ISSN : 2455-9679
SJIF Impact Factor : 6.008

IJRTSM

INTERNATIONAL JOURNAL OF RECENT TECHNOLOGY SCIENCE & MANAGEMENT

"MACHINE LEARNING AND DEEP LEARNING APPROACHES FOR INTRUSION DETECTION IN IOT-ENABLED CRITICAL INFRASTRUCTURES"

Kushal Kanwar

Ph.d Scholar, Department of Computer Science Engineering, Banasthali Vidhyapith, Jaipur Rajasthan, India
rathorek30@gmail.com

ABSTRACT

The rapid integration of Internet of Things (IoT) technologies with Industrial Control Systems (ICS) and Cyber–Physical Systems (CPS) has significantly enhanced automation, efficiency, and intelligent decision-making across critical infrastructures. However, this integration has also expanded the attack surface, making these systems highly vulnerable to sophisticated cyber threats such as denial-of-service, advanced persistent threats, malware, and data integrity attacks. Intrusion Detection Systems (IDS) have therefore become a crucial defense mechanism for identifying malicious activities in real time and ensuring system resilience. This study reviews recent advances in intrusion detection techniques for IoT-, ICS-, and CPS-based environments, with particular emphasis on machine learning, deep learning, and federated learning approaches. The analysis highlights the strengths and limitations of existing IDS models in terms of detection accuracy, computational efficiency, scalability, privacy preservation, and adaptability to emerging attacks. The findings indicate that while advanced learning-based IDS models achieve high detection performance, challenges related to resource constraints, real-time implementation, and false-positive reduction remain. The study underscores the need for lightweight, adaptive, and privacy-preserving IDS frameworks to enhance the security and reliability of next-generation smart and industrial networks.

Key Words: Intrusion Detection System; Internet of Things (IoT); Industrial Control Systems (ICS); Cyber–Physical Systems (CPS); Machine Learning; Deep Learning; Federated Learning; Cyber security; Smart Infrastructure.

I. INTRODUCTION

Over the past two decades, internet usage has increasingly integrated into the lives of individuals globally, serving a crucial role in facilitating international communication. Currently, the Internet has roughly three billion users globally [1].This is attributable to innovations and reduced prices in this sector, which have significantly enhanced the availability, utilization, and performance of the Internet. [2] Assert that the Internet has facilitated the creation of a vast global network, leading to the annual generating of billions of dollars for the national economy. The majority of economic, commercial, cultural, social, and governmental activities and interactions across countries are presently conducted in cyberspace [3] this includes contacts among individuals, non-governmental organizations, and governmental entities and agencies. Governments are finding it progressively challenging to uphold their security due to the integration of critical and sensitive infrastructures and systems within them. Cyber warfare, cybercrime, cyber terrorism, and cyber espionage have arisen in cyberspace due to its absence of public transparency, anonymity, minimal entrance barriers, and the ambiguous nature of the threatening geographical domain [4]This has made conventional national security vulnerable and ineffective in this domain, as opposed to cyber threats, which are inherently opaque and whose perpetrators are states and nations located in a particular geographic region The potential repercussions of

ISSN : 2455-9679
SJIF Impact Factor : 6.008

cyber attacks have been under the consideration of analysts for over ten years. Potentially catastrophic and far-reaching physical or economic harm can occur in a variety of ways; for example, a virus could compromise a nation's stock market or financial records; a power plant could shut down and fail due to a miscommunication; or air traffic control could be compromised, leading to collisions in the sky. It will be extremely challenging for experts to address the multi-faceted nature of the issue and offer legal analysis and advice until governments agree on a universally accepted definition of a cyber-attack. With that said, we must ask: what exactly is a cyber attack, what are its defining features, and can every assault that occurs in cyberspace be deemed an attack in the conventional sense?.No, it cannot. An all-encompassing concept of cyber-attack will surely influence the regulatory framework to sustain and recognize the repercussions of this form of attack. In addition to obscuring the main legal road, the absence of a clear and complete definition not only leads to a variety of interpretations and practices, but it also finally results in the realization of sometimes contradictory legal conclusions. This is without a doubt the case. The value and requirement of having a definition that is acceptable, at least for the beginning of the issue and its explanation, adaption, and analysis, in addition to the fact that a detailed research is required, are therefore very important. This study commences by elucidating the nature of cyber attacks from the viewpoint of global experts and enterprises. The subsequent analysis focuses on the segmentation and classification of cyber attacks, followed by an examination and evaluation of the already utilized definitions. The conclusion is presented in the latter section of the work.

Fundamental Concepts

The concept of information operations is broader in scope than that of cyber-attacks alone. It integrates key elements of psychological warfare, cyber warfare, and security operations, supported by specialized expertise, with the objective of influencing, disrupting, controlling, or manipulating human decisions and behaviors. Such operations are widely adopted by national institutions as part of strategic decision-making processes. Figure 1 presents a generalized framework of a cyber-attack. According to the United States Navy cyber strategy, cyberspace operations consist of three primary components: offensive actions, defensive measures, and operational enablement [5]. Unlike conventional network attacks and defenses, these operations prioritize intelligence gathering and information analysis rather than direct network disruption and often function as preparatory stages preceding an attack Additionally, information operations may be employed to achieve propaganda and information dissemination objectives (Thomson, 2015). Another significant goal of such operations is the unauthorized acquisition of sensitive computer data through network exploitation. Tools such as trapdoors and sniffers play a critical role in cyber surveillance; trapdoors allow unauthorized users to gain covert access to software systems, while sniffers are commonly used to intercept and steal credentials such as usernames and passwords [6,7].

Cyber Threats

International actors with diverse cultural perspectives, legal frameworks, and strategic priorities find themselves with more congested cyberspace [9-10]. At this juncture, countries globally have become so dependent on cyberspace for communication and the exercise of power in the physical realm that independence from it is unequivocally unattainable. Consequently, the security responsibilities and operations of each nation are progressively influenced by cyberspace [11] Guarantees cannot be provided in the product supply chain process due to the global production of software and hardware products.

The scalability of cyberspace differentiates it from other areas. A bomb has a restricted physical range, even in extreme conditions; but, cyber threats have an extensive range of effects, hence providing a mechanism capable of influencing real-world operations. The activities occurring in cyberspace are governed by a relatively small group of experts, similar to various other domains of expertise. Users cannot modify or exert control over the software and technologies they utilize. A limited number of individuals can proficiently oversee or govern cyber warfare [12]. Due to the fragmented nature of the cyber domain, it is unfeasible for an individual or collective to attain total control, notwithstanding the necessity for concentration and specialized knowledge.

ISSN : 2455-9679
SJIF Impact Factor : 6.008

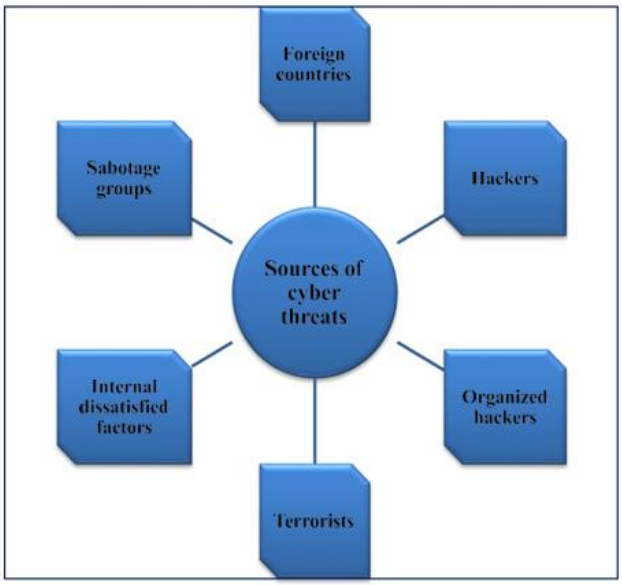

Fig.1. Sources of cyber threats.

Critical industry processors and controllers, computer networks, and the Internet together make up what is known as "information infrastructures." have been the target of numerous instances of misuse and destruction across the globe. These incidents have been documented in a number of countries. A growing number of assaults are also coming from organized groups of persons that target cyber systems with the intention of making money [13] on rare occasions, other groups with malicious intent may also get access to the network and launch attacks. One can access networks with minimal expertise or experience by getting requisite tools and protocols from the internet and subsequently employing them against other websites. This is the current situation. Another group, known as hacktivism, is responsible for attacks on major websites or email providers. These attacks are motivated by political agendas. These groups typically impose greater demands on email hosts and disseminate their political views by infiltrating websites [14]. However, the majority of cybercrime originates from disgruntled insiders who have access to the organization's systems and can steal sensitive data without much specialized knowledge of cyberattacks. Attacks on critical infrastructure by terrorists pose a threat to national security, economic growth, public confidence, and the country's ability to recover from disasters [15-16] Also, by introducing a duplicate of it into system files, which are ordinarily practical programs, a virus contaminates such files. They activate by reading infected files into memory, which then allows the virus to spread to additional files. Although worms can spread unintentionally, viruses can only spread when people touch them. Conversely, the worm is an independent system program that replicates itself by transferring from one computer to another within the network [18] ultimately, a botnet is a network of hijacked remote control devices that facilitates virus dissemination, attack coordination, spamming, and message theft.

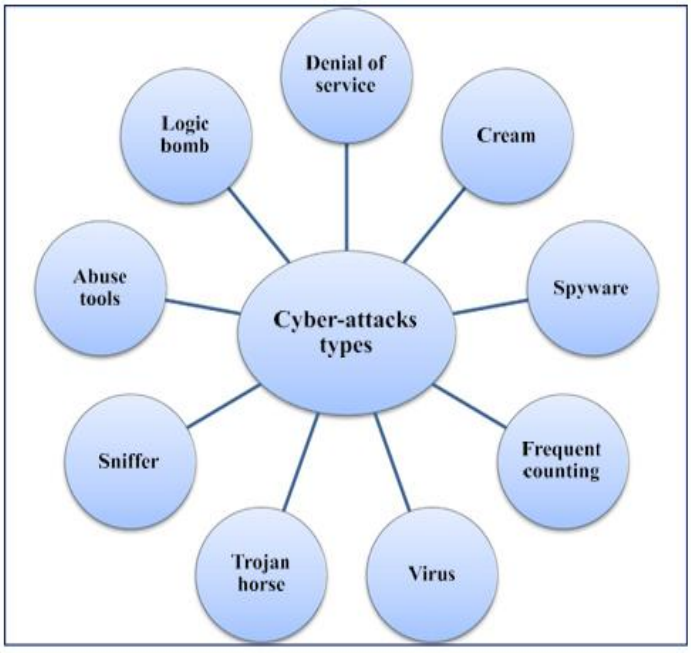

Fig.2 Main cyber-attacks types.

ISSN : 2455-9679
SJIF Impact Factor : 6.008

It is common practice for botnets to be covertly installed on compromised computers, giving malicious actors remote access and the ability to carry out their nefarious objectives.Botnets are alternatively termed electronic troops [19].

II. CYBER-SECURITY

Over time, cyber has communicated knowledge more effectively and raised community yield. The goal of increasing output has always been there, regardless of the application or business that uses cyber. Rapid data transmission to the internet typically compromises the overall security of the system. For IT workers looking to boost output, security indicators can be a real pain in the neck. This is because prevention indicators limit, ban, or postpone user access, while consumption indicators seek out and consume indicators that pinpoint vital system resources [20] Equipment that is both satisfactory and immediately available is changed in the system. In the context of cyber-security policy, the tension between the current state of affairs and the need for cyber performance is pertinent. "Policy" can mean several things depending on the context; it might refer to regulations and guidelines for the distribution of information, data conservation aims in the private sector, or plans for system operations to govern technology. To be clear, the phrase cyber-security policy serves multiple functions in the literature of this area. There is no universally accepted definition of cyber-security policy, similar to the lack of consensus around the term "cyberspace" [21]However, when used as an adjective in the context of policy, the term implies a shared understanding. Upon obtaining official clearance from the regulatory framework, the cyber-security policy is implemented only inside the requisite regulatory departments. The components of security policy differ based on the policy spectrum [22] For instance, although the national cyber-security policy includes all citizens and potentially foreign businesspeople involved in cyber activities, corporate cyber-security pertains solely to employees who are either legally obligated to the company or possess a contractual obligation to act in a specific manner towards the organization. In the absence of a formal agreement, it is illogical to anticipate that resource suppliers with a sole customer will adhere to the customer's security policy [23] The objectives of the relevant regulatory agency determine the structure of the security policy. The objectives of business and national security are markedly different. While the regulatory board and the relevant components decide how to interpret and register the policy, the implementing organizations have final say over how it is to be passed. There is a distinction between the two processes in government that lead to the formulation of policies and their ultimately incorporation into legislation. Companies often have a centralized security unit that handles cyber-security policy, standards, and solutions. Policies are based on the recommendations and standards of the company's security department. Another indicator that cyber-security is an organization-wide priority is the cyber-security policy that different departments within the common components wing have released. While attempting to address all of these challenges at once, these shared features can reveal inconsistencies in policy [24].

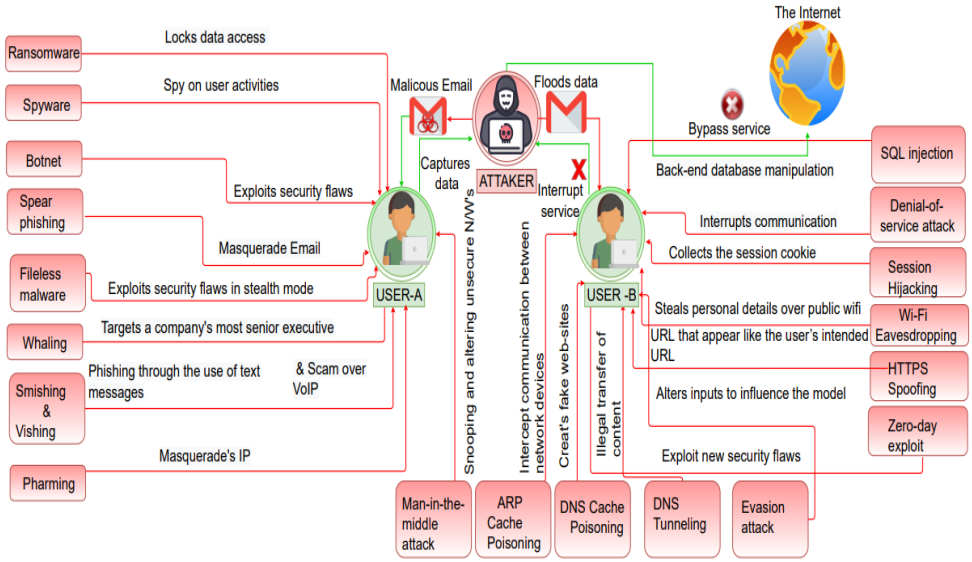

Fig. 3 Types of cyber attacks

ISSN : 2455-9679
SJIF Impact Factor : 6.008

Types of Cyber Security

One thing that each company has is assets, which are really just multi-system combinations. A strong cyber security posture is required for these systems, which necessitates coordinated efforts across all of its systems. Based on this, it is able to classify cyber security into the following sub-domains:

Network Security: This procedure includes installing the software and hardware required to secure a computer network against invasions, attacks, disruptions, misuse, and unauthorized access. With the help of this security, a company can more easily protect its assets from threats both inside and outside the company.

Application Security: It comprises taking precautions to prevent unwanted threats to the software and electronic equipment. Making sure the applications are always up-to-date and secure against attacks is one approach to accomplish this. Effective security is established throughout the design process, which includes activities like as coding, validation, and threat modeling, among others. This occurs immediately prior to the initiation of a device or application.

Information or Data Security: The implementation of a robust data retention system is required in order to preserve the confidentiality and integrity of data while it is being stored as well as while it is being transferred.

Identity management: The process of identifying the degree of access afforded to each individual possesses inside an organization is the subject of discussions in this section.

Operational Security: Performing this task requires processing and making judgments regarding the management and protection of digital assets.

Mobile Security: In the context of portable electronic devices like smart phones, laptops, tablets, and the like, it is necessary to protect the personal and organizational data that is saved on these devices from a variety of hostile attacks. These dangers include illegal access, the loss or theft of a device, malware, and other similar hazards.

Cloud Security: Safeguarding the company's data stored in the cloud or other digital environments is an integral aspect of this procedure. It protects itself from a lot of different kinds of risks by using a bunch of different cloud service providers, like Google, Microsoft Azure, and AWS.

Disaster Recovery and Business Continuity Planning: The focus here is on the procedures, checks, and warnings that a company puts in place to react appropriately in the case that any hostile activity results in the loss of data or operations. The company's policies require that it resume operations to the same capacity as before the crisis occurs, regardless of whether or not the activities were interrupted.

User Education: If any harmful action is leading to the shutdown of activities or the corruption of data, it is concerned with the protocols, monitoring, alarms, and plans that an organization employs in order to respond to the situation. In the event that a disaster occurs, its policies require that operations be resumed to the same level of capacity as they were before the occurrence.

Importance of cyber security in modern networks.

At this point in time, we are living in a digital era, in which every facet of our existence is dependent on the network, different electronic gadgets, and software programs. Devices linked to the internet are fundamental to the functioning of every critical infrastructure, including healthcare systems, government agencies, banks, and manufacturing companies. They carry out their tasks with the help of this equipment. Private information, financial records, and ideas are all examples of the kinds of things that could be considered sensitive and so vulnerable to unauthorized access or disclosure, which could have disastrous consequences. These details provide invaders and threat actors with the ability to enter them for the purpose of monetary gain, extortion, political or social motivations, or even simple vandalism. Hacking systems and other forms of cyber attacks might put the economy of the entire world in jeopardy. That is why cyber attacks have become a worldwide concern. In light of this, protecting vital data from highly publicized security breaches requires a robust cyber security strategy. Furthermore, with the ever-increasing frequency of cyber attacks, it is imperative that organizations and businesses, especially those dealing with sensitive data related to create rigorous cyber security policies and processes to safeguard sensitive information, such as health records, financial information, or national security documents.

Cyber Security Goals

The primary goal of cyber security protocols is data retention. In order to protect themselves against cyber attacks, the security sector has proposed a triangle with three interrelated concepts. The acronym CIA triad refers to these principles. The CIA model is intended to serve as a standard for guiding policies about the information security architecture of a business. The violation of one or more of these principles is the result of any security breaches that

ISSN : 2455-9679
SJIF Impact Factor : 6.008

are discovered. The CIA model can be broken down into three distinct components: availability, integrity, and confidentiality. [25]

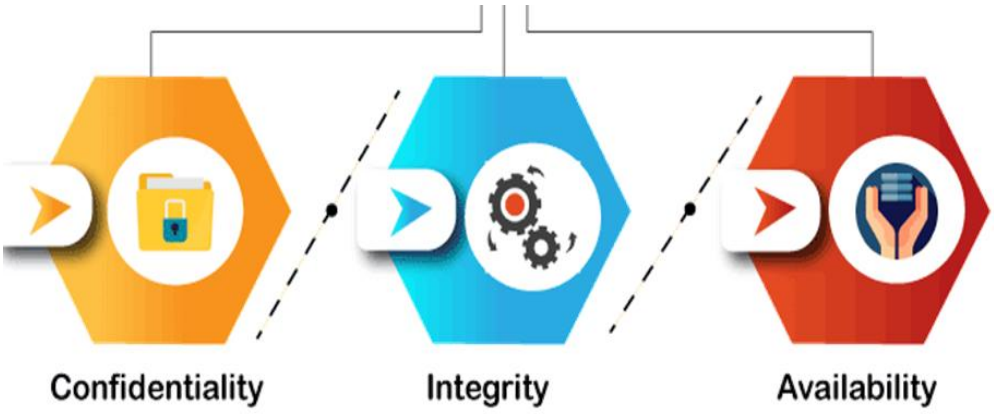

Fig.4 Cyber Security Goals

Confidentiality

For the purpose of preventing unauthorized access to information, confidentiality is analogous to privacy. To be more precise, it means keeping the data accessible only to authorized users while blocking access to everyone else. Therefore, it stops important information from being shared with people who shouldn't have it.

Integrity

This principle guarantees that the data is genuine, correct, and protected from any unauthorized modifications made by threat actors or inadvertent modifications made by users. In the event that any alterations are made, specific precautions must to be followed in order to safeguard the sensitive data against corruption or loss and to provide a speedy recovery from such an occurrence. In addition to this, it suggests that the source of the information should be authentic.

Availability

By adhering to this approach, the information will always be accessible and advantageous to those who are authorized to access it. These accesses are protected from being hampered by any system malfunctions or cyber attacks thanks to this measure.

Types of Cyber Security Threats

One definition of something that could compromise cyber defenses is a harmful act committed by an individual or organization with the intention of stealing or corrupting data, accessing a network or otherwise messing with people's digital lives. As of right now, the following dangers are recognized by the hacker community:[26]

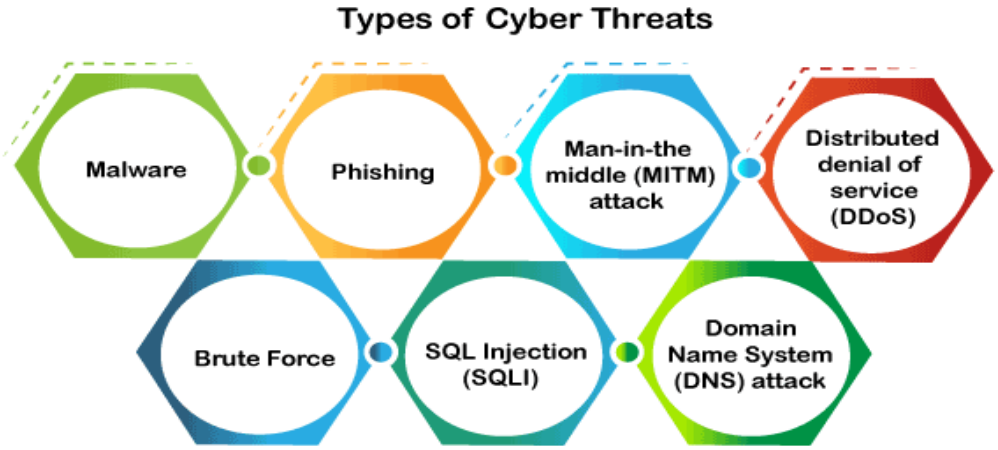

Fig.5 Types of Cyber Security Threats

Malware

The term "malware" refers to malicious software, which is the most frequent type of cyber assault instrument. It is utilized by the hacker or cybercriminal in order to cause disruption or harm to the system of a legitimate user. Some of

ISSN : 2455-9679
SJIF Impact Factor : 6.008

the most significant forms of malicious software that the hacker has generated are as follows:

- **Virus**: They are dealing with a piece of malicious malware that is capable of spreading from one device to another. As it travels throughout a computer system, it can clean data and infect files, steal information, or harm devices. It can also damage devices.
- **Spyware**: This program secretly logs all of the user's computer activity.
- **For example**, Spyware may acquire credit card information that cybercriminals might exploit for fraudulent purchases, withdrawals, and other illicit activities.
- **Trojans**: It is malicious software or code that seems to be something else in order to trick consumers into downloading and running it. By compromising or stealing data from our device or committing other harmful acts on our network, the main goal can be achieved.
- **Ransomware** This program can encrypt all of the user's data and files on their device, making them unreadable or even erasable. Afterwards, evildoers demand payment in order to unlock the encryption.
- **Worms**: In other words, it's software that can spread copies of itself to other devices without any help from humans. For them to illegally get or breach the data, it is not necessary that they be affiliated with any program.
- **Adware**: It is a piece of advertising software that can infect our device with viruses and display ads. It is an app that was installed on the user's device without their knowledge or agreement. The principal objective of this application is to generate revenue for its creator by means of the display of advertising within their web browser.
- **Botnets**: Criminals can commit theft through a network of infected devices connected to the internet, some of which they may even manage. It provides fraudsters with an easier way to steal passwords, data, and sensitive information without the user's awareness or consent.[27]

Phishing

As a kind of cybercrime, phishing occurs when an attacker poses as a trusted third party, such as a bank, PayPal, eBay, friend, or coworker. They reach out to a target or targets by phone, text, or email and offer a link in the hopes that the recipient will click it. Clicking on this link will take visitors to malicious websites that steal important information such as passwords, social security numbers, bank and credit card details, and personal details. In addition to allowing hackers remote access, clicking the link will install malware on the targeted devices.

Distributed denial of service (DDoS)

It is a form of cyber threat when cybercriminals impede the normal operations of targeted servers, services, or networks by inundating them with valid requests through Internet traffic. The requests originate from multiple IP addresses, potentially rendering the system inoperable, overloading servers, drastically decreasing performance, momentarily bringing them offline, or obstructing an organization’s essential operations.

Advertisement

Brute Force

Brave force attacks are a sort of cryptographic intrusion that entails attempting every conceivable combination of inputs until the right one is discovered. This is a common tactic used by cybercriminals to gain sensitive information such as PINs, passwords, login credentials, encryption keys, and more.

SQL Injection (SQLI)

An often-used exploit known as SQL injection allows hackers to get access to sensitive data by manipulating backend databases using malicious SQL scripts. Upon successful execution of the attack, the hostile actor gains the ability to access, modify, delete or remove from the SQL database any personally identifiable information, company records, user lists, or financial data regarding customers.

Domain Name System (DNS) attack

Criminals can steal sensitive information from infected computers and send users to harmful websites by taking advantage of DNS hijacking and other vulnerabilities in the Domain Name System. This type of malware is known as a DNS assault. Because of its central role in the internet's infrastructure, the DNS system is a major target for attacks on computer networks.

Man-in-the-middle (MITM) attack

A cyber danger known as a man-in-the-middle assault characterized by a cybercriminal intercepting communication or data transmission between two parties By disguising themselves as legitimate participants in a two-party conversation,

ISSN : 2455-9679
SJIF Impact Factor : 6.008

cybercriminals can gain access to sensitive data and deliver misleading answers. Gaining access to our company or customer data is the main goal of this attack. Connected devices on an insecure Wi-Fi network leave themselves vulnerable to data interceptions.[28]

Role of intrusion detection systems (IDS).

Notifications are sent out by intrusion detection systems (IDS) if they detect any abnormalities in a network's traffic. While intrusion detection systems mostly report on suspicious activities, some also take action in response to suspicious traffic or malicious conduct. Among these measures is the prohibition of data transfers from unknown or questionable IP addresses. An IPS is similar to an IDS in that it scans incoming network packets for malicious data. The main purpose of an IPS is not to identify and record threats, but rather to prevent them once they have been recognized.

The primary function of intrusion detection systems (IDS) is to identify suspicious activity on a network in order to prevent unauthorized access or damage. There are intrusion detection systems that employ both host-based and network-based architectures.

Both typical and unusual behavior are scrutinized by the system for telltale signs of known assaults. When something out of the ordinary happens, it is reported further up the stack and investigated further at the application and protocol levels. Intrusion detection systems are quite good at catching attacks such as Christmas tree scans and Domain Name System poisoning. The client computer is pre-configured to run an intrusion detection system that is based on the host. Intrusion detection systems that are network-based are one type of network security appliance. Additionally, cloud-hosted intrusion detection systems can assist secure cloud-based systems and data.

Table 1 Cyber Threat Type[28]

Cyber Threat Type	Description	Example/Impact
1. Malware	Malicious software designed to cause harm or disruption to a system.	Virus, Spyware, Ransomware, Trojans, Worms, Adware, Botnets.
2. Phishing	Cybercriminals impersonate trusted entities to trick users into revealing sensitive information through deceptive links.	Stealing passwords, credit card info, and social security numbers.
3. DDoS (Distributed Denial of Service)	Attackers overwhelm a system with high traffic to disrupt its normal functioning.	Server crashes, service disruptions, decreased performance.
4. Brute Force	Attackers attempt every combination of credentials to gain access.	Gaining unauthorized access to login details or encrypted data.
5. SQL Injection (SQLI)	Manipulating SQL queries to access or alter backend databases.	Stealing or altering customer records, financial data, or personally identifiable information (PII).
6. DNS Attack	Exploiting DNS system vulnerabilities to redirect traffic to malicious sites or steal information.	DNS hijacking, sending users to harmful websites to steal sensitive data.
7. MITM (Man-in-the-Middle) Attack	Cybercriminals intercept communication between two parties to steal or alter information.	Stealing company/customer data via unsecure communication (e.g., using insecure Wi-Fi networks).
8. IDS (Intrusion Detection System)	Monitors network traffic for suspicious activity and sends alerts when abnormalities are detected.	Detection of suspicious activities, such as DDoS, SQL injection, and malware activity.

ISSN : 2455-9679
SJIF Impact Factor : 6.008

III. LITERATURE REVIEW

Three classification methods were used by [29] to fix the problem that IDS that use artificial neural networks with fuzzy grouping often have: they aren't very good at finding low-frequency attacks. By dividing the varied training data into more uniform groups, they were able to improve the accuracy by making each training set less complicated. As a result of the tests that were done, J48 trees, Multilayer Perception (MLP), and Bayes network methods were chosen as the most valid. They can't use feature selection to get rid of all the features that aren't needed, are unnecessary, or don't belong in their work, which is a big problem. Researchers [30] used random forest and decision trees on the KDD-NSL dataset to create an intrusion detection system with a single machine learning model. Because it is more accurate, the random classifier gives you a score of 95.323%.

In the work suggested by [31] a single machine learning algorithm was used to find signs of network intrusion. Option tree, logistic regression, random forest, and support vector machine [32] are the methods that were used in the work. This work used the KDD-NSL dataset. Based on the study, the random forest classifier works best with the intrusion detection system. The random forest classification takes the least time to run, they also found. This work can only work well with a single dataset, which is one of its limitations.

Using a voting classifier, [33] created an ensemble-based approach IDS that combined the results of several supervised and unsupervised machine learning techniques. Current intrusion monitoring systems are more accurate and work better because of this work. Because it is older, the Kyoto2006+ dataset is more likely to be useful than the most useful KDDCup '99 dataset. In some cases, the recall of the result is very low, which means that the false negative rate (FPR) is high. By using the abuse approach to find known attacks and the anomaly approach to find new ones, suggested a real-time hybrid intrusion detection method. The high detection rate in this work was possible because the anomaly detection method was able to spot patterns of intrusions that were able to get past the misuse detection. As the model learned and trained the system each day, the rate of false negatives dropped sharply. The model's accuracy gradually rose each day until it reached a significant number of 92.65% on the last day of the experiment. With very large datasets, the problem of a slow recognition rate still exists. [34]

There is room for improvement in anomaly-based breach detection, especially when it comes to the false positive rate, as shown by [35]. A dataset called NSL-KDD was used to test the Extreme gradient boosting (XGBoost) and adaptive boosting (AdaBoost) learning algorithms. Hybrid or ensemble machine learning models need to be used to improve the performance, even though an accuracy of 84.253 was reached. Others that have been suggested can't use feature selection on the datasets they used to get rid of all the features that aren't needed, aren't important, or are redundant.

Different ML models and algorithms were tested with the NSL-KDD dataset in the work by [36]. The wrapping method was used for feature selection. They got a higher level of accuracy than what other studies with the same information had found. The high false positive rate of the model and the fact that most of the work has been done on signature-based attacks only hasn't been fixed yet, which is one of the biggest problems with zero-day detection. Different types of datasets can't be used properly in some of the work that has been done on intrusion detection systems in the past.

Researchers [37] came up with a new way to find intrusions by combining ensemble classifiers with feature selection. This makes the system more efficient and accurate at finding intrusions. Two new datasets, CIC-IDS2017 and AWID, along with the well-known NSL-KDD dataset were used for the study. CFS-BA-based method was used for feature selection. This method improves the ability to classify things into multiple groups even when the datasets aren't evenly distributed. Ninety-nine percent of the time, the model was right on the AWID dataset.

Both feeds forward neural network and pattern recognition neural network are used by [38]. Some other methods they used to train the artificial neural network-based IDS were Bayesian regularization and scaled conjugate gradient training. The suggested work's efficiency and capacity were judged using a number of performance metrics. In different tests of attack identification, the two models did better than each other, as shown by the outcome. This study found that the feed forward artificial neural network was more accurate (98.0742%). Putting the model to the test on various samples will make the work more efficient.[39].

ISSN : 2455-9679
SJIF Impact Factor : 6.008

Table 2 Intrusion Detection Techniques – Advantages, Disadvantages & Limitations

Technique	Description	Advantages	Disadvantages	Limitations
Signature-based IDS	Detects known attacks using predefined patterns or signatures	- High accuracy for known threats - Low false positives	- Cannot detect unknown attacks - Signature updates required	Ineffective against zero-day or polymorphic attacks
Anomaly-based IDS	Learns normal behavior and flags deviations as potential threats	- Can detect novel attacks - Adaptive to new environments	- High false positive rate - Requires training on clean data	Performance depends heavily on the quality of normal behavior modeling
Specification-based IDS	Uses manually defined specifications for system behavior	- Low false positive rate - Detects unknown attacks	- Hard to define exhaustive rules - Manual configuration overhead	Scalability and coverage are limited
Machine Learning-based IDS	Learns patterns from data using classifiers like SVM, RF, KNN, etc.	- Automated detection - Handles complex patterns	- Requires large labeled dataset - May not generalize well	Model overfitting, real-time performance bottlenecks
Deep Learning-based IDS	Uses DNNs, CNNs, LSTM, or Transformer architectures to detect attacks	- High detection accuracy - Good for sequential and large-scale data	- High computational cost - Requires large training data	Expensive to train, often black-box (lacks interpretability)
Rule-Based IDS	Uses expert-defined rules for matching attack behaviors	- Simple to implement - Transparent decisions	- Not flexible - High false negatives	Cannot scale with dynamic or evolving attack patterns
Hybrid IDS	Combines multiple techniques (e.g., signature + anomaly)	- Balanced performance - Better accuracy and coverage	- Increased complexity - Hard to tune	Integration and maintenance challenges
Heuristic-based IDS	Uses heuristic rules or scoring mechanisms to detect abnormal behavior	- Faster than full models - Good for known patterns	- May miss subtle attacks - Prone to evasion	Static heuristics can become outdated
Host-based IDS (HIDS)	Monitors activities on individual hosts (e.g., file access, logs)	- Granular monitoring - Detects local insider threats	- Resource intensive - Limited to host scope	Cannot detect network-level attacks
Network-based IDS (NIDS)	Monitors network traffic for suspicious patterns	- Broad visibility - Detects DDoS, scan, worms	- Encrypted traffic hard to inspect - Packet loss may cause missed alerts	Performance impacted by high throughput

ISSN : 2455-9679
SJIF Impact Factor : 6.008

Table 4 Network Traffic Intrusion Detection Parameters for Military Applications

Parameter	Description	Purpose/Importance
Traffic Flow Duration	Time taken for data packets to travel from source to destination.	Detects abnormal delays or disruptions in mission-critical communication.
Packet Inter-arrival Time	Time gap between consecutive packets in a flow.	Identifies DDoS or covert channels in military systems.
Protocol Type	Communication protocols used (TCP, UDP, ICMP, etc.).	Flags non-standard protocols used in unauthorized access.
Source/Destination Ports	Source and destination port numbers.	Detects use of non-standard ports for backdoor access.
Payload Size	Size of the packet payload.	Flags data exfiltration or malicious payloads.
Traffic Volume Patterns	Amount of data transmitted over a period of time.	Identifies DDoS attacks or large-scale exfiltration attempts.
Flow Direction	Direction of traffic (incoming/outgoing).	Flags abnormal outbound traffic, potential data exfiltration.
Geolocation of Traffic	Origin of traffic based on IP and geolocation.	Detects unauthorized access from foreign locations.
Encryption Type	Type of encryption used (e.g., SSL, IPsec).	Flags malicious tunneling or hidden C2 channels.
Session Time	Duration of active communication sessions.	Detects unusual session lengths indicative of malicious activity.

Table 3 Literature Review Table: Cyber security, IDS, and IoT/CPS (2023)

a	**Domain / Context**	**Proposed Method / Model**	**Dataset / Environment**	**Key Findings / Contributions**
[39]	IoT-based Industrial Control Systems (ICS)	Federated Simple Recurrent Units (Federated-SRUs) IDS	Real-world gas pipeline ICS dataset	Achieved accurate real-time intrusion detection with reduced computational cost and preserved data privacy; outperformed existing IDS models
[40]	Wireless Sensor Networks (WSN)	Lightweight Decision Tree with Gini Index	Enhanced WSN-DS dataset	Achieved 99.5% accuracy with minimal processing time; significantly faster than RF, XGBoost, and KNN
[41]	CPS with Industrial IoT (I-IoT)	Graph Attention Network (GAN-based IDS)	DAPT2020, Edge I-IoT datasets	Achieved detection accuracy of 96.97% and 95.97%; effectively captured hidden APT behaviors
[42]	IoT-driven Industrial Internet of Control	Generative Adversarial Network	NSL-KDD, KDDCup99,	Achieved 95–97% accuracy; improved TNR and HDR while preserving data

ISSN : 2455-9679
SJIF Impact Factor : 6.008

	Systems (IICs)	(GAN) based IDS	UNSW-NB15	confidentiality
[43]	Industrial CPS using NB-IoT	Optimized CNN with Search Economy	NB-IoT industrial traffic	Improved detection of low-rate DoS attacks under limited NB-IoT computational capacity
[44]	Software-Defined CPS	ADAM (Adaptive DDoS Attack Mitigation)	Real SDN-based CPS traffic	Achieved 99.13% mitigation accuracy; reduced false positives by 35–59%
[45]	IoT Trust Management Systems	Context-aware Trust Management System	Simulated IoT environment	Identified new context-based attacks and proposed an effective mitigation TMS
[46]	Maritime IoT Systems	Cyber Risk Assessment Framework	Maritime IoT infrastructure	Highlighted cyber threats and proposed mitigation strategies for maritime cybersecurity
[47]	Deep Learning Recognition Systems	Social IoT-based Collaborative Defense	Deep face recognition systems	Mitigated model inversion attacks using collaborative verification with SIoRS
[48]	Scale-free IoT Networks	Elephant Herding Robustness Evolution (EHRE)	Simulated large-scale IoT networks	Achieved 99% robustness efficiency; significantly outperformed existing robustness algorithms

IV. LITERATURE REVIEW

Intrusion Detection Systems (IDS) play a vital role in safeguarding modern networks, particularly in Internet of Things (IoT), Industrial Control Systems (ICS), and Cyber–Physical Systems (CPS), where security breaches can lead to severe operational and societal consequences. The reviewed studies indicate that traditional rule-based and signature-based IDS approaches are no longer sufficient to counter sophisticated and evolving cyber threats. As a result, machine learning and deep learning–based IDS models have gained prominence due to their ability to learn complex patterns, detect zero-day attacks, and adapt to dynamic network environments.

Recent advancements show that lightweight machine learning techniques are effective for resource-constrained environments such as Wireless Sensor Networks (WSNs) and NB-IoT systems, while deep learning models such as CNNs, RNNs, GANs, and Graph Attention Networks offer superior detection accuracy for complex and high-dimensional data in IoT-enabled ICS and CPS environments. Additionally, federated learning–based IDS solutions address privacy and data-sharing concerns by enabling collaborative model training without exposing sensitive operational data.

However, challenges such as high computational overhead, real-time deployment constraints, scalability, and false-positive reduction persist. Many IDS solutions remain attack-specific and lack generalization across diverse network conditions. Therefore, future IDS research should focus on developing adaptive, scalable, and privacy-preserving intrusion detection frameworks that balance detection accuracy with computational efficiency. Strengthening IDS capabilities is essential for ensuring the security, reliability, and resilience of next-generation IoT, ICS, and CPS infrastructures.

ISSN : 2455-9679
SJIF Impact Factor : 6.008

REFERENCES

[1] Anderson, James P. "Computer Security Threat Monitoring and Surveillance", 15 April 1980 http://seclab.cs.ucdavis.edu/projects/history/papers/ande80.pdf 107120.

[2] 3. Okey, O.D.; Maidin, S.S.; Adasme, P.; Lopes Rosa, R.; Saadi, M.; Carrillo Melgarejo, D.; Zegarra Rodríguez, D. BoostedEnML: Efficient technique for detecting cyberattacks in IoT systems using boosted ensemble machine learning. Sensors 2022, 22, 7409.69–84.

[3] A. Cardenas, J. Baras, and K. Seamon, "A framework for the evaluation of intrusion detection systems," in Proceedings of IEEE Symposium on Security and Privacy, (S&P), p. 15, 2006.

[4] Ahmed Jamal, A., et al., 2021. A review on security analysis of cyber physical systems using machine learning. Mater. Today: Proc..

[5] 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.

[6] 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.

[7] Alghamdi, M.I., 2021. Determining the impact of cyber security awareness on employee behaviour: A case of Saudi Arabia. Mater. Today:

[8] Alibasic, A., et al., 2016. Cybersecurity for smart cities: A brief review. In: Nternational Workshop on Data Analytics for Renewable Energy Integration.

[9] Alix Lachaud, Marcus Adam,Ilija Mišković, (2022) "Comparative Study of Random Forest and Support Vector Machine Algorithms in Mineral Prospectivity Mapping with Limited Training Data" 2023, 13(8), 1073; https://doi.org/10.3390/min13081073, 13 August 2023

[10] Aljabri, M.; Altamimi, H.S.; Albelali, S.A.; Maimunah, A.H.; Alhuraib, H.T.; Alotaibi, N.K.; Alahmadi, A.A.; Alhaidari, F.;

[11] Alzubaidi, A., 2021. Cybercrime awareness among Saudi nationals: Dataset. Data

[12] Amir, M., Givargis, T., 2020. Pareto optimal design space exploration of cyber–physical systems. Internet Things 12, 100308.

[13] Amit Kumar Balyan,SachinAhuja,Umesh Kumar Lilhore,Sanjeev Kumar Sharma,Poongodi Manoharan,Abeer D. Algarni,Abeer D. Algarni,Hela Elmannai ,Kaamran Raahemifar (2022) "A Hybrid Intrusion Detection Model Using EGA-PSO and Improved Random Forest Method" 2022, 22(16), 5986; https://doi.org/10.3390/s22165986, 10 August 2022

[14] Amit Kumar Balyan,Sachin Ahuja,Umesh Kumar Lilhore,Sanjeev Kumar Sharma,Poongodi Manoharan,Abeer D. Algarni Hela Elmannai,Kaamran Raahemifar(2022) "A Hybrid Intrusion Detection Model Using EGA-PSO and Improved Random Forest Method" 2022, 22(16), 5986; https://doi.org/10.3390/s22165986, 10 August 2022

[15] Anderson, James P. "Computer Security Technology Planning Study Volume 2", October 1972 http://seclab.cs.ucdavis.edu/projects/history/papers/ande72.pdf 2applications. Sustain. Energy Technol. Assess. 45, 101219.

[16] Arend, I., et al., 2020. Passive- and not active-risk tendencies predict cyber security behavior. Compute. Secure. 97, 101964.

[17] Ashraf, J., et al., 2021. IoTBoT-IDS: A novel statistical learning-enabled botnet detection framework for protecting networks of smart cities. Sustainable Cities Soc. 72, 103041.attacks. Mater. Today: Proc..

[18] Aziz, A.A., Amtul, Z., 2019. Developing Trojan horses to induce, diagnose and suppress Alzheimer's pathology. Pharmacol. Res. 149, 104471.

[19] C. E. Landwehr, A. R. Bull, J. P. McDermott, and W. S. Choi, "A taxonomy of computer program security flaws," ACM Comput. Surv., vol. 26, no. 3, pp. 211–254, 1994

[20] CaiwuLu,YunxiangCao,Zebin Wang (2024) "Research on Intrusion Detection Based on an Enhanced Random Forest Algorithm" 2024, 14(2), 714; https://doi.org/10.3390/app14020714, 15 January 202

[21] CaiwuLu,Yunxiang Cao,Zebin Wang (2024) "Research on Intrusion Detection Based on an Enhanced Random Forest Algorithm" 2024, 14(2), 714; https://doi.org/10.3390/app14020714, 15 January 2024

[22] Cao, J., et al., 2021. Hybrid-triggered-based security controller design for networked control system under multiple cyber attacks. Inform. Sci. 548,

[23] Cao, Y., et al., 2019. A topology-aware access control model for collaborative cyber–physical spaces: Specification and verification. Comput. Secur. 87,101478.

[24] Chen, H.; Jiang, B.; Ding, S.X.; Huang, B. Data-driven fault diagnosis for traction systems in high-speed trains: A survey, challenges, and perspectives. IEEE Trans. Intell. Transp. Syst. 2020, 23, 1700–1716.

[25] Chunying Zhang,Wenjie Wang,LuLiu,Jing Ren,Liya Wang (2022) "Three-Branch Random Forest Intrusion Detection Model" 2022, 10(23), 4460; https://doi.org/10.3390/math10234460, 26 November 2022

[26] Arend, I., et al., 2020. Passive- and not active-risk tendencies predict cyber security behavior. Comput. Secur. 97, 101964.

[27] Chunying Zhang,Wenjie Wang,LuLiu, JingRen,Liya Wang (2022) "Three-Branch Random Forest Intrusion Detection Model" 2022, 10(23), 4460; https://doi.org/10.3390/math10234460, 26 November 2022

[28] Ashraf, J., et al., 2021. IoTBoT-IDS: A novel statistical learning-enabled botnet detection framework for protecting networks of smart cities. Sustainable Cities Soc. 72, 103041.attacks. Mater. Today: Proc..D. Aldous, "The continuum random tree. I," The Annals of Probability, pp. 1–28, 1991.

[29] D. Ruck, S. Rogers, M. Kabrisky, M. Oxley, and B. Suter, "The multilayer perceptrons as an approximation to a Bayes optimal discriminate function," IEEE Transactions on Neural Networks, vol. 1, no. 4, pp. 296–298, 1990 digital forensics. Digit. Investig. 22, 3–13.

[30] 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

[31] Muawia A. Elsadig (2023) "Detection of Denial-of-Service Attack in Wireless Sensor Networks: A Lightweight Machine Learning Approach" Volume: 11, Page(s): 83537 – 83552,202

[32] 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 – 74020,202

[33] 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

[34] 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 – 5291,202

[35] 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

[36] Harsh Kumar;Oscar. A. Alvarez;Sanjeev Kumar(2023) "Experimental Evaluation of Smart Electric Meters' Resilience Under Cyber Security Attacks"Volume: 11Page(s): 55349 – 55360,202

[37] 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 – 2690,202

[38] 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, Page(s): 2694 - 2704 ,2023

[39] Talha Naeem Qureshi;Zahoor Ali Khan;Nadeem Javaid;Abdulaziz Aldegheishem;Muhammad Babar Rasheed;Nabil Alrajeh(2023)"Cities" Volume, Page(s): 79056 – 79072,2023