International Journal of Advance and Applied Research
www.ijaar.co.in
ISSN – 2347-7075 Impact Factor – 8.141
Peer Reviewed Bi-Monthly
Vol. 7 No. 28 March - April - 2026

Secure IoT Architecture in Various Disciplines

Miss. Changede Ashwini[1] & Mrs. Mhase Poonam Uttam[2]
Assistant Professor, (HOD) Department of Computer Science,
Rajarshi Shahu Mahavidyalaya, Deolali Pravara
Corresponding Author – Miss. Changede Ashwini
DOI - 10.5281/zenodo.19396636

Abstract:

The Internet of Things (IoT) has extended in varied domains to create smart environments. According to the distribution of IoT, security aspects must be concerned and improved. The IoT uses different kinds of technologies to produce results. Therefore, it presents new different challenges and issues in security. Several researchers have examined various security issues, threats, challenges, and solutions to increase security in IoT devices (Ghadi Shaheen, 2024). This paper includes an introduction to IoT and its purposes. IoT includes 4 stages of IoT architecture, ***the various disciplines where IoT architecture helps in security purpose, I****oT Security Threats and Attacks, Security Solutions and Mechanisms.*

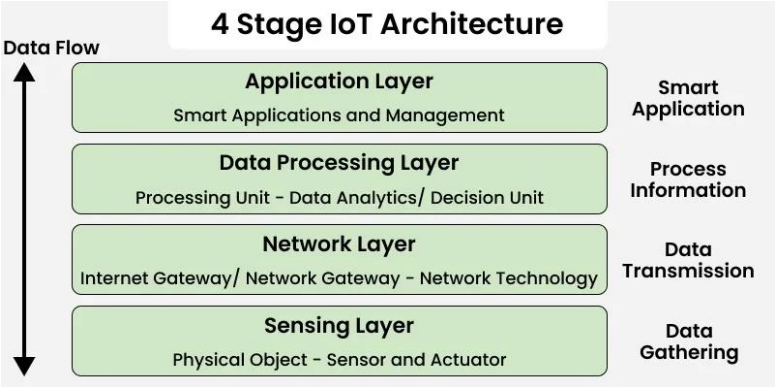
Keywords: Internet of Things (IoT), IoT Security, Botnet and DDoS Attacks, Encryption Techniques, Block chain for IoT, Machine Learning for IoT Security, Zero Trust architecture, Lightweight Cryptography, AI-Driven Anomaly Detection.

Introduction:

The vast network of physical objects such as smart home devices, vehicles to industrial sensor embedded with sensors, software, and connectivity, allowing them to gather and exchange data over the internet without human involvement, developing efficient, smarter, and automated systems called Internet of Things (IoT). Smart home devices (thermostats, lights, security), smart appliances, wearable fitness trackers, connected cars, industrial sensors for monitoring machinery, voice assistants (Alexa, Google Home), and medical devices like pacemakers it ties the digital and physical worlds by enabling everyday "things" to communicate and act on information, improving convenience, efficiency. The main four components of IOT architecture are Sensors, Connectivity, Data Processing, and a User Interface, forming a system where devices collect data (sensors), transmit it (connectivity), analyze it (processing), and present it for action (UI). Some models also highlight underlying technologies like M2M, RFID, WSN, and SCADA as foundational pillars, or focus on abstract concepts like People, Processes, Data, and Objects, but the device-to-insight flow remains central.

Internet of things (IoT) architecture refers to the framework which defines communication of various IoT elements (e.g., devices, networks, sensors, apps) within an IoT environment.

The IoT architecture:



(www.geeksforgeeks.org)

1. Sensing Layer:

- Lowest layer that collects data from the physical environment.
- Uses sensors to detect temperature, humidity, motion, pressure, etc.
- Includes devices like RFID tags and microcontrollers.
- Actuators (motors, valves, switches) perform actions based on sensed data.

2. Network Layer:

- Transfers sensor data to processing systems.
- Enables communication between devices and servers.
- Uses technologies like Wi-Fi, Bluetooth, Zigbee, LoRaWAN, and Ethernet.
- Routers and switches help in routing and transmitting data.

3. Data Processing Layer:

- Processes and analyzes data received from devices.
- Cleans and filters raw sensor data.
- Uses cloud platforms, data warehouses, and analytics tools.
- Generates insights, alerts, and detects abnormalities.

4. Application Layer:

- Top layer that interacts with users.
- Provides mobile apps and web dashboards for monitoring.
- Displays data through charts and reports.
- Enables remote control, real-time monitoring, and automated actions.

The various disciplines where IoT architecture helps in security purpose:

IoT architecture improves **security in various disciplines** by enabling continuous monitoring, data analysis, and automated responses. The different layers of IoT work together to detect threats, collect evidence, and trigger safety measures.

1. Home Security:

- Smart cameras, motion sensors, and door sensors detect unusual activity.
- Real-time alerts are sent to mobile apps when unauthorized access is detected.
- Smart locks and alarms can automatically respond to threats.

2. Healthcare Security:

- Wearable IoT devices monitor patient health conditions continuously.
- Alerts are generated if abnormal health parameters are detected.

- Helps in protecting patient safety and improving emergency response.

3. Industrial Security:

- IoT sensors monitor machines, equipment, and working conditions.
- Detects gas leaks, overheating, or equipment failures early.
- Prevents accidents and ensures worker safety in factories.

4. Transportation Security:

- IoT systems track vehicle location and driver behavior.
- Sensors help detect accidents or unsafe driving conditions.
- Improves traffic management and passenger safety.

5. Environmental Security:

- Sensors monitor air quality, pollution levels, and natural hazards.
- Early warnings systems help detect floods, fires, or earthquakes.
- Supports disaster management and environmental protection.

6. Smart City Security:

- IoT cameras and sensors monitor public areas and traffic.
- Helps law enforcement detect suspicious activities.
- Improves emergency services and public safety.

7. Agriculture Security:

- Sensors monitor soil moisture, crop conditions, and weather changes.
- Detects pests or diseases early to protect crops.
- Smart irrigation systems prevent water misuse and crop damage.

8. Energy and Power Grid Security:

- IoT devices monitor electricity generation and distribution.
- Detects power faults, overloads, or unauthorized access to power systems.
- Improves reliability and prevents energy theft.

9. Banking and Financial Security:

- Smart surveillance and IoT sensors monitor ATMs and bank premises.
- Detects suspicious activities or tampering attempts.
- Helps in preventing theft and fraud.

10. Military and Defense Security:

- IoT sensors are used for border surveillance and monitoring restricted areas.
- Drones and smart sensors help detect enemy movement.
- Improves national security and defense operations.

11. Retail Security:

- Smart cameras and RFID systems track products in stores.
- Prevents shoplifting and inventory loss.
- Monitors customer movement for safety.

12. Airport and Aviation Security:

- IoT systems monitor passengers, luggage, and airport operations.
- Sensors detect unauthorized entry into restricted zones.
- Improves safety and security in airports.

IoT Security Threats and Attacks:

1. Botnet Attacks (Mirai & IoT botnets):

- IoT devices often have weak credentials and default passwords, making them easy to compromise and include in botnets that launch cyber-attacks. **Mirai** is a classic example of such botnets that infected IP cameras and routers. (www.geeksforgeeks.org)

2. Distributed Denial of Service (DDoS) Attacks:

- Botnets of compromised IoT devices are often used to flood servers with traffic, making services unavailable to legitimate users. This is one of the most common types of IoT-related attacks (ciet.ncert.gov.in).

3. Man-in-the-Middle (MITM) Attacks:

- MITM attacks target IoT communications by intercepting data exchanged between devices, gateways, and cloud services. If messages are not properly encrypted, attackers can monitor or alter information.
- Lack of encryption in IoT systems increases risks of eavesdropping and data manipulation during transmission (www.geeksforgeeks.org).

4. Replay Attacks:

- Replay attacks involve capturing valid communication between devices and retransmitting it later to fool systems into accepting duplicate messages. (en.wikipedia.org/)
- IoT communications without protections such as timestamps or random nonce are vulnerable to this type of network replay abuse.

5. Data Interception:

- IoT systems often use insecure or unencrypted communication channels, allowing attackers to capture transmitted data using network monitoring tools.
- Poor encryption and insecure message handling expose sensitive information such as login credentials and device control messages. (infosecacademy.com)

6. Malware Attacks on IoT Devices:

- Malware such as botnets and IoT-specific worms infect devices, change their behavior, or grant attackers remote control. (www.geeksforgeeks.org)
- Botnet malware like Mirai continuously scans for vulnerable IoT devices and infects them for use in further attacks. (en.wikipedia.org/)

7. Unauthorized Device Access:

- Weak credentials, default configurations, and poor authentication mechanisms make it easy for attackers to gain unauthorized access to IoT devices.
- Once inside, attackers can manipulate device functions, steal data, or include them in botnets. (en.wikipedia.org/)

Security Solutions and Mechanisms:

- **Encryption techniques (AES, RSA):** Protect IoT data by converting it into unreadable formats that only authorized devices can decrypt.
- **Block chain-based IoT security:** Uses decentralized ledgers to ensure secure, tamper-proof data exchange between IoT devices.

- **Machine learning for intrusion detection:** Detects unusual patterns or attacks in IoT networks using AI algorithms.
- **Secure authentication protocols:** Verifies the identity of devices and users before granting access to IoT systems.
- **Secure firmware updates:** Ensures IoT devices receive trusted and tamper-free software updates.
- **Device identity management:** Maintains unique, verifiable identities for IoT devices to prevent unauthorized access.

Different tools use for secured IoT devices:

There are some tools are used for securing IoT devices in various applications. The two types of IoT security include:

- **Network Security:** IoT network security solutions are designed to enable users to protect their IoT devices. They inspect network traffic and can filter traffic that contains potential malicious content or violations of corporate security policies (www.checkpoint.com).
- **Embedded Security:** Embedded on-device IoT security solutions help to close the security gaps that are common with IoT devices. Insecure components, unmanaged devices, and insecure development practices can all create vulnerabilities that embedded IoT security solutions can mitigate (www.checkpoint.com).

The network and embedded IoT security solutions together enables defense in depth against IoT security threats. Consumers deploying network IoT solutions can block threats from reaching vulnerable devices, and the integration of embedded security by manufacturers into their devices reduces the threat posed by attacks that might slip through the cracks.

Security Standards and Frameworks:

- ISO/IEC 27030 (IoT security guidelines).
- NISTIR 8228 (managing IoT cyber security and privacy risks).
- IEEE P2413 (standard for IoT architecture and security).

Emerging Security Techniques:

- **Zero Trust Architecture for IoT:** Continuously verifies every device and access request, assuming no device is inherently trusted.
- **Lightweight Cryptography for Resource-Constrained IoT Devices:** Provides encryption and security with minimal computational and energy overhead for low-power IoT devices.
- **AI-Driven Anomaly Detection in Smart Cities or Industrial IoT:** Uses AI/ML to identify unusual behaviour or cyber threats in IoT networks in real time.

Conclusion:

The expansion of IoT has transformed daily life and industries by enabling seamless connectivity and automation. However, it also introduces significant security risks, including botnets, DDoS attacks, malware, and unauthorized access. Implementing layered security measures such as encryption, block chain, secure authentication, and device identity management alongside emerging approaches like Zero Trust Architecture, lightweight cryptography, and AI-driven anomaly detection, can significantly enhance IoT resilience. Adherence to standards such as ISO/IEC 27030, NISTIR 8228, and IEEE P2413 ensures a

structured and comprehensive defense. Overall, a combination of robust architecture, advanced security mechanisms, and proactive monitoring is essential for secure, reliable, and scalable IoT ecosystems.

Bibliography:

(n.d.). Retrieved from www.checkpoint.com: https://www.checkpoint.com/cyber-hub/network-security/what-is-iot/iot-security-architecture/

(n.d.). Retrieved from www.checkpoint.com: https://www.checkpoint.com/cyber-hub/network-security/what-is-embedded-security/

(n.d.). Retrieved from www.geeksforgeeks.org: https://www.geeksforgeeks.org/computer-networks/architecture-of-internet-of-things-iot/

(n.d.). Retrieved from www.geeksforgeeks.org: https://www.geeksforgeeks.org/ethical-hacking/iot-devices-vulnerability-and-attack-vectors/?utm_source=chatgpt.com

(n.d.). Retrieved from ciet.ncert.gov.in: https://ciet.ncert.gov.in/storage/app/public/files/17/Workshop_and_training_files/dnse/Presentation-5.pdf?utm_source=chatgpt.com

(n.d.). Retrieved from www.geeksforgeeks.org: https://www.geeksforgeeks.org/ethical-hacking/iot-devices-vulnerability-and-attack-vectors/?utm_source=chatgpt.com

(n.d.). Retrieved from en.wikipedia.org/: https://en.wikipedia.org/wiki/Replay_attack?utm_source=chatgpt.com

(n.d.). Retrieved from nfosecacademy.com: https://infosecacademy.com/recent-iot-security-breaches-what-you-need-to-know/?utm_source=chatgpt.com

Ghadi Shaheen, F. A. (2024). A Survey on IoT Security: IoT Architecture, Security Issues, Challenges, and Solutions. *International Journal of Computer Applications*.