JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 06 Issue 02
2024

Review Article
https://doi.org/10.56979/602/2024

A Layered Analysis on Navigating the Landscape of IoT Attacks: A Survey

Rania Naveed[1*], Irshad Ahmad Sumra[1], and Ayesha Munir[1]

[1]Department of Information Technology, Lahore Garrison University, Lahore, 54000, Pakistan.
Corresponding Author: Rania Naveed. Email: ranianaveed1509@gmail.com

Received: December 18, 2023 **Accepted:** February 29, 2024 **Published:** March 01, 2024

Abstract: The Internet of Things (IoT) has become a focal point in contemporary research, capturing the imagination of researchers as they explore its transformative potential for the future. Despite the notable progress and development in the field of IoT, a host of vulnerabilities has surfaced, challenging the overall security of this technology. Interestingly, various attacks on IoT have been conceived even before its widespread commercial adoption. This study takes a deep dive into the realm of IoT attacks, categorizing them based on the layers of the IoT architecture. It aims to provide a comprehensive understanding of these attacks without delving into specific countermeasures. The given research study presents a state-of-the-art survey, shedding light on the diverse spectrum of attacks within the IoT framework, and contributing valuable insights to the ongoing discourse on IoT security.

Keywords: Internet of Things (IoT); Denial of Service (DoS); Man in the Middle (MITM); Radio Frequency Identification (RFID), Path based Denial of Service (PDoS), Domain Name Service (DNS), Structured Query Language (SQL), Message Queuing Telemetry Transport (MQTT).

1. Introduction

Today, billions of devices talk to each other through something called the Internet of Things (IoT). The term was made up by Kevin Ashton in 1999 while he was working on making supply chains better at Proctor & Gamble [1]. Now, two decades later, the Internet of Things includes many different uses in areas like healthcare, farming, utilities, and transportation. Even though the meaning of it has changed over time, its main goal is still the same as when it was first created: to make things work well and give people information faster than systems that need humans to do everything [2]. Consequently, the proliferation of connected devices continues to escalate. As per Strategy Analytics, the number of connected things is expected to surpass 38 billion by the close of 2025 and reach 50 billion by 2030 [3].

Even though there's a fast increase in the number of connected devices, leading to the development of new and creative business models, security and privacy often don't get the attention they need [4]. This lack of focus gives rise to various security and privacy problems related to the IoT [5], putting its acceptance at risk [6]. Linking smart devices to the internet without strong security measures can open the door to more potential attacks and give adversaries more ways to get in. This situation poses a threat to the overall security of the system [7].

In order to effectively understand and mitigate these threats, it is crucial to classify cyberattacks within the IoT framework based on the five layers: business, middleware, application, network, and perception. This classification provides a comprehensive approach to analyzing and addressing vulnerabilities across the IoT ecosystem.

1.1 Challenges and Security Concerns in IoT

The realm of the IoT encounters various challenges and security issues that demand attention for effective operation and protection. Following are some of them.

1.1.1 Insecure Network Services

Given the heavy reliance of IoT systems on network communications, securing these networks is

essential. Failure to do so can expose network services to compromise through attacks like buffer overflows, fuzzing, distributed denial-of-service (DDoS), and other forms of intrusion [8].

1.1.2 Bandwidth and Power Consumption

IoT devices are designed to be compact, with limited computing power and memory. This restricts the application of advanced cryptographic algorithms due to their high computing and memory demands. Additionally, IoT systems often involve numerous connected sensors, leading to potential high bandwidth usage. To address this, security measures should be implemented with minimal impact on the IoT system [8, 9].

1.1.3 Insufficient Authentication and Authorization Mechanism

Many IoT devices face issues related to weak and default passwords, insecure credentials, and a lack of access control. This vulnerability can be exploited by attackers to compromise privacy and data integrity. Therefore, implementing robust authentication and authorization mechanisms is crucial [8, 10].

1.1.4 Insecure Web Interface

A significant number of IoT devices have web interfaces that lack the requirement for strong passwords. Some of these interfaces also fail to lock out users after multiple unsuccessful login attempts. Consequently, these interfaces become susceptible to various attacks, such as brute force credentials, injections, and scripting attacks. Strengthening web interface security is imperative [8, 11].

1.2 Need for Security

Securing the IoT at its various layers is crucial for mitigating risks and vulnerabilities. Beginning with the Perception Layer, protection against physical attacks is vital to prevent unauthorized access and manipulation of sensor data. In the Network Layer, ensuring secure data transfer maintains the integrity and confidentiality of exchanged information. The Middleware Layer faces threats like SQL injection, necessitating robust security to prevent unauthorized access and data manipulation. Security in the Application Layer defends against phishing and denial-of-service attacks, preserving user confidentiality. At the Business Layer, comprehensive security guards against zero-day exploits, preventing unauthorized control and data breaches. In summary, securing IoT layers is essential for preserving data integrity, ensuring seamless communication, and protecting user privacy, upholding the trustworthiness of the system. This approach aligns with the fundamental principles of Confidentiality, Integrity, and Availability (CIA), reinforcing the overall resilience of IoT ecosystems.

2. IoT 5 Layer Architecture

Due to the non-standardization of IoT, there are various architectures [12] such as three layer (perception, network and application layer), four layer (perception, network, and middleware and application layer). But in this study, five-layered architectures (perception, network, middleware, application and business layer) is discussed.

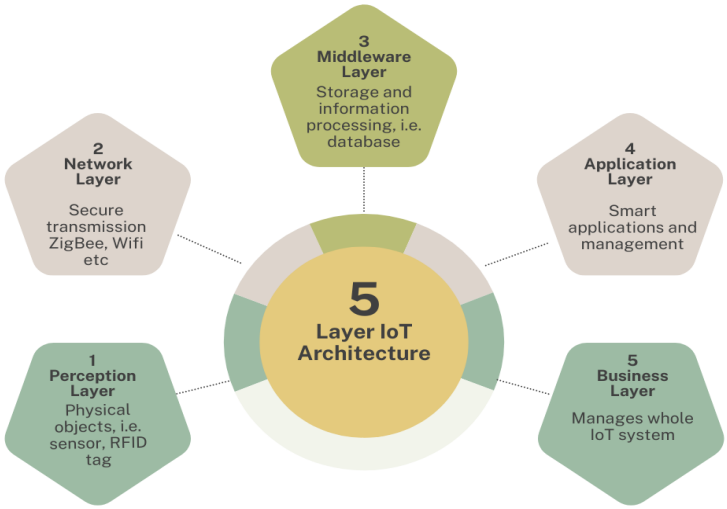

Figure 1. IoT Five Layer Architecture

Here each layer as mentioned in Figure. 1 is described in detail.

2.1 Perception Layer

The perception layer stands as the initial tier in IoT architecture, linking to the real world to sense and gather data from the surroundings. This layer incorporates sensors and actuators, which are devices that measure values like temperature, pH, light, gas, and more, as well as detect functionalities such as location and motion [13].

2.2 Network Layer

The network layer serves as a communication channel, facilitating the transfer of data gathered in the sensing layer to other connected devices. In IoT devices, various communication technologies such as Wi-Fi, Bluetooth, Zigbee, Z-Wave, LoRa, and cellular networks [14] are employed in the network layer. This enables the smooth flow of data between different devices within the same network [15].

2.3 Middleware Layer

The processing layer, also called the middleware layer, is built on the network layer. It provides an Application Programming Interface (API) for creating applications and offers a range of services accessible within this layer [16]. This layer takes charge of managing, analyzing, processing, and storing the data it receives. It has the capability to make decisions based on the processed data without requiring human intervention. Additionally, this layer leverages established solutions such as cloud computing, big data, and databases [13].

2.4 Application Layer

The application layer can provide the specific service requested by the user [13]. The application layer differs significantly across various IoT applications and devices. Given the wide array of IoT devices from different manufacturers, there is no established standard for the appearance of an application layer. This layer is responsible for linking end users to API endpoints using a user interface. Additionally, it manages tasks such as authentication, login, data viewing, and various others [17].

2.5 Business Layer

This layer is responsible for overseeing the entire IoT system [19]. Its function involves regulating applications, business operations, and profit models. Additionally, it plays a crucial role in managing users' privacy within the system [13]. The business layer is where decisions are made based on data and solutions from the application layer. At this level, patterns decoded from the application layer are used to gain further business insights, predict future trends, and make operational decisions that improve productivity, security, cost-effectiveness, customer satisfaction, and other critical business factors. This layer encompasses business process management, business analytics, and business rules. It is responsible for handling business logic and establishing procedures to ensure that all business objectives of the IoT system are met [18].

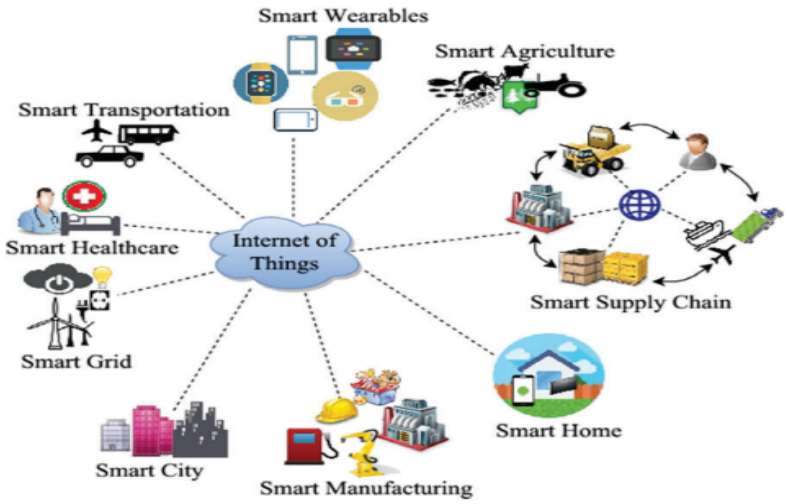

Figure 2. IoT Ecosystem

3. Threats and Attacks on IoT 5 Layer Architecture

3.1 Physical Layer Attack

Physical attacks are employed to discover new vulnerabilities in IoT systems, specifically targeting the hardware devices. These attacks encompass actions like reverse engineering, radio frequency interference, tampering, and social engineering.

3.1.1 Reverse Engineering

In this method, an attacker dismembers a device to uncover vulnerabilities. After identifying both known and unknown vulnerabilities, the attacker can exploit them on other devices within a connected network [17].

3.1.2 Tampering

Tampering occurs when an IoT device is physically altered by an attacker, allowing them to access login credentials, encryption keys, and other sensitive information [17].

3.1.3 Radio Frequency Interference

The attacker executes a Denial of Service attack by transmitting disruptive signals over radio frequency signals, particularly affecting the communication of RFID devices [19].

3.1.4 Social Engineering

Social Engineering involves the attacker manipulating users within an IoT system to obtain private information or coerce them into taking specific actions that align with the attacker's objectives [20].

3.1.5 Malicious Node Injection

The adversary can physically introduce a new malicious node between two or more nodes in the IoT system. This allows them to control all data flow to and from the nodes, manipulating their operation [20].

3.1.6 Sleep Deprivation Attack

Many sensor nodes in the IoT system rely on replaceable batteries and are programmed to follow sleep routines for extended battery life. A Sleep Deprivation Attack keeps the nodes awake, leading to increased power consumption and eventual shutdown [20].

3.1.7 Node Tampering

The attacker can harm a sensor node by physically replacing the entire node or part of its hardware. They may also electronically interrogate the nodes to gain access and modify sensitive information, such as shared cryptographic keys or routing tables. This action could impact the operation of higher communication layers [21].

3.2 Network Layer

These assaults pose a significant danger to the security and privacy of interconnected devices and systems. They have the potential to undermine the functionality, integrity, availability, and confidentiality of the data and services offered by IoT devices [22]. Common network attacks in IoT are following.

3.2.1 Traffic Analysis Attacks

The attacker intercepts and examines messages to gather network information [23].

3.2.2 RFID Spoofing:

Adversaries create false RFID signals to capture information transmitted from RFID tags. Spoofing attacks provide misleading information that the system mistakenly accepts [24].

3.2.3 Sinkhole Attack

The attacker diverts all traffic from Wireless Sensor Network (WSN) nodes, creating a metaphorical sinkhole. This attack compromises data confidentiality and denies service to the network by dropping packets instead of forwarding them to the intended destination [25].

3.2.4 Man-In-the-Middle Attack (MITM)

The attacker intervenes between two sensor nodes over the network, accessing restricted data and violating privacy by monitoring, eavesdropping, and controlling communication. Unlike Malicious Node Injection, this attack doesn't necessarily require physical presence but relies on the network communication protocols of an IoT system [26].

3.2.5 RFID Cloning

In this attack, the adversary copies data from one RFID tag to another without replicating the original ID. This allows the attacker to insert incorrect data or control the information passing through the cloned node [20].

3.2.6 RFID Unauthorized Access

Without proper authentication in RFID systems, adversaries can observe, alter, or remove information on nodes [20].

3.2.7 Denial of Service DoS

An attacker floods an IoT network with more data than it can handle, leading to a successful Denial of Service attack [27].

3.3 Routing Information Attacks

These direct attacks involve the adversary complicating the network by spoofing, altering, or replaying routing information. This can create routing loops, allow or drop traffic, send false error messages, shorten or extend source routes, or even partition the network [28].

3.4 Sybil Attack

A malicious node (Sybil Node) claims the identities of multiple nodes, impersonating them. This leads to neighboring Wireless Sensor Network (WSN) nodes accepting false information, potentially impacting scenarios like a WSN voting system or the selection of a Sybil node as part of a routing path [29].

3.5 Middleware Layer

Various attacks and security threats are linked to this layer due to the accumulation of a large amount of data and the utilization of cloud computing [30]. The primary objective of these attacks is to compromise users' privacy by potentially destroying or unauthorized access to cloud data [33].

3.6 SQL Injection Attack

Middleware is susceptible to SQL injection (SQLi) attacks, where an attacker inserts a malicious SQL query into a program. This enables unauthorized access to private user information and allows manipulation of database entries [30]. SQLi is identified as a significant threat to web security according to the Open Web Application Security Project (OWASP) top 10 in 2018.

3.7 Flooding Attack in Cloud

Cloud-based denial of service attacks adopt a similar method, impacting Quality of Service (QoS) by overwhelming cloud resources with a continuous stream of queries. These attacks can significantly affect cloud systems by straining the cloud servers [31].

3.8 Man-in-the-Middle Attack (MITM)

In the context of middleware using MQTT protocol, subscribers and clients communicate through an MQTT broker, which acts as a proxy. This allows messages to be sent to multiple recipients without disclosing their destinations. If an attacker gains control of the broker, they can take over communication without the clients being aware [31].

3.9 Signature Wrapping Attack

Middleware's web services employ XML signatures, making them vulnerable to a signature wrapping attack. In this attack, an adversary exploits weaknesses in the Simple Object Access Protocol (SOAP) to compromise the signature scheme. This enables them to execute operations or modify intercepted messages [31].

3.10 Application Layer

There are various attacks associated with this layer.

3.11 Phishing Attacks

In a phishing attack, the attacker deceives a user into revealing confidential information by impersonating authentication credentials. This is often done through infected emails or fraudulent websites [34].

3.12 Malicious Software (Viruses, Worms, Trojan Horse, Spyware, and Adware)

Adversaries can compromise the system by introducing harmful software, leading to various consequences such as stealing information, manipulating data, or even initiating a denial of service [35].

3.13 Malicious Scripts

Given the IoT network's connection to the internet, an attacker might trick the gateway controller into running executable active-x scripts. This could result in a complete system shutdown or unauthorized access leading to data theft [35].

3.14 Denial of Service (DoS and DDoS) Attacks

Attackers can launch DoS or DDoS attacks on the IoT network through the application layer, impacting all users. This type of attack can block legitimate users from accessing the application layer, providing the attacker with full access to databases and sensitive data [36].

3.15 Spoofing Attack

An attacker might pretend to be a node and carry out a spoofing attack, a particularly risky type of attack due to its method. By using a portable reader, the attacker can record a transmission. When the attacker pretends to be the node, the retransmission may seem to come from a legitimate node. This kind of attack can occur across all three layers of IoT. Spoofing attacks, involving the impersonation of nodes, fall into the category of authentication attacks and also breach privacy principles [37].

3.16 Path based DoS attack

A Path-Based Denial of Service (PDoS) attack, also known as a PDoS attack, occurs when data packets are flooded through multi-hop end-to-end communication paths [38].

3.17 DNS Spoofing or Poisoning Attacks

DNS, or Domain Name System, translates domain names into IP addresses. In a DNS Spoofing attack, an attacker gains access to a DNS server and alters the IP address of a specific domain or website, redirecting users who access it [39]. DNS Poisoning happens when the attacker sends a fake DNS server response to corrupt the cached data in the DNS server.

3.18 Business Layer

Following are the business layer attacks.

3.19 Zero-Day Exploits

Zero-day exploits refer to vulnerabilities existing in the latest version of software that hackers exploit, and the software manufacturers are yet to discover. These attacks are highly dangerous as they remain undetected, making them challenging to address. Once identified, patches are released to rectify these vulnerabilities, and they are no longer termed Zero-day exploits [40].

4. Comparison of attack based on IoT layers

Table 1. Comparison of Attacks.

Attack	Classification Parameters					
	IoT Layer	**Attack Type**	**Security Goals**	**Damage Level**	**Attacker Location**	**Detection Chances**
DoS/DDoS Attack	Network, Application	Active	Availability	High	External	Moderate to High
MITM Attack	Network, Middleware	Active	Integrity	Moderate	External	Moderate
DNS Poisoning	Application	Passive	Integrity	Moderate	External	Low to Moderate
Spoofing	Network, Application	Active	Integrity, Confidentiality	Low	External	Low to Moderate
Phishing	Application	Active	Confidentiality	Low	External	Moderate
Injection Attack	Physical, Middlew	Active	Integrity,	Moderate	Internal	Moderate to High

	are, Application		Confidentiality			
Malicious Software	Physical, Network, Application	Active	Integrity	Moderate	External, Internal	Moderate to High
Zero Day Exploit	Business	Active	Integrity	High	External	Low to Moderate
Social Engineering	Physical	Active	Confidentiality	Low	External	Low to Moderate
Node Tempering	Physical	Active	Confidentiality	Low	Internal	Low to Moderate

5. Conclusion

In summary, the Internet of Things (IoT) architecture, structured into Perception, Network, Middleware, Application, and Business layers, underpins diverse applications across sectors. Threats and attacks across these layers present a multifaceted landscape. Physical Layer Attacks target hardware vulnerabilities, while Network Layer Attacks disrupt communication. Middleware Layer faces challenges like SQL injection, and Application Layer deals with phishing and injection attacks. The Business Layer confronts the risk of zero-day exploits. Detection chances vary based on attack types, emphasizing the need for a comprehensive security approach. As the IoT landscape evolves, addressing these challenges is pivotal for ensuring the security and resilience of connected devices.

References

1. Ashton, Kevin. "That 'internet of things' thing." RFID journal 22.7 (2009): 97-114.
2. Kenton, Will. "The Internet of Things (IoT): What You Need to Know." Investopedia, Investopedia, 23 Oct. 2020, www.investopedia.com/terms/i/internet-things.asp. Accessed November 1st, 2020.
3. "Strategy analytics: internet of things now numbers 22 billion devices but where is the revenue? strategy analytics online newsroom." https://news.strategyanalytics.com/press-release /iot-ecosystem/strategy-analytics-internet-things-now-numbe rs-22-billion-devices-where (accessed Feb. 23, 2020).
4. Axelrod CW. Enforcing security, safety and privacy for the Internet of Things. IEEE Long Island Conference on Systems, Applications and Technology (LISAT), May; 2015:1-6.
5. Skarmeta AF, HernaÌAndez-Ramos JL, Moreno MV. ¸ A decentralized approach for security and privacy challenges in the internet of things. IEEE World Forum on Internet of Things (WF-IoT), March; 2014:67-72.
6. Anderson M. Vulnerable "Smart" Devices Make an Internet of Insecure Things: IEEE Spectrum; 2004. https://spectrum.ieee.org/riskfactor/computing/networks/ vulnerable-smart-devices-make-an-internet-of-insecure-things. Accessed December 2, 2015.
7. Scott D, Ketel M. Internet of things: a useful innovation or security nightmare? Southeastcon 2016, March; 2016:1-6
8. Khader, R., & Eleyan, D. (2021). Survey of dos/ddos attacks in iot. Sustainable Engineering and Innovation, 3(1), 23-28.
9. S. Deep, X. Zheng, A. Jolfaei, D. Yu, P. Ostovari, and A. K. Bashir, "A survey of security and privacy issues in the Internet of Things from the layered context," arXiv, no. March, 2019.
10. R. Vishwakarma and A. K. Jain, "A survey of DDoS attacking techniques and defence mechanisms in the IoT network," Telecommun. Syst., vol. 73, no. 1, pp. 3–25, 2020, doi: 10.1007/s11235-019-00599- z.
11. K. Dineva and T. Atanasova, "Security in IoT systems," Int. Multidiscip. Sci. GeoConference Surv. Geol. Min. Ecol. Manag. SGEM, vol. 19, no. 2.1, pp. 569–577, 2019, doi: 10.5593/sgem2019/2.1/s07.075
12. A. Irshad, M. Usman, S. A. Chaudhry, A. K. Bashir, A. Jolfaei, and G. Srivastava, "Fuzzy-in-the-Loop-Driven low-cost and secure biometric user access to server," IEEE Transactions on Reliability, vol. 70, no. 3, 2020.
13. Azrour, M., Mabrouki, J., Guezzaz, A., & Kanwal, A. (2021). Internet of things security: challenges and key issues. Security and Communication Networks, 2021, 1-11.
14. H. F. Atlam, R. J. Walters, and G. B. Wills, "Internet of things: state-of-the-art, challenges, applications, and open issues," International Journal of Intelligent Computing Research, vol. 9, no. 3, pp. 928–938, 2018.
15. Sikder, A. K., Petracca, G., Aksu, H., Jaeger, T., & Uluagac, A. S. (2018). A survey on sensor-based threats to internet-of-things (iot) devices and applications. arXiv preprint arXiv:1802.02041.
16. Bel, H. F., & Sabeen, S. (2022). A survey on IoT security: attacks, challenges and countermeasures. Webology, 19(1), 3741-3763.
17. Liang, X., & Kim, Y. (2021, January). A survey on security attacks and solutions in the IoT network. In 2021 IEEE 11th annual computing and communication workshop and conference (CCWC) (pp. 0853-0859). IEEE.
18. Sasi, T., Lashkari, A. H., Lu, R., Xiong, P., & Iqbal, S. (2023). A Comprehensive Survey on IoT Attacks: Taxonomy, Detection Mechanisms and Challenges. Journal of Information and Intelligence.
19. M. Burhan, R. Rehman, B. Khan, and B.-S. Kim, "IoT elements, layered architectures and security issues: a comprehensive survey," Sensors, vol. 18, no. 9, 2796 pages, 2018.
20. Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015, July). Internet of Things: Security vulnerabilities and challenges. In 2015 IEEE symposium on computers and communication (ISCC) (pp. 180-187). IEEE.
21. A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks." Communications of the ACM 47, no. 6 (2004): 53-57.
22. Prakash, R., Jyoti, N., & Manjunatha, S. (2024). A survey of security challenges, attacks in IoT. In E3S Web of Conferences (Vol. 491, p. 04018). EDP Sciences.
23. S.N Uke, A.R Mahajan, R.C Thool "UML Modeling of Physical and Data Link Layer Security Attacks in WSN", International Journal of Computer Applications, Volume 70– No.11, May 2013.
24. Li, Hong, Y. Chen, and Z. He. "The Survey of RFID Attacks and Defenses." 8th International Conference on IEEE Wireless Communications, Networking and Mobile Computing (WiCOM), 2012.
25. V. Soni, P. Modi, and V. Chaudhri, "Detecting Sinkhole attack in wireless sensor network." International Journal of Application or Innovation in Engineering & Management 2, no. 2 (2013).
26. R. P. Padhy, M. R. Patra, and S. C. Satapathy, "Cloud Computing: Security Issues and Research Challenges." International Journal of Computer Science and Information Technology & Security (IJCSITS) 1, no. 2 (2011): 136-146.
27. Deogirikar, J., & Vidhate, A. (2017, February). Security attacks in IoT: A survey. In 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 32-37). IEEE.
28. D. Wu, and G. Hu, "Research and improve on secure routing protocols in wireless sensor networks." In Circuits and Systems for Communications, 2008. ICCSC 2008. 4th IEEE International Conference on, pp. 853-856. IEEE, 2008.
29. J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses." In Proceedings of the 3rd international symposium on Information processing in sensor networks, pp. 259-268. ACM, 2004.
30. M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for internet of things: a survey," IEEE Internet of

1ings Journal, vol. 3, no. 1, pp. 70–95, Feb. 2016.
31. Bharati, S., & Podder, P. (2022). Machine and deep learning for iot security and privacy: applications, challenges, and future directions. Security and Communication Networks, 2022, 1-41.
32. J. Y. Khan, "Introduction to IoT," Internet of Things (IoT), no. January 2019, pp. 1–24, 2019, doi: 10.1201/9780429399084-1.
33. K. Sonar and H. Upadhyay, "A survey on ddos in Internet of Things," Int. J. Eng. Res. Dev., vol. 10, no. 11, pp. 58–63, 2014.
34. T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social phishing." Communications of the ACM 50, no. 10 (2007): 94-100.
35. H. Tobias, et al. "Security Challenges in the IP-based Internet of Things." Wireless Personal Communications 61, no. 3 (2011): 527-542.
36. C. M, Medaglia, and A. Serbanati. "An overview of privacy and security issues in the internet of things." In The Internet of Things, pp. 389-395. Springer New York, 2010.
37. P. Schaffer, K. Farkas, Á. Horváth, T. Holczer, and L. Buttyán, ''Secure and reliable clustering in wireless sensor networks: A critical survey,'' Comput. Netw., vol. 56, no. 11, pp. 2726–2741, Jul. 2012, doi: 10.1016/j.comnet.2012.03.021.
38. S. Raza, S. Duquennoy, J. Höglund, U. Roedig, and T. Voigt, "Secure communication for the Internet of Things-a comparison of link-layer security and IPsec for 6LoWPAN," Secur. Commun. Networks, vol. 7, no. 12, pp. 2654–2668, 2014, doi: 10.1002/sec.406.
39. A. Dua, V. Tyagi, N. Patel, and B. Mehtre, "Iisr: A secure router for iot networks," in 2019 4th International Conference on Information Systems and Computer Networks (ISCON), Nov 2019, pp. 636–643.
40. G. A. Abdalrahman and H. Varol, "Defending against cyber-attacks on the internet of things," in 2019 7th International Symposium on Digital Forensics and Security (ISDFS), June 2019, pp. 1–6.