A STEP FORWARD: FROM INTERNET OF THINGS TO INTERNET OF EVERYTHING

Catalin-Ionut SILVESTRU[1,*], Alexandru-Cristian FIRULESCU[2], Dumitru-Georgian IORDOC[3], Razvan-Nicusor DOBRE[4], Andreea GRECU[5]

[1] Assoc. Prof., PhD, Robots and Production System Department, University "Politehnica" of Bucharest, Bucharest, Romania
[2] Master's student, Robots and Production System Department, University "Politehnica" of Bucharest, Bucharest, Romania
[3] Master's student, Robots and Production System Department, University "Politehnica" of Bucharest, Bucharest, Romania
[4] Master's student, Robots and Production System Department, University "Politehnica" of Bucharest, Bucharest, Romania
[5] Lecturer, Ph.D., Technical University for Civil Engineering, Bucharest, Romania

Abstract: *The Internet of Things (IoT) represents a watershed moment in our modern era, emerging as one of the greatest phenomena of the century due to its rapid growth. Prior to IoT, the World Wide Web made people's lives easier by providing web services and the ability to access personal data regardless of location. Then there was the need for increased efficiency, machine-to-machine communication, smart computing, and automation. The phenomenon of IoT and, later, the concept of Internet of Everything arose from this need (IoE). This article attempts to present the Internet of Everything concept, which began in the Internet of Things, by offering a concise description of what the Internet of Things is and how it has progressed.*

Key words: *internet of things, IoE applications, internet of everything, potential capability.*

¶

1. INTRODUCTION

The Internet of Things / Internet of Everything (IoT / IoE) is a significant change that will enable pervasive computing. The Internet of Things (IoT / IoE) is quickly gaining popularity throughout the globe. Rapid progress has created many opportunities, but it has also raised people's expectations. However, because the IoT/IoE is still in its infant stages, its future structure and ingredients must be studied and defined further. The framework and components of the IoT/IoE necessitate the support of numerous applications, some of which are already in place as well as others that will be developed in the future. In terms of IoT/IoE ingredients, the combination of the cloud and IoT/IoE permits the development of smart environments.

There appears to be a lack of understanding of how the Internet of Everything will affect business, despite the great interest in these new concepts, which have the ability to revolutionize dramatically the way people live, work, and connect with one another and businesses. Companies that successfully adapt old business models to the capabilities of new technologies have great potential for innovation and competitiveness. However, the Internet of Everything presents significant challenges for companies, such as B. the development of interoperability between systems, dealing with established industry partners who refuse to work with cutting-edge concepts, legacy processes and transactions that rely on paths, contracts and responsibilities Issues, security challenges, loss of control, and privacy concerns related to the system The data collected and used by businesses is exploding.

2. IOE ESSENTIALS

Thanks to recent advancements in networking technology and the expanding availability of smart gadgets capable of connecting and sharing massive amounts of data, our world is morphing into the Internet of Everything. The term "Internet of Everything" has evolved to mean adding connectivity and intelligence to nearly any item in order to give specialized functionality. This is all too simple, though, because the Internet of Everything connects not just things, but also data, people, and (business) processes [1]. The evolution of current sensor and device networks, which have a strong interaction with people and social surroundings, will have a significant impact on everything from city planning to first responders, military, and health care. The IoE umbrella encompasses several concepts based on the Internet and connecting different entities, such as:

- Industrial Internet (II), which focuses on data from and about industries.
- The Internet of Things (IoT) is a computing concept that allows everyday physical objects to connect to the "conventional" Internet in order to identify themselves and automatically exchange data.
- With the growth of embedded and wearable technology, the Internet of People (IoP) increases people's duties beyond simple consumers and spectators of the Internet to being a part of it (wearable fitness trackers and wearable or embedded medical equipment).

Figure 1 depicts the fundamental components that make up the IoE:

[*] Corresponding author: Splaiul Independentei 313, sector 6, Bucharest, 060042, Romania,
Tel.: 021 402 9369;
E-mail addresses: *catalin.silvestru@upb.ro* (C.I. Silvestru)

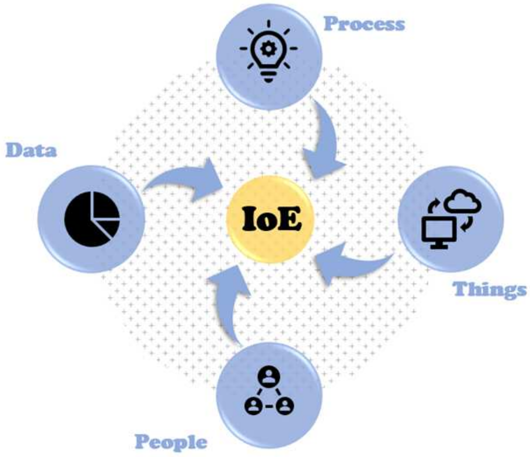

Fig. 1. Fundamental components of IoE.

- Things – Physical devices and items connected to the internet and each other for intelligent decision making.
- Process – giving the appropriate information to the right person (or machine) at the right time.
- People – bringing people together in more meaningful and productive ways.
- Data – transforming data into more actionable information.

By introducing a human aspect into the network, the IoE is constructed on top of the IoT. The Internet of Things, in particular, can improve people's lives by enabling smart connectivity between people, processes, data, and things.

IoE solutions typically include collaboration of people and things in machine-to-people (M2P), machine-to-machine (M2M), and people-to-people (P2P) connections for knowledge sharing, a pervasive observation context, and ubiquitous communication, so benefiting from the IoE lifestyle requires more than a technological perspective [2].

3. INTERNET OF EVERYTHING TECHNOLOGIES

Technology is unquestionably a major driver of the IoE's growing intellectual capacity. Interconnectivity, big data, artificial intelligence, and semantic interoperability are four technological breakthroughs related to the concept of smartness [3].

First, the emergence of the Internet of Things as a global network of interconnected objects creates new potential for improving the intelligence of everything. One of the most important properties of smart objects is their ability to recognize the environment to understand the state of the system and react appropriately. Interconnectivity makes smart components more specialized, as each component can focus on a specific function (such as sensing), while other interconnected components can leverage and enhance their own performance [4]. This specialization of IoE components is beneficial when each component responds to the environment and other components related to it. With regard to IoE, support capabilities now face new challenges, collectively referred to as functions as a service, often delivered through cloud-based services, supporting computer IoE infrastructure technologies such as: B. Computing resources - on-demand services, microservices and so-called Serverless and edge computing.

Second, the principles of smartness have long been researched in the framework of theoretical Artificial Intelligence (AI), where smart things are characterized as objects that sense, think, and conduct actions depending on the given data in order to achieve a preset objective. In this situation, smartness implies autonomous activity, which frequently requires multiple AI systems. The concept of rational, autonomous agents is not new. AI has been studied since its early days, resulting in several specific research groups focusing on different elements. For example, AI planning research examines how to achieve a particular goal by generating a sequence of actions from an initial state and forming an inferential representation. Machine learning research uses advanced statistical methods to improve the quality of interpretation of sensor data and enables intelligent agents to understand how different behaviors significantly contribute to achieving desired goals, as demonstrated by reinforcement learning. Knowledge representation research evaluates the world using a variety of logical models to allow agents to interpret facts and information and draw plausible conclusions. These domains examine not only the behavior of individual agents, but also multi-agent systems where different agents work together to achieve a common goal [5].

Third, Big Data is a critical enabler of technical development that is propelling the creation of smart objects. Technological progress has been made in two directions: improving sensing quality, which results in more data, and improving algorithms to comprehend the huge volumes of sensing data. The ever-increasing amount of data collected allows researchers to use statistical methods that were previously considered less important because they often overfit models due to lack of data, as do multilayer neural networks. The success of big data is due to advances in distributed systems, as we now know how to design scalable, fault-tolerant applications that allow storage (such as databases) and processing of large amounts of data. When it is impractical to send all data across a network for analysis in a centralized data center, improvements in edge computing allow the physical entities that generate the data to perform computations at the source [6]. Additionally, multi-layer neural networks, pattern recognition, and reinforcement learning use large amounts of data to train intelligent systems. This allows intelligent entities to exhibit adaptive capabilities while learning from large amounts of prior data. For example, big data analytics is used to improve objective functions based on real-world improvements such as: B. Improving user comfort, energy efficiency, and other human-defined goals.

Finally, the need for semantic interoperability – the ability for heterogeneous devices to understand each other – has been evident since the inception of the web and has evolved toward a multi-standard semantic web with the proliferation of online services. Mainly involves theoretical work in logic and information processing to allow reuse of logic algorithms. However, the current lack of widely accepted IoT standards hinders global interoperability, at least not unlike the level of seamless connectivity that the traditional internet has. Vendor specific IoT platforms are currently deployed to avoid this problem [7]. With the development of technologies related to service-oriented computing, global interoperability on the Web is becoming more and more available. More recently, distributed ledger technologies such as blockchain have enabled decentralized collaboration between objects and organized interoperability within subsystems that interact through smart contracts. The success of interoperability often leads to so-called intelligent environments, in which multiple cooperating devices are integrated and work together toward a common goal [8]. Despite the success of the Semantic Web, we cannot say that the problem of general semantic interoperability is solved, because different systems, such as the famous IBM Threat Resolution Computer, still require a lot of expert knowledge to achieve any form of semantic interoperability.

4. CHALLENGES OF IOE

The need to collect, store and access information across large areas, continuous service even with intermittent cloud connections and resource-constrained devices, and sometimes optimal data processing in near real-time, these challenges can only be addressed from a holistic perspective resolved above.

The fundamental challenge in the growing world of IoE devices is to increase signal accuracy and expand data interpretation capabilities while also increasing long-term operability and ensuring user privacy. Existing IoE systems that rely on nearby cell phones to operate as gateways, sending sensor data to web services, which then execute complicated DSP and ML algorithms [9]. Depending on the number of sensors used, even short-term tracking may require large amounts of data to be stored in local storage and communicated over wireless networks, affecting the battery life of the device and associated smartphone. It is critical to improve existing cutting-edge IoE solutions by allowing them to analyze and understand a wide range of sensor data trails within the devices and offer actionable warnings in an energy-efficient manner. It is critical to shift the current paradigm for developing IoE solutions from a completely Web-centric to a more distributed one by increasing the available power-efficient computational power of the devices and introducing energy-efficient sophisticated software executed on the devices, allowing them to process sensor data recordings locally and detect abnormal behavior, thereby increasing the solutions' reliability. The goal is to enhance the lifetime of IoE installations by decreasing energy consumption owing to fewer transfers of massive sensor data, and hence to minimize the total size of the electronics. Furthermore, moving data processing closer to the production site improves system response to events as well as overall awareness by removing the data round-trip to the cloud, resulting in better resource efficiency and QoE [10].

The IoE's vision has resulted in significant standardization progress across various bodies of the IEEE and the European Telecommunications Standards Institute (ETSI), offering professional solutions tailored to resource-constrained embedded nodes spanning the lower to upper Open Systems Interconnection (OSI) layers [11]. Still, there is no standard that will attract the overwhelming majority of parties and dominate the field. Current IoE installations often run privately to serve specific applications, forcing a close relationship between the program, the network the application uses, and the sensors that make up that network. Obviously, it is very difficult to develop common standards for specific applications and mission-critical systems that do not use a single protocol stack. Most efforts are inherently non-scalable, cost-effective, ill-adapted, and require a lot of work to integrate with current and established systems.

The core of IoE is the ability to integrate sensing, computation, and wireless communications into small, low-power devices that integrate smoothly into complicated physical environments. These battery-powered tiny, embedded devices have limited sensing, signal processing, and communication capabilities. The available battery resources can meet the power demands of the electronic gadget in this resource-constrained operating condition. Even if the entire energy usage of the device's computing and networking activity is improved, the battery remains the most essential resource limiting the device's longevity. Furthermore, in the case of wearables, the battery is typically a hefty component that affects the device's flexibility and hence its ease of use. As a result, it is vital to create unique energy scavenging strategies for producing energy within the gadget by utilizing the user's inherent energy (movement, heat). Such technologies will considerably increase the lifespan of the IoE solution while also allowing for future reductions in battery size, making it more autonomous.

Embedded device resource constraints, both in terms of processing power and energy capacity, make it difficult to support computationally complex encryption algorithms since they induce data transfer delays and increase energy usage. To address these issues, various approaches have been proposed, including B. Implementing cryptosystem operations on dedicated hardware components, such as the Rivest-Shamir-Adleman (RSA) cryptosystem, to optimize computational speed and energy consumption, or introducing new mechanism-based cryptosystems. Implementation options are available. Elliptic Curve Cryptography is one such example (ECC). It's important to note, however, that sensor node brands have widely disparate capabilities, making a unified solution impossible to provide.

Data acquired by IoE solutions is particularly sensitive and must be safeguarded because it is directly tied to the privacy of the users. Unfortunately, the unchecked proliferation of Internet-based services has forced us to accept many compromises in terms of data sharing. Existing IoE solutions are entirely Web-centric: all personal data collected is housed on the Web, and users rarely own the data they generate [12]. This method substantially restricts the user's capacity to maintain control over their personal data. There is a greater need than ever for privacy-preserving programs that put consumers in control of their sensitive data. These arguments were recently bolstered by the My Data is Mine declaration, which stated: "Consumers must have control over their data and should receive a fair share of the value created by corporations using their data." The ability to integrate resource-constrained IoE sensors with computer skills is critical for data security and privacy. Since the data collected from the IoE device is not sent to the cloud, data control is greatly enhanced as the user remains in control of all data collected. Doing so will leverage the advanced processing capabilities of current generation IoE devices and enhance the confidentiality of sensitive data while complying with all existing data protection regulations.

Until previously, security for embedded systems was generally considered an afterthought, rather than being incorporated directly into low-cost sensor devices. There is an urgent need for cost-effective solutions that provide robust protection while maintaining flexibility to realize real benefits in the face of anticipated risks [13]. The emergence of security services that support use across the industry requires well-designed and interoperable frameworks that span vendors and technologies and are integrated at the software and silicon levels.

End-to-end security in IoE must take into account the fact that embedded devices are more vulnerable to various attacks because their position is unknown at the time of design and protecting against tampering is challenging due to their cheap cost. As a result, it is reasonable to anticipate that the adversary may easily capture the devices and read the contents of their memory, thus acquiring the cryptographic secrets and possibly altering their behavior [14]. Furthermore, the high device-to-human ratio makes it impossible to even consider the presence of an online trustworthy server that constantly monitors and maintains individual devices. As a result, key pre-distribution approaches are far less effective than in traditional networks.

5. THE INTERNET OF BODIES

The present technology exposes an ongoing evolution of the Internet of Things into a network of human bodies known as the "Internet of Bodies" (IoB) [15]. When our human beings' integrity and functionality are reliant on the Internet and related technologies, ethical and legal concerns about the Internet of Things become more urgent. Assume that the Internet of Things poses a threat to a "buyer's" ownership and enjoyment, or that it may result in the disclosure of sensitive data. In that case, the IoB might do actual harm to people and have a direct effect on human minds and bodies. Poor Internet access, for example, could jeopardize the safety and health of IoB users who rely on life-sustaining or hardwired IoB technology.

There are three versions of IoB devices: Body External, Body Internal, and Body Melded [16]. Body External devices encompass regulated medical devices, unregulated low risk IoB devices related to general wellbeing and a healthy lifestyle, and non-health-related products such as cultural and recreational connected body-attached gadgets. Internet-enabled robotic surgery tools, prosthetics linked to a mobile application, and wearables promoting and monitoring a healthy lifestyle are examples of Body External products. Another intriguing example is brain detecting headbands, which are utilized in the classroom to check students' concentration.

Body Internal devices are IoB devices that remain within the human body or gain access to it "by breaking the skin". Pacemakers with digital components, cochlear implants with Bluetooth capabilities, digital medicines, sensor-enabled sutures, and chips with cameras used in medical operations are some examples.

Body Melded devices are IoB gadgets that are merged into the human mind via technology and the Internet. Aside from the technical problems, continuous connectivity may pose complex legal and ethical challenges. IoB devices have an impact on brain-computer interfaces and have the potential to extend and externalize elements of the human mind. The body Melded devices' objective is to achieve the utopian melding of biological intelligence and machine intelligence by linking computers directly to the human brain. These devices are largely used for cognitive improvement research and medical treatment today. Connected brain prosthetic devices, for example, are being utilized to treat Alzheimer's, Parkinson's, and epilepsy patients. Nonetheless, nonmedical applications of third generation IoB are already obvious.

When tackling complicated challenges at the intersection of IoB and criminal law, IoB devices also create legal confusion. It is unclear, for example, whether the data feed provided by an IoB device attached to the brain qualifies as testimonial evidence and should be regarded with greater judicial scrutiny by courts. The third generation of IoB devices integrated into the human brain will likely have an impact on established legal notions such as criminal law and criminal procedural law [17]. Law and ethics may face difficult quandaries in the age of IoB, when non-conscious, yet extremely intelligent algorithms may know us better than we know ourselves.

6. CONCLUSIONS

Intelligent everyday items, automatic real-time insights, and an information-centric network that connects products, processes, people, and data in a single environment are the three pillars of the Internet of Things. This article looks at the Internet of Everything's design, challenges, and barriers. This article also compares and analyzes the pros and cons of some of the more modern IoE technologies. Our lives have been invaded by the Internet of Things. The Internet of Bodies (IoB) will soon become the new normal, with human bodies and minds forming a connected network of bodies pervaded by the Internet. The move from IoT to IoB presents both opportunities for innovation and advancement, as well as risks and problems. The burden of tackling the current difficulties raised by IoT falls mostly on legislators, politicians, regulators, and consumer advocates. Public policy concerns necessitate a sense of urgency and responsiveness from both private and public actors. Because IoT is a global phenomenon, a global reaction must be coordinated. This article explored the most essential themes in depth, including IoT ideas and design, cloud computing, Cloud as a platform, and Integration Issues in Cloud Computing, IoE, and the most prevalent challenges that the Internet of Things faces.

REFERENCES

[1] Guerrieri, V. Loscri, A. Rovella, and G. Fortino. 2016. Management of Cyber Physical Objects in the Future Internet of Things. Internet of Things. Springer, Berlin. doi:10.1007/978-3-319-26869-9

[2] Aheleroff, S. et al. IoT enabled smart appliances under industry 4.0: A case study. Advanced Engineering Informatics , v. 43, 2020.

[3] Yang, L. T., Di Martino, B., & Zhang, Q. (2017). Internet of everything (editorial). Mobile Information Systems, 2017, 1–3.

[4] Russell, S., & Norvig, P. (2009). Artificial intelligence: A modern approach. Prentice Hall Press.

[5] Hippert, H. S., Pedreira, C. E., & Souza, R. C. (2001). Neural networks for short-term load forecasting: A review and evaluation. IEEE Transactions on Power Systems, 16, 44–55. https://doi.org/10.1109/59.910780.

[6] Tesauro, G., Gondek, D. C., Lenchner, J., Fan, J., & Prager, J. M. (2013). Analysis of Watson's Strategies for Playing Jeopardy!. Journal of Artificial Intelligence Research, 21, 205–251. https://doi.org/10.1613/jair.3834.

[7] Anjum, A., Sporny, M., & Sill, A. (2017). Blockchain standards for compliance and trust. IEEE Cloud Computing, 4(4), 84–90. https://doi.org/10.1109/mcc.2017.3791019.

[8] Kaldeli, E., Lazovik, A., & Aiello, M. (2016). Domain-Independent planning for services in uncertain and dynamic environments. Artificial Intelligence, 236(7), 30–64. https://doi.org/10.1016/j.artint.2016.03.002.

[9] D. Amaxilatis, O. Akrivopoulos, G. Mylonas, and I. Chatzigiannakis. 2017a. An IoT-based solution for monitoring a fleet of educational buildings focusing on energy efficiency. Sensors 17, 10, 2296. DOI: https://doi.org/10.3390/s17102296.

[10] F. Angeletti, I. Chatzigiannakis, and A. Vitaletti. 2018. Towards an architecture to guarantee both data privacy and utility in the first phases of digital clinical trials. Sensors 18, 12, 4175. DOI: https://doi.org/10.3390/s18124175.

[11] I. Chatzigiannakis, A. Vitaletti, and A. Pyrgelis. 2016. A privacy-preserving smart parking system using an IoT elliptic curve based security platform. Comput. Commun., 89–90, 165–177. DOI: https://doi.org/10.1016/j.comcom.2016.03.014.

[12] Z. He, T. Chang, S. Lu, H. Ai, D. Wang, and Q. Zhou. 2017. Research on human-computer interaction technology of wearable devices such as augmented reality supporting grid work. Procedia Comput. Sci. 107, 170–175. DOI: https://doi.org/10.1016/j.procs.2017.03.074.

[13] V. Kasapakis and D. Gavalas. 2015. Pervasive gaming: Status, trends and design principles. J. Netw. Comput. Appl. 55, 213–236. ISSN: 1084-8045. http://www.sciencedirect.com/scienc e/article/pii/S1084804515001095. DOI: https://doi.org/10.1016/j.jnca.2015.05.009.

[14] J. A. Martínez, J. L. Hernández-Ramos, V. Beltrán, A. Skarmeta, and P. M. Ruiz. 2017. A user-centric internet of things platform to empower users for managing security and privacy concerns in the internet of energy. Int. J. Distrib. Sens. Netw. 13, 8, 1550147717727974. DOI: https://doi.org/10.1177/1550147717727974.

[15] Botterman, M., & Tallacchini, M. (2018). Ethical design in the internet of things. Science and Engineering Ethics, 24, 905–925.

[16] Matwyshyn, A. M. (2019). The internet of bodies. William & Mary Law Review, 61(1), 77–167.

[17] Popescul, D., & Georgescu, M. (2013). Internet of things – Some ethical issues. The USV Annals of Economics and Public Administration, 13, 2(18), 208–214.