FUTURISTIC TRENDS IN IOT

Abstract

Researchers, academics, and industry specialists will have an excellent forum to exchange ideas and expertise through this book series. There will be publications on a number of cutting-edge technologies, both present and emerging, creative solutions, research findings, and internet of things businesses and applications. The book series is seeking authors to contribute papers that show research findings, projects, surveying studies, and industry experiences that explain noteworthy advancements in the following IOT-related fields, but are not limited to 1. IoT Communication Technologies 2. IoT Architectures & Platforms 3. IoT Performance & Management 4. IoT Privacy and Security 5. IoT Embedded Systems, Sensors, Actuators 6. Practical and Innovative Applications of IoT & IoT 7. IoT for the Industry & Business 8. IoT Operations & Interoperability 9. Augmented Reality and Virtual Reality in IoT 10. IoT & Artificial Intelligence

Authors

Dr. Mahanthesha U
Associate Professor
Department of Artificial Intelligence & Machine Learning
BNM Institute of Technology
Bengaluru, Karnataka, India.

I. INTRODUCTION

The Next Generation Internet (NGI) initiative [1] aims to maintain European leadership in cutting-edge network infrastructures and fully capitalise on the opportunities presented by the connection to physical work, or the Internet of Things (IoT), which is supported by cutting-edge computing and data infrastructure. In order to address current and specific societal challenges, the NGI and its connection to the IoT must work in tandem with artificial intelligence (AI), secure transactions, sovereignty, edge computing, interactive technologies, and social media, as shown in Figure 1. Every technical design must put a strong emphasis on ensuring that data and components are accessible to all users and profitable in a transparent, democratic manner.

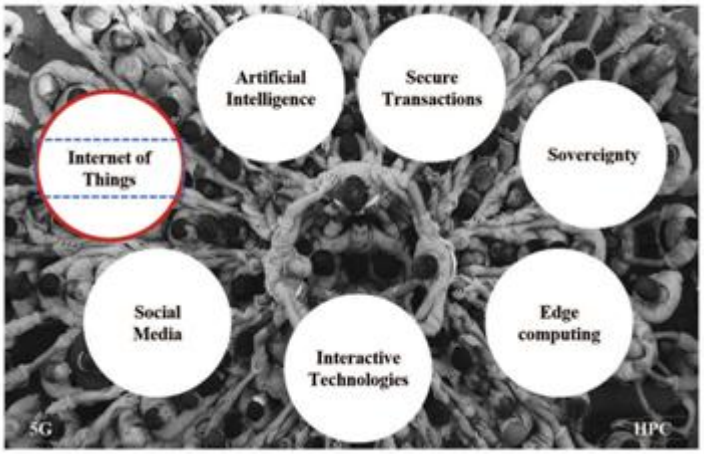

Figure 1: NGI Key Pillars.

Since the Internet of Things (IoT) technologies and applications fundamentally alter how people and society see technology and business, they are a crucial component of the Next Generation Internet. IoT is now seen as a disruptive technology that opens up new possibilities and sparks the development of new services and applications. However, the user has enormous difficulties in maintaining control of his data in terms of regulating access, sharing, and protection due to the immense volumes of data that are collected in daily life. Maintaining the sovereignty of the underlying core infrastructure that computes and stores sensitive information as well as safeguarding IoT devices from exploitation are two more of Europe's biggest issues. The societal potential of IoT is astounding: better use of the environment through smart farming, better food quality through devices allowing food traceability and oversight, better human health through devices linked to remote medicine and independent living, less greenhouse gas emissions from autonomous driving and clever logistics, fewer accidents depending on connected driving, and smart cities through the intelligent use of massive data generated from a variety of new sensors in a city.

1. **Key Technological Game Changers for IoT:** In order to meet new user demands on performance, quality of services, trust, and user control data, novel IoT architecture, platforms, and solutions will emerge and integrate fresh enabling technologies like AI, secure Distributed Ledger Technologies (DLTs), or advanced communication networks. These game-changing IoT architectures, platforms, and solutions will rely on:
   - Next-generation IoT gadgets,

- Edge computing,
- Data-centric designs,
- A community-driven commercial models, and
- A robust infrastructure are all necessary.

2. **Next Generation IoT devices:** With the introduction of tactile interface based on human-centric sensing and actuation, augmented and virtual reality paired with new IoT end-point capabilities collecting contextual surroundings, the IoT platform development will move into the next phase. IoT systems with creative user interfaces that interact with both people and other objects will develop. Real-time control, tactile (haptic) experiences, interactive, context-aware, event-driven IoT services, and greater intelligence at the edge will all be made possible by these interactive platforms. Information flows remain near to the user, choices are made at the point of interest, and data is gathered and processed locally in order to promote trust and security. The applications must integrate edge computing, IoT, and mobile autonomous systems leveraging AI technologies as functionality enablers in order for this to happen.

3. **Edge computing**: moving data processing and computation near to the data source. The typical method used in the majority of contemporary IoT systems is to carry out data processing in the cloud. Because data collecting is spread, this strategy is often the best choice. However, many IoT devices' utility diminishes over time (such as for a thermostat control). With billions of IoT devices, it makes more sense to limit data flow to the cloud and store only the information that is required rather than storing all data there. This will prevent a data flood. There are situations where a sizable volume of data is gathered in one place and the results of local data processing are utilised to regulate local operations.

   In these circumstances, edge processing is preferable than cloud processing. To satisfy real-time demands, protect privacy, and decrease the attack surface on IoT devices by keeping the most sensitive data local, this method, for example, will need additional processing power at the device and gateway level. This strategy implies a break from the vertical silo paradigm favoured by existing commercial solutions, in which all data are collected in cloud repositories and then given back to the user. Setting the confidence level based on data collected from a cloud server, combined data from federated clouds, and/or information acquired from the internet will be one of the most important study areas for edge computing.

   In the age of false news, consumers and linked systems have unprecedented difficulties in determining the right level of confidence or scepticism for any external information, despite fresh opportunities for data aggregation and manipulation utilising AI. Any future AI systems will still have a difficult time changing the way knowledge has been gleaned from sources that can be trusted and from algorithms. Contrarily, the innovative design of edge computing should facilitate more decentralised decision and action support systems that are directly accessible at the device level. Additionally, edge computing systems may undertake data filtering, processing, anonymization, etc. to provide partial views of an environment to aid in decision-making.

4. **Data-Centric Architectures**: It relies on AI approaches for data pre-processing while coping with the exponential growth in the volume of data collected across many

application domains. Having a huge number of devices and objects that require storing, processing, and timely data exchange will put a strain on the IoT platforms' storage and data flow capacities. Apart from Data Sovereignty (subject to the rules of the nation in which data is obtained and located), data storage is closely related to security and privacy elements, data marketplaces, and availability for average citizens rather than just companies and stakeholders.

Due to time restrictions, the deployment of AI (mostly machine learning) across the whole IoT pipeline will need to occur at the edge level, integrated in the devices or the gateways. In particular, an IoT data centre like the IBM Watson will be able to adapt a complete risk assessment of a system state in a complex environment. It will also be able to recognise repeating patterns and systematic failures. As previously stated, crucial tasks must be duplicated and assigned to a local agent to guarantee system functionality even while it is offline.

On the application/services side, AI-powered digital agents may function in the end user's place, communicate with the best sensors, and have access to information about the users' recent behaviours. These agents may behave independently and pro-actively up to a point, enabling a smooth transition between the physical and digital worlds. Such lightweight agents' real-time intelligence would provide smart gadgets a greater understanding of their surroundings and the user's circumstances, enabling them to act appropriately.

5. **Community-driven business models:** based on DLTs, while protecting privacy and security. A building, a neighbourhood, or city may be connected to new business models and services that are increasingly based on social networks and related to daily necessities like mobility, retail, or home care. Success stories in the economy that have developed enormously and are based on the principles of the sharing economy include Uber, Airbnb, and eBay. These peer-to-peer (P2P) markets are propelled by shared ideals and mutual interests.

Scalable and secure solutions for authentication, authorization, and accounting must develop from isolated platforms to an ecosystem of linked platforms in order to secure and permit expansion of those P2P platforms. Without a centralised platform provider, DLT provides autonomy and, in the end, protects machine-to-machine (M2M) transactions. As addition as allowing new revenue models for P2P platform services, DLT may be a solution for managing credentials for access to information from objects, including personal data.

Without a middleman or intermediary, items like money, points from loyalty programmes, intellectual property, credentials, and even identities may be exchanged safely, nearly immediately, and across the world. Blockchain-based security and privacy mechanisms may offer new advantages and opportunities to the individual users to efficiently and securely manage their personal data space, such as authenticating the data's origin and allowing the use of the data for particular stakeholders and applications, as well as allowing the control of the data's resale. The development of microcontracts and the usage of cryptocurrencies may promote the users' ultimate benefit or income. P2P platform services have the potential to disrupt traditional industrial sectors like

energy, transportation, or food chains, which would be damaging to current business structures. It is still a challenge and a duty to embrace P2P platforms that promote community development and highlight the potential of emerging technologies like DLT or blockchains for IoT platforms rather than disregard them. Although next-generation DLT technologies are required to make this a reality, DLT offers potential to mediate interactions in future decentralised IoT contexts. Present-day distributed ledgers don't appear to be scalable and struggle to deal with heavy transaction loads.

6. **Resilient and reliable infrastructure**: Infrastructures for IoT device connectivity, data streaming, and security will be needed for future IoT services and applications, along with new standards for service quality and dependability. Distributed architectures employing DLT, where the management of personal data is much enhanced, would enable decentralised data governance and data security. But in order to build trust and security, a trustworthy DLT platform would need more than just a protocol. It will also need scalable, efficient infrastructure and shared governance. In order to maximise the availability, reliability, and utilisation of data flowing from IoT, the treatment of IoT traffic will provide another difficulty for the infrastructure. New networking capabilities, software defined technologies, and distributed architectures are some of the rising trends.

II. INTEROPERABILITY

IoT settings are rather complicated because they contain heterogeneous physical devices that can support a variety of communication protocols. These devices may also be connected via a middle gateway before being connected to their virtual representations, or services, which are programmes that operate on numerous platforms. As a result, a single IoT device may be interacted with in a variety of ways utilizing its many interfaces and representations.

IoT platforms require interoperability on multiple levels, which entails identifying the distinctive functionalities of each layer and developing meta-protocols that can be mapped onto those used in the platforms (for example, resource access is the distinctive functionality on the level of syntactic interoperability). There has been a significant amount of work done in this area, particularly in the IoT-EPI, which is primarily concerned with architectures and semantic interoperability [2]. As an illustration, Figure 2.2 shows how the INTER-IoT project [3] proposed an IoT multi-layer strategy to allow semantic interoperability.

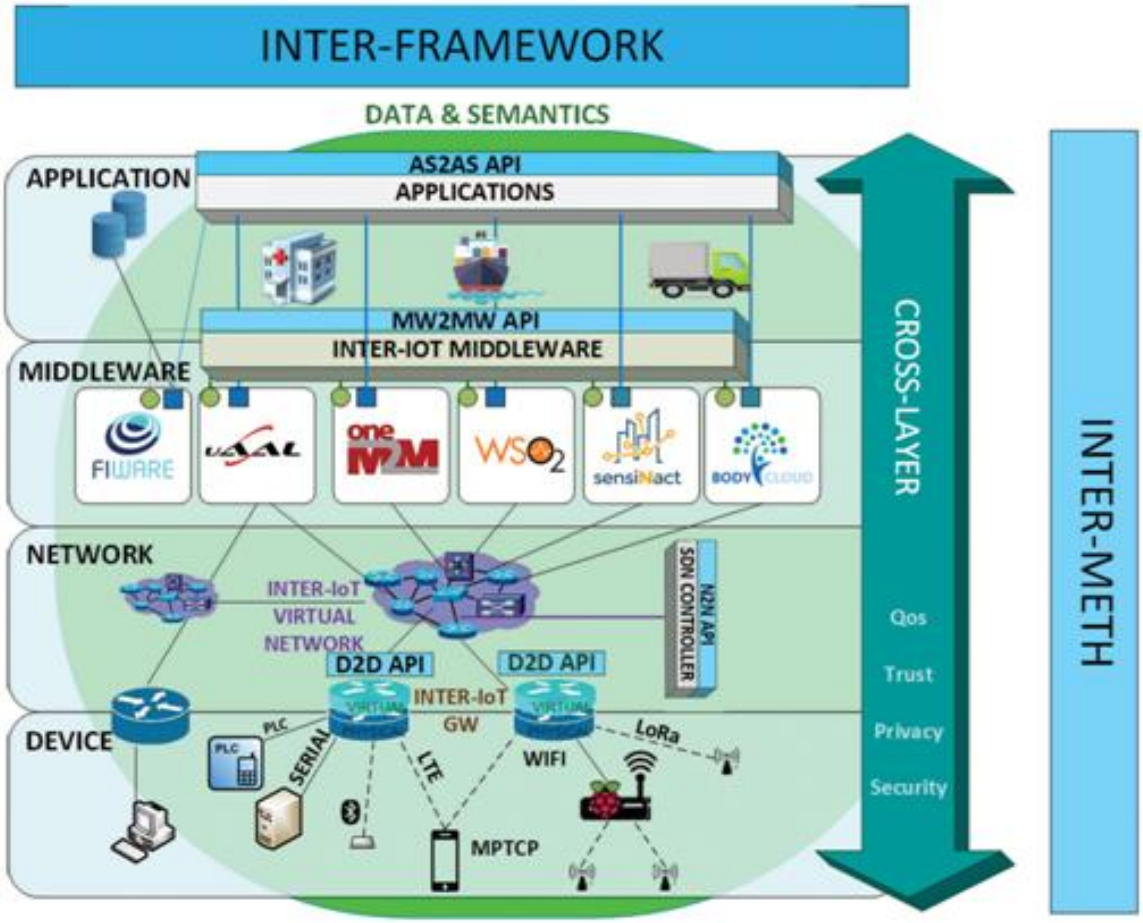

Figure 2: Inter-IoT Multi-layer architecture.

A layer-oriented approach to research is still required, nevertheless, to address tighter interoperability at all IoT system levels (device, network, middleware, application, data, and semantics), with a heavy emphasis on ensuring trust, privacy, and security elements within this interoperability.

Future internet demands, such as those for IoT applications and services, will call for a much larger object space, resource-efficient device implementation, object interaction across previously siloed application spaces, as well as support for intelligent and reliable mechanisms for service delivery. For every item to be effortlessly connected, interoperability must be supported by standards. Users of new connected products can optimise functions in their everyday lives (such as safety, entertainment and comfort, or help for daily activities).

This calls for the smooth and safe connection of items, as well as their identification based on their functioning. Despite several attempts to identify shared ontologies that might be reused and various standardisation initiatives (e.g., SAREF, W3C, or ETSI) in the area of semantic interoperability, new ontologies must be established in order to address unique deployment in a genuine interoperability context. To make ontology matching amongst IoT systems simple to support, efforts must be put into semantic translation or alignment. Continued work is required on the shared data models, vocabularies, and semantic mapping methods that, via joint efforts on the abstract core model for IoT domains, may emerge as the

essential technologies enabling semantic interoperability.

The European Commission issues a request for a pilot on interoperable smart homes and grids as part of the new focus area on digitization in the Horizon 2020 Work Programme 2018-2020 (DT-ICT-10-2018-19). The Internet of Things (IoT) is predicted to make it possible to seamlessly integrate home appliances with relevant home comfort and building automation services, enabling for the control of distributed energy throughout the grid in accordance with user demands. There will be a lot more grid-connected assets that are intelligently talking with the system thanks to the digitization of energy.

Because there are so many distinct IoT platforms from various manufacturers and industries—such as building automation, heating, electrical car charging, appliances, etc.—this presents a variety of interoperability challenges. The grid operator, the energy industry and services, as well as the evolving role of the customer or prosumer, are all part of the energy sectoral ecosystem that is currently going through a time of transformation. If interoperability can be attained across federated systems that permit the integration of data and innovative services, the interconnectedness of various systems and assets will become more strong through IoT platforms.

III. BOOSTING IOT INNOVATION AND DEPLOYMENT

Data will become increasingly important in IoT systems in the future. Identifying the economic worth of the data instances and streams in various IoT infrastructure deployment use-cases is a fundamental problem in measuring the economic value of data. Localised sensor data's accessibility will offer fresh ways to expand the IoT industry. Such data providers will see new income streams. Additionally, a new type of market will emerge: local data marketplaces, which will encourage innovation. The actual advantage from these types of data marketplaces is gained when data from sources that are diverse and sensitive are combined, especially when considering use cases like smart cities, smart transportation, or smart grids.

The European Commission favours communities and ecosystems that offer incentives for sharing data on any kind of assets or resources to create an added value through new services and applications (e.g. shared parking, car-sharing, P2P energy, etc.), in addition to technological enablers for data marketplaces like DLT. It is still difficult for public decision-makers to modify the legislative framework for the new digital economy in order to enable a Digital Single Market through Free Flow of digital, Harmonised Data Access Across Borders, Data Protection, and Data Portability.

A platform ecosystem comprising IoT platforms, IoT nodes, and collections of IoT objects will replace the IoT platform-centric point of view. We will require new common and open interoperation among all these structures rather than IoT platform businesses seeking to lock-in their clients through closed system techniques, building difficult integration linkages. Ecosystem governance is essential for managing access to data and services across the whole ecosystem, notably for the use of personal data, and for regulating the many levels of interoperation.

IV. CONCLUSION

IoT is a crucial technology that cuts across many industries and will be essential to the NGI programme. The next generation of the Internet of Things (IoT) will be based on a new generation of hardware and software that will utilise new infrastructure improvements, better sensing and actuating capabilities, end-to-end semantic knowledge, more powerful edge computing capabilities, intrinsic adoption of AI from the edge to the backbone, and the capacity to establish new relationships (like smart contracts, context awareness, or intelligent behaviour) among things, services, and people, while at the same time maintaining existing relationships.The feedback gathered from the IoT stakeholder communities and pertinent workshops is a vital source of inspiration for the strategic orientations required to promote future IoT research, development, and innovation within the context of the NGI effort. These resources are important contributors to the development of upcoming work programmes for innovation and research within Horizon 2020 and beyond.

REFERENCES

[1] The Next Generation Internet initiative, online at:
[2] https://www.ngi.eu/ IoT European Platforms Initiative – white paper on
[3] “Advancing IoTPlatforms interoperability” INTER-IoT project, online at: http://www.inter-iot-project.eu/

