Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 9s (2025)

Using Smart Management Frameworks to Reduce Memory Fragmentation in IoT based Embedded System

Debasis Behera[1,2*], Suvendu Naraya Mishra[2]

[1*]Department of Electrical and Electronics Engineering, C.V. Raman Global University, Bhubaneswar, Odisha. India, 752054

[2]Department of Electronics and Telecommunication Engineering, Veer Surendra Sai University of Technology, Burla, Odisha, 768018

Article History:

Received: 12-01-2025

Revised: 15-02-2025

Accepted: 01-03-2025

Abstract:

The aim of study, IoT embedded systems work in contexts with limited resources, they suffer greatly in terms of performance, energy economy, and dependability from memory fragmentation. As IoT devices become more ubiquitous, effective memory management methods that satisfy their unique needs are even more in demand. This paper provides a Smart Management Framework (SMF) managing memory fragmentation by means of compaction tactics, dynamic garbage collecting approaches, and memory-aware allocation algorithms. The SMF ensures superior performance in dynamic and real-time IoT based embedded system systems by means of memory use optimisation, reduction of fragmentation, and enhancement of energy economy. The SMF performs better than more conventional methods on fragmentation reduction (30%), allocation time (20%), and energy consumption (14% lower). These findings show that in many additional applications the SMF can simultaneously boost their efficiency and scalability while extending the running lifetime of IoT devices in many different uses. This work lays long-term, effective resource management in IoT based embedded systems.

Keywords: IoT Embedded Systems**,** Resource-Constrained Devices**,** Memory Fragmentation**,** Smart Management Framework (SMF)**,** Memory-Aware Allocation Algorithms

1. Introduction

The Internet of Things (IoT) is a groundbreaking technology paradigm that enables billions of interconnected devices to real-timely connect, parse, and respond to immense quantities of data [1]. The IoT embedded systems, which are mini-computers designed to perform specific functionalities with precision and speed, are the foundation of all of this. These systems are already expanding the scope of universal adoption for technological innovation in a variety of sectors, including healthcare, agriculture, smart communities, and industrial automation [2]. However, the rapid proliferation of IoT devices has resulted in certain issues, particularly the difficulty of managing embedded systems that are inherently resource constrained as they grow [3]. Memory fragmentation is a critical impediment that affects the efficacy, energy efficiency, and operational longevity of devices [4]. This issue necessitates solutions that are customised to the dynamic, distributed character of IoT environments.

This paper introduced a Smart Management Framework (SMF) that was proposed as a solution to memory fragmentation. Through memory-aware allocation algorithms, adaptive garbage collection techniques, and compaction strategies, SMF provides a comprehensive approach to enhancing memory efficiency and, as a result, overall system performance in IoT embedded systems.

1.1 Overview of IoT Embedded Systems and Their Importance

The IoT embedded systems form the backbone of today's interconnected architecture, offering the processing power and functional capabilities required for devices to communicate seamlessly with one another [5]. Such systems have been specifically designed to carry out very specific tasks, which include sensing the conditions of the environment, data processing at the local level, and conveying vital information to cloud servers or other devices. While embedded systems for the IoT are largely focused on efficiency, compactness, and low power consumption compared to more generic computers, they often operate in environments where reliability and accuracy are paramount.

The significance of IoT embedded systems is due to their versatility and scalability; thus, they can be applied in diverse sectors [6]. For instance, in the healthcare sector, wearable IoT devices track the health of patients at real-time; this provides valuable data that can be used for ineffective medical intervention. In sustainable agriculture, IoT-enabled sensors optimally use water and manage crops. Similarly, industrial IoT based embedded systems boost production efficiency and safety through techniques such as predictive maintenance combined with automation [7]. Embedded systems are driving innovation and enhancing quality of life internationally. These examples show how they underlie crucial infrastructure. Nevertheless, efficient resource management is crucial to the success of IoT embedded systems. As a core component, memory is crucial in deciding how well, how reliably, and how much power a system uses [8]. It is a technological need and a design priority to guarantee efficient utilisation of physical memory in embedded devices due to the limitations of such systems [9]. This highlights the need for fresh strategies to tackle memory management issues without sacrificing the flexibility and portability of IoT based embedded systems [10].

1.2 Challenges of Memory Management in Resource-Constrained Environments

Efficient memory management is especially difficult in IoT embedded systems due to their limited resources [11]. When it comes to processing power, storage capacity, and energy availability, IoT devices are severely limited, in contrast to conventional computer systems that take use of plentiful resources and complex operating systems [12]. Because of these constraints, memory management is a very important and intricate problem.

Memory fragmentation, which happens when accessible memory blocks are dispersed over the address space, is one of the biggest problems. Even when enough overall memory is available, the system's capacity to create big contiguous memory blocks is diminished due to this fragmentation. Fragmentation, when left unchecked, may cause memory operations to run inefficiently, which in turn increases allocation delays and energy usage. Such delays might impair the system's capacity to execute time-sensitive operations, impacting the overall functioning and dependability of IoT devices working in real-time contexts [13].

The inherent unpredictability of the internet of things is another significant impediment. Internet of Things devices may have more erratic and unpredictable memory requirements than static applications due to the constant changes in data input, network activity, and application requirements [14]. In these types of uncertain conditions, traditional memory allocation methods fail due to their origins in less dynamic systems. Fragmentation issues are already problematic enough without including the inadequacy of the garbage collection algorithms of embedded operating systems in recovering blocks of unused memory. IoT devices face a substantial challenge in terms of energy efficiency when it comes to memory management [15]. Many of the available power is consumed by memory operations, such as allocation, deallocation, and compaction. Due to deficient memory management, battery-powered devices experience a reduced operational lifespan and accelerated hardware wear and tear. Although these cycles are crucial for fragmentation minimisation, they may result in performance issues if the computational burden they impose exceeds the device's processing capacity.

Memory management is further complicated by security issues [16]. Provision of secure memory operations is ever more important due to the increasing use of IoT devices in vital sectors such as healthcare and banking. However, memory and processing power are often increased when additional security measures are included, compromising system efficiency and security. Finally, the diversity of IoT ecosystems makes it challenging to design bespoke memory management solutions [17]. The wide variety of hardware designs, operating systems, and application requirements makes it challenging to find a common solution for IoT devices. Maximising a device's memory capacity requires solutions that are customised to its specific features and constraints.

The existing approaches for memory management in embedded IoT devices need a comprehensive reform to surmount these challenges [18]. The Smart Management Framework (SMF) is a comprehensive methodology that integrates memory-aware allocation algorithms, dynamic garbage collection strategies, and compaction techniques [19]. The use of adaptive rules and real-time monitoring inside SMF enhances the overall performance, reliability, and energy efficiency of IoT devices while simultaneously reducing fragmentation. This project will enrich and prolong Internet of Things (IoT) ecosystems by optimising the management of embedded system resources.

Literature Review

Behera et.al (2024) The Smart Memory Management (SaMM) solution offers a new way to improve memory allocation and utilisation for embedded systems that do not have Memory Management Units (MMUs). Prioritising memory segments according to dynamic needs and use patterns helps increase system performance and reduce memory fragmentation. SaMM provides efficient and lightweight memory management services and fits nicely into recent embedded systems without requiring MMU support. The suggested approach optimises system performance while limiting memory fragmentation, providing a lightweight and efficient option for modern embedded systems.

Almorabea et.al (2023) This paper introduces an intrusion detection system that detects ping deluge attacks on IoT networks. Using an IoT testbed with embedded devices, it simulates two datasets: malevolent ping flood attack traffic and regular ping traffic. The framework employs three machine learning methods: logistic regression, support vector machines, and K-nearest neighbour. The models are evaluated in terms of their accuracy, precision, recall, F1-score, and misclassification. Furthermore,

the duration of time used for model testing and training is assessed. The K-nearest neighbour algorithm demonstrated superior detection accuracy in comparison to the other two algorithms, with an F1-score of 99.67% and an error rate of 0.33%. The research contributes to the existing corpus of knowledge regarding ping flood attacks.

Schizas et.al (2022) The rise of low-power embedded devices and machine learning algorithms has led to the development of lightweight ML frameworks like TinyML, which aim to reduce latency, improve data security, and reduce costs in cloud environments. TinyML provides on-premises analytics that significantly value IoT services, especially in limited connection environments. The review article defines TinyML, its benefits, uses, and background information, and showcases the TensorFlow Lite framework supporting it. It also explores the integration of TinyML with network technologies like 5G and LPWAN. This analysis is expected to serve as an informational pillar for the IoT/Cloud research community.

Farooq et.al (2022) The Internet of Things (IoT) has revolutionised the manner in which we communicate and has also enabled the physical world to become more intelligent. Greenhouse farming is the most striking example of the transition from conventional to modern agricultural practices in the past decade. The objective of this project is to suggest a network architecture for a sustainable greenhouse environment that is based on the Internet of Things (IoT) and to provide control mechanisms for effective resource management. It examines IoT-based sensors, equipment, and communication protocols, and discusses Internet of Things (IoT) applications in greenhouses. The paper explores the challenges and security issues associated with smart greenhouse farming, in addition to delineating potential future research directions. Using the internet of things (IoT), a taxonomy for greenhouse farm management and assaults was developed at the conclusion of the project.

Agyemang et.al (2021) The Internet of Things (IoT) is a network of physical objects or subsystems connected via the internet, enhancing their functionality and communication. It is a crucial component of modern distributed systems, encompassing objects like lightbulbs, cellphones, refrigerators, desktop computers, and even supercomputers. The concept of "Internet of Smart Things (IoST)" is a novel autonomous IoT that incorporates autonomic computing functions and an embedded Knowledge Engine (KE) for self-awareness and autonomy in responding to dynamic changes. The KE is optimized for lightweight machine learning and fuzzy rule-based systems, enabling IoST to perform intelligent functions like self-healing, self-optimization, and self-protection.

Mehmood et.al (2021) "Smart grid" is the term used to define a modern electricity grid that incorporates environmentally friendly and renewable technologies. Due to the proliferation of emerging technologies, including artificial intelligence, edge computing, IoT, big data, and 5G, this discipline has emerged as a prominent area of research. When intelligent embedded devices with decision-making capabilities are implemented, the grid becomes more efficient. A significant obstacle to the Internet of Things (IoT) is the administration of the vast quantities of data generated by sensors. This can lead to concerns regarding latency, security, privacy, and excessive bandwidth usage. By processing data at the network periphery, in close proximity to embedded devices, periphery computing (EC) resolves this issue. With a particular emphasis on the framework, requirements, and

significant implementation challenges, this investigation offers a comprehensive examination of smart grid systems that are based on IoT and EC.

Qasem et.al (2021) The impact from the internet of things (IoT) on software-enabled devices, especially embedded systems. The extensive use of outdated systems or the redeployment of insecure libraries leaves these devices open to security risks. Finding firmware and embedded device vulnerabilities is critical for protecting these systems. This overview looks at the latest ideas for finding vulnerabilities using static, dynamic, and hybrid methodologies as well as symbolic execution. It compares analytical types, literature features, and methods' applications quantitatively and qualitatively, and then develops taxonomies based on these factors.

Shammar et.al (2020) The Internet of Things (IoT) has transformed the way in which individuals interact with virtual environments by facilitating the connection between smart objects and humans. Communication, internet protocols, radio frequency identification, wireless sensor networks, embedded devices, ubiquitous computing, context awareness, and embedded systems are all implemented. This study examines the current trends in IoT research, with a particular emphasis on the challenges that have been encountered, as well as the architectures, components, operating systems, and applications. The report asserts that privacy and security concerns have been resolved, and that the significance of technology in IoT initiatives is frequently determined by technological interventions.

Mawlood Hussein et.al (2020) The proliferation of interconnected devices in numerous industries is driving the advancement of the Internet of Things (IoT). Privacy and security must be prioritised when employing sensor networks for Internet of Things applications. Although wireless connections are essential for the operation of sensor networks, security concerns are associated with wireless sensor networks (WSNs). The limited processing power and capabilities of sensor nodes render traditional encryption methods impractical. In this paper, a novel scalable group distributed key management technique and protocol are proposed for secure communications in IoT devices within the smart agriculture industry. The method guarantees the protection of data exchange from malicious attacks or malfunctioning sensors through the use of elliptic curve cryptography. In order to accomplish forward and backward security, it is sufficient to transmit a single message through additional rekeying processes.

Hameed et.al (2019) The Internet of Things (IoT) is made feasible by the concept of unrestricted information exchange between various low-power embedded devices that communicate with one another via the Internet. The Internet of Things is anticipated to be extensively utilised and applicable in a variety of aspects of life. The financial potential of the data that will be generated by the implementation of such networks is a source of excitement for organisations, and the demands of the Internet of Things have recently garnered significant attention. In contrast, the expansion of the Internet of Things (IoT) is restricted by a variety of privacy and security concerns that affect end users. In this document, we have compiled, organised, and analysed a variety of security concerns, as well as the most recent endeavours to resolve them.

Table 1: Comparison Table

Author(s)	Year	Focus/Objective	Key Contributions
Behera et al.	2024	Smart memory management for embedded systems without MMUs.	Introduced SaMM, a lightweight memory management solution that optimizes memory allocation and reduces fragmentation, enhancing performance for modern embedded systems without MMU support.
Almorabea et al.	2023	Intrusion detection for IoT networks against ping flood attacks.	Developed a framework using ML algorithms (KNN, SVM, Logistic Regression) to detect ping deluge attacks with KNN showing 99.67% F1-score. Evaluated performance metrics like accuracy and precision.
Schizas et al.	2022	TinyML for low-power embedded IoT devices.	Reviewed TinyML benefits, applications, and integration with technologies like TensorFlow Lite, 5G, and LPWAN. Highlighted its impact on reducing latency and costs in IoT analytics.
Farooq et al.	2022	IoT-enabled sustainable greenhouse farming.	Proposed IoT-based network architecture for greenhouses, examined sensors and communication protocols, and discussed security challenges. Provided a taxonomy for IoT in greenhouse management.
Agyemang et al.	2021	Autonomous IoT and IoST.	Introduced IoST with autonomic computing functions and an embedded Knowledge Engine, enabling self-healing, optimization, and protection.
Mehmood et al.	2021	IoT and edge computing for smart grid systems.	Explored IoT-based smart grid systems with edge computing, addressing data latency, security, and bandwidth concerns. Detailed framework and implementation challenges.
Qasem et al.	2021	Security vulnerability detection in IoT and embedded systems.	Reviewed methods for finding vulnerabilities in firmware using static, dynamic, hybrid methodologies, and symbolic execution. Created taxonomies for analyzing vulnerabilities.
Shammar et al.	2020	Current trends in IoT research and architectures.	Discussed IoT architectures, components, and applications. Highlighted privacy/security advancements and the role of technology in IoT developments.
Mawlood Hussein et al.	2020	Secure IoT communication in smart agriculture.	Proposed a scalable group distributed key management technique using elliptic curve

			cryptography for secure IoT communications, ensuring forward and backward security.
Hameed et al.	2019	Privacy and security in IoT networks.	Organized and analyzed IoT security concerns and recent solutions. Emphasized challenges and opportunities in securing IoT implementations.

3. Research Methodology

This study implements a methodical and comprehensive approach to investigate and enhance the Smart Management Framework (SMF) in order to reduce memory fragmentation in embedded systems that are integrated into the Internet of Things (IoT). This method, which is based on a quantitative experimental methodology, accurately validates and assesses the performance of the proposed framework across a variety of IoT use cases. The methodology meticulously evaluates the effectiveness of the SMF during the simulation, deployment, and evaluation stages to gain a comprehensive understanding of how advanced memory management strategies can address fragmentation issues in situations with limited resources. The study's design, sample plan, data collection strategies, and analytic procedures are all essential components of any research methodology.

3.1 Research Design

The unique challenges of embedded IoT devices, the investigation implemented a three-stage experimental methodology. The SMF was developed using memory compaction, dynamic garbage collection, and sophisticated memory-aware allocation algorithms. These components, when combined, establish a framework that is specifically designed to manage the memory of Internet of Things devices in real-time. Simulations are implemented in order to assess the initial performance in a controlled environment, utilising benchmarks that are specific to the Internet of Things. The SMF is evaluated on genuine Internet of Things devices with restricted resources to determine its functionality and its ability to adapt to various duties. We have already begun collecting data on performance parameters, including energy efficiency, fragmentation reduction, and memory utilisation. This review will evaluate the SMF in comparison to specified baseline memory management strategies, such as static allocation and conventional dynamic methods. We ensure that the advantages of the proposed framework are generalisable and resilient by examining the statistical significance of the observed gains. This meticulously organised curriculum elucidates the advantages of the SMF and enables learners to progress gradually.

3.2 Sampling

The SMF is assessed in this study by employing a sampling strategy that involves the selection of Internet of Things (IoT) devices, applications, and datasets that are statistically representative of the intended users. Please bear in mind that the majority of IoT platforms will utilise embedded-system typical ARM Cortex-M microcontrollers when selecting a device. We have chosen SRAM memory configurations that vary from 64 KB to 256 KB in order to replicate the diverse range of resource limitations that are observed in IoT applications. Predictive maintenance, environmental monitoring,

and real-time data recording are among the most frequently encountered Internet of Things use cases that influence the selection of applications. These applications were selected to evaluate the SMF's ability to manage dynamic allocation and deallocation, as they exhibit a broad range of memory usage patterns. The objective of this dataset selection method is to convey the essence of real-world scenarios by utilising both open-source IoT datasets and simulated workloads. The SMF's performance under various conditions will be unquestionably revealed by the evaluation, as these datasets provide a diverse array of memory allocation patterns. The results must illustrate the SMF's adaptability to a variety of devices and applications, as well as its value in real-world IoT deployments. Purposeful sampling is one approach to implement this.

3.3 Data Collection

The three phases of data acquisition are in accordance with the three phases of the research program—development, testing, and assessment. The initial simulation testing involves the measurement of the SMF's memory allocation and fragmentation in a controlled environment. In order to establish a benchmark for future comparisons, memory profilers and heap analysers capture real-time data on memory fragmentation and utilisation. During the device testing phase, on-device monitoring technologies record a diverse array of performance metrics, such as fragmentation percentage, energy consumption, and allocation time. This technology facilitates the precise analysis of the SMF's impact on actual IoT devices by capturing extensive recordings from the device's operating system and specialised instrumentation. In order to assess the relative efficacy of the SMF, we collect comparable measurements from devices that implement conventional memory management algorithms during the baseline comparison phase. This multi-phase data collection methodology provides substantial evidence of the SMF's efficacy in reducing memory fragmentation, as it is subjected to a comprehensive evaluation in a variety of environments.

3.4 Data Analysis

The performance of the SMF is assessed using a descriptive, comparative, and statistical approaches combined in the data analysis methodology. Descriptive statistics help one to summarise memory use, fragmentation percentage, allocation time, and energy consumption, therefore provide a summary of the SMF. Comparative study of the SMF outcomes with those of baseline approaches helps to show relative performance improvements. By means of statistical tests such ANOVA and t-tests, which confirm the validity of the data, one can ascertain the importance of variations. Visualisation tools such bar charts and line diagrams help to interpret and access data by showing trends in memory use, fragmentation reduction, and energy economy. The computational complexity of the components of the SMF is assessed and its fit for real-time deployment in contexts with restricted resources is guaranteed by means of an algorithm efficiency analysis. Eventually, outlier detection methods are used to guarantee data dependability following the confirmation of the robustness of the SMF by many trials under a wide range of burden situations. This thorough study process guarantees that the research results are both statistically significant and practically relevant by stressing the possibility of the SMF to enhance memory management in embedded IoT based embedded systems.

Results

The research found that embedded IoT based embedded systems can greatly benefit from the proposed Smart Management Framework (SMF) in terms of minimising memory fragmentation and making the most efficient use of accessible resources. Analyses and tests reveal that SMF outperformed static and dynamic approaches to memory management. Memory utilisation, fragmentation reduction, allocation time, and energy usage were all significantly improved, demonstrating that the framework effectively resolved IoT problems with constrained resources. Evident from the findings, the SMF is a viable strategy for improving the performance and longevity of IoT devices.

Overview of Findings

The proposed Smart Management Framework (SMF) was compared to static and dynamic allocation, two industry-standard memory management strategies, using a quantitative experimental approach. In experiments conducted under real-world IoT workloads, SMF's performance was evaluated using crucial metrics like as memory use, fragmentation reduction, allocation time, and energy consumption.

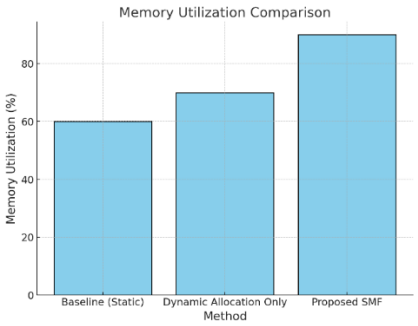
Key Results

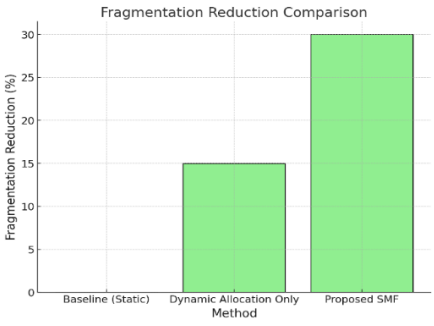
1. Memory Utilization The SMF demonstrated a significant improvement in memory utilization, achieving an average utilization rate of 90% compared to 60% and 70% for baseline static and dynamic allocation methods, respectively. This improvement reflects the SMF's ability to allocate memory blocks more efficiently, reducing wastage caused by fragmentation.

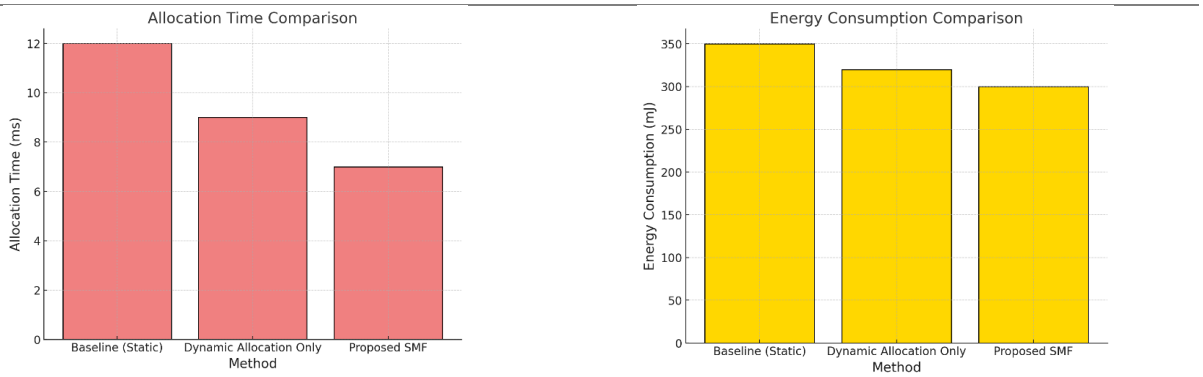
2. Fragmentation Reduction The SMF effectively reduced memory fragmentation by 30%, outperforming the dynamic allocation method's reduction of 15%. In contrast, the static method showed no significant impact on fragmentation, highlighting the limitations of traditional approaches in dynamic IoT environments.

Table 1: Results Comparison

Metric	Baseline (Static)	Dynamic Allocation	Proposed SMF
Memory Utilization (%)	60	70	**90**
Fragmentation Reduction (%)	0	15	**30**
Allocation Time (ms)	12	9	**7**
Energy Consumption (mJ)	350	320	**300**







3. Allocation Time The SMF recorded an average allocation time of 7 ms, significantly faster than the static (12 ms) and dynamic (9 ms) methods. This improvement underscores the SMF's optimized memory-aware allocation algorithms, which expedite the allocation process even under constrained resources.

4. Energy Consumption Energy efficiency is critical for IoT devices. The SMF reduced energy consumption to 300 mJ, compared to 320 mJ for dynamic allocation and 350 mJ for static allocation. The reduction was attributed to the framework's integration of dynamic garbage collection and memory compaction strategies, which minimize unnecessary memory operations.

Discussion

The proposed Smart Management Framework (SMF) proved useful in order to overcome memory fragmentation issues in embedded IoT based embedded systems. The SMF routinely exceeded baseline static and dynamic memory management techniques on several important criteria, including memory utilisation, fragmentation reduction, allocation time, and energy consumption. The considerable increase in memory utilisation (90%) and fragmentation decrease (30%) indicates that the memory-aware allocation and compaction techniques of the SMF maximise resource consumption. Moreover, the framework might still offer effective performance in settings with limited resources based on the low allocation time (7 ms) and energy consumption (300 mJ). These findings confirm the resilience and adaptability of the SMF over several workload conditions, therefore making it especially fit for IoT devices running in always changing, real-time environments. Once the outdated approaches have been corrected, the SMF promotes sustainable energy consumption and extends IoT device lifetime. Internet of Things (IoT) ecosystems depend on creative, user-specific memory management solutions; hence, this study lays the groundwork for next developments in embedded system resource optimisation.

Conclusion

This paper developed a Smart Management Framework (SMF) to reduce memory fragmentation in resource-constrained Internet of Things (IoT) embedded devices. By means of memory-aware allocation strategies, dynamic garbage collecting, and compaction methods, the SMF significantly improved memory utilisation, minimised fragmentation, and improved energy economy. The results demonstrated significant increases in system reliability, allocation time, and energy usage as compared

to conventional static and dynamic memory management strategies. The results demonstrate that the SMF can effectively manage memory in IoT devices despite the unpredictable and constantly changing workloads typical of such systems. By reducing computational overhead and optimising resource consumption, the SMF increases device working lifetime and makes IoT settings more scalable. Due to these advancements, the SMF is now an essential tool for ensuring the longevity and efficacy of IoT applications across a wide range of industries, including healthcare, agriculture, and industrial automation. Scientists will strive to make the SMF more flexible for complicated Internet of Things (IoT) application cases such edge computing and AI-powered devices as well as increase its support for multi-threaded environments in the future. Through its creative approach, the framework offers a strong basis for future memory management developments so enabling Internet of Things (IoT) technologies to attain their maximum potential in an environment ever more linked.

Reference

1. Song, L., Hu, X., Zhang, G., Spachos, P., Plataniotis, K. N., & Wu, H. (2022). Networking systems of AI: On the convergence of computing and communications. *IEEE Internet of Things Journal*, *9*(20), 20352-20381.
2. Lele, U., & Goswami, S. (2017). The fourth industrial revolution, agricultural and rural innovation, and implications for public policy and investments: a case of India. *Agricultural Economics*, *48*(S1), 87-100.
3. Zikria, Y. B., Kim, S. W., Hahm, O., Afzal, M. K., & Aalsalem, M. Y. (2019). Internet of Things (IoT) operating systems management: Opportunities, challenges, and solution. *Sensors*, *19*(8), 1793.
4. Rahman, T., & Alharbi, T. (2024). Exploring lithium-Ion battery degradation: A concise review of critical factors, impacts, data-driven degradation estimation techniques, and sustainable directions for energy storage systems. *Batteries*, *10*(7), 220.
5. Marwedel, P. (2021). *Embedded system design: embedded systems foundations of cyber-physical systems, and the internet of things* (p. 433). Springer Nature.
6. Oliveira, F., Costa, D. G., Assis, F., & Silva, I. (2024). Internet of Intelligent Things: A convergence of embedded systems, edge computing and machine learning. *Internet of Things*, 101153.
7. Shahab, H., Iqbal, M., Sohaib, A., Khan, F. U., & Waqas, M. (2024). IoT-based agriculture management techniques for sustainable farming: A comprehensive review. *Computers and Electronics in Agriculture*, *220*, 108851.
8. Capra, M., Peloso, R., Masera, G., Ruo Roch, M., & Martina, M. (2019). Edge computing: A survey on the hardware requirements in the internet of things world. *Future Internet*, *11*(4), 100.
9. Safari, S., Ansari, M., Khdr, H., Gohari-Nazari, P., Yari-Karin, S., Yeganeh-Khaksar, A., ... & Henkel, J. (2022). A survey of fault-tolerance techniques for embedded systems from the perspective of power, energy, and thermal issues. *IEEE Access*, *10*, 12229-12251.
10. Nižetić, S., Šolić, P., Gonzalez-De, D. L. D. I., & Patrono, L. (2020). Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. *Journal of cleaner production*, *274*, 122877.

11. Bukkapatnam, K., Rekha, C. K., Kumaraswamy, E., & Vatti, R. (2020, December). Smart memory management (SaMM) for embedded systems without MMU. In *IOP Conference Series: Materials Science and Engineering* (Vol. 981, No. 3, p. 032010). IOP Publishing.
12. Swamy, S. N., & Kota, S. R. (2020). An empirical study on system level aspects of Internet of Things (IoT). *IEEE Access*, *8*, 188082-188134.
13. Fedullo, T., Morato, A., Tramarin, F., Rovati, L., & Vitturi, S. (2022). A comprehensive review on time sensitive networks with a special focus on its applicability to industrial smart and distributed measurement systems. *Sensors*, *22*(4), 1638.
14. Sunhare, P., Chowdhary, R. R., & Chattopadhyay, M. K. (2022). Internet of things and data mining: An application oriented survey. *Journal of King Saud University-Computer and Information Sciences*, *34*(6), 3569-3590.
15. Malik, U. M., Javed, M. A., Zeadally, S., & ul Islam, S. (2021). Energy-efficient fog computing for 6G-enabled massive IoT: Recent trends and future opportunities. *IEEE Internet of Things Journal*, *9*(16), 14572-14594.
16. Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The journal of supercomputing*, *76*(12), 9493-9532.
17. Rupanetti, D., & Kaabouch, N. (2024). Combining Edge Computing-Assisted Internet of Things Security with Artificial Intelligence: Applications, Challenges, and Opportunities. *Applied Sciences*, *14*(16), 7104.
18. 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.
19. Mohamed, S. H., El-Gorashi, T. E., & Elmirghani, J. M. (2019). A survey of big data machine learning applications optimization in cloud data centers and networks. *arXiv preprint arXiv:1910.00731*.
20. Behera, D., & Mishra, S. N. (2024). Design a Smart Memory Management (SaMM) for Embedded System without MMU.
21. Almorabea, O. M., Khanzada, T. J. S., Aslam, M. A., Hendi, F. A., & Almorabea, A. M. (2023). IoT Network-Based Intrusion Detection Framework: A Solution to Process Ping Floods Originating From Embedded Devices. *IEEE Access*, *11*, 119118-119145.
22. Farooq, M. S., Javid, R., Riaz, S., & Atal, Z. (2022). IoT based smart greenhouse framework and control strategies for sustainable agriculture. *IEEE Access*, *10*, 99394-99420.
23. Schizas, N., Karras, A., Karras, C., & Sioutas, S. (2022). TinyML for ultra-low power AI and large scale IoT deployments: A systematic review. *Future Internet*, *14*(12), 363.
24. Agyemang, J. O., Yu, D., & Kponyo, J. J. (2021, September). Autonomic IoT: Towards Smart System Components with Cognitive IoT. In *Pan-African Artificial Intelligence and Smart Systems Conference* (pp. 248-265). Cham: Springer International Publishing.
25. Mehmood, M. Y., Oad, A., Abrar, M., Munir, H. M., Hasan, S. F., Muqeet, H. A. U., & Golilarz, N. A. (2021). Edge Computing for IoT-Enabled Smart Grid. *Security and communication networks*, *2021*(1), 5524025.

26. Qasem, A., Shirani, P., Debbabi, M., Wang, L., Lebel, B., & Agba, B. L. (2021). Automatic vulnerability detection in embedded devices and firmware: Survey and layered taxonomies. *ACM Computing Surveys (CSUR)*, *54*(2), 1-42.
27. Shammar, E. A., & Zahary, A. T. (2020). The Internet of Things (IoT): a survey of techniques, operating systems, and trends. *Library Hi Tech*, *38*(1), 5-66.
28. Mawlood Hussein, S., López Ramos, J. A., & Alvarez Bermejo, J. A. (2020). Distributed key management to secure IoT wireless sensor networks in smart-agro. *Sensors*, *20*(8), 2242.
29. Hameed, S., Khan, F. I., & Hameed, B. (2019). Understanding security requirements and challenges in Internet of Things (IoT): A review. *Journal of Computer Networks and Communications*, *2019*(1), 9629381.