A Holistic Analysis of Cybersecurity Threats and Attack in IoT and Critical Infrastructure Systems

Attack Type/Name	Details of Attack	Security Mechanism (to Prevent/Detect)	CIA Triad	Attack Category (Active/Passive)	Attack Sub-Category	Threat (Among Four Kinds)	Ref-erences
Dam cyber-attack	The attackers were able to get data on operations, such as water levels, temperatures, and device statuses, by gaining unauthorised access to the Bowman Avenue Dam SCADA system. It demonstrated how simple it is for attackers to alter the water flow settings, the amount of chemicals used in water treatment, and to release the floodgates during a downpour. The incident also serves as an example of the enormous devastation that an IoT-based critical infrastructure cyberattack of this kind can inflict.	access control measures, ensuring physical security and preventing backdoors or malicious code in login process.	Integrity, availability	Active	Cyber-attacks to critical infrastructures	Disruption, Usurption	1
Healthcare cyberattack	A healthcare company was the target of a highly skilled attack. First, the hackers obtained login credentials from a supplier of IT equipment to the hospital. Second, they used SamSam ransomware's remote execution methods to attack a server. The vital data files of the hospital were then encrypted.	strong encryption methods for data transmission,ensuring regular and remote security updates	Confidentiality, availability	Active	Cyber-attacks to critical infrastructures	Disruption, Unauthorized Disclosure	1
Malware injection	The insertion of malicious software into cyberspace with the intent to harm or disable the system is known as malware injection [26]. Viruses, trojans, worms, spyware, rootkits, ransomware, and adware are examples of common malware. One well-known malware example is the WannaCry ransomware. It's employed to prevent users from accessing their files.	Implementing regular security updates and utilizing intrusion Detection system	Integrity, availability, confidentiality	Active	Supply chain Attack, Remote execution attack	Disruption, Unauthorized Disclosure, Usurption	1

Phishing	is an attack on data requests made by an unreliable source. The unreliable source makes an effort to persuade people that it is a reliable source. The victim carries out specific behaviours that the attacker has previously specified, including clicking the malicious link and submitting sensitive data, if he is persuaded that the attacker is a reliable source.	Implement strong authentication mechanisms and conductiong regular education and awarness training for employees	Integrity, confidentiality	Passive	Torjans,Worms,Spayware	Deception, Unauthorized Disclosure	1
SQL injection	The goal of attacks is to take, change, or remove database content. Attacks on data-driven systems are made with it. Attackers use SQL query statements to get access to the system's database server [30]. Databases are present in nearly all IoT-based critical infrastructures.	Implement input Validation techniques and parameterized queries along with regular updating security patches.	Integrity, confidentiality	Active	Spear Phshing	Unauthorized Disclosure, Usurption	1
Network Attacks	These attacks usually happen on the IoT network.These attacks will allow hackers to have remote access and send wrong instructions to take control of IoT devices	TLS offers secure network communication, guarding against network attacks that try to intercept or alter data while it is in transit.	Confidentiality	Active	Traffic analysis attack, Selective forwarding, Sybil attack, Sinkhole attack, Botnet attack, Hello-flood attack, Man in the middle attack	Unauthorized Disclosure	2
Zigbee Attacks	These attacks will enable hackers to capture the sensitive information and Zigbee traffic.Zigbee is a cheap and energy-efficient wireless system often used in smart devices like home security systems or medical monitors.	Authentication Symmetric algorithum,asymmetric or key cryptrography .	Integrity, confidentiality	Both active and passive	Eavesdropping attack, Replay attack, Packet forging attacks	Deception	2
Z-Wave Attacks	These attacks will allow hackers to execute security attacks against Z-Wave devices.Z-Wave is a common way for smart gadgets in your home, like door locks and lights, to talk to each other wirelessly.	End to end messages secrecy	Integrity, confidentiality	Both active and passive	Z-Wave downgrade attack, Z-Wave injection attack, Z-Wave Man in the middle attack	Unauthorized Disclosure	2
DoS (Denial of Service) Attack:	Data from websites and other services may not be stolen by this type of attack[24]. Attackers use a huge number of botnets to target services, sending thousands of requests to the target, causing the service to crash and become unavailable.	To fix vulnerabilities and stop services from crashing, install the most recent firmware.	Availability	Active	Encryption Attacks	Disruption	3

Man-in-the-Middle Attack	An attacker can launch a man-in-the-middle attack by breaching the communication channels between two systems. by listening in on conversations between two people.	To prevent interception, make sure encrypted communication routes are used and reboot any suspect devices.	Confidentiality and integrity	Passive	Encryption Attacks	Unauthorized Disclosure	3
WIRELESS JAMMING ATTACK	Attackers target the IoT devices' physical actuators and sensors. Common assaults include jamming, which uses high-frequency waves to interrupt communication.it have deep learning based and sensing based jamming attacks	Using reinforcement learning for mitigating jamming based on the Q-learning algorithm,use deep learning framework to divert and corrupt the jammer decisions	Availability	Active	Perception layer attack on iot layers	Disruption	4
Battery Exhaustion Attack	a kind of cyberattack in which malicious code is used to extend operations and utilise large amounts of power, possibly making the device unusable.	An intrusion detection system (IDS) is used to track task power usage. An alarm is triggered if it surpasses a predetermined threshold.	Availability	Active	Transport layer attack on iot layers	Usurption	4
Resource consuming attacks	Attacker misuse system resources, resulting in injustice, crashes, weariness, and eventually poor service delivery.	Using TLS layered security and symmetric encryption to mitigate resource-consuming attacks	Availability	Active	Network layer attack on iot layers	Disruption	4
Ransomware Attack	IoT edge gateways are the focus of an IoT ransomware attack. The IoT system had been infected with malware.The gateway is fully accessible to attackers.All user and data files, including PLC and I/O device data, are encrypted by attackers.Threats of data destruction or ransom demands for data decryption	Install firewalls from the Next Generation, which have better traffic filtering capabilities.	Availability , integrity, Confidentiality	Active	Erebus Linux Ransomware attack	Unauthorized Disclosure, Disruption	5

1. https://dergipark.org.tr/en/download/article-file/2160183
2. https://www.scirp.org/journal/paperinformation?paperid=99316
3. https://arxiv.org/ftp/arxiv/papers/2009/2009.05708.pdf
4. https://arxiv.org/ftp/arxiv/papers/1912/1912.01712.pdf

5. https://www.mdpi.com/2624-831X/2/1/9