International Journal of Scientific Research and Management (IJSRM)
||Volume||12||Issue||12||Pages||1845-1853||2024||
Website: https://ijsrm.net ISSN (e): 2321-3418
DOI: 10.18535/ijsrm/v12i12.ec08

Review on Multi-Domain Interoperability in IoT Gateways: A Cross-Platform Approach to Web and Software Integration for Smart Ecosystems

Gireesh Kambala

MD, CMS Engineer, Lead, Teach for America, USA.

Abstract

Emphasising the integration of web and software platforms inside smart ecosystems, this review investigates the difficulties and solutions related with multi-domain interoperability in IoT gateways. Effective smart ecosystem management depends on smooth communication and data exchange between heterogeneous systems like IoT devices spread throughout many different fields. The study notes main obstacles that impede seamless integration: protocol incompatibility, security concerns, and scale problems. We discuss in great depth middleware channels, blockchain for more security, MQTT, CoAP, & common standards (e.g.). Furthermore noted is how fog computing and the edge might help to tackle bandwidth and latency issues. By means of present strategies and future approaches, this analysis emphasises the need of ongoing growth of standards and technology guaranteeing scalable, safe, and productive interoperability across numerous IoT sectors. The supplied information provides a foundation for increasing IoT system utilisation in ever more complex environments.

Keywords: Multi-domain interoperability, IoT gateways, smart ecosystems, cross-platform integration

I. Introduction

The Internet of Things (IoT) changing how devices, systems, and apps interface has produced vast smart networks spanning sectors include healthcare, smart cities, industrial IoT, crops, and beyond. IoT settings' heterogeneous nature makes integrating many devices, devices, and protocols remain challenging work. Emerging as a vital solution for seamless communication and coordination between several systems is multi-domain interoperability through IoT gateways. IoT gateways translate data and provide smooth interaction as central hubs linking devices utilising several communication protocols like MQTT, Coap, Zigbee as Z-Wave, and HTTP. By employing cross-platform approaches and powerful web and software integration technologies, these gateways guarantee security in smart ecosystems, boost scalability, and enable real-time synchronising. Since they are basic in protocol a translation. data normalisation, and preserving interoperability across various platforms, they are absolutely important for coherent operation in complex IoT environments. Using contemporary designs including microservices, containerisation platforms like Docker, & standard protocols like OPC UA—which guarantee their modularity, adaptability, & dependability—helps businesses to be most functiona [1]–[3]l.

Figure 1 IoT Gateway[4]

Artificial intelligence-driven training and data analysis are also assisting IoT gateways to become more advanced, so enabling them to offer predictive insights, automate tasks, and most effectively manage resources. In real-time applications especially when low latency, great efficiency, and consistent decision-making are demanded, these qualities are particularly important. With gates leveraging encoding, secure access control, based on a immutable records, and other methods to protect user privacy and data integrity, security comes first. Open standards and APIs foster creativity and interoperability; letting outside developers assist IoT ecosystems flourish helps to enable this. Edge computing added into IoT gateways reduces latency, guarantees reliability even in settings with periodic connectivity, and less reliance on centralised cloud services. Especially for rechargeable IoT devices, gateways' capacity to track energy efficiency and assure sustainable operations becomes even more important as IoT networks grow. Gateways, for instance, help traffic systems, energy grids, & public services link in smart cities thereby enabling real-time monitoring and optimisation. Similar productivity in industrial IoT (IIoT) is achieved by linking analytics systems, sensors, & equipment, therefore aiding automation and predictive maintenance. Gateways using hybrid cloud-edge models guarantee that essential data processing takes place at the edge; non-essential activities are offloaded to the cloud, therefore balancing performance and resource use. Hybrid systems also help to address privacy concerns by letting data localisation for private information and applying cloud capabilities for more broad analysis. IoT gateways constitute a basic infrastructure layer for multi-domain interoperability, therefore supporting the seamless integration of web technologies, APIs, and outside apps. Advanced technologies including over-the-air (OTA) updates also ensure devices remain updated with the newest software and security patches, so enabling Adoption of multi-domain interoperability frameworks guarantees that smart ecosystems can scale properly, run safely, and provide consistent, user-centric solutions as the IoT terrain gets more complex. [5]–[7]. Significant benefits come from multi-domain interoperability in IoT gateways, which lets smart ecosystems' many devices, platforms, and protocols be seamlessly integrated and communicated across. Improved scalability is one of its main advantages since IoT gateways translate protocols like MQTT, CoAP, and Zigbee into a consistent form, therefore enabling the control of big-scale, heterogeneous networks. This raises operational efficiency, so allowing real-time data synchronising or choices across areas including industrial IoT, intelligent cities, and healthcare. Computing on the edge and artificial intelligence, among other modern technologies, enable to maximise resource allocation, reduce latency, and raise predictive powers. Through user privacy and data integrity protection, blockchain-based networks, access control, & encryption all assist to increase security. Open standards & APIs let outside developers create suitable solutions driving the adoption of IoT technologies, hence fostering creativity. Furthermore, gateways provide hybrid cloud-edge models that combine bodily processing with cloud analytics and ensure reliability even in cases with limited access. Still, multi-domain openness has certain disadvantages as well. [8]–[10]. Combining numerous rules and regulations can be difficult and raise development time and costs, so particular understanding is needed. Scalability problems arise when the number of devices rises; if not built for high-throughput manufacturing, the network and gateways could overload. Maintaining security in various domains is similarly challenging since flaws in one system could endanger the whole environment. Conflicts about interoperability could originate from non-standard adherence or proprietary systems, therefore limiting compatibility. Dependency on IoT gateways brings possible single points of failure that, should they be disrupted, could affect the operation of the whole network. Notwithstanding these obstacles, multi-domain interoperability is still a pillar for developing IoT ecosystems since it balances its advantages and constraints to produce strong, scalable, and effective smart systems. Apart from enhancing operational efficiency, it generates fresh chances for creativity, teamwork, and service delivery by way of the integration of many disciplines into a coherent system. By including real-time data analytics, edge intelligence, and high connection, IoT gateways are opening the road for a future in which smart ecosystems may reach hitherto unheard-of degrees of automation, intelligence, and connectivity [11].

II. Literature Review

Nagothu 2024 Aiming at creating intelligent, given away, and autonomous infrastructues for IoT ecosystems, B5G networks of connectivity combine Blockchain, IoT, and artificial intelligence (AI). Fast expansion of these networks, however, presents challenges including safety,ability, interoperability, and connectivity. Combining Blockchain Federation with Software Defined Networks (SDN), the proposed Secure Combined Autonomous System Architecture (SIASA) leverages network slicing and decentralised security to enable safe sharing of data among autonomous systems and multi-domain IoT networks [12].

Crispo 2024 Connecting many devices with different designs and platforms becomes difficult given IoT device counts predicted to exceed 30 billion by 2030. Through a modular, open, and generally compatible IoT security stack, the CROSSCon project seeks to solve these difficulties. This stack guarantees vendor independence and is meant to be quite portable across many devices. With 11 partners spread around Europe, the CROSSCon consortium works on improving IoT connectivity and security using flexible solutions fit for heterogeneous semiconductor architectures such as ARM and RISC-V [13].

Gutierrez 2024 The growing use of World of Things (IoT) devices in important sectors has raised security concerns and so, system protection becomes a top issue. Traditional security methods have been useless based on static setups in the face of the dynamic character of developing threats since they cannot react in real time to changes in the surroundings or new attack paths. Security concerns are progressively driving IoT systems, and conventional static security solutions have shown unable to handle these changing hazards. This work presents an adaptive security architecture for IoT systems, competent of real-time detection, mitigating, and adaption to new threats. Applied in an IoT distributed system, the system showed 92% precision in threat identification and a 44% decrease in response time. Furthermore, the framework maximised power usage to just 160 milliamp-hours, therefore demonstrating its effectiveness in settings with limited resources and preserving great security [14].

Hervás 2024 Using microservices and an API-centric approach, this study proposes an API ecosystem for creating assistive technology for people with cognitive impairments. The ecosystem offers flexible applications, lowers development costs, and helps developers cooperate. GraphQL's adaptability helps to foster digital inclusion in many spheres, including healthcare and education. The modular character of the ecosystem guarantees cross-platform compatibility and helps fast development of customised assistive technologies by enabling fast development of Future projects seek to raise real-world applications by means of improved scalability, security, and integration with other systems. The continuous development of the API ecosystem—including the incorporation of sophisticated management systems—promises even more invention and cooperation in assistive technologies. Future work will concentrate on implementing a complete API management infrastructure to improve scalability, security, and monitoring abilities including incorporating and validation of the ecosystem with other apps, and so so proving its adaptability and scalability in real-world scenarios [15]

Ejaz 2024 The demand to coordinate cloud-native apps across geo-distributed groups has surged as fog computing emerges. With its growing support of multi-cluster services, Kubernetes presents difficulties organising services across several domains. According to evaluations, CPU-light microservices cause notable network overhead while spreading CPU-intensive microservices adds little cost. The answer minimises hand-operated tasks and maximises the coordination of fog-native applications among several clusters. Distribution of CPU-light microservices adds a notable network cost that exceeds the microservices workloads according to evaluation results. For CPU-intensive equivalents, the overhead ratio is rather less. The findings also reveal notable savings in hand-operated tasks [16].

Table.1 Literature Summary

Author /Year	Title	Proposed Methodology	Dataset used	Research gap	Future scope

Zhou 2024 [17]	Challenges and solutions in cross-platform mobile development : a qualitative study of Flutter and React Native	Qualitative research through semi-structured interviews with 20 developers to explore real-world experiences of framework adoption.	Developer insights from 20 semi-structured interviews on Flutter and React Native frameworks.	Limited research on real-world challenges and solutions faced by developers in cross-platform mobile app development, particularly regarding Flutter and React Native.	Further exploration into performance optimization techniques, bridging communication with native modules, and mitigating the impact of frequent framework updates.
Sattar 2023 [18]	Accelerating Cross-platform Development with Flutter Framework	Comparing Flutter, Xamarin, and React Native through case studies of cross-platform apps, assessing performance, user experience, and portability.	Case studies of mobile, web, and desktop applications developed with Flutter, Xamarin, and React Native.	Lack of a comprehensive comparison of Flutter with other cross-platform frameworks (Xamarin, React Native) regarding their effectiveness for building multi-platform applications.	Further investigation into the long-term performance and user satisfaction of apps built with Flutter exploring its evolution in supporting new platforms and features
Caminha 2023	Enabling Privacy by Anonymization in the Collection of Similar Data in Multi-Domain IoT	A pub/sub routing scheme for IoT systems that respects privacy constraints, involving routers that publish data offers and aggregate them to avoid overlap while ensuring privacy.	Data-streams from multiple IoT devices or producers, with a focus on privacy-preserving data aggregation.	Limited solutions for efficiently aggregating IoT data-streams across different providers while respecting privacy constraints and avoiding data overlap.	Further development of privacy-preserving data aggregation techniques, optimization of pub/sub routing for large-scale IoT networks,
Kamarudin 2023	Software defined internet of things in smart city	Review of SDIoT in smart cities, focusing on IoT requirements like scalability, security, and low latency.	Research papers and case studies on SDIoT applications in smart cities	Limited in-depth exploration of SDIoT's implementation in smart cities, especially in addressing issues like	Further research on SDIoT architectures, big data management, energy efficiency, and security in

				interoperability, security,	smart cities.
Turner 2023	A Promising Integration of SDN and Blockchain for IoT Networks : A Survey	Comprehensive survey of studies integrating Blockchain and SDN in IoT ecosystems, categorized by six key implementation objectives.	Research studies on BC-enabled SDN in IoT, categorized by security, computing paradigms, trust management, access control, privacy, and networking.	Limited exploration of the integration of BC and SDN into IoT ecosystems, especially regarding security, privacy, and trust management.	Further research on developing comprehensive frameworks, addressing challenges in BC-SDIoT, and exploring emerging domains like edge/fog computing, trust management, and access control.

III. Enhancing Cross-Platform Integration In Iot Gateways

Improving cross-platform interaction in IoT gateways means solving the increasing complexity of linking many IoT devices and applications across several platforms, protocols, & ecosystems. Between edge devices and main systems, IoT gateways act as middlemen allowing data flow, device control, and communication via diverse networks. IoT gateways must guarantee seamless integration between a variety of operating systems, embed hardware, and software platforms and support several methods of communication (e.g., MQTT, Coap, HTTP, etc.) to increase interoperability. Standardised communication interfaces, free to use platforms, and modular designs allowing simple addition of additional devices & protocols without needing major system reconfiguration help to do this [19]–[21].

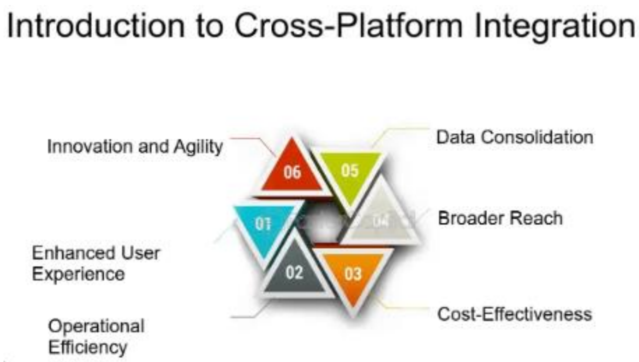

Figure 2 Cross-Platform integration [22]

Middleware or abstraction layers let the gateway abstract the complexity of underlying networking and devices, hence promoting cross-platform interoperability. Containerising technologies like Docker and orchestration tools like Kubernetes can help IoT gateway solutions be more scalable and manageable across many environments. In this environment, security and data privacy are vital and need for strong encryption methods, safe data transmission systems, and authentication processes to stop illegal access across systems. Moreover, combined with cloud integration, real-time data processing and analytics at the edge may maximise network performance and lower latency, therefore guaranteeing speedier decision-making in IoT applications. Cloud-based services may improve gateway characteristics by providing centralised data storage, artificial intelligence capabilities, and advanced analytics—which assures edge devices keep light-weight and energy-efficient. At last, reaching efficient cross-platform integration in IoT gateways would enable scalable, safe, and agile IoT ecosystems able to handle a wide spectrum of devices and applications [23].

IV. Challenges And Solutions In Multi-Domain Interoperability

Multi-domain interoperability in the Internet of Things (IoT) is the smooth integration and communication of equipment and networks housed in several domains or ecosystems. Fast development of IoT technology has produced numerous gadgets and networks spanning many industries including healthcare, intelligent houses, manufacturing automation, & transportation. While these advances provide increased efficiency and capability, establishing connectivity across so many disciplines presents enormous challenges. These challenges include security issues, data format variations and scalability issues to protocol incompatibilities. Good answers are needed to get rid of these challenges so that seamless data exchange and communication between several industries may occur [24].

1. Device Heterogeneity: One of the key challenges in multi-domain interoperability is the variation in tools or communication technology. IoT devices run on a broad spectrum of communication technologies including Zigbee and WiFi, Bluetooth, & cellular depending on their specific usage cases and domain. These protocol variants could make equipment in several domains incapable of effective interaction with one another. This lack of standards limits perfect adoption of devices from various ecosystems and generates compatibility issues. Moreover, many IoT devices are based on proprietary solutions made to run just with other devices or systems, which creates isolated IoT silos [25].

2. Data Format and Schema Inconsistencies: Variations in data structure and schema create even another key challenge for multi-domain connected devices. Sometimes different areas represent information using different data structures & standards. For medical data, for example, healthcare systems might apply HL7 or FHIR standard; smart homes might use Xml or XML for data about appliances. Using several IoT networks, aggregating, evaluating, and interpreting data becomes difficult using these different forms. Absence of a common data model or standard architecture complicates interoperability and compromises data exchange process [26].

3. Security and Privacy Concerns: Integrating internet of things across several areas raises serious questions about security and privacy. Usually, every domain has own security policies, systems, and authentication techniques. But when products from several sectors interact, security flaws could be revealed. Devices in a smart home network, for example, could not be as secure as those in an industrial or medical field. Ensuring sensitive data is delivered securely while ensuring devices can authenticate or trust each other across different domains requires a uniform security architecture, which is sometimes challenging to accomplish due of the difference of systems involved [27].

- **Adopting Common Standards and Protocols**

Using open protocols like CoAP (Forced Application Protocol) and MQTT (Message Waiting Telemetry Transport) will help IoT devices spanning many different fields communicate much more effectively. These lightweight, effective, compatible with limited devices protocols help to close the distance between several systems. Furthermore, using universal data models—such as the Web of Things (WoT) framework—standardizes data representation, hence improving interoperability by simplifying the information flow over disparate platforms [28].

Middleware Solutions: Middleware platforms guarantee seamless interaction among several IoT ecosystems by acting as middlemen between applications, gadgets, and communication systems. Without changing the underlying infrastructure, these systems offer a consistent interface to handle devices and supporting communication. Middleware solutions promote scalability and flexibility by abstracting the complexity of connecting several systems, thereby facilitating the connection of many devices, applications, and services.

Blockchain for Security: Blockchain technology offers a strong way to improve security across several-domain IoT systems. Its distributed, open, unchangeable character guarantees safe authentication, data exchange, and transaction validation across several devices. Using blockchain allows devices from several fields to create trust and safely interact without depending on centralised authorities, therefore limiting unwanted access and improving data privacy.

Edge and Fog Computing: Edge or fog computing help to process data nearer the source, hence lowering latency & bandwidth consumption. Real-time engagement is enabled via edge node or fog layer data processing, therefore addressing network congestion issues and lowering the demand for extensive cloud data transfers. This method guarantees that devices can run effectively, even in remote or resource-limited surroundings, therefore optimising performance and improving interoperability [29].

V. Optimizing Web And Software Integration For Smart Ecosystems

The way to maximise web and software compatibility for smart ecosystems is to combine advanced technologies to improve the compatibility, scalability, and usability of linked systems. Adopting standardised communication protocols as HTTP, web sockets, and RESTful APIs that enable smooth interaction between many devices and platforms is absolutely critical. By use of focused on service design (SOA) and microservices, smart ecosystems can achieve modularity and adaptability, therefore enabling the rapid development and implementation of new services without upsetting existing systems. Combining cloud-based technologies with fog computing & the edge helps to maximise speed and data processing can take place closer to the origin, therefore lowering latency and bandwidth consumption. [30]–[32]. By employing lightweight frameworks like Web of Things (WoT), which helps to simplify device interface, this allows the ecosystem to effectively manage several devices and apps. Strong encryption, token-based verification, and wireless technology including blockchain for secure transaction serve to guarantee the secrecy and reach of the data transported across devices, therefore supporting security as well. Moreover, predictive analytics made possible by machine learning techniques helps the ecosystem to actively control resources, optimise energy use, and react to real-time changes. Combining these methods helps smart ecosystems reach a higher degree of automation, dependability, & scalability, thereby enabling an efficient and healthy environment able to service an extensive array of needs in many different sectors [33].

VI. Future Directions For Iot Gateway Interoperability

Ensuring smooth interoperability among many devices and platforms becomes increasingly important as IoT networks grow. Standardising protocols, using artificial intelligence for intelligent administration, and incorporating blockchain for safe data exchange define future directions for improving IoT gateway interoperability. These developments suggest to maximise scalability, security, and integration in multi-domain IoT systems [34].

1. Enhanced Protocol Standardization: Improved protocol standardising becomes ever more crucial as IoT ecosystems expand. Many IoT devices today employ proprietary protocols, which causes major problems with interoperability. Adoption of widely acknowledged standards as MQTT, CoAP, and LwM2M will help to enable flawless communication across devices from many manufacturers and ecosystems. Standardising communication protocols will help IoT gateways to be integrated easier in the future so that devices may operate across several platforms without compatibility problems. In many different sectors, this approach will reduce integration costs, increase scalability, and promote faster IoT technology acceptance.

2. AI-Powered Interoperability Management: Intelligent technology (AI) can greatly help overcome interoperability restrictions by means of smart control over connected devices and data flow in IoT ecosystems. AI-powered systems help to increase system performance and dependability by dynamically altering channels for communication, optimising data flow, and real-time anomaly control. Moreover, predictive models can be used to project possible integration issues and so be resolved before they impact corporate operations. Artificial intelligence guarantees that the right data flows via the appropriate IoT gateways & preserves system efficiency, therefore helping context-aware decision-making.

3. Blockchain for Seamless Data Sharing and Security: Especially with relation to safety and data integrity, blockchain-based technology is supposed to be fairly crucial in enhancing IoT gateway compatibility. Blockchain's distributed, immutable ledger can be used for safe device authentication, transaction validation, and data transfer among different platforms. Blockchain makes sure gadgets in many different sectors can trust one another and safely share data, therefore removing privacy and data manipulation problems. Blockchain paired with IoT gateways offers not only safe communication but also streamlines cross-domain interoperability by allowing all stakeholders a shared platform to validate and exchange data. For sensitive application in industrial automation especially, smart cities, or healthcare, this will be absolutely vital [35]–[37].

VII. Conclusion

Effective integration of numerous devices and platforms into smart ecosystems depends mostly on multi-domain connectivity in IoT gateways. Different protocols for communication, security issues, and data management difficulties create problems that need for creative ideas dispersed throughout numerous systems. Support of standard protocols like MQTT and Coap helps to facilitate integration across several IoT environments in addition to middleware solutions. Furthermore by means of distributed, open channels of data sharing and authentication, innovations like blockchain can improve security and give confidence among devices. Reducing traffic on networks and allowing immediate access to data as well as managing bandwidth restrictions depend on edge and fog computing absolutely. Future developments should focus on enhancing existing interoperability solutions and applying creative technologies including artificial intelligence and machine learning for autonomous system management as IoT ecosystems evolve. Standardising interfaces and protocols guarantees sustainability by means of long-term scalability and sustainability. The study underlines the need of continuous research in these fields to improve the integration and performance of IoT gateways, therefore paving the route for more secure and efficient smart environments. Perfect multi-domain interoperability will allow IoT technologies to fully reach their potential, therefore enabling many other sectors more intelligent, linked, and safe systems.

References

1. F. Guo, G. Shen, Z. Huang, M. Cai, and L. Wei, "DABAC : Smart Contract-Based Spatio-Temporal Domain Access Control for the Internet of Things," vol. 11, no. April, 2023.
2. N. Slamnik-krijeˇ, G. M. Yilma, M. Liebsch, F. Z. Yousaf, and J. M. Marquez-barja, "Collaborative orchestration of multi-domain edges from a Connected , Cooperative and Automated Mobility (CCAM) perspective," vol. 4, 2023.
3. A. Mater and S. Universit, "A Web-based approach for ecosystems of heterogeneous Digital Twins," 2023.
4. G. Tripathi, J. Hamdard, S. Zafar, and J. Hamdard, *Principles of Internet of Things (IoT) Ecosystem : Insight Paradigm*, no. June. 2023. doi: 10.1007/978-3-030-33596-0.
5. M. Hassan, M. A. Gregory, and S. Member, "Multi-Domain Federation Utilizing Software Defined Networking — A Review," *IEEE Access*, vol. 11, no. January, pp. 19202–19227, 2023, doi: 10.1109/ACCESS.2023.3242687.
6. K. Y. Hong, "Graph - enabled digital twins for intelligent product lifecycle management : a multi - dimensional approach to design , manufacturing , and supply chain transformation GRAPH-ENABLED DIGITAL TWINS FOR INTELLIGENT PRODUCT LIFECYCLE MANAGEMENT : A MULTI-DIMENSIONAL," 2023.
7. M. S. Far *et al.*, "JTrack-EMA + : A Cross-platform Ecological Momentary Assessment Application Table of Contents," 2023.
8. A. Al-najjar and N. S. V Rao, "Virtual Infrastructure Twin for Computing- Instrument Ecosystems : Software and Measurements," *IEEE Access*, vol. 11, no. March, pp. 20254–20266, 2023, doi: 10.1109/ACCESS.2023.3246954.
9. W. Zhang and L. Na, "Revolutionizing Mobile App Development : The Swift Advantage in Cross-Platform Programming," vol. 6, no. 6, pp. 2347–2360, 2022.
10. P. Agbaje, A. Anjum, A. Mitra, E. Oseghale, G. Bloom, and S. Member, "Survey of Interoperability Challenges in the Internet of Vehicles," 2022, doi: 10.1109/TITS.2022.3194413.
11. L. Yang, S. Ni, Y. Wang, A. Yu, J. Lee, and P. Hui, "Interoperability of the Metaverse : A Digital Ecosystem Perspective Review," vol. 1, pp. 1–25, 2023.
12. R. Xu, D. Nagothu, Y. Chen, A. Aved, E. Ardiles-cruz, and E. Blasch, "INTERNET OF THINGS A Secure Interconnected Autonomous System Architecture for Multi-Domain IoT Ecosystems," *IEEE Commun. Mag.*, vol. 62, no. October, pp. 52–57, 2024, doi: 10.1109/MCOM.001.2300354.
13. B. Crispo *et al.*, "CROSSCON : Cross-platform Open Security Stack for Connected Devices," no. 101070537, pp. 1–8, 2024.
14. W. Villegas-ch and R. Gutierrez, "Adaptive Security Framework for the Internet of Things : Improving Threat Detection and Energy Optimization in Distributed Environments," vol. 12, no. November, 2024, doi: 10.1109/ACCESS.2024.3486983.
15. R. Hervás, V. Francisco, E. Concepción, A. F. G. Sevilla, and G. Méndez, "Creating an API Ecosystem for Assistive Technologies Oriented to Cognitive Disabilities," vol. 12, no. November,

2024, doi: 10.1109/ACCESS.2024.3487308.
16. S. Ejaz and M. Al-naday, “FORK : A Kubernetes-compatible Federated Orchestrator of Fog-native applications over multi-domain edge-to-cloud ecosystems,” no. February, 2024, doi: 10.1109/ICIN60470.2024.10494435.
17. C. Zhou, “Challenges and solutions in cross-platform mobile development : a qualitative study of Flutter and React Native,” 2024.
18. A. Sattar, P. Soni, M. K. Ranjan, and A. Kumar, “Accelerating Cross-platform Development with Flutter Framework,” no. August, pp. 0–11, 2023, doi: 10.37591/joosd.v10i2.580.
19. R. Zhao, X. Tao, D. Conzon, and E. Ferrera, “A Cross-Platform Communication Mechanism for ROS-Based Cyber-Physical System,” no. December, 2022.
20. R. Ruby, C. Xu, and Z. Zhang, “Explainable AI Over the Internet of Things (IoT): Overview , State-of-the-Art and Future Directions,” vol. 3, no. September, 2022.
21. M. Ahmed, “Importance of semantic interoperability in smart agriculture systems,” no. August, 2022, doi: 10.1002/ett.4448.
22. A. Kumar, S. Sharma, A. Singh, A. Alwadain, and B. Choi, “Revolutionary Strategies Analysis and Proposed System for Future Infrastructure in Internet of Things,” pp. 1–36, 2022.
23. B. Zhou, “Building a Smart Education Ecosystem from a Metaverse Perspective,” vol. 2022, 2022, doi: 10.1155/2022/1938329.
24. J. María, J. Valero, P. Miguel, and S. Sánchez, *Design of a Security and Trust Framework for 5G Multi - domain Scenarios*, vol. 30, no. 1. Springer US, 2022. doi: 10.1007/s10922-021-09623-7.
25. J. Stanojević, U. Šošević, M. Minović, and M. Milovanović, “An Overview of Modern Cross-platform Mobile Development Frameworks,” pp. 489–497, 2022.
26. O. J. Ajayi, J. Rafferty, J. Santos, M. Garcia-constantino, and Z. Cui, “BECA : A Blockchain-Based Edge Computing Architecture for Internet of Things Systems,” pp. 1–23, 2021.
27. I. Conference and O. N. Engineering, “SYSTEM OF SYSTEMS LIFECYCLE ENGINEERING APPROACH INTEGRATING SMART PRODUCT AND SERVICE,” no. August, pp. 16–20, 2021, doi: 10.1017/pds.2021.552.
28. A. Belsa, “Reviewing SDN adoption strategies for Next Generation Internet of Things networks Reviewing SDN adoption strategies for Next Generation Internet of Things networks,” no. February, 2021.
29. E. A. Affum, K. A. Agyekum, C. A. Gyampomah, K. Ntiamoah-sarpong, and J. D. Gadze, “Smart Home Energy Management System based on the Internet of Things (IoT),” vol. 12, no. 2, 2021.
30. R. Bahsoon, Y. Zhang, and R. Kazman, *Architecting Internet of Things Systems with Blockchain : A Catalog of Tactics*, vol. 30, no. 3. 2021.
31. D. Hummel, “Multi-domain maturity model for AI and analytic capability in power generation sector,” 2021.
32. H. Xu, “Key technologies of Secure Multi-Party Computing for Perceived Data Transmission in Internet of Things,” vol. 3, no. 5, pp. 30–42, 2021, doi: 10.25236/IJFET.2021.030504.
33. G. E. Modoni, E. G. Caldarola, N. Mincuzzi, and M. Sacco, “Integrating IoT platforms using the INTER-IoT approach : A case study of the CasAware project,” vol. 12, pp. 457–474, 2020, doi: 10.3233/AIS-200578.
34. D. Version, N. Diaz, and D. Francesco, “Semantic Interoperability in the IoT : Extending the Web of Things Architecture Semantic Interoperability in the IoT,” vol. 1, no. 1, 2020, doi: 10.1145/3375838.
35. H. Su, J. Wu, and L. Liu, “Loop Users in : The Key to Cross-Platform Data Interoperability,” no. c, pp. 23–27, 2020.
36. I. Alam, K. Sharif, F. A. N. Li, Z. Latif, M. M. Karim, and S. Biswas, “A Survey of Network Virtualization Techniques for Internet of Things Using A Survey of Network Virtualization Techniques for Internet of Things Using SDN and NFV,” no. April, 2020, doi: 10.1145/3379444.
37. A. Biørn-hansen, C. R. T. Grønli, T. A. Majchrzak, and G. Ghinea, “An empirical investigation of performance overhead in cross-platform mobile development frameworks,” pp. 2997–3040, 2020.