Internet of Things and Embedded System Design: A New Technology Trend

Melvin Divine Pritchard

August 20, 2023

Abstract: The development of the Internet of Things (IoT) has sparked a technological revolution that is reshaping industries all over the world. This paper investigates the growing popularity of embedded system design in high-tech industries, notably in the context of IoT. Everyday devices outfitted with RFID or electronic barcodes can speak with one another via sensors, exchanging data and transforming the environment into a digitally connected universe. Furthermore, the essay emphasises the intimate relationship between embedded system design and IoT, explaining why embedded system design is gaining popularity in high-tech businesses. It discusses methodology, applications, difficulties, and opportunities, with an emphasis on the role of embedded system design in determining the evolution of IoT and its impact on technology.

Keywords: IoT, Security, Embedded System Design, Technological Evolution.

1 Introduction

The Internet of Things (IoT) has transformed how we engage with technology through interconnected gadgets. By seamlessly combining hardware and software to produce intelligent devices, embedded system design plays a critical part in this shift. The Internet of Things (IoT) was coined by Kevin Ashton in 1999 and was first associated with radio frequency identification (RFID) but quickly grew to incorporate varied technologies such as sensors and mobile devices (Wortmann and Flüchter, 2015; Xu et al., 2014). Because of its evolving nature, the Internet of Things (IoT) is described by Xu et al. (2014) as a global interconnected network. Identification and tracking technologies, sensor networks, communication protocols, and distributed intelligence are driving this integration, necessitating interdisciplinary collaboration (Atzori et al., 2010). IoT's impact spans home automation, e-health, and industrial sectors, ushering in transformative changes in daily life and business operations (Atzori et al., 2010). Despite its relatively short existence, IoT has influenced various industries, connecting everyday objects with Internet capabilities and data analytics (Rose et al., n.d.). Li et al. (2015) emphasize IoT's significance in an Internet-driven future, presenting concerns over its heterogeneous and expansive nature. However, IoT introduces data security risks like breaches and hacking, raising vital challenges in ensuring authentication and data integrity (Rose et al., n.d.; Atzori et al., 2010). As Embedded System Design and IoT intertwine, understanding their synergy becomes essential for harnessing the transformative potential of IoT across industries and daily life.

2 Methodology

This essay investigation is based on thorough research of the literature, analysis of relevant case studies, and examination of industry reports. By combining ideas from these various sources, this study gains a comprehensive understanding of the critical role that Embedded System Design plays in driving the IoT phenomena.

3 Discussion

3.1 Embedded System Design's Rising Prominence:

3.1.1 Evolution and Innovations:

Embedded System Design has evolved from basic microcontrollers to sophisticated System-on-Chip (SoC) archi-

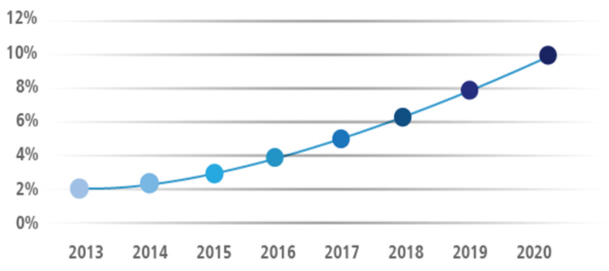


Figure 1: IoT Embedded Systems Growth Rate Source: https://radixweb.com/

tectures, driven by the pursuit of efficiency and functionality, making it a cornerstone of IoT innovation. Advanced embedded development plays a vital role in optimizing IoT by facilitating efficient data collection, management, and analysis through current sensors. IDC predicts that data from embedded systems will increase from 2 percent of the digital universe in 2013 to 10 by 2020. This growth presents opportunities and challenges. High-tech embedded development leads to more potent devices and secure data connectivity. The IoT landscape demands quick responses, centralized data management, cloud-based updates, and endpoint device control. Embedded systems are crucial for ensuring the seamless, secure, and efficient functioning of the interconnected IoT ecosystem.

3.1.2 Hi-Tech Industries and Embedded Systems:

The integration of Embedded Systems across several hi-tech sectors has resulted from the necessity for sophisticated, energy-efficient solutions. Healthcare, transportation, manufacturing, and other industries are leveraging embedded technology to create smarter, networked systems. Medical wearables with embedded technologies, for example, provide real-time health monitoring, changing patient care.

4 The IoT Revolution

4.0.1 IoT's Architecture and Potential:

The Internet of Things (IoT) encompasses a network of interconnected devices and seamless data exchange, facilitated by Embedded System Design. This foundational aspect enables devices to autonomously gather, process, and transmit data, driving innovation across sectors from smart homes to industrial automation (Li et al., 2015). The architecture of IoT plays a pivotal role in data processing and has implications for security and privacy. Insufficient confidentiality in IoT architecture can lead to risks such as economic espionage and unauthorized data disclosure (Weberand Weber, 2010). IoT architecture typically involves four stages of data flow: data collection from sensors, transmission to a network, processing, analysis, and storage in a corporate data center or the cloud. The architecture evolves alongside IoT technology, with a focus on security and interoperability. Ara et al. (2016) classify IoT architecture into three layers: Perception layer dealing with physical devices, Network layer collecting and transmitting data, and Application layer for processing and decision-making. However, their research suggests a more secure five-layered architecture, emphasizing interoperability and standardization.

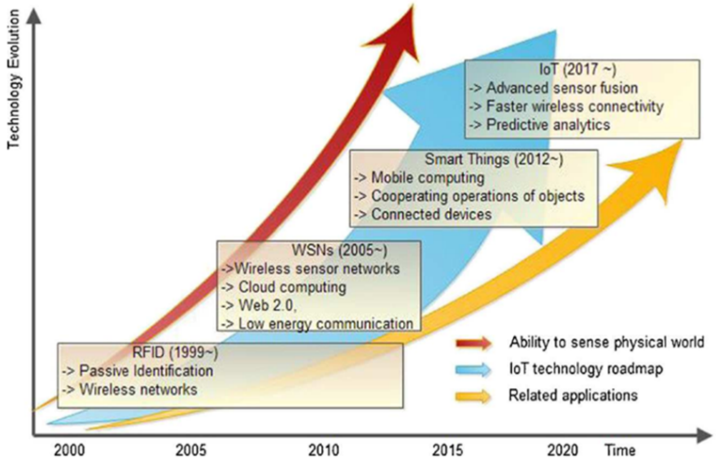


Figure 2: Figure .2 IoT evolutions (based on Li et al. 2015)

IoT architecture accommodates diverse data formats, including commands for actuators to control physical processes autonomously. Scalability, interoperability, reliability, and Quality of Service (QoS) are vital considerations in proposed IoT architectures, given the exponential growth of network traffic and storage (Khan et al., 2012). Future IoT architecture aims for ubiquity, connecting everything through sensors to meet global infrastructure requirements (Ning and Wang, 2011). Open architecture is essential for IoT, enhancing interoperability among heterogeneous systems and resources. Research is needed in

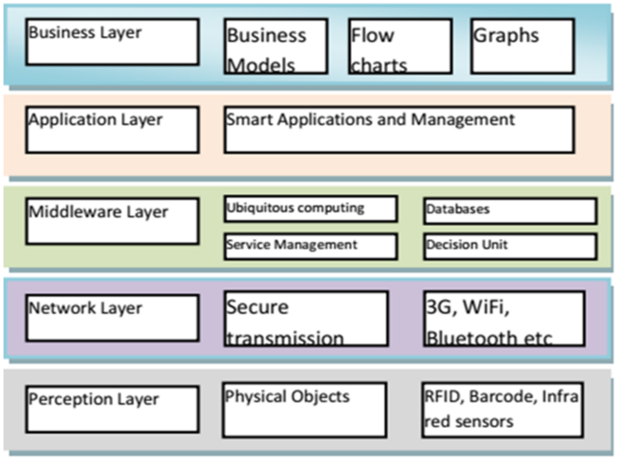


Figure 3: Five Layers architecture of IoT

sensor network technology, data models, interfaces, and protocols to align with IoT's requirements (Ahmad et al., 2019). The complexity of IoT architecture is evident in its layers, where (Ara et al., 2016; Khan et al., 2012) delineate a five-layer structure:

- Perception Layer: Collects specific information from physical objects like location, temperature, and motion, transmitting it to the transmission layer.
- Transmission Layer: Utilizes wired or wireless technologies (e.g., Wi-Fi, Bluetooth) to securely transmit data from physical objects to the middleware layer.
- Middleware Layer: Stores data, processes information, and makes decisions based on analysis results, serving as the core processing system.
- Application Layer: Manages applications based on data processed in the middleware layer, with diverse implementations such as smart health, smart farming, and intelligent transportation.
- Business Layer: Oversees the overall IoT system, developing business models, strategies, and actions based on data from the application layer, ultimately influencing the success of IoT technology.

4.1 IoT Applications and Impact:

The transformative influence of the Internet of Things (IoT) is evident across sectors like agriculture, smart cities, and industry, where Embedded Systems drive real-time data analysis, remote monitoring, and predictive maintenance. These systems form the backbone of IoT applications, enabling seamless communication and enhancing efficiency (Ara et al., 2016).

- Diverse Applications of IoT: IoT's convenience and efficiency extend to various domains, with everyday objects becoming remotely controllable through sensors. However, this rapid expansion poses challenges, including addressing threats like RFID tag attacks and data leakage (Li et al., 2015). In healthcare, IoT wearables monitor patient conditions and improve disease detection and treatment efficiency. Networked medical devices encompass consumer health monitoring, wearable and internally embedded medical devices, and stationary equipment (Ara et al., 2016). IoT's impact reaches beyond traditional sectors. Logistics, supply chains, sports, retail, social media, travel, libraries, and restaurants have all been transformed by IoT, enhancing user experiences, product tracking, and data exchange (Li et al., 2015).
- Expanding IoT Applications: IoT's potential applications span manufacturing, transportation, energy, healthcare, and government sectors. Wearable IoT devices have found use in patient monitoring, data collection, and treatment improvement. Networked medical devices, categorized as consumer health monitors, wearables, and stationary equipment, are enhancing healthcare processes (Ara et al., 2016). IoT's influence also stretches to logistics, retail, social media, libraries, and restaurants. These diverse sectors have enhanced user experiences, improved product tracking, and novel data exchange techniques (Li et al., 2015).
- Future IoT Possibilities: IoT's impact is projected to grow, encompassing disaster prediction, industry solutions, water scarcity monitoring, smart home design, agriculture, intelligent transport, smart cities, and security enhancements. Prominent organizations like Microsoft and the European Commission are actively contributing to IoT research to address pri-

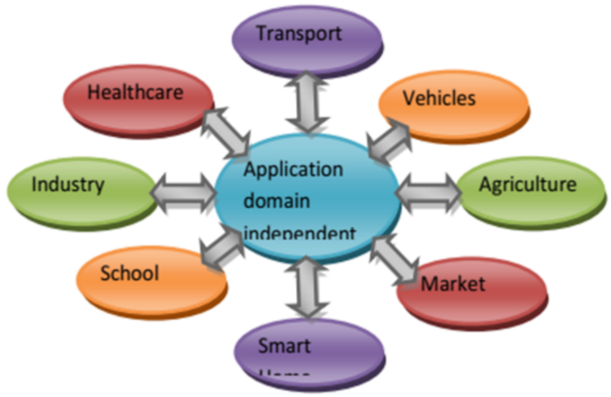
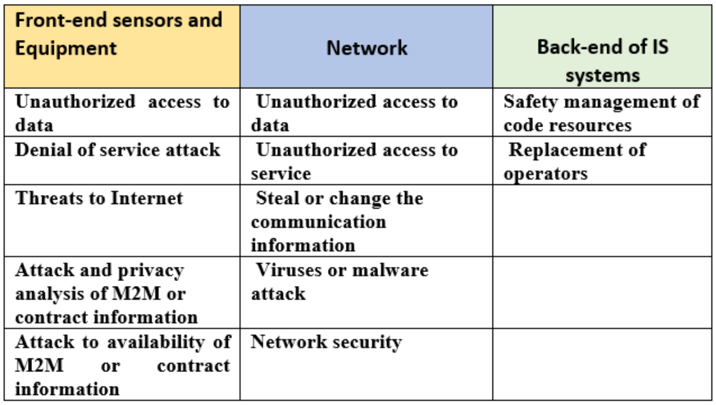


Figure 4: application of IoT



Front-end sensors and Equipment	Network	Back-end of IS systems
Unauthorized access to data	Unauthorized access to data	Safety management of code resources
Denial of service attack	Unauthorized access to service	Replacement of operators
Threats to Internet	Steal or change the communication information	
Attack and privacy analysis of M2M or contract information	Viruses or malware attack	
Attack to availability of M2M or contract information	Network security	

Figure 5: Threat in IoT Security

vacy, security, scalability, and complexity challenges (Khan et al., 2012). As IoT applications continue to evolve, they hold immense potential for revolutionizing industries and daily life, but these advancements also warrant careful consideration of their challenges and implications (Khan et al., 2012).

5 Embedded system and IOT security

The fusion of Embedded Systems and the Internet of Things (IoT) has revolutionized modern living through seamless connectivity and transformative applications across various sectors. IoT's potential is exemplified by its ability to interconnect everyday objects via sensing devices and RFID tags, generating massive data streams that enhance efficiency and resource allocation. However, this interconnected landscape exposes both IoT and Embedded Systems to an array of security vulnerabilities. The integration of smart devices, from televisions to refrigerators, underscores the need for robust security mechanisms that encompass authentication, encryption, regular updates, and secure communication protocols. Inadequate security measures, including weak encryption, lack of timely updates, and vulnerable protocols, can compromise data confidentiality, integrity, and availability. Additionally, the diverse and extensive network of IoT devices magnifies security concerns, necessitating a multi-layered approach to defense against attacks, unauthorized access, and data breaches. The security landscape encompasses various layers of the IoT architecture, including the front-end sensors, network, and back-end systems. Addressing these challenges demands industry-wide standardization, robust authentication protocols, encryption practices, and innovative solutions such as blockchain technology. As IoT applications continue to expand, the call for comprehensive security measures becomes more urgent. The collective efforts of researchers and industry stakeholders are crucial in safeguarding the potential of IoT and Embedded Systems, ensuring their transformative impact is realized without compromising privacy, data integrity, or system functionality. According to Salih (2016), while the Internet of Things improves social efficiency, it also introduces a slew of new issues, such as the confidentiality, authenticity, and integrity of data sensed and exchanged by things. Concerns about privacy and information security have arisen as a result of these issues. His research has categorized threats in the security of IoT into three as below. Following the identification of these threats, his research follows the likes of Li et al. (2015) in recommending the standardization of the IoT as a preventive measure, because the IoT supports interactions among many heterogeneous data sources and devices via the use of interfaces and data models to ensure a high degree of interoperability among diverse systems. He came to the conclusion that addressing the issue of interoperable protocol stacks and open standards for the IoT, as well as expanding the HTTP, TCP, and IP stacks to the IoT-specific protocol stack, can help to improve IoT standardization. Li et al. (2015) summarized the challenges in security and privacy protection as resilience to attacks, data authentication, access control, and client privacy. Their study proposes the following security schemes and authentication protocols to address the security threat in RFID systems:

- The Juel's method of "block tag' to prevent the unauthorized tracing.
- Low-cost RFID tags that have implemented some asymmetric key cryptography algorithms like Elliptic curve cryptography (ECC) for security.
- The security protocols developed for WSN that can be integrated as an intrinsic part of IoT.

Ara et al. (2016) research collectively identified and list some security threat faced by IoT and proposed measures to solve these security concerns.

Security threats: *Open security issues and challenges:*

- Certificate based mutual authentication using public key cryptography
- Secure bootstrapping of things.
- Privacy of sensor data in the cloud environment.
- Authentication.
- Authorization.
- Encryption and cache poisoning.

RFID System Threats:

- abuse of tags
- reader risks and
- personal privacy leak

Communication security threats

- wired and wireless communication risk and
- Denial of services (DoS).

Proposed Solutions:

- Use of IPsec and DTLS for Secure communication in the IoT.
- Use of lightweight IDS for 6LoWPAN networks that use RPL as routing protocol in the IoT
- To address these issues, IoT naming and discovery techniques may be enhanced with security schemes.
- Tag killing,
- Tag sleeping and
- Blocking of tags

6 Challenges and Considerations:

While the convergence of Embedded System Design and IoT has enormous promise, it also poses significant obstacles. Security flaws, interoperability challenges, and data privacy concerns highlight the importance of robust system design and regulatory frameworks (Salih, 2016).

7 Results and Future Outlook:

The integration of Embedded System Design with IoT ushers in an era of intelligent automation, data-driven decision-making, and superior user experiences. This IoT innovation trajectory is inextricably related to the ongoing advancement of Embedded Systems, which drives the creation of intelligent devices, efficient communication protocols, and seamless interaction with emerging technologies. As a result, the combination of Embedded System Design and IoT technology promises a future in which things, devices, and environments work in unison to improve convenience, efficiency, and sustainability.This ongoing evolution of IoT and embedded systems is poised to unveil innovative applications that transcend current imagination. In the journey ahead, hi-tech industries will persistently harness the potential of embedded systems to propel innovation and guide the unfolding of the IoT revolution towards uncharted horizons.

8 Conclusion:

The growing significance of Embedded System Design in high-tech businesses emphasises its critical role in driving the Internet of Things revolution. Embedded Systems have emerged as the backbone of innovation, providing connectivity, data-driven insights, and efficiency benefits as IoT applications alter numerous sectors. This symbiotic relationship between Embedded System Design and the Internet of Things shows technology's revolutionary potential in defining our interconnected future. While the open-standard nature of IoT technology encourages its growth, there are still concerns regarding future security and standardisation difficulties. The continual investigation of the IoT security landscape emphasises the necessity for collective security measures to maintain a safe and prosperous environment for IoT technology's future growth.

9 References

[1] A. Ahmad, S. Abdulaziz, A. Alanazi, M. Nazel, and M. Alhumaid, ”Software Architecture Solutions for the Internet of Things: A Taxonomy of Existing Solutions and Vision for the Emerging Research,” International Journal of Advanced Computer Science and Applications, vol. 10, no. 10. [Online]. Available: https://doi.org/10.14569/IJACSA.2019.0101073

[2] A. Alreshidi and A. Ahmad, ”Architecting Software for the Internet of Thing Based Systems,” Future Internet, vol. 11, no. 7. [Online]. Available: https://doi.org/10.3390/fi11070153

[3] F. Ara, M. Mahmud, and A. M. Rahmani, ”Secure Data Communication in the Internet of Things: Integration of a Standard with a Trust Model,” Sensors, vol. 16, no. 3, p. 394. [Online]. Available: https://doi.org/10.3390/s16030394

[4] T. Ara, P. Gajkumar Shah, and M. Prabhakar, ”Internet of Things Architecture and Applications: A Survey,” Indian Journal of Science and Technology, vol. 9, no. 45. [Online]. Available: https://doi.org/10.17485/ijst/2016/v9i45/106507

[5] G. Chen, T. Jiang, M. Wang, X. Tang, and W. Ji, ”Design and model checking of timed automata oriented architecture for Internet of Thing,” International Journal of Distributed Sensor Networks, vol. 16, no. 5, p. 1550147720911008. [Online]. Available: https://doi.org/10.1177/1550147720911008

[6] G. Chen, T. Jiang, M. Wang, X. Tang, and W. Ji, ”Design and model checking of timed automata oriented architecture for Internet of Thing,” International Journal of Distributed Sensor Networks, vol. 16, no. 5, p. 1550147720911008. [Online]. Available: https://doi.org/10.1177/1550147720911008

[7] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, ”Future Internet: The Internet of Things Architecture, Possible Applications, and Key Challenges,” Proceedings of the 2012 International Conference on Future Generation Communication Technology, pp. 19-24. [Online]. Available: https://doi.org/10.1109/FIT.2012.53

[8] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, ”Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges,” 2012 10th International Conference on Frontiers of Information Technology, pp. 257-260. [Online]. Available: https://doi.org/10.1109/FIT.2012.53

[9] S. Li, L. D. Xu, and S. Zhao, ”The internet of things: A survey,” Information Systems Frontiers, vol. 17, no. 2, pp. 243-259. [Online]. Available: https://doi.org/10.1007/s10796-014-9492-7

[10] S. Li, L. D. Xu, and S. Zhao, ”5G Internet of Things: A Survey,” Journal of Industrial Information Integration, vol. 1, pp. 28-39.

[11] H. Ning and Z. Wang, ”Future Internet of Things Architecture: Like Mankind Neural System or Social Organization Framework?” IEEE Communications Letters, vol. 15, no. 4, pp. 461-463. [Online]. Available: https://doi.org/10.1109/LCOMM.2011.022411.110120

[12] A. Ouaddah, I. Bouij-Pasquier, A. Abou Elkalam, and A. Ait Ouahman, ”Security analysis and proposal of new access control model in the Internet of Thing,” 2015 International Conference on Electrical and Information Technologies (ICEIT), pp. 30-35. [Online]. Available: https://doi.org/10.1109/EITech.2015.7162936

[13] K. Rose, S. Eldridge, and L. Chapin, ”The Internet of Things: An Overview,” 54.

[14] F. Wortmann and K. Flüchter, ”Internet of Things: Technology and Value Added,” Business and Information Systems Engineering, vol. 57, no. 3, pp. 221-224. [Online]. Available: https://doi.org/10.1007/s12599-015-0383-3