Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 8s (2025)

A study on Mitigation Strategies and Techniques to Reduce IoT Attacks through Cybersecurity and Block Chain Technology

Mala B A[1], M V Sudhamani[2], Ramesh S Chakrasali[3]

[1,3]Department of Computer Science & Engineering, B.M.S. College of Engineering, Bengaluru, Visvesvaraya Technological University, Belagavi, Karnataka, India

[2]Department of Information Science & Engineering, B.M.S. College of Engineering, Bengaluru, Visvesvaraya Technological University, Belagavi, Karnataka, India

malaba.gowda@gmail.com, sudhamanimv.ise@bmsce.ac.in, ramjuly20@gmail.com

Article History:

Received: *27-10-2024*

Revised:*30-11-2024*

Accepted:*28-12-2024*

Abstract:

The Internet of Things (IoT) has completely changed depending on how we engage with technology by enabling automation, monitoring, and cross-domain data sharing by linking billions of devices globally. IoT device development has brought out new security challenges, as these devices frequently lack strong security safeguards, leaving them open to hacker attacks. Even after every attack is thoroughly examined by enlightening the methods that cybercriminals employ to take advantage of weaknesses in IoT devices, network attacks still exist. This paper addresses the reasons behind the attacks, which include espionage, sabotage, privacy invasion, financial gain and data theft. In addition, it also assesses the effects of IoT attacks on people, businesses, and society at large, considering financial losses, reputational harm, service interruptions, data breaches, and safety risks. These effects highlight how crucial it is to protect IoT ecosystems and take preventative action to reduce the dangers associated with cyberattacks. In addition, a framework is provided that includes security best practices, mitigation strategies, technological controls, policy measures, and security awareness training for reducing IoT attacks. Apart from this, integrating Blockchain Technology into IoT security, enterprises/organizations can fortify their IoT infrastructure and protect themselves from ever changing cyber threats by understanding the motivations of attackers is also discussed.

Keywords: Cyberattacks, Threats, stakeholders, data, IoT, security, Block chain

1. Introduction

The IoT has arisen as an extraordinary power, reshaping ventures, upgrading effectiveness, and enhancing our regular routines by interconnecting an immense range of gadgets, sensors, and frameworks. From smart homes and wearable gadgets to modern computerization and shrewd urban areas, the expansion of IoT advancements has introduced a time of phenomenal network and development. In any case, in the midst of the commitment of a hyper-associated world lies a mind-boggling scene of safety difficulties and weaknesses that undermine the uprightness, secrecy, and accessibility of IoT ecosystems.

Increasing frequency, sophistication, and effect of cyberattacks targeting the networked systems has made the networks a critical concern in recent years and security of these devices. IoT's intrinsic features such as limited resources, a wide range of device kinds, and inconsistent communication

protocols, create special difficulties for maintaining a strong cybersecurity posture throughout the IoT ecosystem. Because of this, in an increasingly linked world, comprehending and preventing IoT threats is essential for securing vital infrastructure, safeguarding sensitive data, and maintaining user privacy.

IoT devices count has been rising at an exponential rate. In the global scenario, there were 8.74 billion linked devices in 2020 and by 2030, this figure is likely to rise to 25.44 billion. Naturally, as the number of devices increases, the potential targets for attackers also increases. IoT attacks, for instance, increased by more than twice as much between 2018 and 2023, according to different security reports collected from Symantec, Kaspersky, or Cisco as shown in the figure 1.

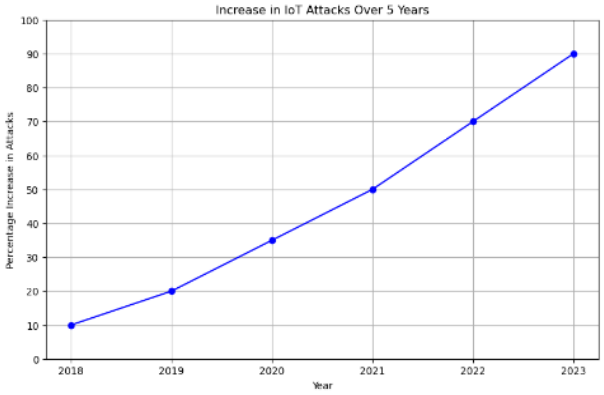

Figure 1: IoT devices Versus attacks [www.cisco.com]

IoT adoption continuing to rise, the estimated global cost of security breaches is also expected to surpass $1 trillion. This covers both direct expenses like intellectual property theft and indirect expenses like reputational harm. For instance, when companies were hit by ransomware attacks, which targeted IoT devices have been claimed to have paid in an average of hundreds of thousands of dollars, with the entire expenses involving recovery efforts and higher.

The key contributions of this paper are:

- The different types of attacks are listed, where detailed study of common IoT attacks and its mitigation strategies are discussed.
- The different methods/techniques are discussed in detail to prevent the IoT attacks which reduces the leaking of sensitive data.
- Along with other methods, a block chain technology is discussed which gives a secured platform for data sharing by reducing IoT attacks.

The remaining of the paper is prearranged as follows: Introduction in 1, a description about review papers is described in section 2, followed by the study of common IoT attacks in section 3. The different methods/techniques are discussed in section 4, block chain technology in section 5 and concluding remarks followed by references.

2. Related Works

In [1], discussion is given about the intrusion detection attack in the Autonomous Distributed Internet of Things system (ADIoTs). It is based on the concept of light weight intrusion detection technique, where every node must participate in the competition to detect neighbour target node. This system uses

analytical model called Stochastic Petri Net (SPN) technique to maximize the lifetime of the system. This system is analysed for voting-based Intrusion detection system (IDS) under various conditions like per-node defence capability and per-node attacker capability by maximizing the Mean Time to Failure (MTTF) through which the lifetime of the system is increased.

The botnet attacks on the physical grid systems are discussed in [2], where the large number of IoT devices are compromised. This detailed about the vulnerabilities of the botnet attacks and developed an optimized framework for the effective mitigation of botnet attacks. An Epidemic model is developed as a solution to maintain the power grids and reduce the cyber risks. This system here improved the grid resiliency by reducing the attacks.

Enhancement of IoT security with respect to patient and medical data for healthcare IoT systems are explained in [3]. This paper addressed the IoT attacks like Man-in-the-middle attack, Spoofing, and Sybil attacks. Also, given various security solutions to overcome these attacks, they are Testing Resource Solutions (TRS), Cryptographic algorithms, Received Signal Strength Indication (RSSI), and Behaviour monitoring techniques. Additionally, a multi-layered security approach by integrating authentication, behaviour monitoring, encryption and anomaly detection provides integrity, privacy and security of patient and medical data were also discussed.

The IoT systems are keep growing in popularity, where the major concern is about the security of huge amount of sensitive data get generated [4]. IoT devices are having limited resources and to reduce the energy consumption, it is integrated with several IoT protocols. A new framework called HARPAGON is introduced, which maximizes the attack efficiency by energy consumption. It also depends on how the victim and the attacker are feeling at that particular moment. It models the interaction between an attacker and a victim using Markov chain theory, which is discussed for jamming attack compared to classical jamming attack. The model is demonstrated using simulation testbed under various energy saving modes so that the attacker energy consumption is reduced to 24.82% by improving the impact to 13.75% for jamming attack.

The IoT adoption for various applications in [5] enables and improves the quality of life, but also suffers from various attacks. This paper discussed about the dynamic botnet attacks and developed an epidemic model to exploit the vulnerabilities of power grids. A strategic cross-layer game-theoretic framework is designed to improve the cyber-physical grid's resilience and aid in decision-making. This technique effectively reduces dynamic botnet attacks in both the physical and cyber layers, allowing grid operators to maintain normal operations.

In [6], discussed about the rapid growth of IoT and its impact on the various sectors. However, there are still security issues with the IoT, including safe communication, device authentication, and data privacy. This paper introduced block chain as a method for secure IoT networks. Block Chain Technology (BCT) is a decentralized, immutable ledger, which provides visible, unchangeable records of interactions and transactions between IoT devices and can enhance security. Here, the comparison is done between conventional techniques and by using BCT, which enhances IoT network security through experimentation and simulations.

In [7], discussed the security of IoT without using block chain technology and also using block chain technology. This paper describes various cryptographic algorithms can be used for securing sensitive

data like Advanced Encryption Standard (AES) for smart home, Elliptic Curve Cryptography (ECC) and Cryptographic Hash Functions (CHF) for IoT applications. Even by using cryptographic algorithms alone not reducing the attacks, so to enhance the IoT security, Block Chain technology is integrated to cryptographic algorithms and the paper provides complete analysis. The analysis shows that using block chain technology, the attacks are reduced and the security is increased.

3. Study of IoT Attacks and Mitigation Techniques

This section discusses about the common IoT attacks, impact and mitigation techniques. As IoT keeps on developing, it holds the possibility to make a hyper-associated reality where for all devices are interconnected and smart. In any case, difficulties like interoperability, information protection, security weaknesses, and moral contemplations should be addressed to open the maximum capacity of IoT while, guaranteeing its mindful and maintainable organization. IoT gadgets are helpless against different sorts of cyberattacks because of their interconnected nature, restricted computation assets, and frequently insufficient safety efforts. A few common attacks focusing on IoT gadgets are shown in the figure 2 and discussed in detail.

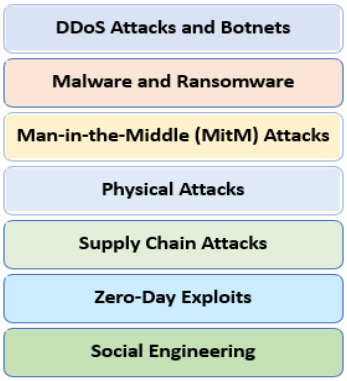

Figure 2: Common IoT attacks

3.1 Distributed Denial of Service (DDoS) attacks and Botnets

- **Distributed Denial of Service (DDoS) attacks**

An intentional attempt to interfere with a targeted server's, administrator's, or organization's routine operations by overloading it with traffic from several sources is known as DDoS attack [8]. Examples are volume attacks, protocol attacks, application layer attacks etc.

- Impact of DDoS
  - DDoS attacks can cause serious issues for the organizations they target, such as Creation of websites, online services, or network infrastructure unavailable to authorized users.
  - Financial Losses like Loss of income, productivity, or client trust as a result of downtime.
  - Reputation damage includes bad press, brand erosion, and diminished consumer trust as a result of data breaches or service interruptions.
  - Operational costs are outlays for things like incident response, mitigation solutions, and legal fees that come with preventing and recovering from DDoS attacks.
- Mitigation Strategies

- Network monitoring: To identify and stop harmful traffic, intrusion detection and prevention systems (IDPS) are used.
- Traffic Filtering: To reduce the effects of DDoS assaults and filter out unwanted traffic, content delivery networks (CDNs), load balancers, and firewalls are deployed.
- Anomaly detection is the process of identifying unusual network activity that could be a sign of botnet activity or DDoS attacks using machine learning algorithms and behavioural analytics.
- Botnet Takedowns: Working together with internet service providers (ISPs), security companies, and law enforcement to take down and interfere with botnet activities.
- Security hygiene: Maintaining a high standard of cybersecurity by patching vulnerabilities, upgrading software on a regular basis, and encrypting and password-protecting IoT devices.

- **Botnets**

A botnet is organization of compromised PCs, cell phones, IoT gadgets, or other web associated gadgets that are constrained by a headquarters and control (C&C) server [9]. For example, phishing messages, programming weaknesses, or animal power assaults on feeble passwords [10].

- Impact of Botnets

- When attacked, these gadgets become piece of the botnet and can be utilized to do different malicious exercises.

- Botnets are used in DDoS Attacks, spam distribution, credential theft, cryptocurrency Mining and Information Theft.

- Mitigation Strategies

- Authentication: To protect IoT device access, use strong authentication algorithms like AES, RSA etc.
- Firmware Updates: Patch vulnerabilities by regularly updating the device's firmware.
- Segmentation of the Network: To stop the spread of a botnet, segment IoT devices.
- Tools for Monitoring: Make use of systems for detecting anomalies and traffic monitoring.
- Firewalls and intrusion detection systems (IDS): To stop malicious traffic, use firewalls and IDS.
- Management of passwords: Make sure that default passwords are changed.
- Accountability of Vendors: Select vendors whose security is prioritized.
- Client Training: Instruct clients about botnet gambles.
- Response to an Incident: Create and test a strategy for dealing with botnet attacks.

3.2 Malware and Ransomware

- **IoT Malware**

Malicious software created expressly to target IoT devices connected to networks is referred to as IoT malware [11]. This malware can take advantage of holes in security and vulnerabilities found in IoT devices, giving hackers access to the device without authorization, stealing data, or performing other malicious tasks.

Examples: viruses, worms, Trojans, spyware, email attachments, removable media and adware.

- Impact of IoT Malware
  - Data Breach: IoT device's sensitive data can be hacked by malware, resulting in identity theft and invasions of privacy.
  - Service Disruption: Malware has the ability to disrupt the normal operation of IoT devices, causing users and businesses inconvenience or even financial loss.
  - Formation of a Botnet: IoT devices that have been compromised can be recruited into botnets, which can be used for a variety of malicious activities like DDoS attacks, spreading more malware, or mining cryptocurrencies.
  - Malware can cause physical damage to infrastructure or equipment in industrial IoT settings, posing a risk to safety and costing money.
  - Damage to Reputation: IoT malware incidents may cause damage to an organization's reputation, which could result in a loss of market share and customer trust.
- Mitigation Strategies
  - Strong Authentication: To safeguard access to IoT devices, we can make use of multi-factor authentication (MFA).
  - Maintaining IoT devices with the most recent security patches requires regular updates.
  - Network Segmentation: To contain malware outbreaks, divide IoT devices into isolated networks.
  - Data Encryption: To prevent unauthorized access, data should be encrypted both while it is at rest and in transit.
  - Behavioural Analysis: In order to keep an eye on how IoT devices behave, install IDS. Disable unnecessary services and features on IoT devices with device hardening.
  - Standards for Vendors: Work with vendors who place security first and follow industry standards.
  - User Education: Inform users of the dangers and best practices associated with IoT security.
  - Firewall and IPS: Monitor and filter network traffic with firewalls and intrusion prevention systems.
  - Plan for an Incident: To quickly respond to IoT malware incidents, create and maintain a plan for an Incident.

- **Ransomware**

It can infect IoT devices and encrypt data or prevent users from using them until a ransom is paid and also leads to data loss, device bricking, or unauthorized access to IoT devices [12].

- Impact: Attacks by ransomware can have severe repercussions for individuals and organizations, including the following:
  - Data Loss: Permanent data loss as a result of ransomware deletion or encryption.
  - Financial Losses: The payment of ransom demands, downtime, and costs associated with recovery can all result in substantial financial losses.
  - Negative publicity, a decline in customer confidence, and reputational harm brought on by data breaches or service interruptions are all examples of reputational damage.
  - Operational Disruption: Ransomware infections can cause downtime, productivity losses, and operational disruptions that disrupt business operations and continuity.

- Mitigation Strategies
  - Data Backup and Recovery: Keeping regular offline or cloud backups of important data to restore systems in the event of ransomware infections [13].
  - Security Patching: Applying security updates and patches promptly to fix known vulnerabilities that ransomware exploits.
  - Educating users about phishing scams, safe browsing practices, and the significance of verifying email attachments and links are all parts of user training and awareness.
  - Endpoint protection platforms (EPP) and endpoint detection and response (EDR) solutions are used in endpoint security solutions to identify and prevent ransomware infections.
  - To stop the spread of ransomware infections, networks are segmented and access to important systems and data is restricted.

3.3 Man-in-the-Middle (MitM) Attacks

"Man-in-the-Middle" (MitM) cyberattacks happen when an intruder secretly intercepts and potentially modifies communications between two parties [14]. As a "middleman" to eavesdrop on or alter the data being exchanged, the attacker positions themselves between the communicating parties.

- Impact of MitM attack
  - Attackers have the ability to intercept and steal sensitive data that is exchanged between parties.
  - Data Manipulation attackers can alter or forge data packets, which can lead to unauthorized transactions or misinformation.
  - Identity Theft attacks can make it easier to pretend to be someone else, which can lead to identity theft or unauthorized system access.
- Mitigation Strategies
  - Encryption: To safeguard data from being intercepted and altered, use end-to-end encryption.
  - Digital Certificates: To authenticate communication endpoints, use digital certificates and implement Hyper Text Transfer Protocol Secure (HTTPS).
  - Network Segmentation: To limit the scope of MITM attacks, segment networks and make use of VLANs.
  - Strong Authentication: To confirm the identities of parties communicating, use strong authentication mechanisms like passwords, two factor authentication and encryption algorithms etc.
  - Network Monitoring: Keep an eye on what's going on in the network to look for anything odd or suspicious that might be MITM attacks.
  - Security Awareness Training: Inform users about the dangers of MITM and the most effective methods for detecting and avoiding such attacks.
  - HTTPS Everywhere: To prevent plaintext interception, promote the use of HTTPS for all web communications.
  - Avoid using unsecured public Wi-Fi networks and secure Wi-Fi networks with strong encryption method such as WPA3.
  - Secure Configuration: To avoid MITM flaws, make sure that applications and devices are securely configured.

3.4 Physical attacks

Utilizing physical access to hardware, infrastructure, or facilities to compromise the confidentiality, integrity, or availability of data and systems constitutes a physical attack in the field of cybersecurity [15]. These attacks can have devastating effects on businesses and frequently circumvent conventional cybersecurity measures. Examples are theft, unauthorized access to facilities and hardware tampering etc.

- Impact of physical attacks
  - Data Theft: Attackers can physically steal sensitive data or equipment from devices or locations.
  - Disruption of Operations: Infrastructure can be damaged or critical systems disabled by physical attacks, which can disrupt business operations.
  - Unauthorized Access: An attack can compromise security by gaining unauthorized access to restricted areas or systems.
  - Sabotage: Intentional damage to infrastructure or equipment can result in physical attacks that cause financial losses and downtime.
- Mitigation Strategies
  - Physical Security Measures: To prevent unauthorized access, put in place physical security measures like locks, access control systems, and surveillance cameras.
  - Environmental Controls: Protect infrastructure and equipment from environmental hazards like fluctuations in temperature, humidity, and power surges.
  - Training for Employees: Instruct employees on the significance of physical security and teach them how to recognize and report suspicious behaviour.
  - Management of Visitors: To keep an eye on and regulate who has access to the building, implement visitor management procedures like issuing visitor badges and escorting visitors.
  - Asset Inventory and Tracking: Use RFID-based tracking technologies to keep track of where important equipment is and how it's moving.
  - Security Guards: Put trained security guards on the job to keep an eye on the premises and respond quickly to security incidents.
  - Redundancy and Backup: To lessen the impact of physical damage or equipment failure, implement redundancy and backup systems.
  - Remote Monitoring: Security personnel can be alerted to potential threats by using remote monitoring systems to monitor the facility and its equipment in real time.
  - Physical Barrier Protection: To prevent unauthorized access and safeguard sensitive areas, install physical barriers like bollards, fences, and barriers.
  - Plan for an Incident: Create and test a plan for an Incident to effectively respond to physical security breaches and minimize their impact on operations.

3.5 Supply Chain attacks

In order to gain unauthorized access to critical systems, compromise the integrity of data, or disrupt operations, supply chain attacks involve insightful vulnerabilities in the ecosystem of the supply chain

[16]. In order to penetrate target organizations indirectly, attackers target dependable suppliers, vendors, or third-party partners.

- Impact of supply chain attacks
  - Software and hardware compromise: Attackers enter the supply chain to install malicious software or hardware, compromising goods.
  - Data Breach: In the supply chain, sensitive data can be exposed or stolen, resulting in intellectual property theft or privacy violations.
  - Attacks on the supply chain have the potential to disrupt business operations, resulting in financial losses and damage to the company's reputation.
- Mitigation Strategies
  - Assessment of Vendor Security: To ensure that suppliers and vendors adhere to security best practices, conduct comprehensive assessments of their security.
  - Code Signing and Verification: Software components obtained from the supply chain can be verified for authenticity and integrity using code signing.
  - Supply Chain Monitoring: To identify and respond to suspicious activities or anomalies, implement continuous supply chain monitoring.
  - Vendor Risk Management: To assess and reduce risks associated with third-party suppliers, develop a robust vendor risk management program.
  - Secure Communication Channels: To safeguard against eavesdropping and tampering, supply chain partners should encrypt their communications.
  - Multi-factor Authentication: To safeguard access to supply chain resources and systems, implement multi-factor authentication.
  - Regular Audits and Compliance Checks: To ensure that suppliers adhere to security standards and regulations, conduct regular audits and compliance checks.
  - Planning for an Incident: To effectively respond to attacks on the supply chain and minimize their impact, a plan for an Incident should be developed and tested on a regular basis.

3.6 Zero-Day Exploits

A cyberattack that exploits a flaw in software, hardware, or firmware that was not previously known about is known as a zero-day exploit. There are no security updates or patches available to fix the vulnerability because neither the vendor nor the developer is aware of it. This leaves systems open to being exploited.

- Impact of Zero-Day Exploits
  - Unpatched Vulnerabilities: Zero-day exploits target vulnerabilities that have not been discovered, making systems vulnerable.
  - Data Breach: Attackers can take advantage of zero-day vulnerabilities to break into systems or steal sensitive data.
  - Disruption of Business Operations: Zero-day attacks can cause downtime and financial losses for businesses.
- Mitigation Strategies
  - Management of Vulnerabilities: To quickly identify and patch vulnerabilities and also find vulnerabilities in network, hardware, and software infrastructures, by regularly scanning when needed.

- Behaviour-based Detection: To identify and prevent malicious activities linked to zero-day exploits, use behaviour-based detection mechanisms.
- Segmenting a network is a method for limiting the impact of zero-day exploits and preventing lateral movement.
- Zero Trust Architecture: To reduce the attack surface and verify all network communications, adopt a zero-trust architecture.
- Threat Intelligence: To stay up to date on new threats and zero-day vulnerabilities, subscribe to threat intelligence feeds.
- Education of Users: Inform users about the dangers posed by zero-day exploits and encourage them to promptly report suspicious activities.

3.7 Social Engineering

Attackers use the psychological manipulation technique known as "social engineering" to trick individuals or organizations into giving away confidential information, granting access to restricted systems, or engaging in activities that could compromise security [18].

- Impact of social engineering
  - Data Breach: Social engineering attacks can get people to reveal sensitive information by tricking them, which can lead to data breaches.
  - Unauthorized Access: Attackers can exploit human trust to gain unauthorized access to systems or locations.
  - Financial Losses: Through extortion, fraud, or phishing, social engineering attacks can cause financial losses.
  - Damage to an Organization's Reputation: Successful social engineering attacks can undermine customer trust and damage an organization's reputation.
- Mitigation Strategies
  - Training for Employees: Train employees on a regular basis to recognize and resist social engineering techniques.
  - Security Policies and Procedures: Clearly define security policies and procedures for handling sensitive data and responding to attempts at social engineering.
  - Multi-factor Authentication: To protect against unauthorized access, use multi-factor authentication.
  - Email Filtering: Phishing emails can be identified and blocked by utilizing email filtering and spam detection tools.
  - Access Controls: Use the principle of least privilege to restrict access to sensitive systems and information.
  - Plan for an Incident: Create a plan for an Incident and regularly test it to respond quickly and effectively to social engineering attacks.
  - User Awareness: Inform users about the strategies utilized in social engineering attacks and encourage them to report anything that seems suspicious.
  - Verification Procedures: In order to verify the requestor's legitimacy, implement verification procedures for sensitive transactions or requests.

The common IoT attacks, its impact and mitigation strategies on the IoT networks is discussed in detail in above section. The common mitigation strategies versus IoT attacks that can applied to reduce the IoT attacks are summarized in the table 1.

Table 1: Mitigation Strategies V/S IoT attacks

IoT Attacks	Mitigation Strategies															
	Firewalls/ Traffic Filtering/Segmentation of network	Anomaly detection/ Tools for network monitoring	Botnet takedowns	security Hygine/Firmware Updates/Managing passwords	Authentication	Selection of vendors	Client Education/training/	Repones to an incident	Data Encryption	Data backup & recovery	Digital certificates	HTTPS everywhere	Secure Configuration	Environmental Controls	Zero Trust Architecture	Threat Intelligence
DDoS [8]	✓	✓	✓	✓												
Botnets [9-10]	✓	✓		✓	✓	✓	✓	✓								
Malware [11]	✓			✓	✓	✓	✓	✓	✓							
Ransomware [12-13]				✓						✓						
Man-in-the-Middle attack [14]	✓	✓			✓				✓		✓	✓	✓			
Physical attacks[15]	✓	✓		✓	✓		✓	✓		✓			✓	✓		
Supply Chain attacks [16]	✓	✓			✓	✓	✓	✓	✓							
Zero Day Exploits [17]	✓	✓					✓								✓	✓
Social Engineering [18]				✓	✓		✓	✓					✓			

4. Methodology/Techniques to Reduce IoT Attacks

Some of the multidimensional approach that spans technical, organizational, and human aspects of cybersecurity techniques are discussed here to reduce the IoT attacks. The figure3 shows the various methodologies.

Figure 3: Methodologies to reduce IoT attacks

4.1 Threat Intelligence and Risk Assessment

Create a threat intelligence program to collect and examine data regarding new threats, weaknesses, and attack methods related to the IoT [19] and also, regularly conduct risk assessments, taking into account elements like asset criticality, threat likelihood, and effect severity, to identify and rank security threats inside IoT ecosystems.

- Risk Calculation

The following formula is used to calculate the risk.

$$\text{Risk} = \text{Likelihood} \times \text{Impact}$$

where, likelihood and impact values are evaluated based on the table 2.

Table 2: Risk Prioritization Matrix

Impact →	Low	Medium	High
Likelihood ↓			
Low	Low Risk	Low Risk	Medium Risk
Medium	Low Risk	Medium Risk	High Risk
High	Medium Risk	High Risk	High Risk

- Vulnerability Score

To evaluate the seriousness of vulnerabilities, apply the Common Vulnerability Scoring System (CVSS). The CVSS score, which is 0 to 10, takes into account a number of variables. The CVSS is given by

$$\text{CVSS Score} = \text{Base Score} \times \text{Temporal Score} \times \text{Environmental Score}$$

where, Base Score- Indicates a vulnerability's inherent qualities that remain consistent over time and in various user contexts, Temporal Score- Indicates a vulnerability's attributes that could alter over time, Environmental Score- Modifies the baseline score in accordance with the vulnerability's possible effects in a particular setting.

- Threat Probability

Determine the likelihood of an attack using threat intelligence feeds and past data. The threat probability is calculated by using

$$\text{Threat Probability} = \text{Number of Incidents/Total Observation Period}$$

where, the total number of events that have been reported in relation to a certain threat type, Total observation period is the entire amount of time that events were tracked.

- Threat Score

It is used to calculate and prioritize threats based on various factors and the threat score is given by

$$\text{Threat Score} = (\text{Threat Severity} \times \text{Exposure Level} \times \text{Detection Difficulty})$$

where, Threat Severity the potential impact of the threat on a scale (e.g., 1 to 5), Exposure Level- Assess how exposed your IoT environment is to the threat (e.g., 1 for low exposure, 5 for high exposure), Detection Difficulty- Rate how difficult it is to detect the threat before it causes harm (e.g., 1 for easy detection, 5 for difficult detection).

4.2 Security by Design

For IoT devices, implementing security by design is essential to prevent potential threats and vulnerabilities early on. With this strategy, security is integrated throughout every stage of the development, deployment, and maintenance of Internet of Things devices [20]. Use secure coding practices, security architecture reviews, and threat modelling methodologies to detect and mitigate security vulnerabilities early in the development lifecycle. Here is how to improve IoT security by implementing security by design using some pertinent formulas:

- Security Requirement Identification

Determine security needs as early as possible in the design process. To evaluate possible threats and vulnerabilities, apply threat modelling. The security requirement is given by

$$\text{Security Requirements} = \text{Threats} - \text{Mitigations}$$

where, Threats is to enumerate every possible danger that threat modelling has revealed and mitigations is to controls or security mechanisms in place that can thwart these attacks.

- Layered Security Model

Establish a layered security architecture to defend against many attack vectors using several security layers and is given by

$$\text{Effective security} = \sum_{i=1}^{n} Layer_i$$

where, n is the total number of levels of security. Layer i the security efficacy of every layer, including data encryption, network security, and device security, is represented by layer i.

- Vulnerability Reduction

Design with frequent testing and secure coding techniques to reduce vulnerabilities and is given by

$$\text{Residual Vulnerability} = \text{Initial Vulnerability} - \text{Mitigation Measures}$$

Where, Initial Vulnerability is the degree of vulnerability prior to the implementation of security controls, mitigation measures are the implemented security controls and secure coding techniques.

4.3 Secure Authentication and Access Control

For IoT devices, implementing secure authentication and access management is essential to lower the risk of attacks [21]. By limiting illegal access and potential breaches, these protections guarantee that the only authorized people and devices can access resources. Here is how to put these security tactics into practice, along with some useful formulas to measure and enhance security measures are given. The robust authentication methods are used to confirm the identification of people and devices, such as biometric, token, or certificate-based authentication. Implement access controls that follow the least privilege principle, allowing only authorized people and devices to access sensitive data and essential system functions.

- Implementation of Secure Authentication

Put Multi-Factor Authentication (MFA) into practice to improve security over passwords alone. It combines your knowledge (password), possessions (token), and identity (biometric). Which is given by

$$\text{Authentication Security} = \text{Password Strength} + \text{MFA Level}$$

Where, the strength of a password is determined by its difficulty and unpredictable nature, MFA Level- How well extra authentication factors work. Strength of Password- Establish robust password restrictions to thwart brute-force or easy guessing attacks:

$$\text{Password Strength Score} = (\text{Length Factor} \times \text{Complexity Factor} \times \text{Uniqueness Factor})$$

Length Factor- Rises as the character count grows. The usage of capital, lowercase, digits, and special characters increases the complexity factor. Ensures that passwords are not reused called as the uniqueness factor.

- Access Control Mechanisms

Apply Role-Based Access Control (RBAC) to limit access according to the roles and responsibilities of users and is given by the formula

$$\text{Access Control Score} = \text{Number of Correctly Assigned Permissions} / \text{Total Permissions}$$

Where, Appropriately Assigned Permissions- Access rights that correspond with user roles, Total Permissions- All of the system's permissible uses.

- Least Privilege Principle

Make sure devices and users have the minimal amount of access required:

$$\text{Anomaly Detection Rate} = \text{Detected Anomalies} / \text{Total Access Events}$$

Where, Detected Anomalies- Number of patterns identified as unusual access, Total Access Events- The total number of logs of access events.

- Security Effectiveness Evaluation

It gives evaluation of authentication and access control measures, and given by the formula

Security Effectiveness=Prevented Unauthorized Access Events/Total Unauthorized Access Attempts.

where, Prevented Unauthorized Access Events is Number of trails blocked and Total Unauthorized Access Attempts is all the unauthorized access.

4.4 Secure Communication Protocols

It is imperative to implement secure communication protocols in order to safeguard IoT devices and the data they exchange [22]. This entails protecting the authenticity, confidentiality, and integrity of data while it is being transmitted. To stop replay, tampering, and eavesdropping attacks, implement secure key management procedures, message integrity checks, and protocol hardening techniques.

- Protocol Selection: Select protocols with robust security features supported. TLS/SSL- Encrypt data in transit to guarantee confidentiality and integrity by using Transport Layer Security (TLS) or Secure Sockets Layer (SSL). MQTT with TLS- To secure connections, use MQTT with TLS for lightweight IoT devices.
- CoAP using DTLS- To secure CoAP (Constrained Application Protocol) communications, use Datagram Transport Layer Security (DTLS).
- Encryption Strength: Apply strong encryption algorithms to secure data:

$$\text{Encryption Strength} = \text{Key Length} \times \text{Algorithm Security}$$

where, Key Length is the Length of the encryption key (e.g., 128-bit, 256-bit), Algorithm Security is the robustness of the encryption algorithm (e.g., AES, RSA).

- Data Integrity: data integrity is by using hashing algorithms.

$$\text{Integrity Score} = \text{Successful Integrity Checks} / \text{Total Integrity Checks}$$

where, Successful Integrity Checks are data integrity was verified successfully, Total Integrity Checks is the total number of integrity checks.

- Mutual Authentication: used to verify the mutual authentication of both parties.

$$\text{Authentication Confidence} = \text{Verified Authentication Events} / \text{Total Authentication}$$

where, Verified Authentication Events- Successful instances of authentication, Total Authentication Attempts- All successful authentication attempts made.

4.5 Continuous Monitoring and Threat Detection

To protect IoT environments from possible assaults, threat detection and continuous monitoring are essential elements [23]. They facilitate the early identification of irregularities and dangers and offer real-time insights into network activities. Here's how to put these techniques into practice, along with some formulas to evaluate and improve their efficacy.

- To identify and address unusual activity and security incidents, put intrusion detection systems (IDS), security information and event management (SIEM) platforms, and real-time monitoring solutions into place.
- Employ anomaly detection methods and machine learning algorithms to find patterns that point to possible security flaws or threats.
- Network Traffic Analysis: Identifies the unusual network traffic patterns.
- Baseline behaviour: standard traffic patterns for each IoT device.

- Anomaly Detection: Use statistical methods and machine learning algorithms to detect deviations.

$$\text{Anomaly Score} = (\text{Observed Traffic Pattern} - \text{Baseline Pattern}) / \text{Baseline Pattern Variance}$$

where, Observed Traffic is Current traffic, Baseline Pattern is Normal traffic pattern and Baseline Pattern Variance is normal traffic pattern.

- Log Monitoring: complete logs of IoT devices
- Centralized Logging: Use a centralized logging system to aggregate logs from various sources.
- Log Analysis: Apply log analysis tools to identify potential security incidents.

$$\text{Log Coverage} = \text{Analysed Logs} / \text{Total Collected}$$

Analysed Logs is the Logs that have been analysed and all the logs collected is total collected logs.

- Signature-Based Detection: malicious activities are identified using threat signature and calculated using

$$\text{Detection Rate} = \text{Detected Threats} / \text{Known Threat}$$

where, Detected Threats are the threats identified using known signatures and Known Threat Signatures is total signatures existing in the database.

- Incident Response: implemented to address the response time using identified threats and given by

$$\text{Response Efficiency} = \text{Incidents Resolved} / \text{Total Incidents Detected}$$

where, Incidents Resolved is number of security incidents and Total Incidents Detected is all the security incidents identified.

4.6 Incident Response and Containment

To mitigate IoT attacks, a strong incident response and containment strategy must be put into place [24]. This methodology guarantees that in the event of a security issue, it is promptly detected, confined, and addressed to mitigate harm. The following formulas can be used to assess and improve incident response and containment processes.

- Create and record communication protocols, processes, and incident response plans to help direct the handling of IoT security incidents.
- Regularly test the efficacy of incident response procedures and enhance team collaboration by conducting simulations and table top exercises.

- Preparation Index: It is to find the readiness of incident response plan and is given by:

$$\text{Preparation Index} = (\text{Trained Personnel} + \text{Updated Procedures}) / \text{Total Required Components}$$

where, Trained Personnel is the number of people trained in incident response. Updated Procedures Are Procedures updated in the past year. Total Required Components is total number of components needed.

- Detection Rate: to find the effectiveness of incident detection systems and is given by:

$$\text{Detection Rate} = \text{Incidents Detected} / \text{Total Incidents}$$

where, Incidents Detected is Number of security incidents recognized by the detection system, Total Incidents is All the security incidents detected.

- Recovery Time: time taken to restore the failure and given by

$$\text{Mean Time to Recovery (MTTR)} = \text{Total Recovery Time} / \text{Number of Incidents}$$

where, Total Recovery Time- time taken to recover all the incidents, Number of Incidents- Number of incidents during that period.

- Containment Effectiveness: strategies used to quickly contain incidents to reduce further damage and measured by

$$\text{Containment Effectiveness} = \text{Successfully Contained Incidents} / \text{Total Incidents}$$

where, Successfully Contained Incidents is number of successful incidents and total Incidents is all incidents.

- Containment Speed: incidents contained speed is measured using:

$$\text{Containment Speed} = \text{Total Containment Time} / \text{Number of Incidents}$$

where, Total Containment Time is total time taken to contain all incidents and Number of Incidents is number of incidents in the measurement period.

4.7 Security Awareness and Training

Enabling security awareness and training initiatives is essential for decreasing IoT assaults because they provide people the information and abilities they need to identify and address possible security risks [25]. Here are some tips for putting a successful program into action and some formulas to gauge its success. Offers training courses to stakeholders, administrators, and users of the Internet of Things by using online or offline;

- Needs Assessment

$$\text{Training Needs Index} = \text{Identified Needs} / \text{Total Needs Assessed}$$

where, Identified Needs is the number of specific security topics training identified and Total Needs Assessed is all the potential areas for training.

$$\text{Training Method Effectiveness} = \text{Engaged Participants} / \text{Total Participants}$$

where the Engaged Participants is number of participants engaged in the training and total participants is total number of participants in the training.

- Raising Security Awareness: Conduct awareness sessions to reinforce key security messages through newsletters, posters, and emails to keep security top-of-mind and recognize as well as report phishing attempts, using:

$$\text{Awareness Level} = \text{Correct Responses} / \text{Total Simulations Conducted}$$

where, awareness level is number of correct responses over total simulations conducted.

- Knowledge Retention: conduct tests and quizzes to check the knowledge, which is measured using

$$\text{Knowledge Retention Rate} = \text{Post-Training Test Scores} / \text{Initial Test Scores}$$

where, Post-Training Test Scores is the average scores of participants after completing the training and Initial Test Scores is average scores of participants before starting the training.

4.8 Collaboration and Information Sharing

Reducing IoT assaults requires the use of teamwork and information-sharing techniques [26]. By using these tactics, businesses can exchange threat knowledge, benefit from one another's experiences, and improve their security postures as a group. Here are several strategies for putting into practice efficient information-sharing and collaboration, along with some equations to gauge how successful they are.

- Encourage cooperation amongst all parties involved, such as producers of IoT devices, suppliers, service providers, trade associations, and governmental bodies.
- Exchange threat intelligence, best practices, and lessons discovered to strengthen IoT ecosystem resilience and collective protection against IoT threats.

- Threat Intelligence Sharing: some of the platforms like as Information Sharing and Analysis Centres (ISACs) are used between trusted partners to enhance the Information Sharing.

Sharing Frequency=Shared Intelligence Reports/Total Reporting Periods

where, Shared Intelligence Reports is the number of reports shared and total number of periods considered for sharing.

- Data Privacy and Security: The shared information should be protected and regulated for privacy using

Compliance Rate=Compliant Sharing Instances/Total Sharing Instances

where, Instances of data sharing is the Compliant Sharing Instances and all instances is the Total Sharing Instances that meet privacy and security requirements.

- Impact Assessment

The information-sharing and collaboration together impact the efforts on reducing IoT attacks and is given by:

Impact Score=Reduced Incidents Post-Collaboration/Incidents Pre-Collaboration

Where, Reduced Incidents Post-Collaboration is the number of IoT incidents after the collaboration efforts and Incidents Pre-Collaboration is the number of IoT incidents before collaboration efforts.

4.9 Regulatory Compliance

Reducing IoT attacks and making sure that systems and devices adhere to legal requirements and established security standards necessitate the implementation of regulatory compliance measures [27]. By enforcing baseline security procedures and promoting confidence among users and stakeholders, compliance helps decrease risks. Here are some tips on how to successfully execute regulatory compliance, along with some formulas to evaluate and improve compliance efforts:

- Verify adherence to industry principles, standards, and applicable laws pertaining to data protection, privacy, and IoT security.
- Keep abreast of changing regulatory requirements so that security policies and procedures can be updated appropriately.

- Compliance Framework: Create a framework for compliance to guide implementation. Rules and guidelines are used to make sure your policies comply with all applicable regulations.

Compliance Readiness Score=Implemented Controls/Required Controls

where, Implemented Controls is the number of controls implemented and the Required Controls is the total number of controls regulated.

- Compliance Audits: Perform routine audits to assess adherence to regulations. Internal Audits: To find compliance weaknesses, conduct internal audits on a regular basis. External Audits: Hire outside auditors to provide an objective evaluation.

Audit Success Rate=Compliant Audit Findings/Total Audit Findings

where, Compliant Audit Findings is the number of findings meeting compliance requirements and the Total Audit Findings is the all findings of compliance audits.

4.10 Continuous Improvement

The ongoing mitigation of IoT attacks necessitates the application of techniques and approaches that gradually increase security [28]. This method focuses on finding weaknesses, examining information, putting fixes in place, and evaluating their efficacy. Here are some principles to help you organize an ongoing process of improvement for IoT security:

- Assess risks on a regular basis to find weak points and possible points of attack in IoT networks and devices.
- Examine and upgrade security measures on a regular basis in response to organizational requirements, improvements in technology, and changes in the threat landscape.
- Perform lessons learned and post-incident evaluations to pinpoint problem areas and boost the efficiency of security procedures and controls.

5. Block Chain Technology

By offering secure identity management, encrypted communication, distributed security upgrades, tamper-resistant data storage, auditability, and immutable event logging, block chain can improve IoT security [29]. For it to be used in IoT contexts effectively, it should be utilized in conjunction with other security measures and take scalability considerations into consideration which is shown in the figure 4.

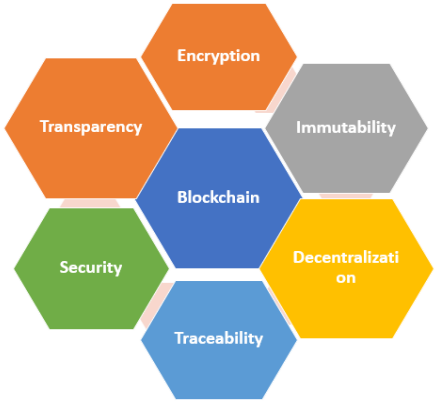

Figure 4: Block Chain Technology

By addressing some of the common weaknesses that these systems experience, block chain technology can greatly improve the security of Internet of Things systems through its features which are discussed below.

- **Decentralization:** The decentralized nature of block chain precludes the possibility of a single point of failure in its network. This increases the difficulty of an attacker using a single point of entry to compromise the entire network. Which is calculated as shown over number of nodes used in communication.

$$\text{Decentralization Index} = \text{Number of Nodes} / \text{Total Nodes Required}$$

- **Data Integrity:** Block chain uses cryptographic hashing to secure data blocks, which guarantees data integrity. It is computationally impracticable to try to update data as doing so would

necessitate changing every block that came after it. Data integrity can be found through the number of records which is given below.

Data Integrity Score=Records Verified/Total Records

- **Authentication:** Strong authentication methods are possible with block chain technology. By enabling mutual identity verification, devices on a block chain can lower the possibility of impersonation and illegal access. The authentication accuracy is calculated over the number of successful attempts.

Authentication Accuracy=Successful Authentications/Total Authentication Attempts

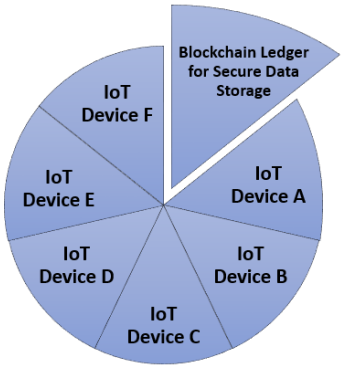

Figure 5: Immutable Ledger for secure data storage using BCT

- **Immutable Ledger:** Information entered onto a block chain cannot be changed later without changing all of the blocks that came before it. Data integrity is maintained by its immutability as shown in the figure 5, where data on any IoT device cannot be modified without the concern about other IoT devices involved in the blockchain network and it is maintained in an immutable shared ledger.

- **Transparency and Traceability:** Since all blockchain transactions are clearly recorded, it is simpler to track down the source and history of data. This openness can aid in spotting harmful activity.

- **Tamper Detection:** Use transparency of blockchain technology to identify any tampering or unauthorized changes is given by number of tampering attempts made to total attempts.

Tamper Detection Rate=Tampering Attempts Detected/Total Tampering Attempts

- **Incident Response:** blockchain can be used to find the incident response efforts and logs. Incident response is found by using resolved incidents and the total incidents as given below:

Incident Response Efficiency=Resolved Incidents/Total Incident Reports

- **Smart Contracts**: Using blockchain smart contracts to improve IoT security means taking advantage of the decentralized, immutable, and automated features of blockchain technology. By guaranteeing that exchanges of data and transactions are safe, open, and impenetrable, smart contracts can contribute to the security of Internet of Things systems. Self-executing contracts with terms encoded in code are known as smart contracts. Based on preset criteria, they can automate procedures like data sharing, device updates, and transaction validation. Smart contracts provide a secure means

of communication between IoT devices, guaranteeing that only approved operations are carried out. By enforcing Access Control Lists (ACLs), smart contracts can restrict access to particular resources or data to only authorized devices

By utilizing block chain's decentralized and immutable characteristics, security can be improved in Internet of Things situations. Blockchain offers an IoT device's secure means of managing data integrity, authentication, and trust. Organizations may greatly improve the security of their Internet of Things ecosystems by putting blockchain smart contracts into place. This will make sure that data and device interactions are visible, safe from intrusions, and secure.

6. Conclusion

The security issues that arise from Internet of Things deployments can be addressed in a variety of ways by comprehending and mitigating IoT attacks. This paper highlighted important insights into the challenges of securing networked IoT ecosystems by looking at common attacks, motives, impacts, and mitigation techniques. Organizations can take proactive steps to improve the security posture and resilience of their IoT deployments by implementing the suggested approaches. Organizations can reduce the risks associated with IoT attacks and protect sensitive data, critical infrastructure, and user privacy by combining technical controls, regulatory measures, industry standards, security awareness campaigns, and blockchain technology. Blockchain is a distributed, immutable ledger of data, one cannot easily access and tamper the devices or data on it. Hence the attacks on IoT devices can be reduced by implementing a secure blockchain system for IoT applications and also various other methods discussed for the better security.

References

[1] Hamid Al-Hamadi, Ing-Ray Chen, Ding-Chau Wang, and Meshal Almashan, "Attack and Defence Strategies for Intrusion Detection in Autonomous Distributed IoT Systems", at IEEE access in 2020.

[2] Juntao Chen, "Enhancing Cyber-Physical Resiliency of Power Grids under IoT-Enabled Dynamic Botnet Attacks", at 2023 IEEE conference on Power & Energy Society General Meeting (PESGM) in 2023.

[3] Fatiha Benabderrahmane. Samir Selmane, And Nardjes Bouchemal, Enhancing Security in Healthcare IoT Systems: Mitigating Threats and Protecting Patient Data", 2023 IEEE 11th International Conference on Systems and Control, Sousse, Tunisia, December 18-20, 2023.

[4] Emilie Bout, Valeria Loscri, and Antoine Gallais, "HARPAGON: An Energy Management Framework for Attacks in IoT Networks", IEEE Internet of Things Journal, VOL. 9, NO. 20, 15 Oct., 2022.

[5] Yuhan Zhao, Juntao Chen, and Quanyan Zhu, "Integrated Cyber-Physical Resiliency for Power Grids Under IoT-Enabled Dynamic Botnet Attacks", at IEEE Transactions on Control Systems Technology, in 2024.

[6] Sadia Showkat, Shaima Qureshi, "Securing the Internet of things using Blockchain" at IEEE 10th International Conference on Cloud Computing, Data Science and Engineering (Confluence) in 2020.

[7] Mala B A, Dr. M V Sudhamani, Ramesh Shiddappa Chakrasali, "Enhancement of Security for IoT based Applications with a Block Chain Technology - A Review"at 2nd IEEE International Conference on Data, Decisions, and Systems Conference '23, 1-2, December, NITK, Surathkal, India, 2023.

[8] Li, Z., Yuan, K., Duan, H., Chen, J., and Wu, J. "The Impact of DDoS Attacks on Organizations and the Mitigation Strategies" by IEEE Transactions on Dependable and Secure Computing, 2020.

[9] Al-Hammadi, Y., Mohamed, A., and Al-Wabil, A "The Future of IoT Botnets: A Comprehensive Study on Emerging Threats, Detection, and Mitigation" by IEEE Internet of Things Journal, 2021.

[10] Shwetarani, Nawab Muhammad Faseeh Qureshi, Dong Ryeol Shin, "A Comprehensive Study of Botnets on Internet of Things and Mobile Devices: Detection and Mitigation Techniques" by Journal of Theoretical and Applied Information Technology during 2020.

[11] Yash Shah, Shamik Sengupta, "A survey on Classification of Cyber-attacks on IoT and IIoT devices", by IEEE, 2020.
[12] Ikra Afzal Chesti, Mamoona Humayun, Najm Us Sama, NZ Jhanjhi, "Evolution, Mitigation, and Prevention of Ransomware", by IEEE, 2020.
[13] Mamoona Humayun, NZ Jhanjhi, Ahmed Alsayat, Vasaki Ponnusamy, "Internet of things and ransomware: Evolution, mitigation and prevention", Egyptian Informatics Journal 2021.
[14] Farooq, M., & Mustafa, M, "Mitigation Techniques for Man-in-the-Middle Attacks in IoT Networks" by Sensors, MDPI, 2020.
[15] A. R. Johnson and L. W. O'Neil, "Integrating Physical Security and Cybersecurity: An Organizational Approach" by International Journal of Information Security, 2021.
[16] S. R. Lee, M. J. Lee, and K. K. L, "Understanding and Preventing Supply Chain Attacks: Strategies and Best Practices" by in ACM Computing Surveys, 2021.
[17] S. L. Davis, A. H. Turner, and M. R. Patel, "Zero-Day Exploits and Zero Trust: A Comprehensive Approach to Modern Cyber Threats" by Journal of Cyber Security and Privacy, 2022.
[18] S. G. Bhattacharya and K. H. Richards, "Mitigating Social Engineering Attacks: Strategies and Best Practices" by Journal of Cyber Security and Privacy, 2021.
[19] J. Wan, S. Tang, H. Yan, D. Li, and J. Wang, "Threat Intelligence and Risk Assessment for IoT: A Survey" by IEEE Internet of Things Journal, 2018.
[20] S. Ravi, T. Shree, and J. Baras, "Security by Design for IoT Devices: A Comprehensive Survey" by ACM Computing Surveys, 2020.
[21] X. Zheng, J. Hu, Z. Cai, H. N. Dai, and V. C. M. Leung, "Secure Authentication and Access Control for IoT Networks: A Survey" by IEEE Communications Surveys & Tutorials, 2019.
[22] T. A. Zungeru, P. M. Ang, S. K. Seng, and K. Z. Goh, "Secure Communication Protocols for the Internet of Things: A Survey" by IEEE Communications Surveys & Tutorials, 2018.
[23] A. Sarker, M. F. Bari, R. Islam, S. M. S. Mahmud, "Continuous Monitoring and Threat Detection in IoT Environments: A Machine Learning Approach" by IEEE Access, 2021.
[24] K. K. Kaur, J. Joshi, and S. H. Ahmed, "Incident Response and Containment Strategies for IoT Attacks" by Journal of Cyber Security and Mobility, 2020.
[25] E. Kumar, N. Subramanian, and P. Abdul, "Security Awareness and Training for IoT: Enhancing User Knowledge and Engagement" by Journal of Information Security and Applications, Elsevier, 2019.
[26] S. Sen, D. Gruber, A. Flores, and D. L. Moore, "Collaboration and Information Sharing for Enhancing IoT Security: A Framework" by IEEE Transactions on Information Forensics and Security, 2020.
[27] R. Chowdhury, M. F. Bari, and K. Salah, "Regulatory Compliance for IoT Security: An Analysis of Existing Frameworks and Future Directions" by Computer Networks, Elsevier, 2018.
[28] A. Mitra, S. Yadav, and M. Das, "Continuous Improvement in IoT Security: A Proactive Approach" by ACM Transactions on Internet Technology, 2021.
[29] R. A. Saad, M. M. Hassan, and A. A. Ali, "Leveraging Blockchain Technology to Enhance Security in IoT Systems" by Journal of Computer Security, 2021.