IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, October 2026
Impact Factor: 8.2

# Comparative Analysis of IoT Security Architectures: A Context-Aware Security–Resource Suitability Framework

**Dr. S. B. Sarvaiya[1], Vedanti C. Yawalkar[2], Sakshi K. Rohankar[3]**
Head, Department of MCA[1]
Students, Department of MCA[2-3]
Vidya Bharati Mahavidyalaya, Amravati, Maharashtra, India
sarvaiya.shilpa@gmail.com, vedantiyawalkar21@gmail.com, sakshirohankar9@gmail.com

**Abstract**: *The Internet of Things (IoT) links sensors, cameras, appliances, vehicles, medical devices and industrial controllers to networks and cloud platforms. This reach creates security problems that conventional networks rarely face: mixed hardware, scarce resources, devices that stay in service for years, wireless links and sensitive data. This paper compares three representative IoT security architectures, the three-layer, five-layer and Fog/Edge-based models, using published literature and recognised cybersecurity guidance. Each is examined along seven dimensions: security coverage, performance, scalability, privacy, resource efficiency, manageability over the device lifecycle, and interoperability. The main contribution is a Context-Aware Security–Resource Suitability Index (SRSI), which reweights these dimensions to suit the application instead of declaring one architecture best in every case. Literature-informed scores are applied to healthcare, smart-home and industrial or agricultural settings. Fog/Edge gives the best overall balance in every scenario tested, while the three-layer model stays attractive where low complexity and frugal resource use come first. The study also argues that lifecycle manageability deserves the same attention as traditional security metrics. SRSI is offered as a transparent decision-support method. Its scores are analytical, so validation on real testbeds with measured latency, energy, detection and resilience data is left for future work*

**Keywords**: Internet of Things, IoT security, security architecture, three-layer architecture, five-layer architecture, fog computing, edge computing, SRSI, authentication, privacy, resource constraints.

## I. INTRODUCTION

Over the past decade the Internet of Things has grown from isolated sensors into a broad ecosystem in which physical objects sense their surroundings, process data, communicate and, in some cases, act on the world. Common deployments include patient monitoring, smart homes, precision agriculture, transport, factory automation and urban infrastructure. Securing such systems differs from protecting a conventional network, because the devices vary widely in hardware, operating system, protocol and update cycle.

Protection must cover devices, communication links, applications and data, all within tight resource budgets. NIST describes a baseline of device capabilities that support common security controls and stresses that these capabilities should be chosen to fit the device and its use [2]. NIST has also revised its manufacturer-focused foundational activities in 2026, which reinforces the view that security spans the whole product lifecycle [1].

Prior studies have classified IoT threats by architectural layer and have proposed authentication, encryption, access control, intrusion detection, blockchain, machine learning and edge or fog techniques
[3]–[6]. The difficulty is that each architecture trades one strength against another. Strong central management can add communication and processing overhead, whereas a lightweight design leaves little capacity for advanced protection.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, October 2026
Impact Factor: 8.2

This paper therefore compares architectures instead of individual technologies, and takes the position that the choice should follow application needs and not a universal ranking.

### 1.1. Problem Statement:

Most IoT security studies assess a single mechanism such as authentication, encryption or intrusion detection, and architecture-level comparisons tend to be qualitative. Deployments also differ sharply in how much latency, privacy exposure, resource use and operational complexity they can tolerate. A simple method is needed to compare architectures on shared dimensions and to adjust that comparison for each application context.

### 1.2. Aim:

The aim is to compare representative IoT security architectures and to build a transparent, context-aware framework that helps select one according to security, performance, scalability, privacy, resource and operational needs.

### 1.3. Objectives:

1. To study representative layered and distributed IoT security architectures.
2. To identify the major IoT security threats and requirements.
3. To compare the architectures on common evaluation dimensions.
4. To bring resource and lifecycle considerations into architecture selection.
5. To propose a Context-Aware Security–Resource Suitability Index (SRSI).
6. To demonstrate the framework in different application contexts.
7. To identify research gaps and the validation work still needed.

### 1.4. Research Questions:

• RQ1: What are the main security characteristics and limitations of the three-layer, five-layer and Fog/Edge-based architectures?
• RQ2: How do they differ in security, performance, scalability, privacy and resource efficiency?
• RQ3: Does adding lifecycle manageability and interoperability improve architecture-level comparison?
• RQ4: Can application-specific weighting give a more useful recommendation than a single fixed ranking?
• RQ5: What evidence and experiments are needed to validate SRSI?

## II. RESEARCH METHODOLOGY

The study combines a literature review with comparative analysis. It does not claim an independent penetration-testing benchmark. Evidence comes from peer-reviewed studies, standards and recognised technical guidance on layered IoT security, emerging security technologies, access control, edge and fog security, and IoT cybersecurity baselines [1]–[8]. Older foundational works are kept where they define widely used architecture concepts, and the analysis weighs security effectiveness against operating cost, device limits and lifecycle issues.

Three architecture models were chosen because they stand for different design philosophies: (i) the three-layer model of perception, network and application layers; (ii) the five-layer model, which adds transport, processing and business functions; and (iii) a Fog/Edge-based model in which security and processing are shared among devices, edge or fog nodes and the cloud.

Seven dimensions are used for comparison: Security Coverage (SC), Performance (PE), Scalability (SCa), Privacy (PR), Resource Efficiency (RE), Manageability/Lifecycle Support (ML) and Interoperability (IN). Each is scored from 1 to 5. These scores are analytical judgements informed by the literature, not measurements from a shared testbed, so they illustrate the framework and make no claim of universal empirical performance.

The suitability index is calculated as follows:

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, October 2026
Impact Factor: 8.2

SRSI = 20 \sum_{i=1}^{7} w_i s_i, \qquad \sum_{i=1}^{7} w_i = 1 Here w_i is the normalised importance weight of dimension i and s_i is its 1–5 score, so the result lies on a 0–100 scale. The comparison runs in two stages. Stage 1 gives a baseline using general IoT priorities. Stage 2 changes the weights for each application context, which prevents any one architecture from being treated as best everywhere.

## III. SECURITY REQUIREMENTS AND THREAT LANDSCAPE

Attacks can occur at several points. On devices, attackers may exploit weak credentials, insecure firmware, exposed interfaces, physical tampering or poor update mechanisms. On communication links they may eavesdrop, replay messages, intercept traffic, jam signals or manipulate routing. At the application and cloud level they may target APIs, authentication services, databases and user privacy. Compromised devices can also be drafted into botnets and used for denial-of-service attacks, as the Mirai episode showed [14].

The resulting requirements include device identification, secure configuration, authentication, authorisation, confidentiality, integrity, availability, secure updates, logging, vulnerability management, privacy and recovery. NIST's baseline lists device capabilities that support common controls [2], and ETSI EN 303 645 sets baseline security and data-protection provisions for consumer IoT, including protected storage of sensitive security parameters [7].

Resource limitation is a central architectural challenge. Many devices have little processing power, memory, storage, battery or bandwidth, and strong cryptographic or monitoring functions can raise energy use and delay. Any architecture comparison therefore has to treat security and resource cost together.

TABLE I- Major IoT security threats and architectural responses:

| Threat | Typical target | Architectural response |
|---|---|---|
| Weak or default credentials | Device layer | Unique identity, authentication, credential management |
| Eavesdropping | Communication layer | Encryption, secure channels, key management |
| Man-in-the-middle | Network and transport | Mutual authentication, integrity protection |
| Malware and botnets | Device and network | Secure boot, updates, anomaly detection, segmentation |
| DDoS and resource exhaustion | Network and cloud | Rate limiting, edge filtering, distributed monitoring |
| Data leakage | Application and data | Encryption, access control, privacy controls |
| Firmware vulnerability | Device lifecycle | Signed updates, vulnerability management, secure update process |
| Privacy violation | Application and data | Data minimisation, access control, local or edge processing |

## IV. REPRESENTATIVE IoT SECURITY ARCHITECTURES

### 4.1. Three-Layer Architecture:

The three-layer model has a perception layer of sensors and actuators, a network layer that carries data, and an application layer that offers services to users. Its appeal is conceptual simplicity and modest complexity. Its weaknesses are that security duties can pile up on limited device or network components, and that processing and business functions are not separated explicitly [3], [9].

### 4.2. Five-Layer Architecture:

The five-layer model separates perception, transport, processing, application and business functions. The added processing and business layers allow clearer functional separation, finer security controls, policy management and analytics. The price is higher architectural complexity and greater management overhead [3], [9].

### 4.3. Fog/Edge-Based Architecture:

Fog/Edge designs place selected computation, filtering, analytics and security functions close to the devices. This can reduce latency, avoid sending all raw data to the cloud, and support local anomaly detection and privacy-sensitive

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, October 2026
Impact Factor: 8.2

processing. The cost is more trust boundaries, more nodes to manage and a larger attack surface. Work on emerging IoT security technologies treats edge and fog computing as both an opportunity and a source of new risk [4], [6].

Table1- Layer structure of the three architectures:

| Position | Three-layer | Five-layer | Fog/Edge |
|---|---|---|---|
| 1 | Perception | Perception | Devices |
| 2 | Network | Transport | Edge/fog nodes |
| 3 | Application | Processing | Cloud |
| 4 | — | Application | Application |
| 5 | — | Business | — |

All three models rely on the same control set: identity, authentication, encryption, access control, monitoring and secure updates. They differ in where those controls are placed and who operates them.

## V. PROPOSED CONTEXT-AWARE SRSI FRAMEWORK

The SRSI extends a conventional architecture comparison in two ways. It adds manageability/lifecycle support and interoperability to the usual security, performance and resource dimensions, and it lets the weight of each dimension change with the application.

The lifecycle dimension matters because an IoT system is not secure merely at the moment of deployment. Devices may run for years and need secure configuration, patching, monitoring, vulnerability handling and end-of-support planning, which is why NIST's 2026 manufacturer guidance frames security activities across the whole product lifecycle [1]. The framework is also transparent: every score and weight can be inspected, changed and recalculated, which suits an academic decision-support study better than an opaque model.

### 5.1. Evaluation Dimensions:

1. Security Coverage: the ability to provide authentication, authorisation, confidentiality, integrity, availability, monitoring and resilience.
2. Performance: the effect of security controls on latency, throughput and responsiveness.
3. Scalability: the ability to support growth in devices, traffic and services.
4. Privacy: the ability to limit needless data exposure and support privacy-preserving processing.
5. Resource Efficiency: suitability for limited processor, memory, storage, bandwidth and energy.
6. Manageability/Lifecycle Support: the ability to support configuration, monitoring, updates, incident response and long-term maintenance.
7. Interoperability: the ability to work across varied devices, protocols, gateways, cloud and application environments.

### 5.2. Architecture Scores

TABLE 2-Literature-informed architecture scores (1–5):

| Dimension | Three-layer | Five-layer | Fog/Edge |
|---|---|---|---|
| Security Coverage | 4 | 5 | 4 |
| Performance | 5 | 3 | 4 |
| Scalability | 4 | 5 | 5 |
| Privacy | 3 | 4 | 5 |
| Resource Efficiency | 5 | 3 | 4 |
| Manageability/Lifecycle | 3 | 4 | 5 |
| Interoperability | 4 | 5 | 4 |

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, October 2026
Impact Factor: 8.2

### 5.3. Baseline Index and Context Weights:

For a general-purpose IoT environment the baseline weights are Security Coverage 25%, Performance 15%, Scalability 15%, Privacy 15%, Resource Efficiency 15%, Manageability/Lifecycle 10% and Interoperability 5%. Applying the formula gives illustrative baseline values of 81 for the three-layer, 83 for the five-layer and 88 for the Fog/Edge architecture. These are not measured security scores; they show how the framework turns qualitative evidence into a transparent index. Table III gives the weights used for each context.

TABLE 3- Context-specific weights (%):

| Dimension | General | Healthcare | Smart home | Industrial/agricult ure |
|---|---|---|---|---|
| Security Coverage | 25 | 30 | 20 | 25 |
| Performance | 15 | 10 | 15 | 15 |
| Scalability | 15 | 10 | 15 | 20 |
| Privacy | 15 | 20 | 15 | 10 |
| Resource Efficiency | 15 | 10 | 20 | 15 |
| Manageability/Lifecycle | 10 | 15 | 10 | 10 |
| Interoperability | 5 | 5 | 5 | 5 |

TABLE 4- Context-aware SRSI results (0–100):

| Application context | Three-layer | Five-layer | Fog/Edge | Preferred | Lead over runner-up |
|---|---|---|---|---|---|
| General IoT | 81 | 83 | 88 | Fog/Edge | 5 |
| Healthcare | 77 | 85 | 89 | Fog/Edge | 4 |
| Smart home | 82 | 81 | 88 | Fog/Edge | 6 |
| Industrial/agri culture | 82 | 84 | 88 | Fog/Edge | 4 |

## VI. RESULTS AND DISCUSSION

### 6.1. Interpretation of the Results:

Fog/Edge scores highest in all four contexts, between 88 and 89, because it combines local processing, distributed monitoring, scalability and privacy advantages. Its lead is narrowest in healthcare and in industrial or agricultural settings (4 points over the five-layer model) and widest in the smart home (6 points over the three-layer model).

Context weighting is useful even where the winner does not change, because the order of the other two architectures does. In healthcare, where security, privacy and lifecycle support carry the most weight, the three-layer model drops to 77 and the five-layer model reaches 85. In the smart home, where resource efficiency is weighted at 20%, the three-layer model rises to 82 and overtakes the five-layer model at 81. The three-layer design therefore remains attractive when simplicity and frugal resource use dominate, while the five-layer design offers stronger functional separation and interoperability at the cost of extra processing and management overhead.

A future measured study could replace the illustrative scores with benchmark results without changing the framework itself.

### 6.2. Comparison with Existing Research:

Earlier surveys mapped threats and security solutions onto three-layer or four-layer IoT models and highlighted how hard it is to secure constrained devices, while other work examined access control, emerging technologies and secure architectural solutions [3]–[6], [10]–[12]. These studies establish the value of layered security, but none by itself offers a single transparent, context-aware index that joins security with resource, lifecycle and interoperability concerns.

SRSI is therefore positioned as a decision-support layer over existing architectural knowledge. It does not replace detailed threat modelling or formal security evaluation. It gives a repeatable way to compare alternatives before implementation and shows which dimensions need deeper technical validation.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, October 2026
Impact Factor: 8.2

TABLE 5- Proposed approach compared with a basic architecture comparison:

| Feature | Basic comparison | Proposed SRSI approach |
|---|---|---|
| Architecture comparison | Yes | Yes |
| Security, performance and resource factors | Usually | Yes |
| Privacy explicitly weighted | Sometimes | Yes |
| Lifecycle and manageability | Often limited | Explicit |
| Interoperability | Often qualitative | Explicit |
| Application-specific weights | Rare | Yes |
| Transparent 0–100 index | Not always | Yes |
| Support for future measured data | Limited | Yes |

### 6.3. Research Gaps and Original Contribution:

• Gap 1, fixed rankings: a single ranking hides the fact that applications have different priorities. SRSI introduces context-specific weights.

• Gap 2, security-only comparison: security cannot be judged apart from resource limits and performance. SRSI includes both.

• Gap 3, deployment lifecycle: long-lived devices need secure configuration, updates, monitoring and end-of-support management. SRSI adds a lifecycle dimension.

• Gap 4, decision transparency: complex models are hard for practitioners to interpret. SRSI shows its scores and weights so that a recommendation can be challenged or adjusted.

The original contribution is a structured analytical framework that combines seven architecture-level dimensions with application-specific weighting. It is not a new cryptographic algorithm or intrusion-detection model, and its value is to be tested in future work on common IoT datasets and real testbeds.

## VII. SECURITY ENHANCEMENT STRATEGIES:

Several techniques can strengthen any of the three architectures, and each carries its own cost.

• Machine learning. Anomaly detection, device-behaviour profiling and intrusion detection can run at edge or cloud nodes. The models themselves need protected training data, monitoring and defences against adversarial manipulation [6].

• Blockchain and distributed ledgers. These may support selected identity, integrity or audit uses, but their computation, storage and communication overhead must be evaluated before they are placed on constrained devices [4], [12].

• Lightweight cryptography and hardware protection. Secure boot, signed firmware, hardware-backed key storage, strong device identity and secure update mechanisms are the foundation for constrained devices. ETSI EN 303 645 and the NIST baseline give practical requirements that can be mapped into the architecture evaluation [2], [7].

• Zero-trust principles. Requiring explicit authentication, authorisation and continuous evaluation, instead of trusting a request because of its network location, complements any layered or distributed design [13]. In IoT it must be applied with attention to device capability and operational overhead.

These measures work best in combination. A hardware-protected device identity, local enforcement at an edge node, continuous verification of access and centrally managed updates address different threats, which is why a hybrid is usually stronger than any single approach.

## VIII. LIMITATIONS AND FUTURE VALIDATION

### 8.1. Limitations:

First, the scores are analytical and literature-informed; they do not come from one controlled experimental environment. Second, the three architecture categories are abstractions, and real deployments often mix them. Third,

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, October 2026
Impact Factor: 8.2

the weights express reasonable illustrative priorities and were not gathered from a survey of domain experts. Fourth, security performance varies with protocol choice, cryptographic implementation, device hardware and threat model.

SRSI also compresses many considerations into one number, so a high index must not be read as proof of security. Threat modelling, penetration testing, protocol verification, vulnerability assessment and operational monitoring remain necessary.

### 8.2. Future Validation Plan:

A follow-up study can implement representative versions of the three architectures on a common IoT testbed and measure end-to-end latency, processor use, memory use, energy consumption, network overhead, authentication delay, detection latency, false-positive and false-negative rates, recovery time and resilience under controlled attack traffic. SRSI can then be recalculated from measured values in place of the qualitative scores.

Sensitivity analysis should vary the weights to see whether the preferred architecture changes under different priorities, and expert evaluation by IoT security practitioners could validate the weights themselves. Later versions could add risk severity, deployment cost, compliance requirements, device lifetime and carbon or energy impact. A software tool that lets users choose a domain, enter scores, adjust weights and receive a transparent recommendation is a natural next step.

## IX. RECOMMENDATIONS:

1. Build defence in layers instead of relying on one control.
2. Give every device a unique identity and strong authentication.
3. Protect communication and sensitive data with suitable encryption and integrity checks.
4. Use secure boot, signed firmware and secure updates wherever the hardware allows.
5. Build privacy and data minimisation into the architecture from the start.
6. Choose edge or fog processing when latency, privacy or bandwidth needs justify the extra management effort.
7. Judge security controls together with their processor, memory, energy and communication cost.
8. Plan for the full lifecycle, including vulnerability handling and end of support.
9. Treat AI and machine learning as an added monitoring layer, not a replacement for deterministic controls.
10. Confirm architecture decisions with real measurements before production deployment.

## X. CONCLUSION:

IoT security takes more than choosing an authentication method or an encryption algorithm. Constrained devices, mixed communication technologies, distributed processing, sensitive data and long operating lives pull in different directions, so the security architecture has to balance competing demands.

This paper compared the three-layer, five-layer and Fog/Edge-based architectures on security coverage, performance, scalability, privacy, resource efficiency, lifecycle manageability and interoperability. In the illustrative comparison Fog/Edge gave the strongest overall balance, while simpler designs stay relevant where low complexity and resource efficiency matter most.

The main contribution is the Context-Aware Security–Resource Suitability Index. Instead of naming one universal winner, SRSI lets the importance of each dimension follow the application, which makes the comparison more transparent and easier to adapt to healthcare, smart-home, industrial and agricultural settings. The framework is presented as a decision-support model and not as an experimentally validated benchmark. Its next step is empirical validation on a common testbed with measured resource and security metrics, sensitivity analysis and expert assessment, to learn whether its recommendations hold under realistic workloads and attacks.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, October 2026
Impact Factor: 8.2

## REFERENCES

[1] M. Fagan, K. Megas, B. Cuthill, J. Marron, and B. Hoehn, "Foundational Cybersecurity Activities for IoT Product Manufacturers," NISTIR 8259 Rev. 1, National Institute of Standards and Technology, Apr. 2026.
[2] M. Fagan, K. Megas, K. Scarfone, and M. Smith, "IoT Device Cybersecurity Capability Core Baseline," NISTIR 8259A, National Institute of Standards and Technology, 2020.
[3] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, vol. 76, pp. 146–164, 2015.
[4] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395–411, 2018.
[5] O. Yousuf and R. N. Mir, "A survey on the Internet of Things security," International Journal of Information Security, 2019.
[6] A. Ghaffari, N. Jelodari, S. Pouralish, N. Derakhshanfard, and B. Arasteh, "Securing internet of things using machine and deep learning methods: a survey," Cluster Computing, vol. 27, pp. 9065–9089, 2024.
[7] ETSI, "Cyber Security for Consumer Internet of Things: Baseline Requirements," ETSI EN 303 645 V3.1.3, 2024.
[8] M. Fagan, J. Marron, K. G. Brady Jr., B. B. Cuthill, K. N. Megas, and R. Herold, "IoT Non-Technical Supporting Capability Core Baseline," NISTIR 8259B, National Institute of Standards and Technology, 2021. doi: 10.6028/NIST.IR.8259B.
[9] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347-2376, 2015.
[10] P. Williams, I. K. Dutta, H. Daoud, and M. Bayoumi, "A survey on security in Internet of Things with a focus on the impact of emerging technologies," Internet of Things, vol. 19, Art. no. 100564, 2022. doi: 10.1016/j.iot.2022.100564.
[11] A. A. Laghari, H. Li, A. A. Khan, Y. Shoulin, S. Karim, and M. A. K. Khani, "Internet of Things (IoT) applications security trends and challenges," Discover Internet of Things, vol. 4, Art. no. 36, 2024. doi: 10.1007/s43926-024-00090-5.
[12] H. Pourrahmani, A. Yavarinasab, A. M. H. Monazzah, and J. Van Herle, "A review of the security vulnerabilities and countermeasures in the Internet of Things solutions: A bright future for the Blockchain," Internet of Things, vol. 23, Art. no. 100888, 2023. doi: 10.1016/j.iot.2023.100888.
[13] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST Special Publication 800-207, National Institute of Standards and Technology, 2020.
[14] M. Antonakakis et al., "Understanding the Mirai botnet," in Proc. 26th USENIX Security Symposium, pp. 1093-1110, 2017