Headway in IoT and Robotics the Preamble of Embedded Systems in Evolving the Technology

Md. Maniruzzaman
Department of Electrical Engineering,
School of Engineering,
San Francisco Bay University,
Fremont, CA 94539, USA.
mmaniruz158@student.sfbu.edu

Abstract— **One significant growth in the in short order evolving computer era is implanted frameworks. They are elementary to pushing headways in a comprehensive extent of commercials, from customer hardware to the endless grounds of the Internet of Things (IoT) and embedded Internet of Things (EIoT). This exposition points to dismembering the modern scene and, from now on direction of inserted frameworks, supporting the cabalistic patterns and innovative breadths that are forming this dynamic field. Amid the surge of computerized transformation, inserted frameworks have risen above continuous petitions, commendable necessarily to the rise of clever systems and imaginative arrangements. Eminently, the exploding development of remote associations, ascribed to the approach of networking and internet, is set to open the omnipresent IoT time, changing divisions such as fabricating, healthcare, robotics, artificial intelligence, autonomous vehicle, and transportation systems. A modern age of momentous handling execution is being proclaimed by multicore processors and quantum computing at the same time. These progressions give more complex and fast-dealing capabilities that are essential for today's data-driven needs. Furthermore, with modern systems at the cutting edge of battling off the developing frequency of cyber threats with expanded security measures, cybersecurity is getting to be a progressively critical issue. Belatedly, a noteworthy progression has been made with the consolidation of counterfeit insights into embedded systems, empowering more Cleve and independent decision-making. This ponder looks at these squeezing patterns, giving experiences into the openings and issues they display, and anticipating long-term proposals for the embedded systems division.**

Keywords— Embedded Systems, Internet of Things (IoT), Embedded IoT (EIoT), Robotics, Multicore Processors, Quantum Computing, Cybersecurity, Artificial Intelligence (AI), Digital Transformation.

I. INTRODUCTION

Inserted frameworks, the unsung heroes of advanced insurgency, are necessary for the consistent operation and advancement inside different electronic gadgets, past the ubiquitous smartphones, portable workstations, and customer hardware [1]. These frameworks, implanted inside bigger gadgets, execute devoted capacities, hence playing an urgent part in the advanced innovative scene [2][4]. This paper digs into the transformative patterns and headways inside the inserted framework segment, highlighting its basic part within the appearance and multiplication of the Web/Internet of Things (IoT) and the Embedded Internet of Things (EIoT). These improvements imply a jump towards more associated, brilliantly, and robotized biological systems across different businesses.

The center of this article or essay is twofold. Firstly, we look at the exponential development in remote networks, impelled by progressions in internet advances, which guarantee to revolutionize divisions such as fabricating, healthcare, and savvy cities by empowering omnipresent IoT applications. Besides, we investigate the noteworthy jumps in computing control through the advancement of multicore processors and quantum computing, which guarantee to drastically upgrade preparing speeds and capabilities for implanted frameworks.

Moreover, this discussion delves deeper into the growing cybersecurity challenges, highlighting the fundamental importance of combining strong security measures inside installed frameworks to counteract the onslaught of cyber threats [3]. Finally, we draw attention to the incorporation of robotics equipment like sensor artificial intelligence (AI) with an embedded systems into inserted frameworks, highlighting the potential for these frameworks to foster more intelligent and autonomous decision-making forms.

This investigation dives deep into such pivotal contexts to establish a complete standpoint on the existing and future pathways of implanted frameworks, underscoring the possibilities, hurdles, and pointers for the widening mechanical surroundings with embedded systems and current technology.

II. METHODOLOGY

A thorough method is used to analyze IoT headways and inserted frameworks, aiming to provide a deep grasp of the long-term trajectory of IoT applications and the most recent technological advancements. This improved illustration advance outlines every stage of the method:

A. Literature Review

The written survey, which is the basis of this research, includes a thorough analysis of previous studies, innovations in technology, and theoretical frameworks related to embedded systems and the Internet of Things[5][8]. This step involves:

Sourcing Material: Uncovering credible academic articles, firm indicates, fact sheets, and case studies that can provide relevant data concerning embedded integration, IoT technologies, and their applications in several industry segments.

Critical Analysis: Analyzing strategies, evidence, as well as discussion and debate proffered manuscripts to recognize trends, shortfalls, and inconsistencies in line with the development data analysis.

Synthesis: melding data from multiple sources to form a meaningful grasp of the issues while also even though it stands at the moment, creating trends in IoT and embedded structures.

B. Data Collection

The main goal of this phase is information to support assemble noteworthy the independent inquiry:

Sources of Data: Assemble information from a multitude of sources, including instinctual sensors, Internet of Things devices, client interaction logs, and system execution records.

Tools platforms and operating systems Techniques: Application Programming Interfaces (APIs), Software Development Kits (SDKs), other electronic equipment have been utilized to retrieve information from [7].

Information characterization is just this same process of separating gleaned information in a way which is intellectually honest (unambiguous) and computational (numerical) for some further evaluation.

C. Technology Analysis

A quantitative approach to the robotic standpoints of successive IoT models and implantable cardiac structures is decided to be carried out, with just an emphasis on:

Hardware Review: analyzing the effectiveness and functionality of sensing devices, processing units, and many other embedded system components, as well as how they affect Internet of Things applications.

Software Assessment: investigating the hardware and software stuff that clinch the Internet of Things platform, with emphasis on contemporary capabilities, agility, and interconnectivity.

Connectivity Examination: Exploring cellular, Wi-Fi, and Bluetooth foundations, as well as their commitment to empowering dependable communication in Web of Things situations.

D. Security Evaluation

In IoT applications, security continues to be of utmost importance. This action entails:

Threat investigation: identifying potential risks to IoT environments' cybersecurity and counting vulnerabilities specific to implanted systems.

Countermeasure Procedures: Examine the security protocols and standards currently in use to guarantee IoT devices and data, including encryption, validation, and safe coding techniques.

Best Hones: Making recommendations based on industry benchmarks for enhancing security in IoT applications and then looking into the results.

E. Performance Metrics

Performance evaluation is crucial for IoT systems to be dependable and satisfy users:

Benchmarking: Establishing performance criteria based on user experience, power consumption, speed, and reliability for Internet of Things systems.

Testing and Validation: The performance of an Internet of Things application is compared to pre-established benchmarks through empirical testing.

Suggestions for Optimization: Highlighting areas that require enhancement and proposing suggestions for optimization to increase system effectiveness.

By carefully adhering to these principles, the technique aims to deliver a thorough analysis of current trends and future prospects in embedded systems and the Internet of Things [9]. This will offer significant insights to industry practitioners, developers, and researchers.

III. METHOD AND DISCUSSION

The model being discussed is a fictitious Internet of Things ecosystem that incorporates cutting edge embedded systems for applications related to smart cities [8]. Nowadays cloud computing systems and embedded systems has an crucial impact on IoT due to updates internet high speed internet technology like 5G, LTE, satellite internet systems (Star-link) and security systems with secure embedded systems software design, programming and size of hardware. And also robotics, micro-robotics is the important end of the physical systems. Moreover multi-tasking systems are effective and always knock to the new trends in technology.

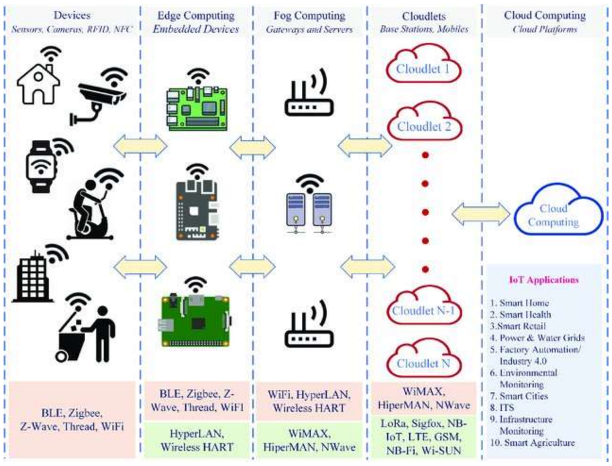


Fig. 1. Hybrid Architecture of embedded IoT

In order to increase In order to increase processing power, this model makes use of multicore processors and integrates AI algorithms for data analysis and decision-making.

Table I. IoT Ecosystem Components

Component	Description	Role in IoT Ecosystem
Multicore Processor	High-speed processing	Handle computations quickly
Sensors	Data collection	Gether real-time data
AI Algorithm	Artificial Intelligence models	Analyze data for action
Embedded Systems	Controlling systems with own program	Execute the function according to requirements

An exploded view demonstrating the hyperlinks between Internet of Things devices, embedded technology, and data processing equipment in the larger context of intelligent cities. This illustration would violently symbolize the information movement from sensors through embedded systems, multicore processor processing, and AI analysis of algorithms to help in city administration choices.

A. Concept of hypothetical ecosystem

In this model demonstrate and analysis different parts of the model which blend with Internet of Things (IoT) and the embedded system [10]. The eco systems merge with robotics equipment, control system, cloud server and security of the software.

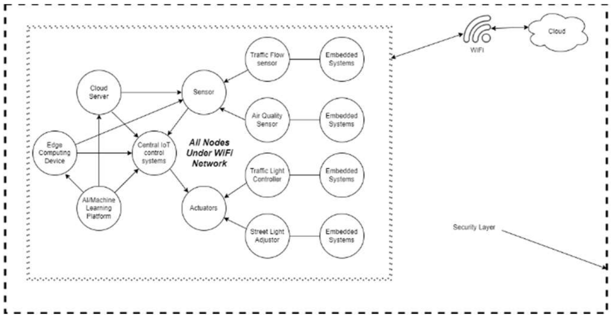


Fig. 2. Hypothetical IoT Ecosystem with embedded infrastructure

Sensors: Deployed throughout the city for monitoring various parameters like traffic flow, air quality, noise levels, and energy usage. These sensors collect real-time data, serving as the foundation for data-driven decision-making.

Actuators: Devices that perform actions based on instructions from the control system, such as adjusting traffic signals, controlling street lighting, and managing water distribution to optimize resource use and improve city services.

Embedded Systems: Embedded in every IoT device, these systems ensure the efficient processing and transmission of data. They are tailored for specific functions, from simple data logging to complex real-time analytics, operating under constraints of power, size, and connectivity.

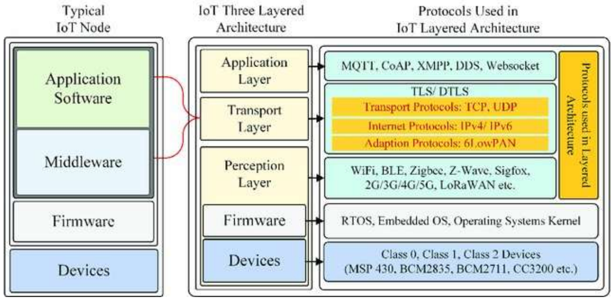

Typical IoT Node
IoT Three Layered Architecture
Protocols Used in IoT Layered Architecture
Application Software
Middleware
Firmware
Devices
Application Layer
Transport Layer
Perception Layer
Firmware
Devices
MQTT, CoAP, XMPP, DDS, Websocket
TLS/ DTLS
Transport Protocols: TCP, UDP
Internet Protocols: IPv4/ IPv6
Adaption Protocols: 6LowPAN
WiFi, BLE, Zigbee, Z-Wave, Sigfox, 2G/3G/4G/5G, LoRaWAN etc.
RTOS, Embedded OS, Operating Systems Kernel
Class 0, Class 1, Class 2 Devices (MSP 430, BCM2835, BCM2711, CC3200 etc.)
Protocols used in Layered Architecture

Fig. 3. Relation between embedded systems and IoT

Data Processing Units: Including both edge computing devices and centralized cloud servers. Edge computing nodes process data locally to reduce latency, while cloud servers perform large-scale data analysis and storage [10][12].

The arranging director can carry out tasks like device monitoring and diagnostics, software updates and maintenance, device configuration, and device control with the help of device administration. The following factors have made managing devices more difficult: 1. a growth in the quantity of equipment; 2. heterogeneous devices; 3. device versatility; 4. energetic topology; and 5. a variety of firmware updates.

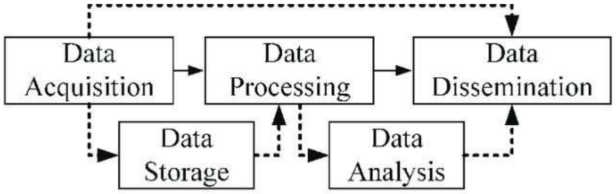


Fig. 4. Data management cycle

Communication Networks: Utilize a mix of wireless technologies, including Wi-Fi, LTE, and emerging 5G networks, to ensure seamless connectivity among IoT devices, edge computing nodes, and central servers.

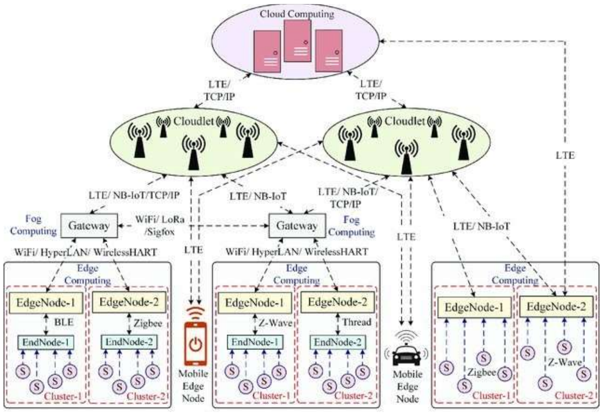


Fig. 5. IoT deployment with cloud system

AI and Machine Learning Platforms: Analyze the vast amounts of data generated by sensors to identify patterns, predict trends, and automate decision-making processes, from traffic management to environmental protection.

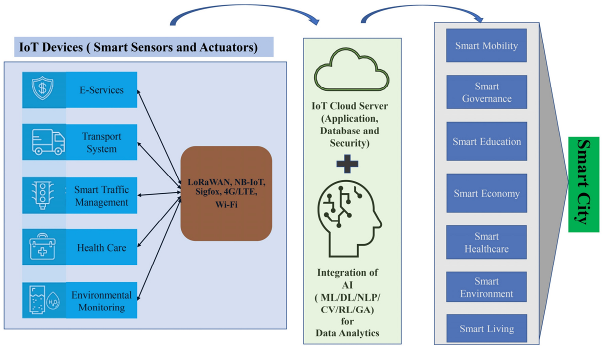
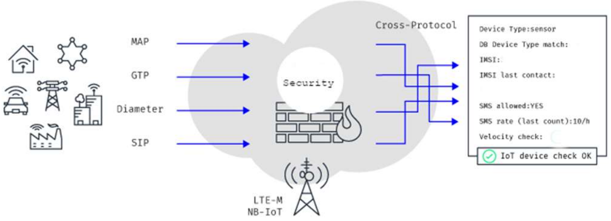


Fig. 6. Relation between AI, IoT and embedded system

Security Systems: Implement advanced encryption, blockchain technology, and secure authentication protocols to protect the ecosystem from cyber threats and ensure data privacy.



Device Type:sensor
DB Device Type match:
IMSI:
IMSI last contact:
SMS allowed:YES
SMS rate (last count):10/h
Velocity check:

Fig. 8. Cloud Security systems

This component is amazing at preventing tampering and unwanted access to an IoT system's devices, communications, and services [9][13].

Confidentiality for Appliances: Safeguarding the products attributed to a threat from the aggressor is a method of IoT device security. Smart objects traditionally go through four stages in their lifecycle: startup (building a connection and gathering data), operation (determining the question's desired use), and upgrading (installing unnecessary software and restarting). Security algorithms should be used throughout the lifespan of IoT items to ensure their security.

Communication security: It provides end-to-end protection for the channels used for communication between objects. The majority of the IoT framework's objects use remote communication technologies, and these channels are highly vulnerable to many types of assaults.

Security in Administrations: Using lightweight security calculations to protect application administrations and their data from unwanted access and modification.

B. *System application of IoRT with embedded systems*

This section will look at the suggested configuration and how it can be used with a mechanical robot. The framework is designed as a circle that gathers data from two different sources and places it in the middle. Throughout the chapter, these two segregated channels for obtaining information from mechanical robots both internal and external are discussed. which shows the information stream format in a simplified OSI (Open Source Interconnection) schematic diagram [17][20][21]. Additionally, the framework is capable of operating in reverse, which involves transmitting data from the cloud stage to the robot controller and implanted device. The entire setup was laid out for the automated cell to compile information about nearly mechanical robots and their surroundings. The chapter promotes discussions regarding the selected framework for gathering, managing, and envisioning the assembled information.

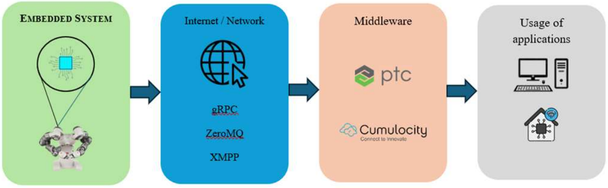
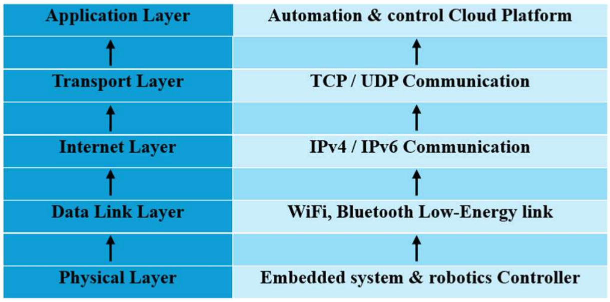


Fig. 9. The reference of embedded IoT systems

The limited information gathering capability of the robot's controller necessitates the use of various external information gathering devices. There are several advantages to developing a remote edge device for mechanical robots. The robot's functionality is maintained by removing the wire from the device or, at the very least, restricting its use. Simultaneously, the introduction of these devices on mechanical robots and frameworks is faster than before. Therefore, the obstacle that prevents the robot from working is essentially fundamental for several minutes, and the device can be re-deployed in a few minutes. The device is so simple to use that anyone can operate it without any special training.



Application Layer	Automation & control Cloud Platform
↑	↑
Transport Layer	TCP / UDP Communication
↑	↑
Internet Layer	IPv4 / IPv6 Communication
↑	↑
Data Link Layer	WiFi, Bluetooth Low-Energy link
↑	↑
Physical Layer	Embedded system & robotics Controller

Fig. 10. Simplified OSI layout with IoT works with embedded / robotics system

This method of communication is utilized for obtaining data that comes from embedded systems or robot controllers. The operator is accountable for overseeing the commercial robot's secure operation in addition to advising it by means of its tasks. It is possible to build an activity for an embedded and microcontroller robot through the use of software that is distinctive to the developer [19]. You may develop an action that functions individually compared to the one being carried out by the robot or device in addition to the task at hand itself. precisely a result, an application was developed that occasionally examines and records data regarding the robot's tandem parameters. It is essential to apply a wide range of assignments to sustain a steady flow of information gathering throughout this entire procedure. Real-time measurements of the robot joint's acceleration, status, and speed are attainable by bankruptcy. We looking forward to this information through the control and automation layer likewise. The data is processed into web-visible types of information through the robot's control system following it has read the information. As a consequence, the information assembled by the robot's joints during the time it functions appears on the server where it is stored. This strategy has been picked because it is relatively simple to apply in an industrial context, allowing eventual integration towards the system that is intended.

Industry programs obtain information released through the internet using the Open Platform Communications United Architecture server [21]. Through incorporating diverse computing and communication devices and promoting the interoperability of various apps and services, IoT software is frequently utilized to speed up the development technique. In this particular case, this application's main responsibility is to ensure that the data is readable on the intended platform. Knowing that the technique allows us to communicate data again to the robot control device is an enormous advancement. When rupture up an avenue for interaction, this has been succeeded in.

Sending Data from an Embedded Device: Both data flows are conducted via an internet-based intranet. Everyone is going to employ our network, established for Internet of Things devices, for the stated embedded device.

The primary objective of the proposed approach is to steer clear of congestion in the network. The information transfer protocol additionally requires less energy from batteries due to the fact that it lacks as much computational power. The method of communication is publish/subscribe in the environment. The recipient is able to download this message's contents using an identical unique address that the client's computer transmits to the server in a message.

The information is uploaded to the cloud-based system after it is already visible on the server. After transferring files, the information is prepared for further processing and retained in the cloud for future use [15]. The transmission of information from the device that was recommended glanced out to be extremely effective and adequate for the purposes we had in mind. Alongside accumulating information from sensors, the looping code also announces the data to the broker with this alliance. The cloud-based platform obtains notifications from the server whenever they become readily accessible. Although the machine was performing an activity, the measurement was conducted. A single minute had been utilized for calculating the time frame. In accordance with the chart, every parameter's entire data volume in a single minute is 3780 bytes. 11,340 bytes is the total quantity of data required to be transferred. Ten bytes constitute a single information volume, and we may utilize this for calculating the sampling rate, which is 6.3 samples per second.

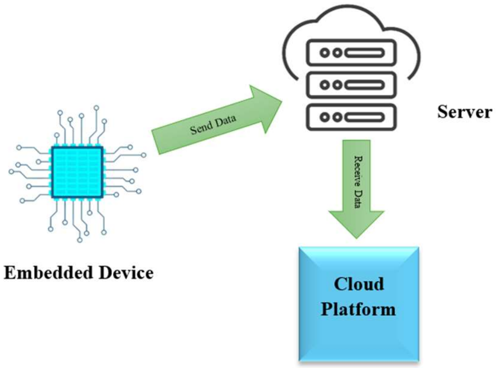


Fig. 11. Data send and receive method

Data loss during the transfer of data from the built-in device to the cloud is negligible, according to a closer examination of the data. 3.3% of the entire volume was lost in an hour. Network congestion is the primary cause of this phenomenon. The reason for this is the lab network, to which a large number of users have access during the day [15]. Data loss is a minor issue in our scenario, where the robot performs cyclical work that is, performing the same task repeatedly and the error ratio can be filtered by taking multiple cycle measurements. In the long term, we are getting the system ready for the switch to the 5G network, which promises relatively lossless data transfer.

Instructions are also sent via the communication channel between the robot controller and the cloud platform. The cloud platform can finally instruct the robot controller after processing the gathered data. One of the most significant benefits of the entire system is the ability to modify the robot's behavior in real-time in response to data gathered from multiple sources via the cloud platform.

IV. Result and consideration

A. Results

The study's inferences demonstrate a ground-breaking development in the fusion of embedded systems and the Internet of Things, bringing about a plethora of novelties ranging from enhanced cybersecurity and artificial intelligence applications to multi-core processing and quantum computing. This progression is distinguished by:

Enhanced computational capacity: The emergence of processors with multiple cores and quantum computer technology encounters significantly the use of augmented information technology capability, enabling intricate data assessment as well as prompt decision-making processes.

Modern security systems observation and measures: The investigation distinguishes significant improvements in information security tactics that preserve the integrity and confidentiality of information from worsening attacks via the internet in IoT networks.

Embedded system implementation with AI: The smooth integration of artificial intelligence techniques alongside embedded systems, which allows autonomous functioning and predictive modelling throughout IoT frameworks, is an important consequence of the convergence of machine learning and artificial intelligence.

B. Discussion

Implications for Industry and Technology: Earlier studies have established a framework for figuring out the opportunities of IoT and embedded systems. However, the research presented here deepens the discussion by illustrating how innovative technologies like intelligence from machines and quantum computing work in conjunction to strengthen IoT ecosystems, as well as contributing to a notable trend toward enhanced intelligence and unified systems.

C. Comparison with Previous Research

The foundation for figuring out the upcoming possibilities of embedded systems and the Internet of Things has been laid through earlier studies. Nevertheless, by revealing the mutually beneficial impact of cutting-edge technologies like artificial intelligence and quantum computing on IoT ecosystems, this study broadens the subject matter and information an important evolution towards enhanced intelligence and integrated systems.

D. Future Pathway

The investigation recommends that continued advancements will be possible in the direction of integrating sophisticated AI models with digital safety frameworks in the not-too-distant future. Increasing autonomy, protection, as well as effectiveness will probably be the main objectives of IoT ecosystem development, which will encourage inventiveness in applications related to smart cities, healthcare, and means of transport.

V. CHALLENGES AND OPPORTUNITIES

These developments present numerous chances for productiveness and innovative thinking, yet they additionally bring obstacles, notably in the realms of security of information, consumption of energy, and the complexity of the system. Investigation interaction, manufacturing interaction, as well as expertise in making decisions are all appropriate for tackling these hurdles.

VI. CONCLUSION

The analytical data of the acquiring disciplines with embedded systems and webs of things reveals an era of evolution marked by swift technological developments that are drastically altering the way we interact with technology the IoT and embedded are collaborating to usher in a new era of intelligence and connectedness the outcomes of this study convey crucial blueprints for maneuvering the rapidly developing IoT ecosystem environment. They stress how important it is to put in place stringent safety regulations and cutting-edge algorithms for computers and neural networks these kinds of projects are essential to creating next-generation embedded systems that are enhanced with revolutionary security features in addition to being knowledgeable and effective.

Its expansion pattern emphasizes an enormous value on expanding the IoT ecosystem comprehensively. This necessitates the thoughtful integration of technological advancements with real-world concerns like structure scalability, energy efficiency, and user confidentiality. Furthermore, through facilitating intelligent infrastructure, enhancing remote monitoring, and simplifying traffic with autopilots, this examination points out the enormous opportunity of IoT and embedded systems to entirely transform the business landscape.

Although summed up, what was learned from the research provides an in-depth comprehension of the prospects and constraints that exist with the Internet of Things. It customer demand that technology be applied proactively for the benefit of society as a whole taking into account the ethical and safety ramifications of new developments. The future development of IoT ecosystems that are safe, effective, and able to improve the way people experience the world of connectivity will be greatly facilitated by the blueprints provided by this study.

REFERENCES

[1] N. Bălău and S. Utz, ‘‘Information sharing as strategic behaviour: The role of information display, social motivation and time pressure,’’ Behav. Inf.Technol., vol. 36, no. 6, pp. 589–605, Dec. 2017.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] H. Liu, D. Han, and D. Li, ‘‘Fabric-IoT: A blockchain-based access control system in IoT,’’ IEEE Access, vol. 8, pp. 18207–18218, 2020.

[3] P. Sethi and S. R. Sarangi, ‘‘Internet of Things: Architectures, Protocols, and Applications,’’ J. Electr. Comput. Eng., vol. 2017, pp. 1–25, Jan. 2017.

[4] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, ‘‘A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications,’’ IEEE Internet Things J., vol. 4, no. 5, pp. 1125–1142, 2017.

[5] V. Miori and D. Russo, ‘‘Improving life quality for the elderly through the social Internet of Things (SIoT),’’ in Proc. Global Internet of Things Summit (GIoTS), Geneva, Switzerland, 2017, pp. 1–6.

[6] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, ‘‘The effect of IoT new neatures on security and privacy: New threats, existing solutions, and challenges yet to be solved,’’ IEEE Internet Things J., vol. 6, no. 2, pp. 1606–1616, Jun. 2019.

[7] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, ‘‘Internet of Things: A survey on enabling technologies, protocols, and applications,’’ IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[8] K. A. P. da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, ‘‘Internet of Things: A survey on machine learning-based intrusion detection approaches,’’ Comput. Netw., vol. 151, pp. 147–157, Mar. 2019.

[9] I. U. Din, M. Guizani, B.-S. Kim, S. Hassan, and M. K. Khan, ‘‘Trust management techniques for the Internet of Things: A survey,’’ IEEE Access, vol. 7, pp. 29763–29787, 2019.

[10] J. Marietta and B. C. Mohan, ‘‘A review on routing in Internet of Things,’’ Wirel. Pers. Commun., vol. 111, no. 1, pp. 209–233, Mar. 2020.

[11] S. Shin and T. Kwon, ‘‘A privacy-preserving authentication, authorization, and key agreement scheme for wireless sensor networks in 5G-integrated Internet of Things,’’ IEEE Access, vol. 8, pp. 67555–67571, 2020.

[12] Liu, Y.; Liu, X.; Gao, X.; Mu, X.; Zhou, X.; Dobre, O.A.; Poor, H.V. Robotic Communications for 5G and Beyond: Challenges and Research Opportunities. IEEE Commun. Mag. 2021, 59, 92–98.

[13] Al-Khafaji, M.; Elwiya, L. ML/AI Empowered 5G and beyond Networks. In Proceedings of the 4th International Congress on Human-Computer Interaction, Optimization and Robotic Applications, Ankara, Turkey, 9–11 June 2022.

[14] Madaan, G.; Swapna, H.R.; Singh, S.; Arpana, D. Internet of Robotic Things: Issues and Challenges in the Era of Industry 4.0. Lect. Notes Netw. Syst. 2023, 445, 89–101.

[15] Kareem, H.; Dunaev, D. The Working Principles of ESP32 and Analytical Comparison of using Low-Cost Microcontroller Modules in Embedded Systems Design. In Proceedings of the 2021 4th International Conference on Circuits, Systems and Simulation, ICCSS 2021, Kuala Lumpur, Malaysia, 26–28 May 2021; pp. 130–135.

[16] Khalifeh, A.; Mazunga, F.; Nechibvute, A.; Nyambo, B.M. Microcontroller Unit-Based Wireless Sensor Network Nodes: A Review. Sensors 2022, 22, 8937.

[17] Mijuskovic, A.; Ullah, I.; Bemthuis, R.; Meratnia, N.; Havinga, P. Comparing Apples and Oranges in IoT Context: A Deep Dive into Methods for Comparing IoT Platforms. IEEE Internet Things J. 2021, 8, 1797–1816.

[18] Ali, B.H.; Mohammedali, M.A.; Abdul-Rahaim, L.A.; Al-Kharsan, I.H.. Design of Surgical Arm Robot Based on Cloud Computin-gIn Proceedings of the IICETA 2022–5th International Conference on Engineering Technology and its Applications, Al-Najaf, Iraq, 31 May 2022–1 June 2022; pp. 289–293.

[19] Jun Na, Handuo Zhang, Jiaxin Lian, and Bin Zhang. Partitioning dnns for optimizing distributed inference performance on cooperative edge devices: A genetic algorithm approach. Applied Sciences, 12(20):10619, 2022.

[20] W. Wolf and J. Madsen, "Embedded systems education for the future", Proc. IEEE, vol. 88, no. 1, pp. 23-30, Jan. 2000.

[21] S. Loughney and A. J. Edesess, Applications of Industrial IoT and WSNs in O&M Programmes for Offshore Wind Farms, Cham, Switzerland: Springer, pp. 223-245, 2022, [online] Available: https://doi.org/10.1007/978-3-030-70787-3_15.

[22] Deploy a multilayered protection against IoT connectivity attacks. Link: https://www.mobileum.com/solutions/iot-solutions/iot-security

[23] “Next-Gen IoT: Unleashing the Potential of AI and Machine Learning for Smarter Systems”. Link: https://medium.com/@fasateaniket5/next-gen-iot-unleashing-the-potential-of-ai-and-machine-learning-for-smarter-systems-e1be7f3814d9

[24] The Latest Advancements in Embedded System Technology: Trends and Innovations. Link: https://skill-lync.com/blogs/the-latest-advancements-in-embedded-system-technology-trends-and-innovations