized modern technology through the interconnectedness of smart devices, creating unprecedented opportunities across various sectors. However, these innovations also introduce complex security challenges, with cybersecurity becoming a pivotal concern, especially for intrusion detection systems (IDS). Deep Learning has shown promise in effectively detecting and preventing cyberattacks on IoT devices. Despite the critical role of IDS in safeguarding sensitive information by identifying and mitigating suspicious activities, conventional IDS solutions face significant challenges within the IoT context. This paper explores the cutting-edge intrusion detection methods for IoT security, anchored in Deep Learning. We review recent advancements in IDS for IoT, focusing on the underlying deep learning algorithms, relevant datasets, types of attacks, and evaluation metrics. Additionally, we discuss the challenges encountered in deploying Deep Learning for IoT security and suggest potential areas for future research. This comprehensive survey aims to guide researchers and industry experts in adopting Deep Learning techniques for enhancing IoT security and intrusion detection, highlighting emerging trends and recent developments in the field.

Keywords -Cyber-Physical Systems (CPS), Internet of Things (IoT), Convolutional Neural Network, Attacks

Introduction

The Internet of Things (IoT) is an emerging industry that will significantly change how we use technology and the physical environment. By 2025, it is expected that there will be 30 billion IoT-connected devices. As the number of connected devices grows, so does the risk of data breaches caused by IoT gadgets' frequently inadequate processing and storage capabilities. Since IoT devices often have limited computational power and storage, they can be vulnerable to invaders as the IoT grows. Improvements in mobile technology have paved the way for the proliferation of the IoT, reshaping fields including healthcare, real estate, and smart cities. These linked devices are smart gadgets that use network interface cards and lightweight central processing units managed by many interface services. The IoT can potentially impact our collective future as technology develops significantly. The rapid growth of the IoT has made security one of the most critical issues in a networked, interdependent system. Hackers, viruses, and other harmful software could compromise the safety and reliability of data. In addition, data insecurity has the potential to directly undermine the security of the entire IoT and usher in several perilous circumstances. Robust IoT security solutions are, therefore, in high demand. As the number of IoT devices grows and new risks appear, it will become increasingly important to gather and analyze data to maintain the safety of these gadgets. Because of this, IoT security has emerged as a top priority. Existing security methods include, but are not limited to, systemic security architecture and cryptographic security mechanisms. Network attacks, such as a flood of requests to IoT services quickly or unauthorized access to particular services, could have severe repercussions. Therefore, installing intrusion detection systems (IDSs) to identify malicious actors and maintain the availability and safety of IoT networks is crucial. However, complex IDSs are rarely useable due to IoT devices' limited resources and power. An intrusion detection system monitors a network's health and activity. An alert is issued to the network administrator once an intrusion is discovered. When dealing with different volumes and incorrect sequences of event streams, conventional IDSs' architecture, built essentially to handle the Internet's priority management characteristics, falls short. The IoT has profoundly impacted our daily lives by connecting billions of devices and producing massive amounts of data. However, this rapid growth of IoT networks has prompted new security concerns due to the inherent vulnerabilities of IoT devices. To detect and block malicious activity, an IDS is crucial for protecting IoT networks. Rule-based IDS methods have traditionally been used, but the complexity and diversity of IoT networks have rendered them inefficient. Deep learning is one approach that could be used to improve the efficiency and precision of IDS for IoT devices. To maximize the use of IDSs in the IoT using deep learning and further identify the flaws and strengths of these systems, it is essential to evaluate the available literature and

IoT—An Internet-Connected Framework and the Scope of This Work

According to Kiran et al. (2019), the Internet of Things (IoT) is described as "a framework or system of Internet-connected, interrelated devices or objects that collect and transmit the data over the wireless network without the assistance of human interaction." IoT platforms make it possible to develop IT solutions that are superior, more cost-effective, and more expedient. As seen in Figure 1, the overall architecture of an Internet of Things system is given. The following are the essential elements that are necessary for the Internet of Things to function properly: (1) connectivity between networks and devices; (2) interaction between devices; (3) analysis; (4) administration of devices and networks; (5) security; and (6) data storage. These devices make use of Internet of Things protocols and standards whenever they are required to communicate and deliver data. Prototypes and standards for the Internet of Things can be broken down into two primary categories: (1) data protocols, which include MQTT, CoAP, AMQP, DDS, HTTP, and Web Socket; and (2) network protocols, which include WiFi, Bluetooth, ZigBee, Lora Wan, and Z-Wave. In order to protect data or devices from malicious assaults, it is necessary to implement security protocols. Some examples of these protocols include Wireless Hart, Lora Wan, LPWAN IEEE 802.15.4, DTLS, and AMQP. These protocols are included in the scope of this study.

IoT Security and Datasets

When referring to the protection of devices that are network-based or connected to the Internet, the term "Internet of Things security" would be used. The fundamental language of the Internet of Things (IoT) has been in the process of being established for a long amount of time (Sharma et al. 2019). This is despite the fact that the introduction of the Internet of Things (IoT) concept occurred approximately twenty years ago. In order to simplify communication, the sharing of data, and control, the Internet of Things (IoT) is primarily designed to connect nodes, smart cities, systems, frameworks, and sensors through the utilization of the Internet by means of the Internet. The Internet of Things is intended to make everyday tasks and the modern world more user-friendly and efficient. These days, the Internet of Things is everywhere. To name a few examples, smart sensors, fitness mobile applications, thermostats, photovoltaic systems, air conditioners, and culinary appliances are all connected to the Internet. According to Khan et al. 2021, the rapid development of Internet of Things technology is making it more difficult to safeguard and protect data obtained from the Internet of Things from malicious traffic, hackers, unauthorized users, and attackers. Consequently, in order to safeguard information, a variety of protection mechanisms and tactics are currently being created and put into practice within Internet of Things frameworks and systems. In order to create detection methods for malicious assaults in Internet of Things (IoT) systems, many datasets have been utilized in the research literature. T.

The Necessity for an Up-to-Date Review

It has been demonstrated through the preceding evaluations of the most recent relevant research findings that there are several Internet of Things challenges as well as significant Internet of Things issues, structures, and key application areas that need to be investigated. As a result of the rapid expansion and broad use of (IoT) devices, the security concerns associated with IoT devices have become increasingly complex, which has led to an increased demand for the development of network-based security solutions. It is still difficult to find all of the cyber attacks, despite the fact that the mechanisms that are already in place are excellent at recognizing them. There is no question that there is a broad selection of current methods that may be utilized to enhance the security of a network. This is because the number of assaults on networks is growing, the amount of information that is available on networks is also growing, and the need for faster and more effective methods to detect attacks is growing. The protection of users' privacy and security is a crucial aspect of the Internet of Things that requires further attention and investigation. There has been a significant improvement in the detection of cyber security attacks utilizing AI on the internet of things. In light of this, it is of the utmost importance and demand that a comprehensive analysis be provided by examining the prior studies. They wanted to identify the machine learning and deep learning techniques that are the most efficient for identifying threats and attacks on Internet of Things (IoT) systems, with us also wanted to investigate the existing ways that may be used to mitigate those attacks by employing successful strategies. There have been a few studies that have concentrated on the conventional approaches, while others have concentrated on the deep learning tactics for the protection of the Internet of Things (IoT). They investigated both machine learning and deep learning approaches to Internet of Things (IoT) security, and we also considered potential future paths.

The most important contributions that this work produces are associated with the investigation and identification of the creation of semi-supervised machine learning and advanced deep learning methods for the detection of cyber attacks in systems and devices that are connected to the Internet of Things. In addition, one of our goals is to provide a bridge between the numerous datasets that are used for cyber threat detection in Internet of Things (IoT) systems and devices and the feature selection methods that are used.

Fundamental concepts

Cyber-attacks fall into a broader context than what is traditionally called information operations. Information operations integrated use of the main capabilities of electronic warfare, psychological, computer network, military trickery and security operations in coordination with special support and relevant abilities and to penetration, stop, destroy or hijack human decisions and It is one of the decision-making processes of national institutions. Fig. 1 describes the anatomy of a cyber-attack. From the USNM Strategy for cyberspace operations, computer network operation is composed of the attack, defense, and utilization enabling. The latter is different from network attacks and network defense, because this type of operation focuses more on collection and analyzing information than interrupting networks, and may itself be the prelude to an attack. These operations can be carried out of disseminating information and propaganda purposes. Computer network exploitation enabling operations can also be carried out with the aim of stealing important computers data. In such a context, Trap Sniffers and Doors are beneficial tools for cyber espial. Trap Doors permit an external user to accessibility software at any time without the knowledge of the computer user. Sniffers are a tool to steal usernames and passwords. Table 1 describes the basic definitions and concepts of cyberspace. The consequences of cyber warfare can include.

Cyber space threats

Naturally, it is the scope of the global cyberspace, which creates overlapping and overlapping areas of control for national actors with different legal and cultural approaches and different strategic interests (Iqbal and Anwar, 2020). Countries around the world have become sufficiently dependent on cyberspace for communications and control of the physical world; in a way that it is definitely impossible to separate from it. Therefore, the security tasks and functions of each country are increasingly affected by cyberspace (Zhao et al., 2020). Due to the global production of software and hardware products, it is impossible to provide guarantees in the product supply chain process. The scalability of the cyber domain makes it qualitatively different. A bomb has a limited physical range in the most extreme conditions; however cyber-threats have a very wide range of effects, therefore we have a mechanism that can control real-world operations. Like many other areas of knowledge, operations within the cyberspace are controlled by a relatively small number of individuals. Users do not have the ability to modify or control the software and hardware they use. It is no secret that a small number of people can effectively control or manage cyber warfare (Zhang et al., 2021). Despite the required concentration and specialized knowledge, the distributed nature of the cyber domain prevents a person or group of individuals from seeking complete control.

Numerous such cases have been reported worldwide for the misuse and destruction of countries' information infrastructures, comprising the computer systems, Internet information networks, and processors and controllers embedded in vital industries. Another source of attacks is groups of people who attack cyber systems to make money, and the attacks of these groups are increasing (Beechey et al., 2021). In addition, other groups (hackers) sometimes enter the network to express themselves. In the current situation, it is possible to infiltrate networks with a minimum of knowledge and skills, by downloading the necessary programs and protocols from the Internet and using them against other sites. Meanwhile, another group (called Hacktivism) with politically motives attacks popular web pages or e-mail hosts. These groups usually impose increased loads on e-mail hosts, and by infiltrating the web sites, they announce their political messages (Solomon, 2017). On the other hand, internal dissatisfied agents operating within the organization are the main source of cybercrime, and these agents do not need to have significant knowledge of cyber-attacks; because their target system awareness mostly allows unlimited access to hit the system or steal the organization's information. Terrorists are another source of threat that seeks to destroy, disabling, or maliciously exploit vital infrastructure to menace national security, inflict heavy losses, weaken the country's economy, and undermine public mentality and trust (Saxena and Gayathri, 2021).

Threats and attacks

Over the past decade, IoT devices have faced numerous attacks, leading to heightened user apprehension regarding their usage. These malicious activities targeting IoT devices and networks are termed as IoTbased threats and attacks. The primary objectives of attackers encompass information collection, data theft, and denial of service to authentic users. With the anticipated rise of IoT-connected devices into billions by 2020, there is also an expected increase in potential vulnerabilities. The lack of standardization in IoT technologies can amplify these vulnerabilities, resulting in security breaches in IoT systems. Subsequent sections delve into prevalent security challenges in IoT. This segment collates details about predominant threats and attacks within the IoT sphere. Over recent years, multiple attacks have targeted IoT devices, prompting users to exercise added caution. Attackers commonly seek information, purloin data, or inhibit services intended for genuine users. This segment elucidates specific attacks and their objectives, categorizing them into active and passive types. A broad overview of these attacks is depicted in Fig. 2. Additionally, we have compiled a table categorizing the attacks, defining them, and listing tools for their execution.

Denial of service

A DoS attack comprises attacks that render a service or network inaccessible to its intended audience. These attacks primarily aim to disrupt services for all users by targeting individual users or devices or by overloading network resources.

Distributed denial of service

DDoS represents a multifaceted Denial of Service attack executed via compromised nodes from diverse locations. Common techniques employed by attackers include TCP SYN Flood, UDP flood, HTTP flood, and ICMP flood.

TCP SYN Flood: Attackers leverage the TCP connection sequence to incapacitate a victim's network. By swiftly dispatching TCP connection requests, they intend to inundate the target system, leading to a network overload [65].

UDP Flood: By deluging a target with UDP packets, it prompts the host to check for an application, causing inaccessibility repeatedly. The flood of User Datagram Protocol (UDP) packets hampers the system's capacity to process them, making it unavailable to genuine users.

HTTP Flood: This involves overwhelming a target server with HTTP requests. Using malware-infected devices, attackers assemble botnets to enhance the impact.

HTTP flood attacks can be of two types: HTTP POST and HTTP GET.

ICMP Flood: Attackers use ICMP Echo requests or ping messages to hamper network functionality, employing a rapid-fire approach to send packets without awaiting responses.

Jamming attack: Attackers purposefully disrupt wireless connections among IoT devices. This is achieved by sending potent radio signals matching the frequency of targeted devices, thereby impeding their operation.

Universal Plug and Play (UPnP): UPnP consists of networking protocols facilitating real-time interactions among IoT devices. However, the absence of robust security measures within its framework means that UPnP can facilitate amplification attacks.

Information gathering

Information gathering entails collecting data about a specific system or network to pinpoint vulnerabilities and weaknesses potentially exploitable in subsequent attacks. Reconnaissance attacks can be categorized into passive and active forms. Passive reconnaissance is characterized by collecting information on a target without engaging in detectable activities, like perusing publicly accessible data, social engineering, or passive scanning. On the other hand, active reconnaissance involves directly probing the target to uncover vulnerabilities, such as through port or vulnerability scanning [68].

Vulnerability Scanning: This approach can be employed by security professionals or malicious actors to uncover vulnerabilities in a target system or network. Once identified, these vulnerabilities might pave the way for further attacks, potentially leading to unauthorized access or malware installation.

OS Fingerprinting: This method enables an attacker to ascertain a specific device's operating system (OS). With this knowledge, they can target inherent weaknesses in the OS. OS fingerprinting can manifest as active or passive attacks. In an active approach, attackers send packets to the target, await a response, and dissect the TCP message contents. Conversely, passive attackers act like ”sniffers,” avoiding deliberate alterations or interactions with the network.

Port Scanning: In this technique, attackers survey their target environment by dispatching packets to specific ports on a host. By analyzing the responses, they can detect vulnerabilities and determine which services and their respective versions are active on the host .

User-to-Root: In this scenario, an attacker possessing limited rights on a system seeks elevated administrator privileges. This is often achieved by exploiting software or OS vulnerabilities.

Remote-to-Local: Here, an attacker seizes control of a remote system or network. Leveraging this control, they target a local system—like a workstation or server by exploiting vulnerabilities in the communication protocols or connection software.

Sybil Attack:

In this approach, a malicious node purports to have multiple identities either by impersonating legitimate nodes or fabricating new, fictitious identities. The attacker might present all the Sybil identities concurrently or sequentially. Systems like routing protocols or voting-based fault tolerance mechanisms can fall prey to Sybil attacks.

Man-in-the-middle attack

A Man-In-The-Middle (MITM) attack occurs when an adversary intercepts cmmunications between two parties, enabling them to covertly eavesdrop, modify, or inject data into the communication. Prominent MITM attacks encompass techniques such as Address Resolution Protocol (ARP) cache poisoning, Domain Name System (DNS) attacks, session theft, ICMP redirection, and port snatching.

DNS Spoofing:

This involves poisoning the DNS server records, leading a user to a malicious site controlled by the attacker. Such attacks exploit the DNS protocol's vulnerabilities and how domain name servers use the protocol.

Notable types of DNS spoofing include:

DNS Cache Poisoning: The attacker introduces fraudulent DNS data into the server's cache to mislead users.

DNS ID Spoofing: The attacker manipulates the DNS transaction ID to send deceptive DNS responses to the target server.

ARP Spoofing: The attacker broadcasts counterfeit ARP messages over a local area network. This maps the attacker's MAC address to the IP of another host on the network, causing the network data to be redirected to the attacker's machine.

njection attacks

An injection attack introduces malicious input data into applications from the client side. Prominent examples include Cross-site Scripting (XSS), SQL Injection, Uploading Attack, and Buffer Overflow. attempt to run harmful commands on a Web server. They insert malicious web content using XSS, such as rogue HTTP or JavaScript codes. This vulnerability can leak data, authentication mechanisms, session tokens, and cookies between IoT devices and remote Web servers.

SQL Injection: Attackers exploit vulnerabilities in database-driven applications. By inserting malicious SQL commands into input fields, they can modify or exfiltrate data from the app's database.

Uploading Attack: Attackers exploit vulnerabilities in web applications to upload files containing malevolent code (e.g., web shells) to a web server. Once uploaded, they can execute this code to gain unauthorized access, pilfer sensitive data, modify or delete files, or inflict other damages. These attacks might be manual or automated.

Buffer Overflow: This happens when excessive data is written into a buffer without proper validation or boundary checks in a sensor node. The overflowing data can overwrite adjacent memory spaces, corrupting the stored data.

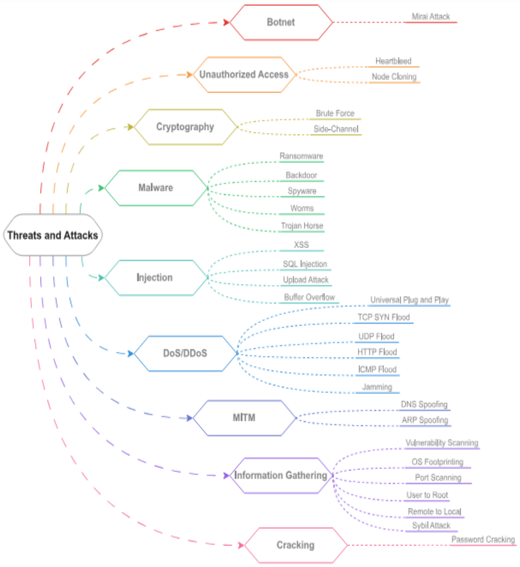

Fig. 2. Different categories of threats and attacks to which IoT devices are susceptible.

Malware attacks

Malware attacks represent a prevalent type of cyber attack, where, malicious software executes unauthorized actions on a victim's system. Malware can propagate through multiple mediums, such as email attachments, malevolent web pages, and compromised software. Upon penetration, malware can undertake various harmful activities, including credential theft, data encryption, or complete system takeover Examples of malware include backdoors, viruses, Trojan horses, ransomware, and adware.

Ransomware: A refined type of malware that restricts access to systems or services, making them inaccessible to users until a ransom is paid. The attackers typically communicate their demands to the victim, promising to restore access to the system or provide the decryption key for the ransom.

Backdoor: This is when an attacker exploits a vulnerability or injects malicious code into a system or network to gain unauthorized access and control. Utilizing system vulnerabilities, this software grants intruders unrestricted remote access to a breached device With this access, an attacker can eavesdrop on users, control their sessions, target other systems, install additional software, or monitor the entire network.

Spyware: Unauthorized software installed on IoT devices to surreptitiously gather data. Through monitoring user activities, attackers aim to harvest confidential information using this method.

Worms: These malicious programs replicate themselves on an IoT device and can propagate to other devices. They can inflict various damages, such as file deletion, data theft, or even full system compromise.

Trojan horses: A deceptive form of malware masquerading as legitimate software. Once activated, it gives the attacker the same privileges as a regular user, enabling activities like file transfers, data edits, deletions, or altering device content Attackers often initiate Trojan horse attacks on IoT devices by camouflaging the malware as a legitimate application or driver and then persuading the user to install it.

Authentication attacks

Authentication attacks involve malicious entities seeking unauthorized access to a system or network. This often entails exploiting vulnerabilities in security measures or acquiring valid login credentials. Once this unauthorized access is achieved, the attacker can engage in various malicious activities such as stealing sensitive data, altering system configurations, introducing malicious software, or launching subsequent attacks within the IoT ecosystem.

Heartbleed: In 2014, a vulnerability dubbed “Heartbleed” was discovered in the OpenSSL encryption software library. This vulnerability, specifically in the library's implementation of the Transport Layer Security (TLS) heartbeat extension, allows attackers to access sensitive data from machines running the affected OpenSSL versions, such as user passwords .

Node cloning: A vast majority of IoT devices, ranging from sensor nodes to CCTV cameras, lack hardware tamper-proofing, primarily due to a void in standardization for IoT device designs. Consequently, these devices can easily be replicated or mimicked for malicious objectives. Attackers can replace genuine nodes with these clones through various methods, like acquiring cryptographic keys or compromising the device's firmware.

Cryptographic attack

Brute Force: This type of attack involves systematically trying every possible password or passcode combination to gain access to a system. Eventually, the attacker determines the correct credential and gains access.

Side-Channel Attacks: These attacks exploit information gathered from the side channels of encryption devices, such as data related to the device's processing time or power consumption during encryption and decryption processes. This can also include information collected while computing various cryptographic protocols like the Diffie Hellman (DH) key exchange or the Digital Signature Standard (DSS).

Botnet attacks

Botnets refer to networks of compromised devices controlled by an attacker. These networks can be leveraged to launch large-scale attacks, such as disseminating spam emails for financial benefits or orchestrating DDoS attacks on critical infrastructures or websites to render them dysfunctional.

Mirai attack: Discovered in 2016, the Mirai botnet has been associated with some of the most notorious DDoS attacks. It utilizes a vast network of hijacked IoT devices, including routers, cameras, and DVRs, to flood a target website or server with overwhelming traffic, making it inaccessible to genuine users .

Password cracking: This method involves guessing or breaking a password to gain unauthorized access to an IoT device. It generally employs automated tools or software to attempt different passwords until the correct one is identified repetitively.

Physical/backdoor attacks

A physical or backdoor attack involves gaining direct access to computer hardware, devices, or systems to exploit vulnerabilities, bypass authentication, or tamper with device operations. This type of attack contrasts with remote cyberattacks that are executed over networks. In IoT devices, physical access allows attackers to exploit interfaces and ports primarily designed for debugging, testing, or other benign purposes. JTAG is a common interface for debugging and testing integrated circuits [93]. Given their diversity and need for testing during development, IoT devices often incorporate JTAG interfaces. However, if these interfaces are not secured post-development, they provide a potential backdoor. Attackers with physical access can connect to the JTAG interface.

Extract Sensitive Information: This can include cryptographic keys, personal data, or proprietary software

Modify Device Functionality: They can alter the firmware, change device settings, or install malicious code.

Disrupt Service: An attacker can render a device nonfunctional or perform actions leading to malfunctioning. From an IDS perspective, addressing physical or backdoor vulnerabilities requires.

Physical Security: Strengthen the physical security around devices.

Disable Debug Interfaces: Ensure interfaces such as JTAG are disabled post-development.

Hardware-based IDS: Implement IDS solutions that monitor hardware-level operations.

Integrate with SIEM: Incorporate IDS alerts into a Security information and event management (SIEM) system.

Regular Audits: Periodically audit devices for vulnerabilities. Observations, challenges, and future directions the surge in IoT adoption has integrated it seamlessly into our daily lives due to its adaptability in catering to diverse user needs. Yet, this proliferation of IoT devices has simultaneously attracted malicious actors

The technique of conducting systematic literature reviews (SLRs) has swiftly become a well-established review procedure in the area of software engineering. A systematic literature review (SLR) is a process that involves finding, evaluating, and interpreting all of the study material available to provide answers to specific research questions, as stated by Kitchenham and Charters (2007). This method is characterized by a structured approach to discovering, evaluating, and interpreting these study materials. Using the principles initially established by Kitchenham and Charters (2007), this literature research was conducted in the form of a systematic literature review.

Search Strategy

A search involves several steps, such as choosing which digital libraries to use, defining the search string, running a pilot search, changing the search string, and getting a first set of primary studies from digital libraries that match the search phrase. The thorough search process incorporates each of these steps. Prior to initiating the search, select a collection of databases that enhances the likelihood of discovering articles particularly relevant to the topic under consideration. This crucial step must be taken before beginning the search, as it holds significant importance. To find the most complete collection of research that is not only possible but also possible, you need to search the most well-known literature sources in the field. In order to provide an accurate and thorough analysis of the books, it is crucial to examine them from various perspectives. Here is a list of the digital sources we examined:

The search string was constructed in the following way using the techniques listed below:

The identification of search phrases that are included in titles, abstracts, and keywords that are relevant to the search

• The development of a complicated search string by making use of the search keywords that have been identified, ANDs and ORs in Boolean logic

• The discovery of probable synonyms, variant spellings, and antonyms for the words that are being searched for on the internet.

Data Selection: The initial search yielded a large number of articles. To refine the selection, the following inclusion and exclusion criteria were applied:

Inclusion Criteria:

- Peer-reviewed articles
- Studies published between 2018 and 2023
- Articles written in English
- Studies focused on cyber-physical systems, IoT, and related security aspects
- Research that presented empirical data, proposed novel methodologies, or provided comprehensive reviews relevant to the study topics

Exclusion Criteria:

- Articles not available in full text
- Studies published before 2018
- Non-peer-reviewed articles (e.g., opinion pieces, editorials)
- Research not directly related to CPS, IoT, or cybersecurity
- Duplicates or studies with insufficient data or methodological details

Data Extraction: For the selected articles, data extraction was performed using a structured format to ensure consistency and comprehensiveness. The following information was extracted from each study:

- Title, authors, and year of publication
- Objectives of the study
- Methodologies used
- Key findings and contributions
- Limitations of the study
- Future research directions proposed by the authors

The extracted data was then synthesized to identify common themes, significant advancements, and gaps in the current research landscape. This systematic approach facilitated a thorough understanding of the current state of research in the areas of CPS, IoT, and cyber security, and provided a solid foundation for identifying potential areas for future investigation.

Determined that using the following search string would be the most effective: AND (fault, defect, quality, or error-prone) this also applies to the terms "predict, prone, probability, evaluate, detect, estimate, or classify." AND (classify by evaluating, detecting, or estimating) The term encompasses both software and applications, as well as systems. Besides defects, flaws, quality issues, or a tendency to make mistakes, THEN. We adjusted the search string, but the previous one remained in use. This was because altering the search phrase would significantly expand the already vast list of irrelevant studies. This was the reason for it. Subsequently, we modified the search phrase to align with the specific requirements set by each database in this instance. The databases utilized titles, keywords, and abstracts in their search operations. The years 2005–2024,only considered for review.considered two categories of publications for inclusion in this collection: articles from journals and proceedings from conferences.and only considered items written in English for this search.

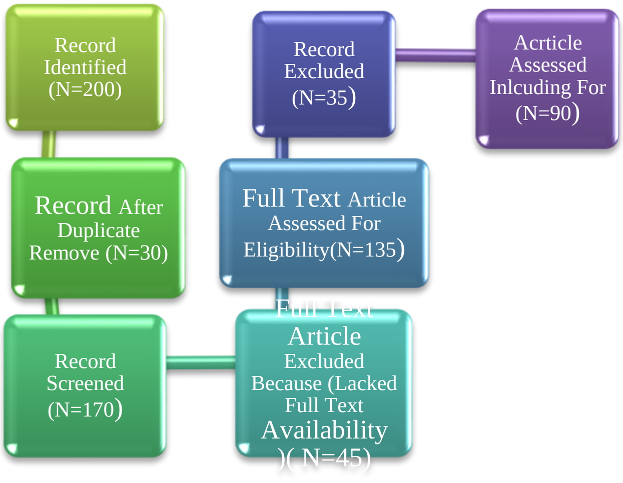
Record Identified (N=200)
Record Excluded (N=35)
Acrticle Assessed Inlcuding For (N=90)
Record After Duplicate Remove (N=30)
Full Text Article Assessed For Eligibility(N=135)
Record Screened (N=170)
Full Text Article Excluded Because (Lacked Full Text Availability)(N=45)

Figure 1 Systematic Literature Review Steps

LITERATURE WORK

Supervised Machine Learning Method in IoT Security

The research conducted by Ioannou, C. et al. in 2020 utilized a support vector machine (SVM) classifier to identify the incursion of selective forward and blackhole network layer assaults in a network. The model was put through its paces against selected forward (SF) and blackhole (BH) attacks by using data from an Internet of Things testbed. For the purpose of evaluating the detection, sink in the middle and top network topologies were utilized simultaneously. The precision rate was lower than fifty percent, and the SVM detection model was not able to identify all of the malicious nodes that were being used for the SF attack. For the purpose of determining precision, accuracy, PPV, NPV, and TPR, the equation about the Matthews correlation coefficient was utilized. The findings indicate that a total probability of success (TPR) of one hundred percent and an accuracy rate of ninety-nine point eight percent were accomplished for SF and BH network routing attacks. It was proposed in (Ioannou, C et al. 2019) that c-support SVM might be used to identify irregularities inside Internet of Things networks. The KDD-99 dataset was utilized for the purposes of training and evaluating both normal and malicious data instances. On the other hand, when alternative network topologies were examined for all routing attacks, the detection accuracy reached 81%. Detecting the invasions of DoS, probe, U2R, and R2L in an Internet of Things network was accomplished by Rani et al. 2020 through the utilization of a consistent intrusion detection method. When it came to supervised machine learning, the datasets NSL-KDD and KDDCUP99 were applied, and random forest **was utilized as the classifier.**

Semi-Supervised Machine Learning Methods in IoT Security

Khonde et al. (2019) used classifiers such support vector machines (SVM) and kernel neural networks (KNN) to categorize the feature sets, and the ensemble approach was used to determine if the packets were normal or malicious. The NSL-KDD dataset was the one that was utilized for this particular paper. To lessen the likelihood of future attacks, it is important to note that all classifiers functioned in a distributed setting. An increase in accuracy of 10% was observed when hybrid approaches and fewer features were utilized, and a reduction in the incidence of false positives was demonstrated to be 0.05. It is therefore possible to draw the conclusion that the detection performance was enhanced by a higher true positive rate and a reduced number of characteristics. For the purpose of producing alerts on anomalous and malicious attacks, a flow-based network intrusion detection system (SSLEEK) technique was developed in (Leslie et al.2018). For the purpose of identifying botnet traffic during a network session, NetFlow data are utilized. In comparison to the conventional NIDS, this technique demonstrates significant enhancements in both accuracy and efficiency. The classifiers that were chosen were the GMM, K-means, and K-NN categories. Within the realm of machine learning, the K-NN classifier is the most often used.

Unsupervised Learning in IoT Security

When it comes to identifying botnet assaults that originate from Internet of Things devices, the grey wolf optimization one class support vector machine (GWO-OCSVM) was proposed in the article by Al Shorman et al. 2020. The suggested model was put through its paces by using the OCSVM, IF, and LOF algorithms. The results demonstrated that the GWO-OCSVM method is superior than the other algorithms in terms of its ability to detect botnets and perform categorization. As a consequence of the trials, it was revealed that GWO-OCSVM achieved superior outcomes when compared to the other three algorithms in terms of FPR, TPR, and G-means. All of these outcomes were achieved with the ass**istance of the NN-BaIoT dataset**. There was a 92% improvement in the performance. Applications of MCS have been utilized in the study by Banerjee et al. (2018) in order to safeguard the dependability and accuracy of user data collection. Because of the presence of cunning and cunning adversaries, the MCS report was able to maintain its credibility in the cyberspace. This approach is demonstrated to be useful and accurate by using real datasets from the Internet of Things (IoT).

Deep Learning Methods

Izhar Ahmed Khan et al. (2023): This study proposes a federated-Simple Recurrent Units (SRUs) Intrusion Detection System (IDS) to enhance security in IoT-based Industrial Control Systems (ICSs). The model addresses computational costs and gradient vanishing issues, using federated learning for privacy-preserving data aggregation. Tested with real-world ICS data, it demonstrates superior intrusion detection capabilities and outperforms existing methods.

Muawia A et al. (2023): The authors present a lightweight machine learning approach using a decision tree algorithm with Gini feature selection to detect Denial-of-Service (DoS) attacks in Wireless Sensor Networks (WSNs). Their method achieves a high accuracy rate of 99.5% and significantly reduces processing time, making it highly suitable for WSN constraints.

Safdar Hussain Javed et al. (2023): This research introduces a Graph Attention Network (GAN) for detecting Advanced Persistent Threats (APTs) in Industrial Internet of Things (I-IoT) enabled Cyber-Physical Systems (CPSs). By using masked self-attentional layers, the GAN captures complex behavioral features, achieving high detection accuracy and rapid prediction times, outperforming conventional machine learning techniques.

Irfan Ali Kandhro et al. (2023):

The study proposes a deep learning-based intrusion detection method using a Generative Adversarial Network (GAN) for IoT-driven Industrial Internet of Things (IIC) networks. This approach shows significant improvements in accuracy and detection rates across multiple datasets, ensuring the confidentiality and integrity of sensitive information during training and testing phases.

Hsin-Hung Cho et al. (2023): This study explores the vulnerabilities of Narrowband IoT (NB-IoT) devices in industrial Cyber-Physical Systems (CPS) to low-rate denial-of-service attacks. Due to limited computing capabilities, NB-IoT devices can't support robust security software. The authors propose a novel convolutional neural network-based detection method that enhances weight combination search, improving the detection rate of such attacks.

Cody Lewis et al. (2023): This research introduces an adaptive DDoS attack mitigation (ADAM) scheme for software-defined CPSs. ADAM uses information entropy and unsupervised anomaly detection to identify and mitigate DDoS attacks. The method includes a pipeline filtering mechanism, which can be integrated into existing SDN networks without additional devices. Experimental results demonstrate ADAM's high accuracy (99.13%) and a significant reduction in false-positive rates compared to similar methods.

Harsh Kumar et al. (2023): The authors propose a new attack on context-aware trust models in IoT systems, termed context-based attacks. These attacks manipulate context to impact specific IoT devices without others noticing. The study demonstrates this attack's effectiveness on seven trust models and proposes a new Trust Management System (TMS) to mitigate such attacks.

Imran Ashraf et al. (2023): This study examines cyber security threats in the maritime industry, emphasizing the risks posed by technological advancements. It analyzes the impact of cyber threats on maritime security and suggests risk assessment methods and mitigation strategies. The authors highlight the need for efficient security policies to protect the maritime industry from cyber-attacks.

Mahdi Khosravy et al. (2023): The research addresses model inversion attacks (MIA) on deep-learning-based recognition systems (DLRSs). By generating data clones for targeted class labels, MIAs pose significant threats. The authors propose a Social IoT-based collaborative cyber-defense among online recognition systems, using log-likelihood ratio tests to verify recognition results and prevent MIA-targeted data clones. The technique shows improved security in evaluations.

Talha Naeem Qureshi et al. (2023): This paper presents a communication model and the Elephant Herding Robustness Evolution (EHRE) algorithm to enhance the robustness of scale-free IoT networks. These networks, prone to targeted attacks, benefit from EHRE by offloading computationally intensive robustness tasks to high-power processing clusters. The algorithm demonstrates high efficiency and performance, outperforming previous methods in robustness enhancement.

Conclusion

Cyberspace and related technologies are one of the most important sources of power in the third millennium. The characteristics of cyberspace, such as low entry prices, anonymity, vulnerability and asymmetry, have created the phenomenon of power dissipation, which means that if governments have so far divided the game of power among themselves, then it must be Other actors, such as private companies, organized terrorist and criminal groups, and individuals, although it is still governments that play an important role in this. Naturally, this phenomenon will not deprive governments of their national security. This effect can be evaluated in several ways. First is the concept of security. National security can no longer be defined in terms of military issues and internal and external borders, but today, the risk of declining quality of life of citizens is a threat to national security. The second is the disappearance of the geographical dimension of cyber threats. In the past, military threats had a specific geographical location. As a result, it was not difficult to deal with, at least in terms of identification. Third is the extent of vulnerabilities posed by cyber threats. These threats are sporadic, multidimensional, and because they are associated with sensitive networks and infrastructure, their level of damage are very high. Fourth, these threats cannot be contained by traditional means alone, such as the use of military and police force, and governments alone are not sufficient to counter them, and effective and bilateral cooperation between governments and the private sector, which has common interests in dealing with them. With such threats are, he demands. Fifth, as the previous point shows, cyber threats are not limited to governments, but individuals and companies will not be immune to the harms of these threats. Sixth, since security in the information age is not merely governmental, the various theoretical approaches in international relations whose theories are based primarily on government are easily overlooked or confusing.

REFERENCES

1. Izhar Ahmed Khan; Dechang Pi;Muhammad Zahid Abbas;Umar Zia; Yasir Hussain; Hatem Soliman (2023) “Federated-SRUs: A Federated-Simple-Recurrent-Units-Based IDS for Accurate Detection of Cyber Attacks Against IoT-Augmented Industrial Control Systems” Volume: 10, Issue: 10, Page(s): 8467 – 8476, Page(s): 8467 – 8476, 2023,
2. Muawia A. Elsadig (2023) “Detection of Denial-of-Service Attack in Wireless Sensor Networks: A Lightweight Machine Learning Approach” Volume: 11, Page(s): 83537 – 83552,2023
3. Safdar Hussain Javed;Maaz Bin Ahmad;Muhammad Asif;Waseem Akram;Khalid Mahmood;Ashok Kumar Das;Sachin Shetty (2023)“APT Adversarial Defence Mechanism for Industrial IoT Enabled Cyber-Physical System” Volume: 11, Page(s): 74000 – 74020,2023
4. Irfan Ali Kandhro;Sultan M. Alanazi;Fayyaz Ali;Asadullah Kehar;Kanwal Fatima;Mueen Uddin;Shankar Karuppayah(2023) “Detection of Real-Time Malicious Intrusions and Attacks in IoT Empowered Cybersecurity Infrastructures” Volume:11, Page (s) : 9136 – 9148,2023
5. Hsin-Hung Cho;Min-Yan Tsai;Jiang-Yi Zeng;Chia-Mu Yu;(2023)

"LDoS Attacks Detection for ICPS NB-IoTs Environment via SE-Based CNN" Volume: 19, Page(s): 5280 – 5291,2023

6. Cody Lewis;Nan Li;Vijay Varadharajan(2023) "Targeted Context-Based Attacks on Trust Management Systems in IoT" Volume: 10, Issue: 14, Page(s): 12186 – 12203,2023
7. Harsh Kumar;Oscar. A. Alvarez;Sanjeev Kumar(2023) "Experimental Evaluation of Smart Electric Meters' Resilience Under Cyber Security Attacks"Volume: 11Page(s): 55349 – 55360,2023
8. Imran Ashraf;Yongwan Park;Soojung Hur;Sung Won Kim;Roobaea Alroobaea;Yousaf Bin Zikria;Summera Nosheen(2023) "A Survey on Cyber Security Threats in IoT -Enabled Maritime Industry" Volume: 24, Issue: 2,Page(s): 2677 – 2690,2023
9. Mahdi Khosravy;Kazuaki Nakamura;Naoko Nitta;Nilanjan Dey;Rubén González Crespo;Enrique Herrera-Viedma;Noboru Babaguchi(2023) "Social IoT Approach to Cyber Defense of a Deep-Learning-Based Recognition System in Front of Media Clones Generated by Model Inversion Attack"Volume: 53, Issue: 5,
10. Talha Naeem Qureshi;Zahoor Ali Khan;Nadeem Javaid;Abdulaziz Aldegheishem;Muhammad Babar Rasheed;Nabil Alrajeh(2023)"Elephant Herding Robustness Evolution Algorithm With Multi-Clan Co-Evolution Against Cyber Attacks for Scale-Free Internet of Things in Smart Cities"Volume: 11, Page(s): 79056 – 79072,2023
11. Kiran, D. Chapter 35—internet of things. In *Production Planning and Control*; Kiran, D., Ed.; Butterworth-Heinemann: Oxford, UK, 2019; pp. 495–513.
12. Sharma, N.; Shamkuwar, M.; Singh, I. The history, present and future with IoT. In *Internet of Things and Big Data Analytics for Smart Generation*; Springer International Publishing: Cham, Switzerland, 2019; pp. 27–51.
13. Shahid, J.; Ahmad, R.; Kiani, A.K.; Ahmad, T.; Saeed, S.; Almuhaideb, A.M. Data protection and privacy of the internet of healthcare things (IoHTs). *Appl. Sci.* **2022**, *12*, 1927.
14. Abbasi, M.A.; Zia, M.F. Novel TPPO based maximum power point method for photovoltaic system. *Adv. Electr. Comput. Eng.* **2017**, *17*, 95–100.
15. Ashraf, S.; Shawon, M.H.; Khalid, H.M.; Muyeen, S. Denial-of-service attack on IEC 61850-based substation automation system: A crucial cyber threat towards smart substation pathways. *Sensors* **2021**, *21*, 6415.
16. Khalid, H.M.; Peng, J.C.H. Immunity toward data-injection attacks using multisensor track fusion-based model prediction. *IEEE Trans. Smart Grid* **2017**, *8*, 697–707.
17. Khan, H.M.A.; Inayat, U.; Zia, M.F.; Ali, F.; Jabeen, T.; Ali, S.M. Voice over internet protocol: Vulnerabilities and assessments. In Proceedings of the International Conference on Innovative Computing (ICIC), Lahore, Pakistan, 9–10 November 2021; pp. 1–6.
18. Ioannou, C.; Vassiliou, V. Experimentation with local intrusion detection in IoT networks using supervised learning. In Proceedings of the 16th International Conference on Distributed Computing in Sensor Systems (DCOSS), Marina del Rey, CA, USA, 25–27 May 2020; pp. 423–428.
19. Ioannou, C.; Vassiliou, V. Classifying security attacks in IoT networks using supervised learning. In Proceedings of the 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini, Greece, 29–31 May 2019; pp. 652–658.
20. Rani, D.; Kaushal, N.C. Supervised machine learning based network intrusion detection system for internet of things. In Proceedings of the 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 1–3 July 2020; pp. 1–7.
21. Wan, Y.; Xu, K.; Xue, G.; Wang, F. Iotargos: A multi-layer security monitoring system for internet-of-things in smart homes. In Proceedings of the IEEE INFOCOM 2020-IEEE Conference on Computer Communications, Toronto, ON, Canada, 6–9 July 2020; pp. 874–883.
22. Khonde, S.; Ulagamuthalvi, V. Ensemble-based semi-supervised learning approach for a distributed intrusion detection system. *J. Cyber Secur. Technol.* **2019**, *3*, 163–188.
23. Leslie, N.O. Using semi-supervised learning for flow-based network intrusion detection. *Cell* **2018**, *202*, 528-0770.
24. Cheng, Y.; Xu, Y.; Zhong, H.; Liu, Y. HS-TCN: A semi-supervised hierarchical stacking temporal convolutional network for anomaly detection in IoT. In Proceedings of the IEEE 38th International Performance Computing and Communications Conference (IPCCC), London, UK, 29-31 October 2019; pp. 1–7.
25. Al-Jarrah, O.Y.; Al-Hammdi, Y.; Yoo, P.D.; Muhaidat, S.; Al-Qutayri, M. Semi-supervised

multi-layered clustering model for intrusion detection. *Digit. Commun. Netw.* **2018**, *4,* 277–286.

26. Ashfaq, R.A.R.; Wang, X.Z.; Huang, J.Z.; Abbas, H.; He, Y.L. Fuzziness based semi-supervised learning approach for intrusion detection system. *Inf. Sci.* **2017**, *378*, 484–497.
27. Al Shorman, A.; Faris, H.; Aljarah, I. Unsupervised intelligent system based on one class support vector machine and grey wolf optimization for IoT botnet detection. *J. Ambient. Intell. Humaniz. Comput.* **2020**, *11*, 2809–2825.
28. Banerjee, N.; Giannetsos, T.; Panaousis, E.; Took, C.C. Unsupervised learning for trustworthy IoT. In Proceedings of the IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), Rio de Janeiro, Brazil, 8–13 July 2018; pp. 1–8.
29. Janjua, Z.H.; Vecchio, M.; Antonini, M.; Antonelli, F. IRESE: An intelligent rare-event detection system using unsupervised learning on the IoT edge. *Eng. Appl. Artif. Intell.* **2019**, *84*, 41–50.
30. Nõmm, S.; Bahşi, H. Unsupervised anomaly based botnet detection in IoT networks. In Proceedings of the 17th IEEE International Conference on Machine Learning and Applications (ICMLA), Orlando, FL, USA, 17–20 December 2018; pp. 1048–1053.
31. Li, P.; Zhang, Y. A novel intrusion detection method for internet of things. In Proceedings of the Chinese Control Additionally, Decision Conference (CCDC), Nanchang, China, 3–5 June 2019; pp. 4761–4765.
32. Yang, A.; Zhuansun, Y.; Liu, C.; Li, J.; Zhang, C. Design of intrusion detection system for internet of things based on improved BP neural network. *IEEE Access* **2019**, *7,* 106043–106052.
33. Telikani, A.; Gandomi, A.H. Cost-sensitive stacked auto-encoders for intrusion detection in the internet of things. *Internet Things* **2019**, *14*, 100122.
34. Saharkhizan, M.; Azmoodeh, A.; Dehghantanha, A.; Choo, K.K.R.; Parizi, R.M. An ensemble of deep recurrent neural networks for detecting IoT cyber attacks using network traffic. *IEEE Internet Things J.* **2020**, *7,* 8852–8859.
35. Li, F.; Shi, Y.; Shinde, A.; Ye, J.; Song, W. Enhanced cyber-physical security in internet of things through energy auditing. *IEEE Internet Things J.* **2019**, *6,* 5224–5231.
36. Thamilarasu, G.; Chawla, S. Towards deep-learning-driven intrusion detection for the internet of things. *Sensors* **2019**, *19*, 1977. Smys, S.; Basar, A.; Wang, H. Hybrid intrusion detection system for internet of things (IoT). *J. ISMAC* **2020**, *2*, 190–199.
37. Aghajani, G., Ghadimi, N., 2018. Multi-objective energy management in a micro-grid. Energy Rep. 4, 218–225.
38. Ahmed Jamal, A., et al., 2021. A review on security analysis of cyber physical systems using machine learning. Mater. Today: Proc..
39. Akhavan-Hejazi, H., Mohsenian-Rad, H., 2018. Power systems big data analytics: An assessment of paradigm shift barriers and prospects. Energy Rep. 4, 91–100.
40. Al-Ghamdi, M.I., 2021. Effects of knowledge of cyber security on prevention of attacks. Mater. Today: Proc..
41. Al Shaer, D., et al., 2020. Hydroxamate siderophores: Natural occurrence, chemical synthesis, iron binding affinity and use as Trojan horses against pathogens. Eur. J. Med. Chem. 208, 112791.