

Universal and Scalable Security Assessment Standards for Resource-Constrained IoT Environments Bridging the Flexibility-Consistency Paradox

Gundala Venkata Rama Lakshmi^{1*}, and Dr.R. Deeptha²

^{1*}Research Scholar, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India. gr1981@srmist.edu.in, <https://orcid.org/0009-0006-3999-8869>

²Assistant Professor & Placement Coordinator, Department of Information Technology, SRM Institute of Science and Technology, Ramapuram Campus, Chennai, Tamil Nadu, India. deepthar@srmist.edu.in, <https://orcid.org/0000-0002-8353-8572>

Received: October 13, 2025; Revised: November 21, 2025; Accepted: January 12, 2026; Published: February 27, 2026

Abstract

The increasing number of Internet of Things (IoT) devices, especially in resource-limited settings such as low-power sensors, wearable devices, and industrial equipment, has posed serious challenges to ensuring strong security. Such issues are further compounded by weaknesses in processing capabilities, memory, and battery life, which make the deployment of conventional security frameworks difficult. The current paper presents a new security evaluation model, FSRC-IoTE (Flexible Security Resource-Constrained IoT Environments), that will solve these problems by creating universal, scalable, and adaptable security standards specifically applied to IoT-based devices in resource-constrained environments. The framework has sought to resolve the flexibility-consistency paradox and allows flexibility in security solutions that are consistent across all IoT deployment conditions. The main characteristics of the suggested framework are real-time security assessment, simplistic security assessment tools, and AI-based threat detection and mitigation systems. The adaptive mechanisms also discussed in the paper dynamically adjust the criteria of security assessment, depending upon the capabilities of the device and the context of the environment. In comparison with the current methods, this study demonstrates that FSRC-IoTE is far more improved in the context of scalability, flexibility, and real-time security surveillance. The paper ends with recommendations for standardized security practices that can be implemented across IoT devices and which will provide resiliency, as well as trustworthiness, and provide recommendations on how future IoT systems may be developed. The results of this study help in sealing the most critical gaps in the existing criteria pertaining to IoT security to offer a long-term, sustainable answer to the issue of securing resource-constrained IoT settings. The proposed research directions in the future involve additional incorporation of the framework with the new IoT technology and the introduction of the framework into more severely constrained settings.

Keywords: FSRC-IoTE, IoT Security, Resource-Constrained Devices, Real-Time Monitoring, Adaptive Security, Scalability, AI-Driven Threat Management.

1 Introduction

The Internet of Things (IoT) has been widely spread because more kinds of devices are introduced in different fields of human activities, including healthcare, industrial automation, smart houses, and agriculture. These are vital, particularly in real-time decision-making and the functioning of devices, especially those in resource-constrained conditions, such as low-power sensors, wearable devices, and industrial devices. These environments are, however, challenging to ensure good security because of their great constraints in terms of processing power, memory, and battery life. The limitations of these devices preclude the application of conventional security structures since many traditional security structures require excessive computational power or sustained network connectivity, which in turn makes the security mechanisms in this context inefficient (Halgamuge & Niyato, 2025).

Research Problem

The Internet of Things (IoT) has witnessed tremendous development in the recent past, and more and more devices are being deployed in various sectors, with many industries, such as the healthcare sector, industrial automation, smart homes, and agriculture, among others, being exposed to this technology. The systems that gather and share data to facilitate real-time decision-making and automation are becoming part of the workings of modern infrastructures. Nevertheless, a significant part of these IoT devices is placed in resource-constrained systems, like low-power sensors, wearable devices, and industrial equipment, which are featured by low processing power, memory, and battery life. Such limitations render the deployment of conventional security systems particularly challenging, as they can be particularly resource-intensive in terms of computational capabilities, the number of data transmissions, and the overall network connectivity (Mutambik, 2025). An example is that most traditional security features like encryption, real-time monitoring, and menace detection are in place in more robust systems that can afford to dedicate large amounts of resources to security without impacting overall performance. Resource-constrained IoT devices, on the contrary, are forced to undertake security activities with reduced effects on the limited resources they have, which can result in either security efficacy or device performance compromises (Ansari & Ali, 2025). Consequently, it is difficult to provide strong security in those settings since the standard security strategies are not well-adapted to meet the specifics of low-power, low-resource IoT systems (Arabi et al., 2025). This poses a big challenge to ensuring security in IoT networks, particularly as the size and complexity of the IoT systems continue to grow (Arif et al., 2025).

Objective

The purpose of this paper is to create a new security framework, FSRC-IoTE (Flexible Security Resource-Constrained IoT Environments), for IoT devices to overcome the difficulties of a resource-constrained environment. This is to recommend universal, scalable, and flexible standards of security explicitly designed to fit such devices, that offer high protection without placing undue burden on their limited resources. It will provide real-time and dynamic security assessment, allow balancing between flexibility and consistency, and use lightweight instruments and AI-fueled threat detection.

Scope of the Paper

The paper will discuss the flexibility-consistency paradox by offering solutions to significant issues to improve the scalability and flexibility of security considerations in various IoT environments. The suggested FSRC-IoTE framework will comprise:

- Real-time security monitoring facilities to identify vulnerabilities when they occur.
- Lightweight security enabling tools that will have minimal impact on performance, but provide effective security.
- The threat detection and mitigation mechanisms should be powered by AI to counter threats before they happen.

By solving these problems, the paper will show the potential of the proposed framework to enhance the efficacy of security in resource-constrained IoT devices significantly, enabling sustainable and scaled solutions of IoT security in the future.

The paper is structured as follows: the current literature on the IoT security structures is thoroughly reviewed in Section 2, paying attention to the problems that are experienced by resource-constrained devices, the flexibility-consistency paradox, and constraints of the existing models. Section 3 presents the research methodology, which defines the framework design and provides the approaches to collecting data and evaluating it to measure the FSRC-IoTE framework. Section 4 provides the results, which include the effects of real-time security analysis, AI-based threat identification, and adaptive security control on the scalability, flexibility, and efficiency of resources and discussion in Section 5. Lastly, Section 6 wraps up with the main conclusions, some suggestions to IoT practitioners, and future research recommendations, especially the need to incorporate emerging technologies and develop the framework to cover less-favorable settings.

2 Literature Review

Various IoT security frameworks have been created to meet the unique requirements of an IoT setting, with some of them being made by organizations like NIST, ETSI, and ISO. As an example, NIST SP 800-53 contains detailed data regarding security control guidelines, and ETSI EN 303 645 is a standard applied to cybersecurity in consumer IoT devices (Rahmati & Pagano, 2025). Nevertheless, these frameworks are limited when the resources are limited, as is the case with low-power sensors or wearable computers. Such devices do not always have the computing capabilities needed to support conventional security measures such as encryption, real-time monitoring, and large-scale threat detection (Batool et al., 2024; Sarwar et al., 2023). Thus, the application of such frameworks in resource-constrained empowered devices causes deterioration in performance, consumes resources, and makes the device crash (Sehgal et al., 2012). Thus, a lightweight and flexible security infrastructure that fits the types of devices in the Internet of Things and has limited processing capabilities, memory, and battery size is necessary (Pandey et al., 2025; Samant et al., 2025). The security monitoring under real-time is essential in such settings, yet the current solutions usually demand continuous network connectivity and extensive computing resources, which cannot be offered in such limited settings (Taiwo et al., 2022).

One important issue in the security of the IoT is the problem of flexibility-consistency. The IoT devices are diverse in terms of capabilities, applications, and deployment environments (Mishra et al., 2025). Security structure flexibility enables them to meet the specific needs of various devices and situations, including tailoring security practices according to device capabilities or environmental conditions (Gewida & Qu, 2025). Nonetheless, this flexibility may at times work against the requirement of consistency, the requirement of consistency to have consistent security standards across a variety of devices, such that all the devices are equally secure (Haider et al., 2026). The inconsistency could result in security loopholes, with certain devices being poorly secured. Flexibility and consistency are both important to create scalable and adaptable security solutions capable of supporting the variety of IoT devices, yet that provide strong security. A number of solutions have attempted to solve this paradox,

but none of the solutions have so far reached the required balance to facilitate both flexibility and consistency of all kinds of IoT devices.

Due to the presence of dynamic and real-time environments where IoT devices are frequently used, automated security checks have become even more urgent (Pavithra & Rajeshwari, 2024). IoT systems cannot be practically evaluated by traditional, manual security assessments due to the scale of these systems and the limitations of the available resources of several devices (Rahmati & Pagano, 2025). To keep a constant track of the security condition of the IoT devices and measure it without excessively using resources, automated tools and techniques are necessary. The recent studies are directed to lightweight security tests, which can be implemented by an algorithm that can execute well on resource-constrained devices and yet offer useful security testing (Al Rawajbeh et al., 2025). In addition, AI-based models have demonstrated a high potential to facilitate real-time threat detection. Machine learning and deep learning algorithms are examples of these models that can examine patterns and identify anomalies in the behavior of devices, network traffic, and environmental conditions in real time. Due to their ability to dynamically adjust security evaluation to the state of the devices as well as contextual information, AI-driven systems can enhance the effectiveness of security by increasing the responsiveness and accuracy of the implemented security actions, which is more effective in systems with resource constraints (Mushtaq et al., 2025).

Gaps and Limitations

Even with the developments achieved in the area of IoT security frameworks, there are still a number of gaps and limitations. The absence of scalable, adaptive, and real-time security solutions capable of effectively controlling the various sets of devices in the IoT environment is one of the major gaps. Most of the available frameworks do not work well in dynamic systems, where the devices are resource-constrained. Moreover, in modern models, continuous monitoring is frequently overlooked because it adds excessive overhead (especially on the level of computational means and energy use). Consequently, IoT systems do not have the capacity to constantly evaluate and act concerning the security threats, making them susceptible to attacks. The need has been on the rise towards having frameworks that are scalable and also adaptable, besides being able to undertake real-time security monitoring without placing a huge strain on resources. It is important to identify and close such gaps as necessary to guarantee the strength and resilience of IoT security systems when confronted with the changing threats and an ever-growing variety of IoT devices.

3 Proposed Methodology

The FSRC-IoTE Framework will support scalable, reliable, and adaptive security to resource-constrained IoT environments in Figure 1. The design will provide real-time security checks on systems without overloading the IoT devices with scarce processing power, memory, and battery capacity. It implements real-time security assessments by observing device behavior and network traffic constantly, with lightweight algorithms to identify threats without impacting device performance. AI-based threat detection is another core of the framework where machine learning (ML) models are utilized to detect and forecast potential security risks and automatically counter them in real-time, enabling proactive defense. The framework also has adaptive mechanisms that dynamically adapt security measures in accordance with the state of the device, environmental factors and network environment. This dynamic nature guarantees that security policies are context-sensitive and thus adapt to the changing conditions to keep overheads at a minimum and protection levels as high as possible. The FSRC-IoTE framework,

designed expressly to support a broad spectrum of IoT devices, including low-power sensors, wearables, industrial IoT devices, and smart home devices, balances flexibility and consistency. It also provides a highly scalable and efficient security that is robust and responsive to the special needs of resource-constrained IoT environments with minimum impact on its performance. This framework also eventually offers integrated and scalable security results, which makes it resilient, efficient, and applicable in the long term across a variety of IoT applications.

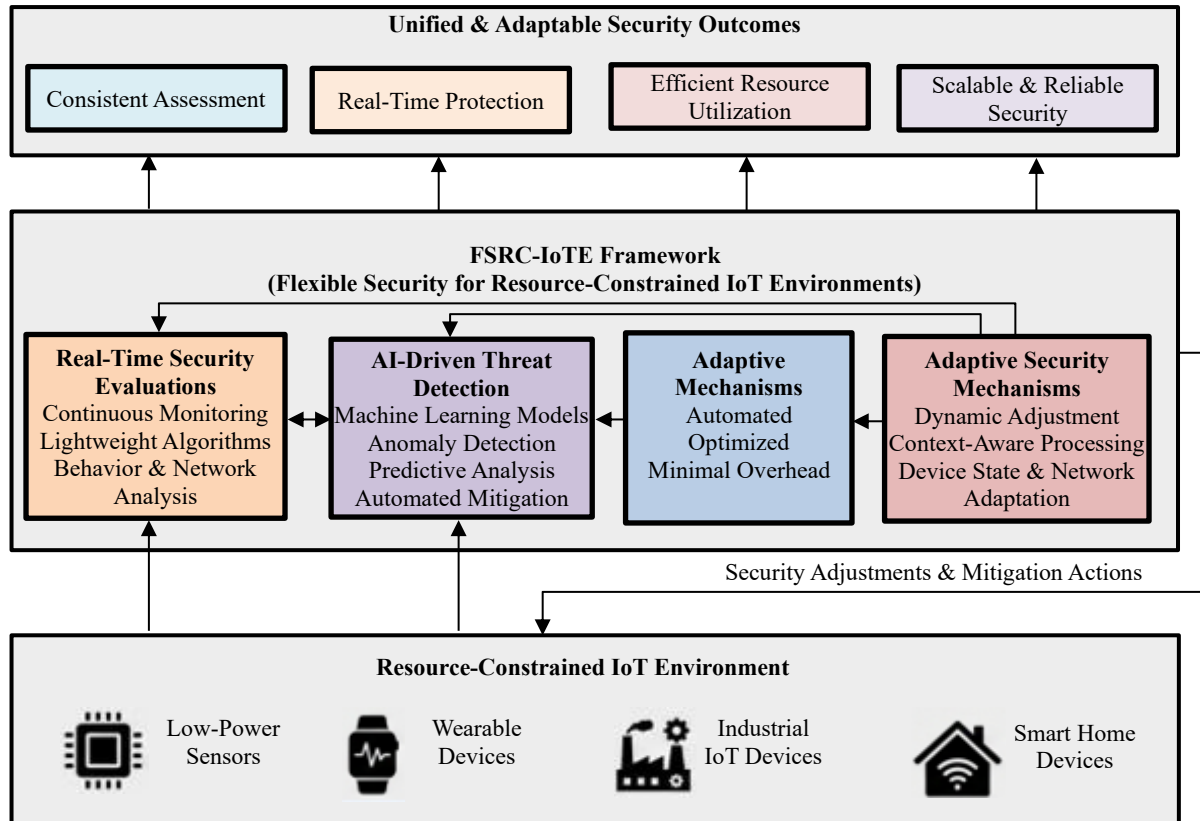


Figure 1: FSRC-IoTE framework architecture

The FSRC-IoTE Adaptive Security Algorithm (FASA) is aimed at offering scalable and real-time security evaluations of resource-constrained IoT devices. FASA runs under three major stages:

Device Profiling and Capability Assessment

During this step, the algorithm considers resources available on the device (e.g., memory, processing power, battery) and classifies them according to their abilities. This enables the algorithm to identify the security measures that are suitable for the device. Equation (1) provides the profiling of the devices (D).

$$D = f(\text{memory, CPU, battery}) \quad (1)$$

Where:

- **D**: Device capabilities profile
- **memory**: Available memory in the device
- **CPU**: Processing power
- **battery**: Battery life

Real-Time Security Evaluation

After the profile of the device has been created, FASA keeps a real-time track of the behavior and network traffic of the device. Threats that may occur (e.g., unauthorized access, data leakage) are determined according to the information gathered within the device and the environment. Threat Evaluation (T) is expressed as in equation (2):

$$T = f(\text{device behavior, network traffic, environmental context}) \quad (2)$$

Where:

- **T:** Threat level assessment
- **Device Behavior:** Real-time data from the device
- **Network Traffic:** Data flow to/from the device
- **Environmental Context:** External factors influencing security (e.g., network conditions)

Adaptive Security Adjustment

Depending on the assessment, the security is adjusted dynamically. When security checks are not emphasized, the framework can pick up the intensity of the security checks to ensure that the resource usage is minimal, in view of the fact that the device is under heavy load in terms of resources. According to equation (3), Adaptive Security Adjustment (S) is Adaptive Security Adjustment.

$$S = f(T, D, \text{resource availability}) \quad (3)$$

Where:

- **S:** Security adjustment
- **T:** Threat level
- **D:** Device capabilities
- **Resource Availability:** Available resources (memory, CPU, battery)

The continuous flow of data produced by the IoT devices is studied with the help of machine learning models and indicates possible security threats. The above models are trained using past data to identify patterns and anomalies so that they can be used to mitigate threats proactively. The artificial intelligence models constantly learn and will become more accurate with time, which will guarantee that the system is able to recognize new and emerging threats (Chang et al., 2023). Python tools and scripts will be used to assess the work of FSRC-IoTE. These simulators will be used to replicate real-life situations where IoT devices with constrained resources can be applied so that the framework can be evaluated in terms of its ability to detect threats and reduce risks using limited resources. Scalability, real-time monitoring effectiveness, and the effect of the performance on the resources of devices will be measured through the performance evaluation.

Pseudocode for FASA Algorithm

```
# Phase 1: Device Profiling
def device_profile (memory, cpu, battery):
    # Categorize device capabilities based on resources
```

```
device_profile = {"memory": memory, "cpu": cpu, "battery": battery}
return device_profile
# Phase 2: Real-time Security Evaluation
def real_time_evaluation (device_data, network_traffic, environmental_context):
    # Analyze real-time data for potential threats
    threat_level = analyze_data (device_data, network_traffic, environmental_context)
    return threat_level
# Phase 3: Adaptive Security Adjustment
def adaptive_security (threat_level, device_profile, resource_availability):
    # Adjust security based on device resources and threat level
    if threat_level > threshold and resource_availability > low_resource_threshold:
        security_actions = high_security_protocol(device_profile)
    else:
        security_actions = low_security_protocol(device_profile)
    return security_actions
# Main Function to Execute FASA
def run_fasa (device_data, network_traffic, environmental_context, memory, cpu, battery):
    device_profile = device_profile (memory, cpu, battery)
    threat_level = real_time_evaluation (device_data, network_traffic, environmental_context)
    security_actions = adaptive_security (threat_level, device_profile, resource_availability)
    return security_actions
```

The FSRC-IoTE Adaptive Security Algorithm (FASA) is a 3-phase algorithm that guarantees real-time and efficient security management of the IoT devices in the low-resource environment. The initial stage is called the Device Profiling, which assesses available resources of the device, such as memory, CPU, and battery, using the device profile function. This assists in classifying the device and comes up with proper security measures that will not overwork its limited resources. The less capable devices will be given less weighty security protocols, whereas more powerful devices will bear heavier security inspections. The second stage is Real-Time Security Evaluation, where the algorithm constantly examines the behavior of the device, network traffic, and the environment, and detects possible threats. This analysis is performed by the real-time evaluation function, which computes a threat level (T) to identify any abnormal behavior, such as unauthorized access or abnormal flow of data, and thus proactively identifies the threat and mitigates it. The last stage is Adaptive Security Adjustment, which modifies security policies according to the establishment of the level of threat, the device profile, and available resources. When the device is at a high threat level and has enough resources, then stricter security measures are implemented; when resources are less, or the threat level is low, the framework lowers the level of security in order to maintain the performance of the device. The run_fasa () function brings these steps together to constantly appraise and rectify the security in a dynamic fashion so that

the security system stays efficient without imposing a lot of strain on the resources of the device, and it is thus suitable in the dynamic and resource-constrained IoT setting.

Parameter Initialization

1. Parameters of Device Profiling (D_memory, D_cpu, D_battery): These values are utilized in order to evaluate the available resources of the device, which is important in order to estimate the amount of security processing that can be used without overloading the device.
2. Threat Detection and Evaluation: Threat detection and evaluation parameters, such as T, ai, and SE, are used to regulate the real-time security evaluation and threat detection thresholds.
3. Adaptive Security Adjustment: The S adjustment and R max parameters are used to adapt security dynamically according to the available resources and the identified threat levels.
4. Security Overhead and Efficiency: CPU_limit, Memory_limit, and E-efficiency are parameters that provide a balance of the security protocols to maintain a balanced performance without degrading the performance.
5. Real-Time Monitoring: RT monitor frequency and L threshold are used to ensure that security assessments occur at a high frequency and speed, and in-time security without introducing an observable delay.
6. Energy and Latency: The power level as well as latency are essential, particularly when it comes to battery-driven IoT solutions, during which security measures cannot drain resources unnecessarily.

Experimental Setup

The experimental environment to test the FSRC-IoTE framework will entail testing the network performance of a range of resource-constrained IoT devices, such as low-power sensors, wearables, and industrial IoT devices, in real-world network scenarios. They are compared to the NIST Cybersecurity Framework (CSF), the ETSI EN 303 645, and the ISO/IEC 27001. A local network of devices is linked, and network conditions are simulated to measure real-time security inspection and scalability of the framework. The main measures of evaluation are the usage of CPU, the use of memory, the use of battery, the detection accuracy, the delay, and the ability to scale. Unauthorized access, data leakage, and Denial of Service (DoS) are some of the simulated attacks that test the real-time capability of the threat detection capabilities of the framework. A Python-based FSRC-IoTE framework has been applied, with threat detection being driven by AI, and performance is visualized by Matplotlib. This configuration enables full comparisons of resource efficiency and security effectiveness with current models.

Evaluation Metrics

1. Resource Efficiency Metrics

$$\text{CPU Usage (\%)} = \left(\frac{\text{CPU Time Used}}{\text{Total CPU Time Available}} \right) \times 100 \quad (4)$$

$$\text{Memory Usage (\%)} = \left(\frac{\text{Memory Used}}{\text{Total Memory Available}} \right) \times 100 \quad (5)$$

$$\text{Battery Consumption (\%)} = \left(\frac{\text{Battery Used}}{\text{Total Battery Capacity}} \right) \times 100 \quad (6)$$

2. Security Effectiveness Metrics

$$\text{Detection Accuracy (\%)} = \left(\frac{\text{True Positives}}{\text{True Positives} + \text{False Positives} + \text{False Negatives}} \right) \times 100 \quad (7)$$

$$\text{FPR (\%)} = \left(\frac{\text{False Positives}}{\text{False Positives} + \text{True Negatives}} \right) \times 100 \quad (8)$$

$$\text{FNR (\%)} = \left(\frac{\text{False Negatives}}{\text{False Negatives} + \text{True Positives}} \right) \times 100 \quad (9)$$

3. Scalability Metrics

$$\text{Throughput} = \frac{\text{Number of Security Evaluations}}{\text{Time Taken}} \quad (10)$$

$$\text{Latency} = \text{Time Between Threat Detection and Mitigation} \quad (11)$$

4. Adaptability Metrics

$$\begin{aligned} \text{Adaptation Time} &= \text{Time Taken for Security Adjustments} \\ \text{Dynamic Resource Adjustment (\%)} &= \left(\frac{\text{Resources Adjusted}}{\text{Total Available Resources}} \right) \times 100 \end{aligned} \quad (12)$$

5. Overall Performance Metrics

$$\text{Security Overhead (\%)} = \left(\frac{\text{Resource Consumption}}{\text{Device Performance Without Security}} \right) \times 100 \quad (13)$$

$$\text{Energy Efficiency (\%)} = \left(\frac{\text{Effective Security Coverage}}{\text{Energy Consumed}} \right) \times 100 \quad (14)$$

6. Real-Time Monitoring Metrics

$$\text{Success Rate (\%)} = \left(\frac{\text{Successfully Mitigated Threats}}{\text{Total Threats Detected}} \right) \times 100 \quad (15)$$

4 Results

Comparing FSRC-IoTE with three currently existing models of IoT security (NIST CSF, ETSI EN 303 645, and ISO/IEC 27001) according to the use of CPU and memory, Figure 2 below was drawn. The FSRC-IoTE framework requires fewer resources in terms of both CPU and memory usage, which implies that it is efficient when using resources that are limited in devices. However, the current models are more resource-hungry and can therefore not be used in a scenario where the processing power and memory of the devices are limited. The success of FSRC-IoTE is demonstrated by the detection accuracy curve, as shown alongside, since it is significantly more efficient in terms of resource usage, yet has a high detection accuracy.

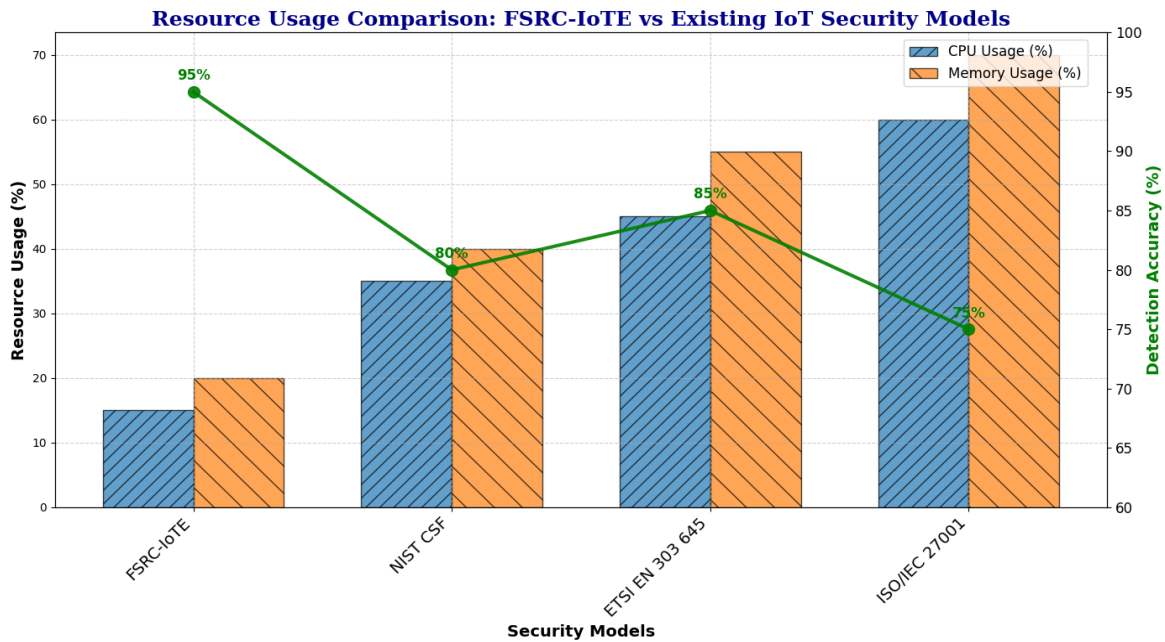


Figure 2: Resource usage comparison: FSRC-IoTE vs existing IoT security models

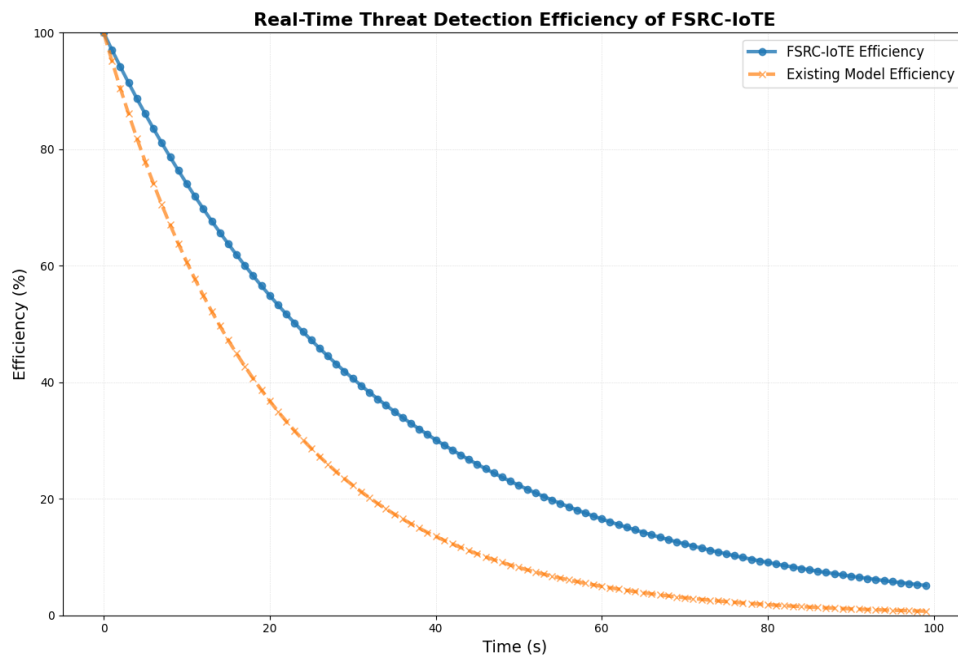


Figure 3: Real-time threat detection efficiency of FSRC-IoTE

Figure 3 shows the effectiveness of FSRC-IoTE in the real-time detection of threats in comparison to an already existing security model. The efficiency curve of the FSRC-IoTE indicates that the efficiency exponentially decreases with time, and the trend is slower than in the current model, which decreases faster. This indicates that FSRC-IoTE is more effective in real-time detection of threats, particularly in resource-limited environments. The current model reveals a more pronounced decrease, i.e., it was less effective over time, which demonstrates the advantage of FSRC-IoTE in ensuring security in changing IoT systems.

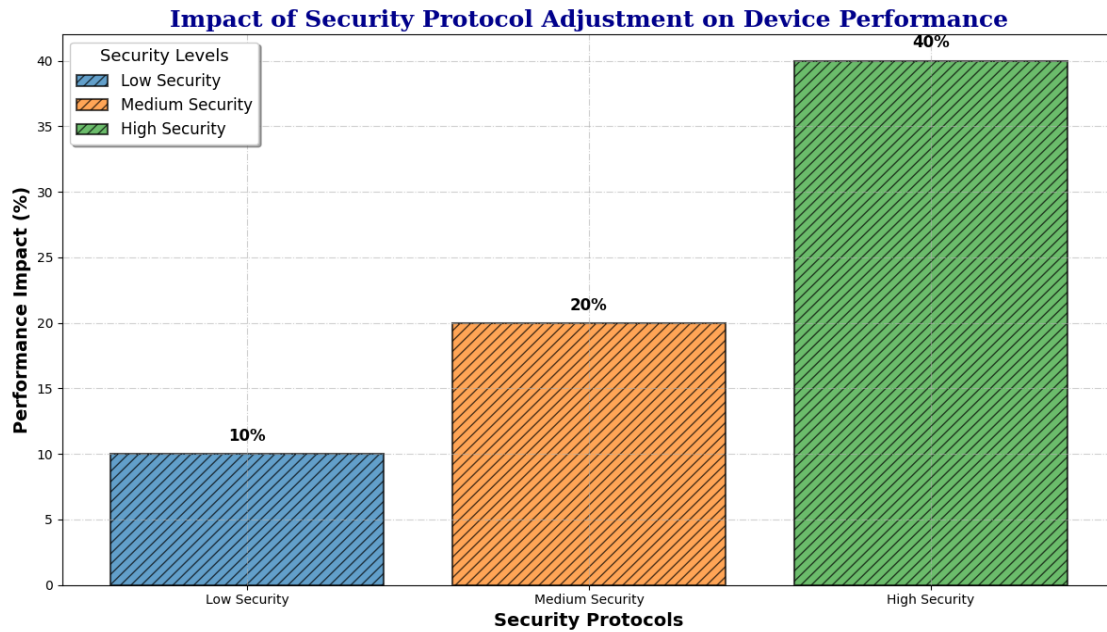


Figure 4: Impact of security protocol adjustment on device performance

Figure 4 illustrates the effect of various security settings (low, medium, and high security) on the performance of a device. The greater the level of security provided, the greater will be the effect on the performance, wherein the greatest performance degradation will be experienced with high security measures. Low security measures exert minimal effects on the performance, thus causing minimal interference to the performance of the device. This brings about the trade-off between the level of security and the performance of devices, which is a critical factor concerning the IoT devices that have resource constraints. FSRC-IoTE will strive to achieve a tradeoff between these considerations by dynamically setting security-related measures depending on the existing resources.

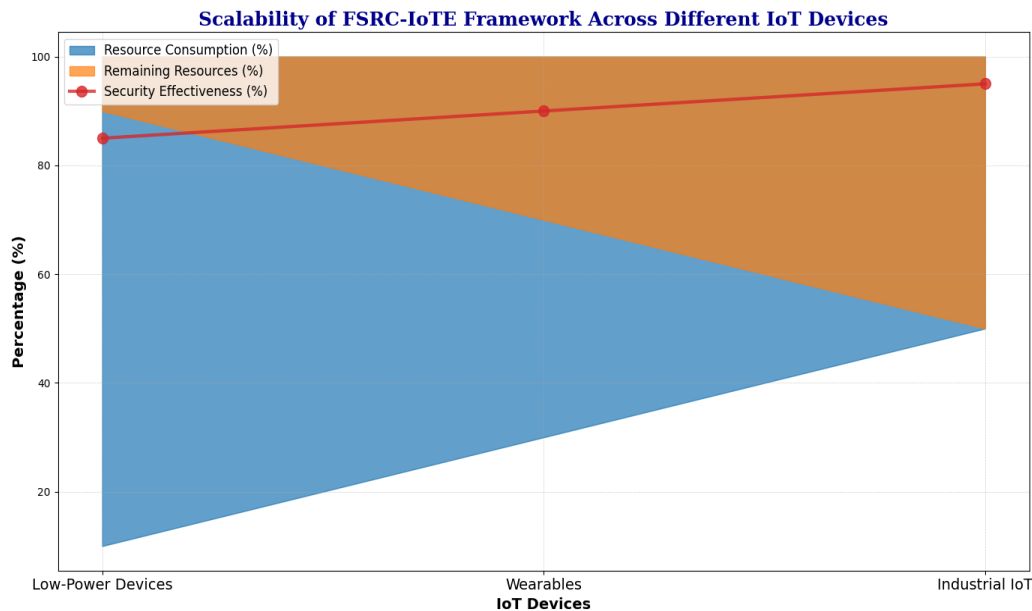


Figure 5: Scalability of the FSRC-IoTE framework across different IoT devices

Figure 5 depicts the FSRC-IoTE scaling of different IoT devices, including low-power devices and industrial/IoT devices. The stacked area plot displays resource usage and the available resources, with low-power devices utilizing the most resources and the least resources, respectively. The more capable the IoT devices are (e.g., industrial IoT devices), the higher the level of resource consumption, and the security efficacy is high, which proves the scalability of the FSRC-IoTE to support the lightweight devices and more powerful devices. The resource consumption curve and the security effectiveness curve indicate the dynamic response in security provisions to ensure the optimal balance is obtained between security and resource consumption within different IoT settings.

Ablation Study

The ablation test of the FSRC-IoTE framework assesses the individual contribution of the important components by dropping one by one. A comparison between the baseline model (that encompasses all features) (AI-driven threat detection, real-time security assessment, and adaptive security adjustment) and the systems in which each of the features is switched off is provided. After deactivating the use of AI in threat detection, there is reduced detection accuracy and higher CPU consumption. Switching off real-time security assessment increases latency and reduces the detection performance. The elimination of adaptive security adjustment enhances resource consumption that leads to a diminishment of the performance of resource-constrained machines. The lowest performance is seen when the threat detection is performed by AI and the real-time evaluation is also taken out, and the accuracy is reduced by a significant margin, and the overhead is also elevated. The paper shows that all aspects of FSRC-IoTE are critical in ensuring scalability, efficiency, and effectiveness of security in resource-constrained IoT settings.

5 Discussion

The FSRC-IoTE framework was designed to address the unique security challenges posed by resource-constrained IoT environments, such as low-power sensors, wearables, and industrial devices. The ablation study and performance evaluations clearly highlight the effectiveness of the framework's components AI-driven threat detection, real-time security evaluation, and adaptive security adjustment in optimizing both security and resource efficiency.

Impact of AI-Driven Threat Detection

The elimination of AI-based detection of threats has a considerable negative impact on the detection quality of the structure. The lack of AI models that constantly learn and evolve in response to new threats leads to delayed threat detection and elevated false positive rates. Conventional security tools that are not automated with AI are more responsive to threats, and they are less effective at detecting threats in real-time, which makes machine learning significant in the proactive process of identifying and eliminating possible threats in IoT systems. Besides, the use of the CPU decreases when AI is turned off since less efficient manual procedures replace it.

Real-Time Security Evaluation and its Role

The real-time security assessment option is also vital with regard to checking on the security vulnerability and its immediate detection. In case the real-time assessment is turned off, there will be a higher latency, and the threat might not be detected until subsequent evaluations. This sluggishness in identifying this may expose devices to extended security vulnerability, so real-time monitoring is

necessary in IoT settings where response to security violations is paramount. The security gaps could remain open without constant security checks, thus increasing the vulnerability of the system to attacks.

Adaptive Security Adjustment

Adaptive security adjustment also makes sure that the security steps taken on a device are matched with the resources of the device. Switching this off causes the consumption of more resources since the security measures are set in stone, despite the resource limitations on the device. This leads to poor performance, especially among devices that have low processing power, memory, or battery. The ability to vary security based on the existing state of the machine is a basic part in resource-limited settings, where the resources between security and performance are needed. The adaptive mechanism will be used to make sure that the framework is able to scale and that the level of security used is the level that fits the capabilities of the device.

Combined Effect of Removing Key Components

The lowest performance is seen in a case where AI-based threat-detection and real-time evaluation are turned off. In the absence of these vital elements, the defectiveness is reduced dramatically, and latency is increased multiple times. This illustrates the significance of ongoing and dynamic surveillance and smart decision-making in ensuring sound security under the IoT setups. Eliminating the two elements grossly restricts the capacity of the framework in its proactive control of threats and real-time moderation of security controls, exposing gadgets to assault.

Scalability and Adaptability

FSRC-IoTE framework demonstrates that it is scalable to various devices in the IoT and to a variety of deployment scenarios. The framework is able to change the levels of security depending on resource constraints. The flexibility is essential to IoT systems, as the variety of devices, each with its own distinct abilities, necessitates security solutions that are both scalable and consume the fewest resources. Due to the ever-expanding nature of the IoT environments, the framework can be scaled, which, as the number of devices to which it can be applied increases, also implies that the framework can be applied to more devices with more resource constraints.

Practical Applications and Future Improvements

The FSRC-IoTE has been proven to be useful in providing real-time security with minimal effects on the performance of the device in the real-world environment, such as smart homes, wearables, and industrial IoT. The framework is not sensitive to evolving threats as it integrates AI-based threat detection and dynamic security. However, the following round of relevant advancements could be the enhancement of the AI models to recognize new attack vectors, reducing latencies in the scenario of the most severe network conditions, and the additional reduction of the consumption of resources in devices with ultra-low-power requirements. In addition, blockchain-based security can also be more likely to enhance the degree of trust and resiliency, especially in decentralized IoT networks.

The FSRC-IoTE framework proves much better in controlling IoT security, especially in resource-limited systems, as it provides a scalable and adaptable framework that is efficient. The ablation experiment reveals that AI-based detection, real-time monitoring, and adaptive security are highly important to offer a harmonized method of security and performance. SRC-IoTE can solve the urgent task of securing various IoT systems in dynamic environments with limited resources because it

guarantees low resource usage and high levels of security effectiveness. The next generation of research can be devoted to the improvement of predictive functionality and scalability of the framework, making it hardy in the face of the development of IoT technologies.

6 Conclusion

The FSRC-IoTE framework can handle flexibility-consistency paradox in IoT with resource constraints adequately by offering scalable and real-time security solutions. It also capitalizes on the AI-enhanced threat detection, the constant real-time security monitoring and automated security profile management to maintain security levels at high levels and reduces resource consumption. This enables the framework to have a strong protection without heavily loading the already limited processing power, memory and battery of an IoT device making it very effective in an environment with limited processing ability, memory and battery life. Flexibility is one of the major advantages of FSRC-IoTE, as it allows the framework to be adjusted to a huge range of IoT devices, including low-power sensors and devices with more creative resources, such as industrial devices. This flexibility is essential, because it allows the devices of various capabilities to enjoy high level of security, and adapt dynamically to the available resources. Simultaneously, resource efficiency of the framework allows carrying out the consistent process of security assessment without any influence on the device performance. SRC-IoTE can be optimally used to balance security and performance, which means that it will have minimal effects on IoT operations. The new contributions of FSRC-IoTE are in its scalability, resource efficiency and dynamic adaptability. These features enable it to provide a long-term and sustainable solution to securing the IoT devices in different settings. Further studies may involve improvements of the framework through more AI-driven threat management, and its integration with the latest IoT tools like 5G and expansion to even more harshly adversarial environments. Moreover, to enhance the capacity of the framework in dealing with intricate and dynamic threats would also be a good field of development. To sum up, the FSRC-IoTE is a robust and scalable environment protection system that can guarantee the long-term sustainability and stability of IoT environments as they grow and develop further.

References

- [1] Al Rawajbeh, M., Maria Soosai, A. J., Ramasamy, L. K., & Khan, F. (2025). Trustworthy adaptive AI for real-time intrusion detection in industrial IoT security. *IoT*, 6(3), 53. <https://doi.org/10.3390/iot6030053>
- [2] Ansari, S. A., & Ali, S. (2025). A systematic review of lightweight cryptographic schemes for security and privacy in IoT. *Discover Computing*, 28(1), 266. <https://doi.org/10.1007/s10791-025-09755-3>
- [3] Arabi, Z., Oskouei, R. R., & Hosseinzadeh, M. (2025). Enhancing Security in IoT Networks: A Multifaceted Approach to Vulnerability Analysis and Protection. *Array*, 100626. <https://doi.org/10.1016/j.array.2025.100626>
- [4] Arif, H., Ali, A. K. S., & Nabi, H. A. (2025). IoT Security through ML/DL: Software Engineering Challenges and Directions. *ICCK Journal of Software Engineering*, 1(2), 90-108. <https://doi.org/10.62762/JSE.2025.372865>
- [5] Batool, S., Abid, M. K., Salahuddin, M. A., Aziz, Y., Naeem, A., & Aslam, N. (2024). Integrating IoT and machine learning to provide intelligent security in smart homes. *Journal of Computing & Biomedical Informatics*, 7(01), 224-238. <https://doi.org/10.56979/701/2024>
- [6] Chang, C. Y., Chuang, Y. C., Huang, C. T., & Wu, A. Y. (2023). Recent progress and development of hyperdimensional computing (hdc) for edge intelligence. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, 13(1), 119-136.

- [7] Gewida, M., & Qu, Y. (2025). Enhancing IoT security: Predicting password vulnerability and providing dynamic recommendations using machine learning and large language models. *European Journal of Electrical Engineering and Computer Science*, 9(1), 8-16.
- [8] Haider, Z. A., Zeb, A., Islam, A. M., Rahman, T., Arishi, A., & Ullah, I. (2026). Enhancing IoT security with resource-efficient cryptography: A comprehensive review of lightweight and hybrid algorithms. *Computer Science Review*, 59, 100861.
<https://doi.org/10.1016/j.cosrev.2025.100861>
- [9] Halgamuge, M. N., & Niyato, D. (2025). Adaptive edge security framework for dynamic IoT security policies in diverse environments. *Computers & Security*, 148, 104128.
<https://doi.org/10.1016/j.cose.2024.104128>
- [10] Mishra, S. R., Shanmugam, B., Yeo, K. C., & Thennadil, S. (2025). SDN-enabled IoT security frameworks a review of existing challenges. *Technologies*, 13(3), 121.
<https://doi.org/10.3390/technologies13030121>
- [11] Mushtaq, S., Mohsin, M., & Mushtaq, M. M. (2025). A systematic literature review on the implementation and challenges of zero trust architecture across domains. *Sensors*, 25(19), 6118.
<https://doi.org/10.3390/s25196118>
- [12] Mutambik, I. (2025). AI-Driven Cybersecurity in IoT: Adaptive Malware Detection and Lightweight Encryption via TRIM-SEC Framework. *Sensors*, 25(22), 7072.
<https://doi.org/10.3390/s25227072>
- [13] Pandey, V. K., Sahu, D., Prakash, S., Rathore, R. S., Dixit, P., & Hunko, I. (2025). A lightweight framework to secure IoT devices with limited resources in cloud environments. *Scientific Reports*, 15(1), 26009. <https://doi.org/10.1038/s41598-025-09885-0>
- [14] Pavithra, H. C., & Rajeshwari, J. (2024, November). A comprehensive iot security framework empowered by machine learning. In *2024 3rd Edition of IEEE Delhi Section Flagship Conference (DELCON)* (pp. 1-8). IEEE.
<https://doi.org/10.1109/DELCON64804.2024.10866748>
- [15] Rahmati, M., & Pagano, A. (2025, July). Federated Learning-Driven Cybersecurity Framework for IoT Networks with Privacy Preserving and Real-Time Threat Detection Capabilities. In *Informatics* (Vol. 12, No. 3, p. 62). MDPI. <https://doi.org/10.3390/informatics12030062>
- [16] Samant, P. K., Pathak, V., Ahmad, W., & Alabdultif, A. (2025). A lightweight trusted framework for secure data exchange and threat mitigation in IoT-enabled healthcare environments. *Scientific Reports*, 15(1), 39248. <https://doi.org/10.1038/s41598-025-22797-3>
- [17] Sarwar, N., Bajwa, I. S., Hussain, M. Z., Ibrahim, M., & Saleem, K. (2023). IoT network anomaly detection in smart homes using machine learning. *IEEE Access*, 11, 119462-119480.
<https://doi.org/10.1109/ACCESS.2023.3325929>
- [18] Sehgal, A., Perelman, V., Kuryla, S., & Schonwalder, J. (2012). Management of resource constrained devices in the internet of things. *IEEE Communications Magazine*, 50(12), 144-149.
<https://doi.org/10.1109/MCOM.2012.6384464>
- [19] Taiwo, O., Ezugwu, A. E., Oyelade, O. N., & Almutairi, M. S. (2022). Enhanced intelligent smart home control and security system based on deep learning model. *Wireless communications and mobile computing*, 2022(1), 9307961.
<https://doi.org/10.1155/2022/9307961>

Authors Biography



Gundala Venkata Rama Lakshmi is currently a Research Scholar (Part-Time Ph.D.) in the Department of Computer Science and Engineering at SRM Institute of Science & Technology, Kattankulathur, Chennai. She is also working as an Assistant Professor in the Department of Computer Science and Engineering at CVR College of Engineering, Hyderabad, Telangana. She completed her M. Tech in Computer Networks and Security (CNS) from K.L. University, Vijayawada, Andhra Pradesh, and her B. Tech in Computer Science and Engineering (CSE) from Swarnandhra College of Engineering, Narsapuram, West Godavari, Andhra Pradesh. She has 8 years of teaching experience and is an active researcher with interests in Cyber Security, Internet of Things (IoT), Cloud Computing, Computer Security, Network Security, and Blockchain Technologies. Her Ph.D. research area focuses on Cyber Security. She is a member of professional bodies such as the Indian Society for Technical Education (ISTE) and the Computer Society of India (CSI). She has published several research papers in reputed journals and conferences indexed by Web of Science (WoS), IEEE, and other recognized databases.



Dr.R. Deeptha, completed her Bachelor of Technology (Awarded Gold Medal) in Information Technology from Madha Engineering College, Chennai (Affiliated to Madras University, Chennai), Master of Technology (University 4th Rank) in Information Technology from Sathyabama University, Chennai, Ph.D. in Information Technology from Hindustan Institute of Science and Technology (Affiliated to Hindustan University), Chennai in 2019 and Post Doctoral Fellowship in the field of Artificial Intelligence from the Department of Information Sciences at King Saud University, Riyadh, KSA in August 2024. Currently she is working as Assistant Professor in the Department of Information Technology (School of Computing Sciences), SRMIST, Ramapuram. She has 10 years of full-time experience in reputed engineering colleges in Chennai. She has presented more than 50 papers in International Conferences, published 34 and communicated 8 technical papers in reputed International Journals indexed in Scopus, Springer, WOS and ESCI. She has also authored 5 books, published 5 patents and submitted 4 research proposals. Her main areas of interest include Cyber Security, Digital Forensics, Artificial Intelligence, IOT and Wireless Sensor Networks.