Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 2 (2024)

"Uncovering Vulnerabilities and Security Challenges in IoT Devices: A Comprehensive Investigation"

Smitha Rajagopal[1] , Sheela Ramachandra[2]

Virendra Kumar Shrivastava[3]
[1,2,3] Alliance University, Dept of Computer Science & Engineering,
Anekal, Bengaluru-562 106, Karnataka, India

Abstract. Wireless Sensor Networks (WSNs) and the Internet of Things (IoT) have emerged as significant innovations, promising unmatched connection and ubiquitous data access across a wide range of applications. Their combination has resulted in a paradigm shift in how we perceive and interact with our surroundings. However, this rise in connectivity has created a new set of challenges, mostly centred on safeguarding the integrity of these interconnected systems. The adoption of WSNs and IoT is due to their low cost, unsupervised operational abilities, and long-term autonomy. This integration has contributed to the convergence of sensor-driven data gathering and internet-enabled devices, resulting in a tremendous influx of data that can be accessed via the internet. Despite these developments, users and network managers are concerned about the inherent vulnerabilities and security flaws in these networks. The lack of a centralised security architecture in WSNs and IoT contributes to vulnerabilities, rendering these networks vulnerable to a broad spectrum of attacks. The need of ensuring the confidentiality, integrity, and accessibility of data (CIA) becomes crucial, especially in applications where these properties are critical. Aside from the previously mentioned problems, the complications imposed by the changing dynamics of IoT ecosystems and the enormous number of networked devices heighten security vulnerabilities. As these systems mature, new attack avenues emerge, emphasising the importance of thoroughly investigating potential vulnerabilities. This paper emphasises the importance of presenting an extensive examination of security threats, including both known and developing attacks on WSNs and IoT. Such an examination is required for categorising and comprehending distinct forms of attacks. Furthermore, it emphasises the need of tackling the complex issues provided by WSN-IoT integration, such as protecting communication protocols, managing large-scale networks, and maintaining data integrity across varied devices and platforms. Understanding those risks and protecting these interconnected systems against future attacks are critical to establishing trust, dependability, and mainstream acceptance of these significant technologies.

Keywords: Wireless Sensor Networks, Internet of Things, vulnerabilities, attacks, security threats

1. Introduction

The integration of Wireless Sensor Networks (WSNs) and Internet of Things (IoT) frameworks has significantly impacted Industry 4.0, revolutionizing various sectors through innovative applications.[1] The convergence of advancements in wireless communication and Micro Electro Mechanical Systems has revolutionised the design and deployment of Wireless Sensor Networks, allowing them to successfully gather and transfer valuable data and thus significantly contributing to several fields and applications.[2] IoT is an area of engineering that focuses on providing thousands of small, physically connected things that can work together to achieve a common purpose. IoT has grown in popularity as a result of the widespread use of these tiny networked devices. These are smart, yet simple, devices that can detect and communicate wirelessly.[3] The Internet of Things (IoT) is an exciting development in technological advances, destined to revolutionise the information technology (IT) industry in a manner comparable to the internet's immense influence. Studies show a surprising trajectory of growth for

the Internet of Things (IoT) market, with a projected increase from over 15 billion linked devices in 2015 to more than 75 billion devices by 2025. [4] The potential applications of IoT are Smart Manufacturing, Supply Chain Management, Asset Tracking and Management, Energy Management, Healthcare and Remote Monitoring, Smart Cities and Infrastructure, Agriculture and Precision Farming, Environmental Monitoring, Retail and Inventory Management, etc..,[5]

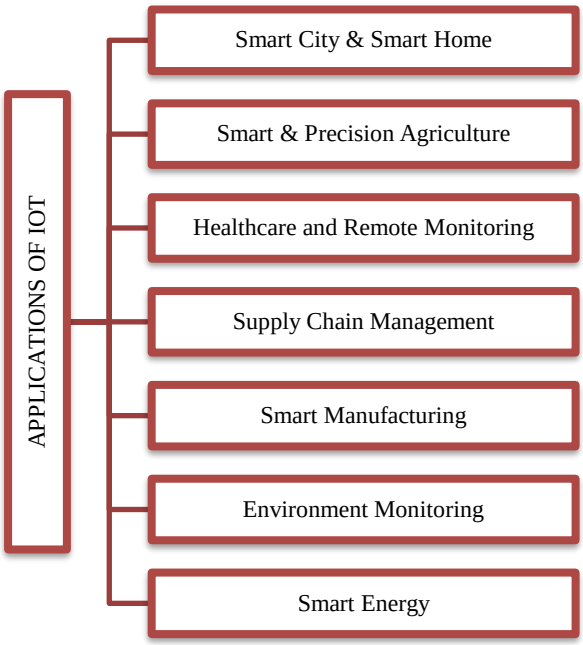

Fig 1. Applications of IoT

The Internet of Things (IoT), Internet of Everything (IoE), and Internet of Nano-Things (IoNT) are cutting-edge approaches to merging the internet into one's private, business, and social interactions, as well as the impersonal world of inanimate quasi-intelligent appliances. [6] The interconnectedness between the virtual realm and IoT devices facilitates the emergence of cyber-physical systems capable of interacting and cooperating. A fundamental aspect of Industry 4.0 revolves around a fully integrated production system that functions autonomously, leveraging data transmission, reception, and processing without direct human intervention. This system handles various tasks necessary for manufacturing diverse items. Industry 4.0 is structured around three core elements: peoples, things and business. [7] A typical IoT system consists of five basic components: Sensors: These devices are largely in charge of gathering and translating data from their surroundings into digital format. [a] Computing Node: This component acts as a processing unit, handling data and information from sensors and executing computations or analysis as needed. [b] Receiver: The receiver component supports the collection of messages delivered by computing nodes or other system-connected devices. [c] Actuator: The actuator causes related devices to perform certain functions or actions in response to decisions made by the Computing Node based on processed information. [d] User interface: When activated by the actuator, this component is responsible for executing the desired tasks or activities, contributing to the overall functionality of the system. [8] Security is a major concern in WSN and the Internet of Things (IoT), especially when these networks are used for crucial tasks. As these innovations grow more integrated into vital tasks and sensitive locations, comprehensive security measures are important for protecting against potential assaults and breaches. Based on recent studies, the majority of currently utilised systems fail to include strong security services that could protect the confidentiality of patients.[9] Techniques and practices established for securing WSNs, or wireless sensor networks are still applicable to any IoT system that includes one or more sensor networks. The integration of WSNs into the larger IoT environment is extremely likely in the near future. As a result, addressing all cybersecurity problems, including assaults and their prevention and mitigation, is critical in developing a safe and dependable IoT framework. [10] The paper aims to discuss an intensive investigation on the attacks on IoT devices, vulnerabilities and challenges.

2. Typical IoT Attacks

Because of their networked nature and frequently poor security mechanisms, IoT (Internet of Things) devices are vulnerable to numerous sorts of attacks offering substantial security issues. The security categories within IoT applications are primarily categorized into Commercial, Service, Consumer, and Infrastructure domains. [11] We present a summary of the most prevalent IoT risks, their types, and their potential impact on applications.

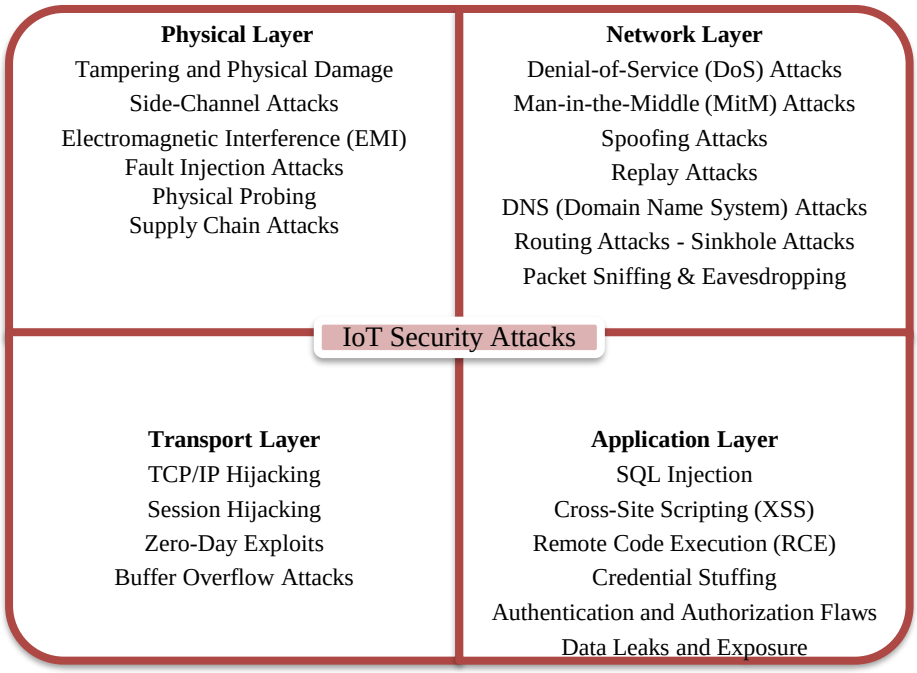

Fig 2. IoT Security Attacks

3. Physical Layer - Physical Attack

Physical security, often known as hardware security, entails securing a system's silicon element. [12] Having close proximity to the device is one important, distinguishing feature from the security of the software. Physical attacks need to be conducted at close segments, but software attacks can be conducted from a distance. Physically altering an IoT device might result in malware installation, data theft, or illegal access. Vulnerability physically comes in two distinct types: invasive and non-invasive. In order to alter device behaviour or obtain sensitive data, non-invasive assaults necessitate the attacker to get close enough to the target chip to detect electrical properties. The chip surface must be accessible for invasive attacks to occur so that the chip can be physically altered. Any IoT application, including smart automation systems, industrial control systems, and healthcare equipment, that is not adequately protected against physical attacks might be compromised in this type of attack.

Table 1. Table summarizes the Physical Layer Attack

Attack Type	Literature	Key Contributions or Findings	Countermeasures
Physical Tampering	[13] Nawir, M., et al. (2016)	Taxonomy of security attacks in IoT	Dynamic Address Allocation (DAA)
	[14] Pathak, A. K., et al. (2021)	Anomaly detection for sensor tampering in IoT systems	Continuous monitoring and behavioral analysis

Side-Channel Attacks	[15] Devi, M., & Majumder, A. (2021)	Survey on side-channel attacks in IoT	Use of robust encryption algorithms
	[16] Lo'Ai, A. T., & Somani, T. F. (2016)	More secure IoT using robust encryption algorithms against side-channel attacks	Implementation of secure cryptographic systems
Electromagnetic Interference (EMI)	[18] Wu, J., et al. (2019)	Review of EMC aspects of IoT	Regulatory efforts to minimize overlapping frequencies
	[19] Fang, K., et al. (2022)	Detection of weak EMI attacks in IIoT systems	Use of shielding and EMI-resistant components
Fault Injection Attacks	[25] Barenghi, A., et al. (2012)	Fault injection attacks on cryptographic devices	Secure boot mechanisms
	[26] Benevenuti, F., et al. (2017)	Evaluation of fault attack detection on SRAM-based FPGAs	Hardware redundancy and resilience
	[27] Joye, M.; Tunstall, M. (2012)	Fault analysis in cryptography	Error detection and correction
	[28] Rahman, M. Tanjidur, et al. (2018)	Exploration of physical inspection & attacks in hardware security	Hardware-level security measures
Physical Probing	[28] Rahman, M. Tanjidur, et al. (2018)	Exploration of physical probing techniques in hardware security	Use of tamper-resistant packaging
Supply Chain Attacks	[29] Rao, V. V., et al. (2021)	Trends, vulnerabilities, and preventive measures in IoT supply chain attacks	Risk analysis using methodologies like Attack Trees,
	[30] Kieras, T., et al. (2020): RIoTS	- Risk analysis of IoT supply chain threats	Supplier Networks, and System Graphs

4. Network Layer Attacks

Denial-of-Service (DoS) attacks targeting the network layer in IoT (Internet of Things) systems aim to disrupt the normal operation of devices, networks, or services by overwhelming them with a flood of traffic or malicious requests. These attacks impact the availability and performance of IoT devices, rendering them inaccessible or non-operational. A distributed denial of service (DDoS) attack uses a torrent of internet traffic to try and bring down the targeted server entirely or in part. This attack's main goal is to stop routine traffic from reaching the victim's network or server. [31] DoS is more detrimental to reputable organisations like banks and governments, resulting in significant time and financial losses. [32]

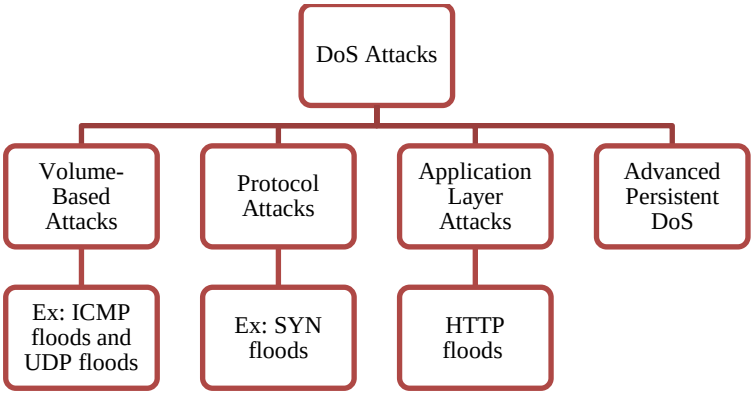

Fig 3. Types of DoS Attacks

Table 2. Table Summarizes Network Layer Attack

Attack Type	Literature Reference(s)	Key Contributions or Findings	Countermeasures
DDoS	[33] Mahjabin et al. (2017), [34] Sonar & Upadhyay (2014)	Orchestrated flood of malicious traffic from multiple systems (botnet) to overwhelm a target.	Implementing DDoS mitigation techniques, traffic filtering, and rate limiting.
Flooding Attacks	[34] Sonar & Upadhyay (2014)	Inundating devices/networks with excessive traffic (UDP flood, ICMP flood, SYN flood, HTTP flood, DNS flood).	Deploying intrusion detection/prevention systems, traffic filtering, and rate limiting.
Buffer Overflow Attacks	[35] Xu et al. (2018)	Exploiting programming errors to write data beyond buffer limits, potentially leading to system crashes or unauthorized access.	Regular code audits, input validation, and implementing stack protection mechanisms.
Man-in-the-Middle (MitM) Attacks	[36] Toutsop et al. (2020)	Intercepting communication between two parties, posing a risk in IoT due to device limitations on encryption.	Implementing advanced encryption approaches, secure key exchange protocols, and secure channels.
Spoofing Attacks	[42] Khan et al. (2022)	Presenting false information, exploiting identifiers (MAC, IP addresses). Common types include MAC, IP, DNS, ARP, NTP, Bluetooth, and Wi-Fi spoofing.	Using cryptographic techniques, secure device authentication, and monitoring for anomalous activities.
Replay Attacks	[43-45] Rughoobur & Nagowah (2017), Feng et al. (2017), Al-Shareeda et al. (2022)	Recording and replaying commands or sensitive data to alter device controls or gain unauthorized access.	Implementing secure communication protocols, encryption, timestamping, and unique session identifiers.
DNS Attacks	[46] Hesselman et al. (2020)	Threats to DNS integrity and availability in IoT, including Spoofing/Cache Poisoning, Amplification, Tunneling, and DDoS via DNS.	Implementing DNS security extensions (DNSSEC), using authoritative DNS servers, and traffic monitoring.

Routing Attacks	[47] Yadollahzadeh Tabari & Mataji (2021), Choudhary & Kesswani (2018)	Intentional attempts to disrupt routing protocols or procedures, including Sinkhole and Selective Forwarding attacks.	Implementing secure routing protocols, detecting malicious nodes, and using intrusion detection systems.
Packet Sniffing & Eavesdropping	[49] Kulshrestha & Dubey (2014), [50] Cvetković et al. (2020)	Unauthorized access to network traffic for data theft. Sniffers steal data, compromising confidentiality.	Implementing encryption, using virtual private networks (VPNs), and regular network monitoring.

5. Transport Layer Attacks

Transport layer attacks in IoT pose significant threats to the security and reliability of connected devices. Denial of Service (DoS) attacks can overwhelm IoT devices, disrupting communication by flooding the network. Man-in-the-Middle (MitM) attacks exploit vulnerabilities in transport layer protocols, intercepting and manipulating data between devices. Session hijacking allows unauthorized control over communication sessions, compromising confidentiality and integrity. Packet spoofing involves forging packet headers, leading to unauthorized access and data manipulation. Protocol exploitation targets vulnerabilities in transport layer protocols, risking unauthorized access and disruption of IoT communication. To counter these threats, robust security measures such as encryption, authentication, and intrusion detection systems are essential for safeguarding IoT devices and ensuring the integrity of their communication.

Table 3. Table Summarizes Transport Layer Attack

Attack Type	Literature Reference(s)	Key Contributions or Findings	Countermeasures
TCP/IP Hijacking	[51] Feng et al. (2021)	Exploits TCP vulnerability in the three-way handshake process. Attackers predict/guess sequence numbers to insert themselves into ongoing communication. Consequences include unauthorized access, data manipulation, and service disruption in IoT.	Implementing intrusion detection systems, encryption for communication, and regularly updating and patching systems to address TCP vulnerabilities.
Session Hijacking	[52] Sarika (2022), [53] Humaira et al. (2020)	Session hijacking poses a threat to web applications by taking over legitimate sessions. Secure frameworks have been proposed in the literature to detect and perceive these attacks.	Implementing secure frameworks that detect and prevent session hijacking, using strong authentication mechanisms, encrypting session data, and conducting regular security audits.
Zero-Day Exploits	[54] Lamba et al. (2016), [55] Zoppi et al. (2021)	Zero-Day attacks exploit previously unknown vulnerabilities. Types include ransomware, phishing, and cloud-native breaches. Studies focus on unsupervised algorithms for detection. Mitigating involves proactive measures such as software updates, intrusion detection systems, multi-layered security, and continuous monitoring.	Regularly updating software, employing intrusion detection systems, implementing multi-layered security protocols, conducting continuous monitoring, educating users on phishing awareness, and adopting strong cloud security practices.

Buffer Overflow Attacks	[56] Mullen & Meany (2019)	Buffer overflow attacks exploit weaknesses to overrun buffers with data. Consequences include unauthorized access, system crashes, and execution of malicious code. Previous research focuses on assessing vulnerabilities and implementing unsupervised algorithms for detection.	Implementing code reviews, input validation, using languages with built-in security features, applying stack protection mechanisms, and conducting regular security audits.

6. Application Layer Attacks

The application layer of the Internet of Things (IoT) stack is crucial for facilitating specific functionalities and communication protocols. However, this layer is susceptible to various types of attacks that can compromise the security and functionality of IoT devices. One prevalent threat is the injection of malicious code, where attackers exploit vulnerabilities in the application layer to insert unauthorized commands or manipulate data exchanged between devices. Another significant concern is API (Application Programming Interface) abuse, where attackers exploit weaknesses in APIs to gain unauthorized access, tamper with data, or launch attacks. Additionally, IoT devices are vulnerable to application layer DDoS (Distributed Denial of Service) attacks, which overwhelm specific applications, rendering them unresponsive. Security measures, including code validation, secure API design, and traffic monitoring, are essential to mitigate these application layer attacks and ensure the robustness of IoT ecosystems.

Table 4. Table Summarizes Application Layer Attack

Attack Type	Literature Reference(s)	Key Contributions or Findings	Countermeasures
SQL Injection	[57] Jemal et al. (2020), [58] Tang et al. (2020), [59] Kar et al. (2016), [60] Hasan et al. (2019)	Malicious insertion of SQL commands into web application queries. Exploits vulnerabilities to access and manipulate databases. Identification techniques include Artificial Neural Networks[58], Hidden Markov Model[59], Machine Learning[60], etc.	Implementing parameterized queries, input validation, stored procedures, and using web application firewalls (WAFs). Regularly updating and patching web application software to address vulnerabilities.
Cross-Site Scripting (XSS)	[61] Rodríguez et al. (2020)	Malicious script injection into web applications, targeting vulnerabilities. Can impact user information, lead to network hacking, phishing, or cookie theft.	Implementing input validation, output encoding, Content Security Policy (CSP), and using security mechanisms like WAFs. Educating developers and users about XSS risks and best practices.

Table 5. Other Type of Application Layer Attacks:

Attack Type	Description of Attack	Countermeasures
Credential Stuffing	Involves testing stolen usernames and passwords from data breaches on	Encouraging strong, unique passwords, implementing multi-factor authentication, and avoiding default

	various accounts across platforms. In IoT, can exploit default or weak credentials for unauthorized access.	credentials. Monitoring and detecting anomalous login activities in IoT platforms.
Authentication & Authorization Flaws	Authentication flaws allow unauthorized access; authorization flaws grant elevated privileges. Attackers exploit these to control devices or access sensitive data.	Implementing strong authentication mechanisms, secure login processes, and access controls. Regularly auditing and reviewing authentication and authorization configurations. Employing least privilege principles for user access.
Data Leaks and Exposure	Involves unintentional disclosure of sensitive information in IoT environments. Weak data encryption and insecure communication channels can lead to data leaks.	Implementing strong data encryption, secure communication protocols, and robust data protection mechanisms in IoT systems. Regularly monitoring and auditing data transmission for anomalies. Educating users and developers about data protection and privacy best practices.

7. Vulnerability Assessment Techniques

"A flaw within a system, application, or service which allows an attacker to circumvent security controls and manipulate systems in ways the developer never intended" is the definition of a vulnerability.[62] The purpose of vulnerability assessments is to evaluate a system, network, or application on a computer in order to find, quantify, and prioritise system weaknesses for methodical remediation. [63] Vulnerability assessment in IoT involves evaluating and identifying potential weaknesses or security gaps within IoT devices, networks, or systems. The table below listed the vulnerability assessment techniques and tools for IoT devices. [65]

Table 6. Vulnerability Assessment Tools

S. no	Vulnerability Assessment Techniques	Tools
1.	Penetration Testing	Metasploit, Burp Suite, Nmap Wireshark, SQLMap
2.	Vulnerability Scanning	Nessus, OpenVAS, Qualys, Nexpose, Acunetix
3.	Static Code Analysis	Veracode, Checkmarx, Fortify, SonarQube, Klocwork
4.	Dynamic Code Analysis	AppScan, HP WebInspect, OWASP ZAP, Acunetix, Netsparker
5.	Fuzz Testing (Fuzzing)	Peach Fuzzer, American Fuzzy Lop (AFL), Radamsa, Sulley, boofuzz
6.	Security Audits and Reviews	Lynis, OpenSCAP, Security Auditor's Research Assistant (SARA), Nikto, Retina
7.	Threat Modeling	Microsoft Threat Modeling Tool, IriusRisk, ThreatModeler, OWASP Threat Dragon, SecuriCAD
8.	Protocol Analysis	WireShark, tcpdump, Charles Proxy, Fiddler, Wireshark

9.	Configuration Management Review	Chef, Puppet, Ansible, SaltStack, Terraform
10.	Supply Chain Risk Assessment	BitSight, Resilience360, Panorays, RiskRecon, UpGuard
11.	Security Test Beds	Kali Linux, Security Onion, OWASP IoT Security Project, Docker, VMware
12.	Machine Learning	TensorFlow, Scikit-learn, Keras PyTorch, Microsoft Azure Machine Learning
13.	Honeypots	Cowrie, Dionaea, Honeyd, Snare, KFSensor

This paper presents a conceptual framework aimed at addressing the prevalent vulnerabilities and security challenges inherent in Internet of Things (IoT) devices. The proposed framework encompasses a comprehensive approach to fortifying IoT device security and mitigating potential risks through a structured block diagram representation. The block diagram delineates the intricate layers of IoT device infrastructure, emphasizing key components and security measures integrated at each level.

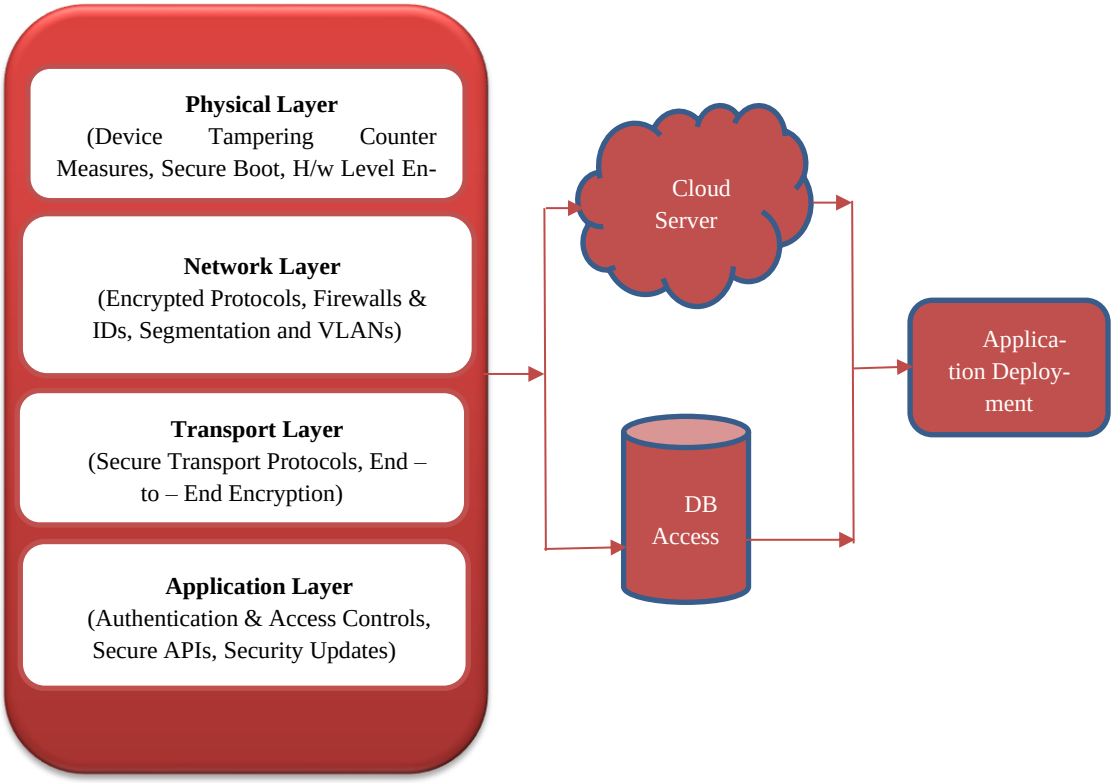

Fig 4. Secure Architecture for sample IoT Deployment

Implementing the proposed framework for fortifying IoT device security may encounter several significant challenges.

Conclusion:

The Internet of Things is a group of interconnected gadgets [65]. The way people engage with linked gadgets, even though they have been around for a long, is what makes the Internet of Things unique. However, this interconnected landscape brings forth a multitude of security challenges, exposing IoT ecosystems to diverse risks across different layers of the technology stack. Exploring the layered security risks within IoT, we have identified vulnerabilities prevalent at each layer—from the physical and data link layers to the application and user layers. These risks encompass a wide array of threats, including physical tampering, network layer attacks, application layer vulnerabilities, and data exposure, highlighting the complexity of securing IoT environments comprehensively. To mitigate these risks and safeguard IoT systems, a robust and proactive approach to vulnerability assessment is essential. Our examination of vulnerability assessment techniques has underscored the importance of employing diverse methodologies of the same. Despite the advancements in security measures, it's crucial to acknowledge that IoT security remains an evolving landscape, demanding continuous improvements and adaptive strategies. By comprehensively understanding and addressing security risks through effective vulnerability assessment techniques, we can pave the way for a more secure and resilient IoT ecosystem, ensuring the continued advancement and safe adoption of this transformative technology.

References

[1] Majid, M., Habib, S., Javed, A. R., Rizwan, M., Srivastava, G., Gadekallu, T. R., & Lin, J. C. W. (2022). Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. Sensors, 22(6), 2087.

[2] Butun, I., Österberg, P., & Song, H. (2019). Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. IEEE Communications Surveys & Tutorials, 22(1), 616-644.

[3] Landaluce, H.; Arjona, L.; Perallos, A.; Falcone, F.; Angulo, I.; Muralter, F. A review of iot sensing applications and challenges using RFID and wireless sensor networks. J. Sens. 2020, 20, 2495.

[4] V. Friedman. (2018) On the edge: Solving the challenges of edge computing in the era of iot. [Online]. Available: https://data-economy.com/on-the-edge-solving-thechallenges-of-edge-computing-in-the-era-of-iot/

[5] Attia, T. M. (2019). Challenges and opportunities in the future applications of IoT technology.

[6] Miraz, M. H., Ali, M., Excell, P. S., & Picking, R. (2018). Internet of nano-things, things and everything: future growth trends. Future Internet, 10(8), 68.

[7] Osterrieder, P., Budde, L., & Friedli, T. (2020). The smart factory as a key construct of industry 4.0: A systematic literature review. International Journal of Production Economics, 221, 107476.

[8] Keramidas, G., Voros, N., & Hübner, M. (2016). Components and services for IoT platforms. Cham: Springer International Pu.

[9] P. Gope and T. Hwang, “Bsn-care: A secure iot-based modern healthcare system using body sensor network,” IEEE Sensors Journal, vol. 16, no. 5, pp. 1368–1376, 2016.

[10] S. Li, L. Da Xu, and S. Zhao, “The internet of things: a survey,” Information Systems Frontiers, vol. 17, no. 2, pp. 243–259, 2015.

[11] Rizvi, S., Kurtz, A., Pfeffer, J., & Rizvi, M. (2018, August). Securing the internet of things (IoT): A security taxonomy for IoT. In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 163-168). IEEE.

[12] Pan, Y., White, J., Schmidt, D., Elhabashy, A., Sturm, L., Camelio, J., & Williams, C. (2017). Taxonomies for reasoning about cyber-physical attacks in IoT-based manufacturing systems.

[13] Nawir, M., Amir, A., Yaakob, N., & Lynn, O. B. (2016, August). Internet of Things (IoT): Taxonomy of security attacks. In 2016 3rd international conference on electronic design (ICED) (pp. 321-326). IEEE.

[14] Pathak, A. K., Saguna, S., Mitra, K., & Åhlund, C. (2021, June). Anomaly detection using machine learning to discover sensor tampering in IoT systems. In ICC 2021-IEEE International Conference on Communications (pp. 1-6). IEEE.

[15] Devi, M., & Majumder, A. (2021). Side-channel attack in Internet of Things: A survey. In Applications of Internet of Things: Proceedings of ICCCIOT 2020 (pp. 213-222). Springer Singapore.

[16] Lo'Ai, A. T., & Somani, T. F. (2016, November). More secure Internet of Things using robust encryption algorithms against side channel attacks. In 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA) (pp. 1-6). IEEE.

[17] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," IEEE Commun. Surv. Tuts., vol. 19, no. 2, pp. 855–873, Second quarter 2017.

[18] Wu, J., Qi, Y., Gong, G., Fan, J., Miao, M., Yu, W., ... & Drewniak, J. L. (2019). Review of the EMC Aspects of Internet of Things. IEEE Transactions on Electromagnetic Compatibility, 62(6), 2604-2612.

[19] Fang, K., Wang, T., Yuan, X., Miao, C., Pan, Y., & Li, J. (2022). Detection of weak electromagnetic interference attacks based on fingerprint in IIoT systems. Future Generation Computer Systems, 126, 295-304.

[21] Sahu, A.; Mao, Z.; Wlazlo, P.; Huang, H.; Davis, K.; Goulart, A.; Zonouz, S. Multi-Source Multi-Domain Data Fusion for Cyberattack Detection in Power Systems. *IEEE Access* **2021**, *9*, 119118–119138.

[22] Shrivastwa, R.-R.; Guilley, S.; Danger, J.-L. Multi-source Fault Injection Detection Using Machine Learning and Sensor Fusion. In Security and Privacy; Springer: Berlin/Heidelberg, Germany, 2021; pp. 93–107.

[23] Lee, H. Framework and development of fault detection classification using IoT device and cloud environment. J. Manuf. Syst. 2017, 43, 257–270.

[24] Jiang, W.; Wen, L.; Zhan, J.; Jiang, K. Design optimization of confidentiality-critical cyber physical systems with fault detection. J. Syst. Archit. 2020, 107, 101739.

[25] Barenghi, A.; Breveglieri, L.; Koren, I.; Naccache, D. Fault Injection Attacks on Cryptographic Devices: Theory, Practice, and Countermeasures. Proc. IEEE 2012, 100, 3056–3076.

[26] Benevenuti, F.; Kastensmidt, F.L. Evaluation of fault attack detection on SRAM-based FPGAs. In Proceedings of the 2017 18th IEEE Latin American Test Symposium (LATS), Punta del Este, Uruguay, 27–29 October 2017; pp. 1–6.

[27] Joye, M.; Tunstall, M. Fault Analysis in Cryptography; Springer: Berlin/Heidelberg, Germany, 2012; p. 147

[28] Rahman, M. Tanjidur, Qihang Shi, Shahin Tajik, Haoting Shen, Damon L. Woodard, Mark Tehranipoor, and Navid Asadizanjani. "Physical inspection & attacks: New frontier in hardware security." In 2018 IEEE 3rd International Verification and Security Workshop (IVSW), pp. 93-102. IEEE, 2018.

[29] Rao, V. V., Marshal, R., & Gobinath, K. (2021, October). The IoT Supply Chain Attack Trends-Vulnerabilities and Preventive Measures. In 2021 4th International Conference on Security and Privacy (ISEA-ISAP) (pp. 1-4). IEEE.

[30] Kieras, T., Farooq, M. J., & Zhu, Q. (2020, June). RIoTS: Risk analysis of IoT supply chain threats. In 2020 IEEE 6th World Forum on Internet of Things (WF-IoT) (pp. 1-6). IEEE.

[31] Salim, M. M., Rathore, S., & Park, J. H. (2020). Distributed denial of service attacks and its defenses in IoT: a survey. The Journal of Supercomputing, 76, 5320-5363.

[32] Abughazaleh, N., Bin, R., & Btish, M. (2020). DoS attacks in IoT systems and proposed solutions. Int. J. Comput. Appl., 176(33), 16-19.

[33] Mahjabin, T., Xiao, Y., Sun, G., & Jiang, W. (2017). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *International Journal of Distributed Sensor Networks*, *13*(12), 1550147717741463.

[34] Sonar, K., & Upadhyay, H. (2014). A survey: DDOS attack on Internet of Things. International Journal of Engineering Research and Development, 10(11), 58-63.

[35] Xu, Bin, Weike Wang, Qiang Hao, Zhun Zhang, Pei Du, Tongsheng Xia, Hongge Li, and Xiang Wang. "A security design for the detecting of buffer overflow attacks in IoT device." IEEE Access 6 (2018): 72862-72869.

[36] Toutsop, O., Harvey, P., & Kornegay, K. (2020, October). Monitoring and detection time optimization of man in the middle attacks using machine learning. In 2020 IEEE Applied Imagery Pattern Recognition Workshop (AIPR) (pp. 1-7). IEEE.

[37] Z. C. Dong, R. Espejo, Y. Wan, and W. Zhuang, "Detecting and locating man-in-the-middle attacks in fixed wireless networks," Journal of computing and information technology, vol. 23, no. 4, pp. 283–293, 2015, doi:10.2498/cit.1002530.

[38] N. N. Santhosh, "Future black board using internet of things with cognitive computing: Machine learning aspects," in 2016 International Conference on Communication and Electronics Systems (ICCES), 2016, pp. 1–4, doi:10.1109/CESYS.2016.788987 .

[39] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in iot security: current solutions and future challenges," IEEE Communications Surveys & Tutorials, 2020, doi:10.1109/COMST.2020.2986444.

[40] N. Gupta, V. Naik, and S. Sengupta, "A firewall for internet of things," in 2017 9th International Conference on Communication Systems and Networks (COMSNETS), 2017, pp. 411–412, doi:10.1109/COMSNETS.2017.7945418.

[41] M. Mamdouh, M. A. I. Elrukhsi, and A. Khattab, "Securing the internet of things and wireless sensor networks via machine learning: A survey," in 2018 International Conference on Computer and Applications (ICCA), 2018, pp. 215–218, doi:10.1109/COMAPP.2018.8460440.

[42] Khan, F., Al-Atawi, A. A., Alomari, A., Alsirhani, A., Alshahrani, M. M., Khan, J., & Lee, Y. (2022). Development of a Model for Spoofing Attacks in Internet of Things. Mathematics, 10(19), 3686.

[43] Rughoobur, P., & Nagowah, L. (2017, December). A lightweight replay attack detection framework for battery depended IoT devices designed for healthcare. In 2017 international conference on Infocom technologies and unmanned systems (trends and future directions)(ICTUS) (pp. 811-817). IEEE.

[44] Feng, Y., Wang, W., Weng, Y., & Zhang, H. (2017, July). A replay-attack resistant authentication scheme for the internet of things. In 2017 IEEE international conference on computational science and engineering (CSE) and IEEE international conference on embedded and ubiquitous computing (EUC) (Vol. 1, pp. 541-547). IEEE.

[45] Al-Shareeda, M. A., Manickam, S., Laghari, S. A., & Jaisan, A. (2022). Replay-attack detection and prevention mechanism in industry 4.0 landscape for secure SECS/GEM communications. Sustainability, 14(23), 15900.

[46] Hesselman, C., Kaeo, M., Chapin, L., Claffy, K., Seiden, M., McPherson, D., ... & Rasmussen, R. (2020). The dns in iot: Opportunities, risks, and challenges. IEEE internet computing, 24(4), 23-32.

[47] Yadollahzadeh Tabari, M., & Mataji, Z. (2021). Detecting sinkhole attack in rpl-based internet of things routing protocol. Journal of AI and Data Mining, 9(1), 73-85.

[48] Choudhary, S., & Kesswani, N. (2018, August). Detection and prevention of routing attacks in internet of things. In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 1537-1540). IEEE.

[49] Kulshrestha, A., & Dubey, S. K. (2014). A literature reviewon sniffing attacks in computernetwork. International Journal of Advanced Engineering Research and Science (IJAERS), 1(2).

[50] Cvetković, A. S., Jokić, S., Adamović, S., Ristić, N., & Pavlović, N. (2020). Internet of Things Security Aspects.

[51] Feng, X., Li, Q., Sun, K., Fu, C., & Xu, K. (2021). Off-path TCP hijacking attacks via the side channel of downgraded IPID. IEEE/ACM transactions on networking, 30(1), 409-422.

[52] Sarika, S. (2022). An Approach to Perceive Session Hijacking in IoT Health Care. In Information and Communication Technology for Competitive Strategies (ICTCS 2021) Intelligent Strategies for ICT (pp. 525-533). Singapore: Springer Nature Singapore.

[53] Humaira, F., Islam, M. S., Luva, S. A., & Rahman, M. B. (2020). A Secure Framework for IoT Smart Home by Resolving Session Hijacking. Glob. J. Comput. Sci. Technol, 20(2), 9-20.

[54] Lamba, A., Singh, S., & Balvinder, S. (2016). Mitigating zero-day attacks in IoT using a strategic framework. International Journal for Technological Research in Engineering, 4(1).

[55] Zoppi, T., Ceccarelli, A., & Bondavalli, A. (2021). Unsupervised algorithms to detect zero-day attacks: Strategy and application. Ieee Access, 9, 90603-90615.

[56] Mullen, G., & Meany, L. (2019, June). Assessment of buffer overflow based attacks on an IoT operating system. In 2019 Global IoT Summit (GIoTS) (pp. 1-6). IEEE.

[57] Jemal, I., Cheikhrouhou, O., Hamam, H., & Mahfoudhi, A. (2020). Sql injection attack detection and prevention techniques using machine learning. International Journal of Applied Engineering Research, 15(6), 569-580.

[58] Tang, P., Qiu, W., Huang, Z., Lian, H., & Liu, G. (2020). Detection of SQL injection based on artificial neural network. Knowledge-Based Systems, 190, 105528.

[59] Kar, D., Agarwal, K., Sahoo, A. K., & Panigrahi, S. (2016, March). Detection of SQL injection attacks using Hidden Markov Model. In 2016 IEEE International Conference on Engineering and Technology (ICETECH) (pp. 1-6). IEEE.

[60] Hasan, M., Balbahaith, Z., & Tarique, M. (2019, November). Detection of SQL injection attacks: a machine learning approach. In 2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA) (pp. 1-6). IEEE.

[61] Rodríguez, G. E., Torres, J. G., Flores, P., & Benavides, D. E. (2020). Cross-site scripting (XSS) attacks and mitigation: A survey. Computer Networks, 166, 106960.

[62] Kennedy, D., Gorman, J., Kearns, D., & Aharoni, M. (2011). Metasploit. (W. Pollock & T. Ortman, Eds.). William Pollock.

[63] Hu, Y., Sulek, D., Carella, A., Cox, J., Frame, A., Cipriano, K., & Wang, H. (2016). Employing Miniaturized Computers for Distributed Vulnerability Assessment, 57–61.

[64] Anand, P., Singh, Y., Selwal, A., Alazab, M., Tanwar, S., & Kumar, N. (2020). IoT vulnerability assessment for sustainable computing: threats, current solutions, and open challenges. IEEE Access, 8, 168825-168853

[65] IEEE. (2015). IEEE-SA Internet of Things (IoT) Ecosystem Study, 1– 35. Retrieved from http://standards.ieee.org/innovate/iot/study.html