Internet of Energy (IoE): A Comprehensive Review of Design, Principles, and Architectural Frameworks

Rania Salih Abdalla[1], Elmustafa Sayed Ali[2,3(✉)], Sara A. Mahbub[3], Rania A. Mokhtar[1,3], and Zeinab E. Ahmed[4,5]

[1] Department of Computer Engineering, Taif University, Al-Taif, Saudi Arabia
[2] Department of Electrical and Electronics Engineering, Red Sea University, Port Sudan, Sudan
elmustafasayed@gmail.com
[3] Department of Electronics Engineering, Sudan University of Science and Technology, Khartoum, Sudan
[4] Department of Electrical and Computer Engineering, International Islamic University Malaysia, Kuala Lumpur, Malaysia
[5] Department of Computer Engineering, University of Gezira, Wad Madani, Sudan

Abstract. Design of energy resources, transmission, distribution, and consumption in network architecture is becoming a challenging energy optimization issue. The demand for power analysis becomes a key pillar in sustainable renewable energy and adaptation to climate change. State-of-the-art technologies can play a vital role in realizing the new architectural design for smart grids and cities. The 4th generation mobile network is considered a critical technology and enabler. The 3GPP standard body is set to a target of 35% of the deployment of the 4G to be Low Power Wide Area (LPWA) network by 2020. LPWA is an Internet of Energy (IoE) structure that can provide a comprehensive stream of energy sector applications. The IoE with intelligent computing tools can dramatically enhance energy efficiency, improve and sustain renewable energy, and diminish energy contamination's ecological effects. This paper reviews the literature on the IoE design principles and architecture models comprehensively. it also explains IoE enabling technologies, including fog computing and various interoperability and data analysis standards.

Keywords: Communications and measurement technology · smart energy systems · smart grid · IoE Computational Tools · IoE Design · IoE Interoperability · IoE Standards · IoE Cyber Security

1 Introduction

The term Internet of Energy (IoE) refers to an electricity solution for power flow and bidirectional information in an internet-style, known as energy internet, and is considered a smart grid extension [1, 2]. IoE evolves into a cloud network in which embedded

A. Sere et al. (Eds.): AFRICOMM 2023, LNICST 587, pp. 83–99, 2025.
https://doi.org/10.1007/978-3-031-81570-6_6

and distributed intelligence power sources communicate with smart grid and mass consumption devices such as intelligent buildings, appliances, and electric automobiles [3, 4].

In IoE, smart metering technology plays a significant fundamental role. With the use of electrical or electromechanical components, its intelligent automation applications enable consumption and energy monitoring, assisting users in managing and optimizing energy resources for both commercial and residential applications, as shown in Fig. 1. This rabid increase of IoE applications in modern life applications and industry led to the innovation of IoE standards, which will be discussed later in this paper and IoE architectures, interoperability, privacy, and security.

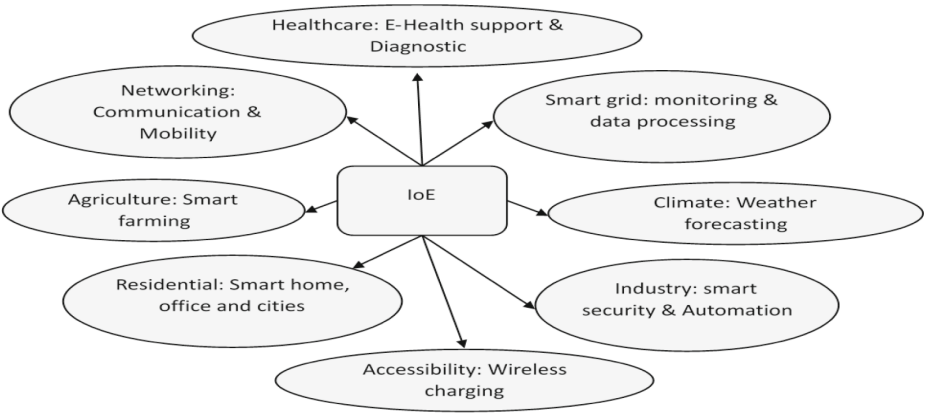

Fig. 1. IoE Applications

2 Internet of Energy Architecture

Traditionally, energy systems deploy generation, transmission, and distribution [5]. Then IoE was invented as an ICT solution to add a communication layer or functionality that integrates all system components in an "end-to-end" fashion while providing other system services [6, 7]. This integration of the IoE platform includes various sectors from system management to data security and development tools. Integrating intelligent end devices, networking, real-time capability, and integrated applications for business and mobile device portals [8]. Technically, to achieve such integration required by the IoE platform proposal, the most practical suitable tactic is the well-known Service-Oriented Architectures (SOA), where networking communication protocols are used to provide service delivery between different system components [9, 10].

2.1 EMS-Based Architecture

An Energy Management System (EMS) refers to the power grid control centre, which takes charge of monitoring and mission management. Besides its essential role in power

system operation's safety and stability, it represents a core factor in IoE architecture development [11, 12]. The developed EMS was based on a Sensor and Actuator Network (SANET) that includes HSANET installed at the customer location. At the service provider location, a Data and Service Center (DSC) is installed. Major structure components employed by EMS are shown in Fig. 2, where necessary information infrastructure is represented by the HSANET, which includes a ZigBee-based home sensor network and Zigbee-internet home gateway and control centre.

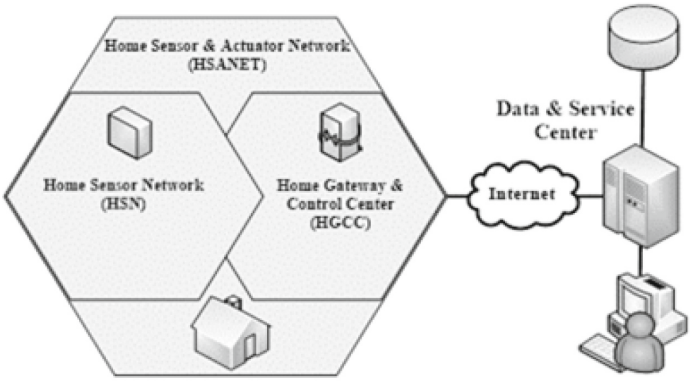

Fig. 2. Basic IoE EMS-Based Architecture

EMS improvement is emerging and reaches all energy grid operation levels from generation to distribution to enable optimal use of traditional or renewable energy sources as in decentralized generation while maintaining system stability and service quality. The architecture above represents a basic form of EMS-based architecture of IoE that was more suitable for centralized energy management. Various developed relative architectures are introduced, especially with decentralized energy generation management, as shown in Fig. 3 [13].

EMS-based IoE architecture's advancement followed different development paths. Architecture involves additional functionality and features such as various energy generation sources, energy storage, enhanced data centres, and smart metering technology. This type of architecture considers decentralized energy generation and management that may include common renewable energy forms like solar and wind; in such architectures, other conditions are also usable such as hydroelectric, geothermal, biomass, etc.

By 2020, more development on EMS-based architecture will be introduced by multiple institutes. The most common one that combines major of these developments is Micro-Service-based EMS architecture [19]. The authors here address significant EMS development factors and express the main facilities and issues with the existing EMS. They also compared their architecture against the service-oriented architecture - Energy Management Systems (SOA-EMS) based architecture from different perspectives [14].

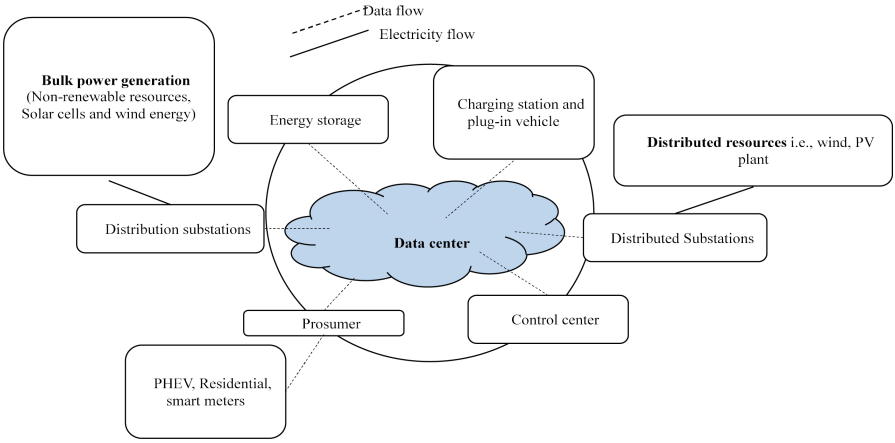

Fig. 3. An advanced EMS-based IoE Architecture

2.2 Fog Based Architecture

The challenge of addressing the optimal use to achieve both operational and business objectives by utilizing companies and customers in distributed energy resources is still an ongoing issue, initiated by the Trans Active Energy (TE) methodology. The Gridwise Architecture Council (GWAC) defined TE as an electric power system management methodology by uses economic or market-based constructs in generation, consumption, or electric power flow to provide market and control functions jointly [15]. The system connectivity map includes the flow of electrical energy through physical components or points referred to by Transactive Nodes (TN).

TNs are controlled in real-time based on economic impulses or incentives, insurance of control system scalability, which is achieved by the decentralized transactions and information exchange between the TNs [16]. A transactive node uses a Transactive Incentive Signal (TIS), which represents the foretoken transferred electric energy cost. The Transactive Feedback Signal (TFS) represents the forecasted total power flow at a particular transactive node. The balance between supply and demand has been achieved by exchanging transactive signals between the neighbouring transactive nodes. Each TN echoes the system situations among decisions related to the conductance of local assets.

The fog-based IoE architecture shown in Fig. 4 includes three different layers [17]. The first layer is responsible for providing an interface between the power grid and customers through the home gateways, by the transaction of collected energy consumption data. By positioning the Fog nodes at the network edge to function as an energy market server agent on behalf of the retail energy market server of the transactive energy system, the second layer is in charge of giving low latency services to the end consumers. The third layer is responsible for providing a high computing environment and perpetual data storage, by supporting various communication protocols such as HTTP, Constrained Application Protocol (CoAP), and Open Automated Demand Response (OpenADR) alliance [18].

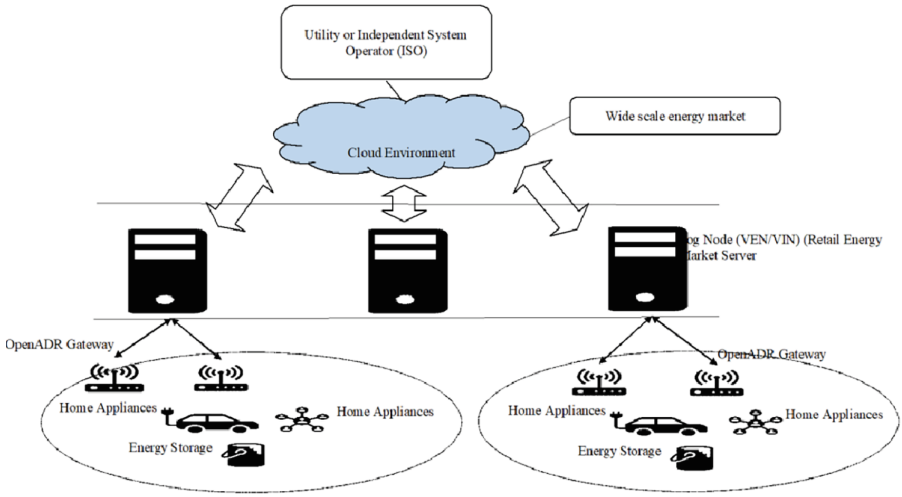

Fig. 4. Fog-based IoE Architecture

3 Hierarchical Context Awareness

Context-aware services are those that provide the user with the most relevant information based on their specific situation, including behavior-based context-aware services. The way that user behavior recognition technology learns behavior is through gathering movement-related data and analyzing it across multiple sensors. One of the key technologies that will drive the next generation of mobile phones is behavior recognition technology [20].

As the mobile phone business evolves, various sensors that are employed in behavioural recognition in mobile phones have been developed. Behaviour recognition technology for mobile phones is constantly evolving. There are several behavioural recognition approaches, the most notable of which being video-based human movement recognition, as well as sensor-based systems [21]. Because of its low power consumption and high accuracy in most wearable contexts, accelerometers are extensively utilised in sensor-based human motion identification.

Such technologies play a crucial role in IoE systems, transforming them into highly dynamic, real-time, resource-constrained, and low-transmission environments. As a result, IoE devices should give real-time behaviour management and reaction service by recognising the local scenario, as well as demonstrate optimal context-aware service by monitoring surrounding situation data such as user, social and industrial experiences [23].

3.1 Hierarchical Context Awareness Engine

Context-aware services are provided by the IoE-based technology depicted in Fig. 5, which monitors user data using smart devices and data from the user's external environment while they are in an IoE environment. This allows for real-time user behaviour

study. Two machines are needed for the IoE-based hierarchical context-aware engine: a fast machine and an adequate machine. As an example, the fast context machine hand phone gathers sensing data in order to rapidly assess a user's low-level circumstances; a low-level position is associated with an event. The required sensor data is sent to the server with the event. It offers assistance by evaluating the high-level scenario using the information base on a server equipped with a sophisticated context machine [24].

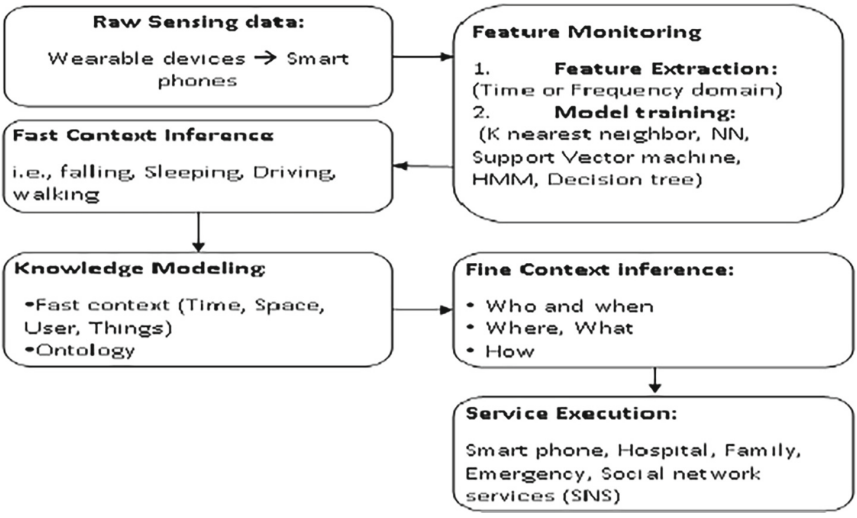

Fig. 5. IoE-based context-aware technology

There are two phases to the context-aware service, which gathers and interprets context information from users of smart devices and then provides relevant services based on the circumstances. It provides sufficient context-knowledgeable assistance for cloud servers and quick context-aware assistance for smart devices.

3.2 Fast Context Awareness Engine

Instant context trigger, ML engine, and service implementer compose the fast context awareness machine. Sensitive data for the smart device is first collected by the machine familiar with the current context when a user asks a context-aware service. At this point, sensor data could come from an internal phone sensor, an IoE sensor attached to a phone, or data gathered from a wearable device. The pre-processed data is gathered, and the ML engine uses the relevant ML algorithm to analyze the data [25].

The identification of user behaviour is facilitated by the process of combining different sensor data. For instance, a mix of weight, touch, and speed sensors in the automobile might be utilised to detect whether or not the user is actually operating the vehicle. Many algorithms in the ML algorithm database can be learned via cloud server-based ML. The real-time context trigger creates an event after evaluating the ML data, and the cloud server uses this event data on a regular basis to deliver enough context-aware service. The event data is kept in the database [26].

The predictive and analytical capabilities used in IoE are consistent with the use of ML algorithms via cloud servers. When these sensors' data is fed into ML algorithms, the algorithms are able to recognize patterns, predict energy consumption, spot any grid problems or inefficiencies, and optimise the distribution of energy [27]. Large-scale data processing can be centralised and scaled with cloud-based ML, which is essential for quickly obtaining actionable insights. Figure 6 shows a flow diagram of the fast context-aware service. Furthermore, real-time context triggers are in line with the Internet of Everything's requirement for quick response and adaptation. Contextual events that require quick responses in IoE applications include abrupt changes in energy demand, weather that affects the output of renewable energy, and system outages. To guarantee continuous and effective energy delivery, these triggers force the system to react dynamically, rerouting energy, modifying loads, or triggering backup devices.

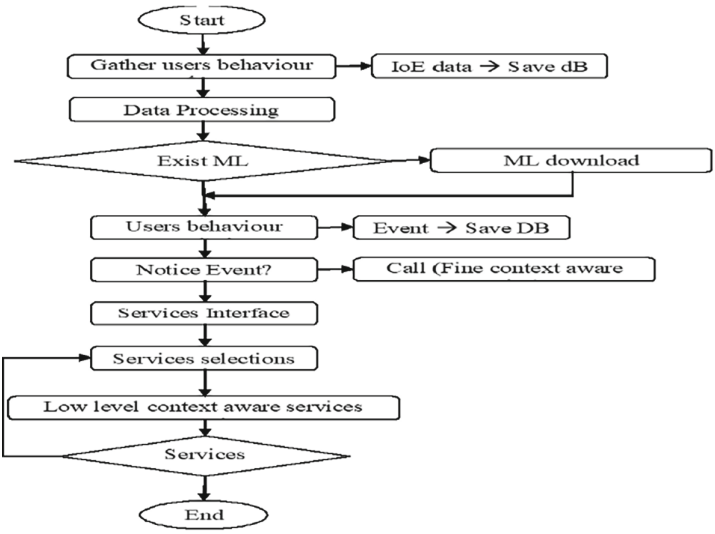

Fig. 6. Fast Context Awareness Service Flowchart

4 Computational Tools for IoE Design

As the development of emerging technology-based systems is rapidly growing and adapting its applications in various real-world fields, data analysis and storage platforms also require a suitable and sophisticated framework to integrate the systems' developments, reliability, and scalability. Especially in real-time applications and such as needed by IoE methodology. Computational environments and tools are found to meet that challenge by enabling more computation and storage capabilities that can affect system performance concurrently [28].

Development in web-based applications represents the main factor behind computation tools development and finds its way into other applications such as networking,

communication, healthcare, industry, energy, etc. As mentioned in previous sections, IoE concept occurrence and architecture evolution mainly depend on computational environment growth in cloud computing, fog or edge computing, and the latest emerging technology known as blockchain technology [29]. These technologies use a common principle: the decentralization and distribution of service nodes somehow but may differ in their locations, properties, and functionalities [30].

4.1 Cloud Computing

Cloud computing represents an evolutionary version of computational tools that consists of an improved and reliable management platform for data warehousing, data analysis, and monitoring. Cloud computing providers promise to maintain data availability and reliability of all data-related operations by providing an evolutionary infrastructure that includes multiple ways for data warehousing and data aggregation framework. Moreover, modern developed functionalities that required for emerging applications such as data monitoring and visualization, big data analysis, real-time and low latency processing, and diversity of computation resources [31]. Cloud computing introduced various solutions for service providers by offering four primary services; Infrastructure as a Service (IaaS), Platform as a Service (Paas), Software as a Service (SaaS), and Backend as a Service (BaaS).

Cloud computing upgraded the traditional computation environment by enabling any on-demand and data availability by distributing services into multiple locations from central servers. Where the Virtual Machine (VM) plays the main role of enabling multiple and different computation capabilities on a single hardware, software development plays an essential role in building Application Programming Interfaces (API) for data interaction and management [32]. Additionally, cloud computing offers excellent integration and compatibility with IoT applications and platforms by enabling multiplicity for various IoT platforms and higher system bandwidth capabilities required by IoT applications [33]. The application of cloud computing in IoE introduces more opportunities and solutions in today's challenges between demand and suppliers.

4.2 Fog Computing

Generally, the Fog Computing concept grows with the spreading of IoT applications. It differs from cloud computing by adding a new concept called edge computing, which are major device at an edge between supplier and customer gateways [34]. These edge devices represent the new layer added to bridge terminals with the system computation core as shown in Fig. 7, Fog computing never eliminates cloud computing but represents an evolutionary version that complements cloud computing by adding an edge node. With the growth of Fog computing and its applications in developing systems, IoE is also involved in this development.

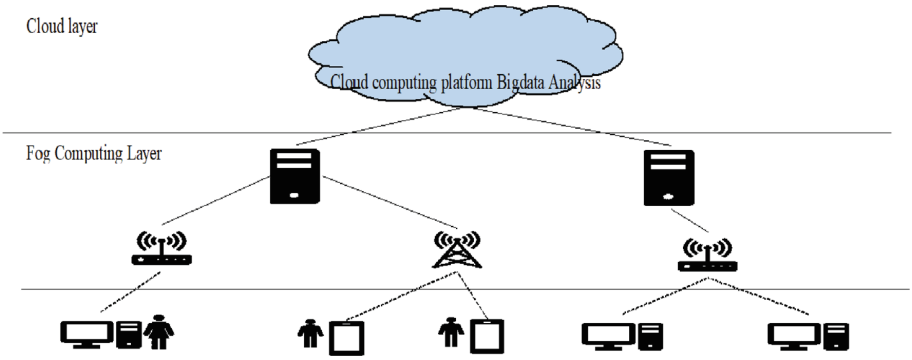

Fig. 7. Fog Computation Architecture

5 IoE Standards

Technical instructions and specifications of most ICT applications are standardized by the Institute of Electronics and Electrical Engineering IEEE. To allow the demands and reliability of renewable energy, IEEE has established multiple standards and guidelines to cover ICT aspects across many geographic; and Standards Development Organization (SDO) boundaries for smart energy systems, which are summarized in Table 1.

Table 1. Main IEEE standard for Smart Energy Systems

Standard series	NAME	Description
IEEE 2030	Smart Grid Interoperability	For data flow security, reliability, bi-directional electric power flow and comprise electric cars.
IEEE 1686, IEEE C37.240, and IEEE 1711 series	Cyber Security for Smart Grid	For cyber security in Smart Electronic node Automation and Substation.
IEEE 170X, IEEE 1377, IEEE 2030.5, and IEEE 1901 series	Smart Metering and Demand Response	For smart network grid protocols, intelligent grid profiles, and intelligent metering functionality.
IEEE C37.118, IEC/IEEE 61850-9-3, IEEE 1815, IEEE C37.238, series	Substation Automation	Includes clock protocol, timing work, and electric power system network.
IEEE 2030.1.1	Electric Vehicle Charging	For interface design of electric cars

Table 2. IEEE 2030 standard recommendations and practice guides

Standards	Description
IEEE 2030	Smart Grid Interface with Data Technology Process and Energy Technology for Electric Power System (EPS)
IEEE 2030.1.1	Standard Technical Specifications of a DC Quick Charger and Bi-directional Charger for Use with Electric Vehicles
IEEE 2030.2	The interface of Energy Storage Systems (ESS) combined with the EP Structure
IEEE 2030.2.1	Operation, Design, and Conservation of Energy Storage Systems (ESS)
IEEE 2030.3	Test process for Energy Storage system and equipment Electric Applications
IEEE P2030.4	Draft Guide for Control and Automation Installations Applied to the Electric Power Infrastructure
IEEE 2030.6	Advantage Assessment of Power Grid Consumer Request Answer
IEEE SA - 2030.5™	Ecosystem Steering Committee
IEEE 2030.5	Smart Energy Profile Application Protocol Standard
IEEE 2030.7	Specification of Microgrid Controllers
IEEE 2030.8	Testing of Microgrid Controllers
IEEE 2030.9	Recommended Practice for the Planning and Design of the Microgrid
IEEE 2030.100	Practice for Implementing an IEC 61850 Based Substation Communications, Protection, Monitoring and Control System
IEEE 2030.101	Designing a Time Synchronization System for Power Substations
IEEE P2030.100.1	Draft Monitoring and Diagnostics of IEC 61850 Generic Object-Oriented Status Event (GOOSE)
IEEE P2030.102.1	Interoperability of Internet Protocol Security (IPsec) Utilized within Utility Control Systems

5.1 IEEE 2030 Standard

IEEE 2030 standard is intended to but the roadmap to achieve smart grid interoperability by establishing the Smart Grid Interoperability Reference Model (SGIRM) that models the framework of engineering principles to apply smart grid interoperability upon all-electric power system components. These visions look beyond the year 2030 and predict how the smart grid will evolve for each of these technology-focused areas. The package of the IEEE 2030 standard series includes many recommendations and guides for the design, implementation, and evaluation sectors of smart grid systems, as summarized in Table 2.

5.2 IEEE 802.15.4g

Design consideration of smart grids requires modern solutions for networking and communication operations. WiFi and Zigbee wireless communication were the available suitable standards and demonstrated with some basic smart grid applications. Still, more specifications and procedures are required; the IEEE 802.15.4g standard is developed to meet that requirement. IEEE-802.15.4g describes the standard wireless network platform for intelligent utility service, the structure of IEEE-802.15.4g network standard, as shown in Fig. 8.

5.3 IEEE 21450 and IEEE 21451

International Organization for Standardization and International Electrotechnical Commission ISO/IEC/IEEE 21450 standard provides a common foundation for members of the ISO/IEC/IEEE 21451 series of International Standards to be able to exchange and make use of data. It realizes the functionalities achieved by the Transducer Interconnect Model (TIM) and joint features for TIM-based nodes. It also defines the setups for Transducer Electric Datasheets (TEDS) and the set of instructions to simplify the configuration and control of the TIM and read and write the data used by the system. To enable transmission with applications, TIM, and Application Program Interfaces (APIs) are defined [35].

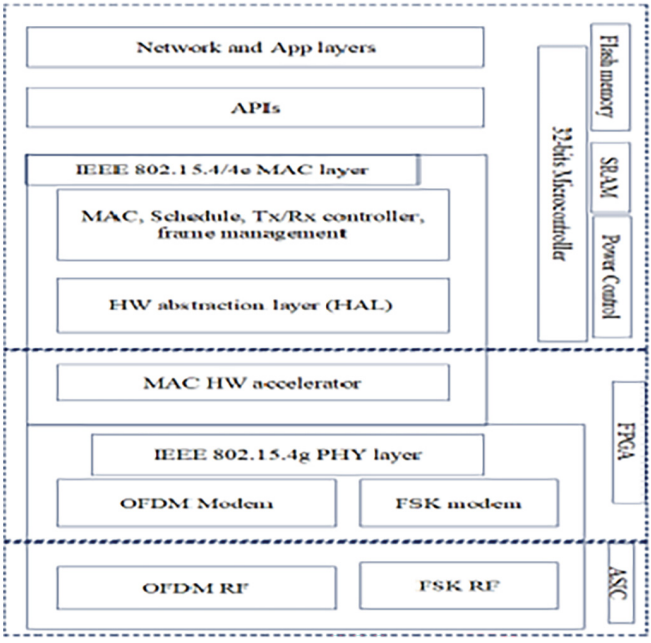

Fig. 8. IEEE 802.15.4G Communication platform architecture

6 IoE Privacy and Security

In critical infrastructures such as smart power grids and IoE, dependability and security are not fully understood yet, and privacy is an additional security objective. The IEEE provides an overview of security issues, strategies, security requirements, risk management, security design, and countermeasures besides the standards and best practice recommendations. Additionally, end-to-end security, security by design, and security in-depth are the most important security concepts that must be included within the conceptual security model.

In the IoE, design security is typically established in relation to the assembly of systems, solutions, and architectures as well as the production of specific goods. The concept of security in depth recognises that no security feature is impenetrable on its own and that the only way to achieve security greater than the sum of its parts is to apply various security controls layered in a concentric manner around assets that are to be safeguarded [36]. Protecting data in a data system from the point of origin to the point of destination is known as end-to-end security. However, full end-to-end security would require all endpoints to support a common control security mechanism [39]. According to IEEE standard recommendations and standards, the IEEE 1686™, IEEE P37.240™, IEEE 1711™, IEEE 1402™, and IEC 62351 series are the best practices for cybersecurity introduced for IoE solutions.

6.1 IoE Cyber Security

Cybersecurity for IoE concerns all procedures and methods of securing communication and networking for data and power flow. According to IEEE, an organization must apply analysis and risk management methods to identify the appropriate solutions to ensure the Distributed Energy Resources (DERs), including related systems and Smart Grids. The security engineer has to understand the data exchange standards to fill the gaps that should be taken into account [37]. The data exchange recommended standards and application programming interfaces that support smart grid technologies and related ISO/RTO services or products based on the data. Demand Response (DR) models are supplied in standard publication documents by the National Institute for Standards and Technology (NIST). The National Electric Sector Cyber Security Organization Resource (NESCOR), Electric Power Research Institute (EPRI), etc. [38]. These recommendations and standards are rich in key functional security regions, various markets, and Critical Infrastructure Protection (CIP) cybersecurity and other pertinent accuracy standards.

6.2 IoE Security Issues

A layer of protection is necessary because the IoE links individuals, information, objects, and processes. Similar to how common equipment are evaluated and rated for conventional attributes like suitability for use, maintainability, etc., IoE items are also subjected to extensive cybersecurity testing. Regulating and establishing common security standards for IoE security is a priority, but the uniform and independent verification of IoE devices' security is still in its early stages.

6.2.1 Threat Modeling

Cybersecurity-related accidents have happened in numerous businesses and sectors, including factories, power grids, water supplies, nuclear facilities, etc., as a result of the expansion of IoT technology [11]. By 2020, the damage climbed by 32%, or $17.7 trillion [22]. Regarding our effort to situate the IoT security challenges inside the framework of a broader architecture that includes more components like people, data, and processes that is, the IoE, many studies have attempted to consider the IoT security issues as an individual problem. Threat-based security analysis of IoT was carried out by particular studies. for example, one study proposed a privacy improvement over Bluetooth Low Energy (BLE) advertising channels. But when taking into account the IoE, this increase is unfeasible and necessitates altering both the protocol and the peripheral. An IoE-driven security mechanism that uses a video camera to detect motion from a visitor while the homeowner is away is reviewed in another study. Home network integrity is crucial for many IoE-based physical security systems, hence maintaining home network security is essential to physical security. Thus, the first step towards improving house physical security is creating a threat model for IoE for homeowners who usually aren't aware of security and privacy problems.

6.2.2 Architecture for Trust Management

IoE is a combination of empowering technologies for Cyber-Physical Systems (CPS), and its structure fits and is compatible with the System-of-Systems (SoSs). The intelligent object is likely to be pervasive, geologically spread, and diverse on the Internet of Energy. IoE clients can create critical associations with other clients and devices in substation networks [40]. IoE can be seen as a node-centric structure where each node or thing, in general, can apply for service from other centric common nodes. It may also offer service for the other utilities and is considered a service provider (SP). In a service-centric Internet of Energy structure, it is compulsory to create a management protocol for trust to assess IoT service providers' reliability and fidelity efficiently and scalable. Indeed, management models for trust are desired since IoE SPs (services providers) may perform maliciously and untruthfully to encourage the IoE nodes to choose them for services on behalf of other SPs (services providers).

Additionally, untruthful IoE service providers may make ballot stuffing, discriminatory and bad-mouthing attacks to disturb the network and control services offered. Thus, it is obvious that the management of trust for service is more than important to defend IoE nodes from malicious SPs. Up to now, there is a huge number of protocols for the management of trust that have been invented for Social, WSN (Wireless Sensor Network), and P2P networks.

7 Internet of Energy Future Trends

IoE enables to collection and organization of the data to simplify the information flow management from single grid edge devices to other grids across the network quickly. In smart grids, IoE presents a principle of smart energy management that helps to keep the network grid stable and balanced in terms of power. In addition, IoE provides smart

forecasting to predict future energy demands. It allows to use of cloud-based systems to integrate industry systems and provides a process management of future grids [41]. The cloud-based IoE platforms enable to development of an open interface software for the development of customer-specific applications easily managed in a wide range of grids with new efficient operation utility.

The integration of real things to the internet with smart advanced applications such as grid data management and analytics, distributed energy resource and substation devices management in the IoE network will promise more efficient and sustainable gird than ever before [11]. IoE can manage and operate the smart device processes and data acquisition systems, in addition to interacting with the problem notifications repair and faults occurred i.e. in electric vehicles metering. Moreover, in electric substations, cloud-based IoE applications can automatically asset protection settings and provide advanced services like remote support and security management [42].

Recently, many technologies related to IoE have been taken into consideration, especially in electric power applications. In the USA, an electric power company developed a self-healing grid system to automatically reconfigure itself in case of home power loss. The developed systems can automatically detect, isolate and reroute power in case of fault occurs [43]. In the national UK power grid, a demand-side response company uses a smart balanced supply technology to aggregate energy consumption from across customers' sites. The technology helps to dynamically response to demands and enables consumers to better manage their consumption [44]. In Europe, IoE is dedicated to exploring the business case for IoT in the energy industry.

In the energy industry, IoE offers many benefits in regulating energy usage levels and maximising revenue opportunities. IoE enables to harvest of renewable resources and integrates them with electrical grids as a power generation [103]. Technologies such as AI and blockchain in IoE future applications will build an effective cybersecurity defence mechanism, and provide great security options for data. Moreover, these technologies will help to build the perfect infrastructure for making IoE a blissful reality.

8 Conclusions

The Internet of Energy (IoE) is the integration of Information and Communication Technology (ICT) into the complex web of energy systems. It includes several different types of energy, such as generation, transformation, storage, distribution, and end-device consumption. The IoE's architectural architecture divides the energy network into layers, allowing for seamless connectivity and effective administration across these disparate components. This integration not only simplifies operations, but it also has the potential to transform how energy systems work and interact.

The rapid advancement of ICT has resulted in the introduction of disruptive technologies such as cloud computing, fog/edge computing, and Blockchain, which play critical roles in current internet-based applications. These advancements are critical in developing infrastructure that is not only efficient and reliable, but also secure and adaptable. Their use inside the IoE framework reshapes the traditional energy environment, offering previously unheard-of levels of dependability, security, and adaptability.

Established standards, suggestions, and best practices are critical to IoE's success. These serve as guiding principles for optimal design and deployment, ensuring that interoperability, scalability, and security are fully addressed. IoE implementations that adhere to these benchmarks can accomplish harmonic integration across disparate systems while protecting against potential weaknesses.

This comprehensive assessment emphasizes the importance of IoE in altering energy systems through the integration of ICT and energy components. It emphasizes the mutually beneficial relationship between technical advancement and the aim of efficient, secure, and sustainable energy management. The Internet of Everything (IoE) is a transformative force poised to revolutionize energy systems, opening the way for a more connected, efficient, and resilient future.

References

1. Kafle, Y.R., Mahmud, K., Morsalin, S., Town, G.E.: Towards an internet of energy. In: 2016 IEEE International Conference on Power System Technology (POWERCON), 2016, pp. 1−6 (2016).
2. Dahab, M.B., Ahmed, E.S., Mokhtar, R.A., Saeed, R.A.: Artificial intelligence and machine learning approaches in smart city services. In: Reddy, K., Roy, D., Mishra, T., Hussain, M., (Eds.), Handbook of Research on Network-Enabled IoT Applications for Smart City Services, pp. 339−352 (2023). IGI Global. https://doi.org/10.4018/979-8-3693-0744-1.ch019
3. Hannan, M.A., et al.: A review of internet of energy based building energy management systems: issues and recommendations. IEEE Access **6**, 38997–39014 (2018)
4. Keen, M.G., Chin, H.H., Ganapathi, C., Ghazaleh, D., Krogdahl, P.: Patterns: Extended Enterprise Soa and Web Services (Redbooks) (2006)
5. Lyu, Z., Wei, H., Bai, X., Lian, C.: Microservice-based architecture for an energy management system. IEEE Syst. J. 1−12 (2020)
6. Munshi, A.A., Mohamed, Y.A.I.: Data lake lambda architecture for smart grids big data analytics. IEEE Access **6**, 40463–40471 (2018)
7. Hassan, M., et al.: BER improvement of cooperative spectrum sharing of NOMA in 5G network. In: 2023 IEEE 3rd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA), Benghazi, Libya, 2023, pp. 647−652, https://doi.org/10.1109/MI-STA57575.2023.10169494.M.
8. Yang, D., Wei, H., Zhu, Y., Li, P., Tan, J.: Virtual private cloud based power-dispatching automation system—architecture and application. IEEE Trans. Ind. Inform. **15**, 1756–1766 (2019)
9. GridWise transactive energy framework version 1.0 The Grid-Wise Architecture Council, US Department of Energy, Washington, DC, USA 2015.
10. Hassan, M., et al.: NOMA cooperative spectrum sharing average capacity improvement in 5G Network. In: 2023 IEEE 3rd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA), Benghazi, Libya, pp. 653−658 (2023). https://doi.org/10.1109/MI-STA57575.2023.10169694.
11. Hasan, M.K., Ahmed, M.M., Musa, S.S.: Measurement and modeling of DTCR software parameters based on intranet wide area measurement system for smart grid applications. In: International Conference on Innovative Computing and Communications 2020, pp. 1139−1150. Springer, Singapore (2020)
12. Khalifa, O.O., et al.: An IoT-Platform-based deep learning system for human behavior recognition in smart city monitoring using the Berkeley MHAD datasets. Systems. **10**(5), 177 (2022). https://doi.org/10.3390/systems10050177

13. Forfia, D., Knight, M., Melton, R.: The view from the top of the mountain: building a community of practice with the gridwise transactive energy framework. IEEE Power Energy Mag. **14**, 25–33 (2016)
14. Miglani, A., Kumar, N., Chamola, V., Zeadally, S.: Blockchain for internet of energy management: review, solutions, and challenges. Comput. Commun. **151**, 395−418 (2020)
15. Khan, M.A., Salah, K.: IoT security: review, blockchain solutions, and open challenges. Future Gener. Comput. Syst. **82**, 395−411 (2018)
16. Reyna, A., Martín, C., Chen, J., Soler, E., Díaz, M.: On blockchain and its integration with IoT. Challenges and opportunities. Future Gener. Comput. Syst. **88**, 173−190 (2018)
17. "IEEE Standard Technical Specifications of a DC Quick Charger for Use with Electric Vehicles," IEEE Std 2030.1.1-2015, pp. 1−97 (2016)
18. Saeed, M.M., et al.: A comprehensive review on the users' identity privacy for 5G networks. IET Commun. **16**, 384–399 (2022). https://doi.org/10.1049/cmu2.12327
19. "IEEE Vision for Smart Grid Communications: 2030 and Beyond," IEEE Vision for Smart Grid Communications: 2030 and Beyond, pp. 1−390 (2013)
20. Muni, B.K., Patra, S.K.: FPGA implementation of ZigBee baseband transceiver system for IEEE 802.15.4. In: Advances in Computing, Communication, and Control, Berlin, Heidelberg, 2013, pp. 465−474 (2013)
21. Nurelmadina, N., et al.: A systematic review on cognitive radio in low power wide area network for industrial IoT applications. Sustainability **13**, 338 (2021). https://doi.org/10.3390/su13010338
22. IEEE Standard for Local and metropolitan area networks - Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 4: Alternative Physical Layer Extension to Support Medical Body Area Network (MBAN) Services Operating in the 2360 MHz – 2400 MHz Band. IEEE Std 802.15.4j-2013 (Amendment to IEEE Std 802.15.4-2011 as amended by IEEE Std 802.15.4e-2012, IEEE Std 802.15.4f-2012, and IEEE Std 802.15.4g-2012), pp. 1−24 (2013)
23. Ryoo, Kim, S., Cho, J., Kim, H., Tjoa, S., Derobertis, C.: IoE security threats and you. In: 2017 International Conference on Software Security and Assurance (ICSSA), Altoona, PA, 2017, pp. 13−19 (2017). https://doi.org/10.1109/ICSSA.2017.28
24. Memon, I., Shaikh, R.A., Hasan, M.K., Hassan, R., Haq, A.U., Zainol, K.A.: Protect mobile travelers information in sensitive region based on fuzzy logic in IoT technology. Secur. Commun. Netw. **18**, 2020 (2020)
25. Khajenasiri, K., et al.: Design and implementation of a multi-standardevent-driven energy management system for smart buildings. In: Proc.IEEE 3rd Global Conf. Consum. Electron. (GCCE), Oct. 2014, pp. 20–21 (2014)
26. Khajenasiri, I., Virgone, J., Gielen, G.: A presence-based control strategy solution for HVAC systems. In: Proc. IEEE Int. Conf. Consum.Electron. (ICCE), Jan. 2015, pp. 620–622 (2015)
27. Gil-Baez, M., Barrios-Padura, Á., Molina-Huelva, M., Chacartegui, R.: Natural ventilation systems in 21st-century for near zero energy school buildings. Energy **137**, 1186–1200 (2017)
28. Favaro, J.: Strategic research challenges in the Internet of Things. Tech.Rep., p. 6630.
29. Billure, R., Tayur, V.M., Mahesh, V.: Internet of things—a study on the security challenges. In: Proc. IEEE Int. Adv. Comput. Conf. (IACC),Jun. 2015, pp. 247–252 (2015)
30. Blaauw, D., et al.: IoT design space challenges: Circuits and systems. In: Symp. VLSI Technol. Dig. Tech. Papers, Jun. 2014, pp. 1–2 (2014)
31. Cao, J., Yang, M.: Energy Internet—Towards smart grid 2.0. In: Proc.Int. Conf. Netw. Distrib. Comput. (ICNDC), Dec. 2014, pp. 105–110 (2014)
32. Wang, K., Hu, X., Li, H., Li, P., Zeng, D., Guo, S.: A survey on energy Internet communications for sustainability. IEEE Trans. Sustain. Comput. **2**(3), 231–254 (2017)

33. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.: Internet of things: a survey on enabling technologies, protocols, and applications. IEEE Commun. Surveys Tuts. **17**(4), 2347–2376 (2015)
34. Zhang, Y., Weng, J., Dey, R., Fu, X.: Bluetooth low energy (BLE) security and privacy. In: Shen X., Lin X., Zhang K. (eds.) Encyclopedia of Wireless Networks. Springer, Cham (2019). https://doi.org/10.1007/978-3-319-32903-1_298-1
35. Khan., Arsalan, M.H.: Solar power technologies for sustainable electricity generation—a review. Renew. Sustain. Energy Rev. **55**, 414–425 (2016)
36. Al Busaidi, S., Kazem, H.A., Al-Badi, A.H., Khan, M. F.: A review of optimum sizing of hybrid PV–Wind renewable energy systems in Oman. Renew. Sustain. Energy Rev. **53**, 185–193 (2016)
37. . Ayhan., Sağlam, A.: A technical review of building-mounted wind power systems and a sample simulation model. Renew. Sustain. Energy Rev. **16**(1), 1040–1049 (2012)
38. Gvozdenovic, H.B.K., Maassen, W., Zeiler, W.: Roadmap to nearly zero energy buildings. Roy. HaskoningDHV, Eindhoven Univ. Technol., Eindhoven, The Netherlands, Tech. Rep. (2014)
39. Wang, K., Bao, J., Wu, M., Lu, W.: Research on security management for Internet of things. In: Proc. Int. Conf. Comput. Appl. Syst. Modeling(ICCASM), vol. 15, Oct. 2010, pp. V15-133–V15-137 (2010)
40. Ma, Z., Cooper, P., Daly, D., Ledo, L.: Existing building retrofits: methodology and state-of-the-art. Energy Buildings **55**, 889–902 (2012)
41. Salamzada, K.H., Shukur, Z., Bakar, M.A.: A framework for cybersecurity strategy for developing countries: case study of Afghanistan. Asia-Pac. J. Inf. Technol. Multimedia. **4**(1), 1 (2015)
42. Strielkowski, W., Streimikiene, D., Fomina, A., Semenova, E.: Internet of energy (IoE) and high-renewables electricity system market design. Nergies **12**, 4790 (2019). https://doi.org/10.3390/en12244790
43. Shahinzadeh, H., Moradi, J., Gharehpetian, G.B., Nafisi, H., Abedi, M.: Internet of energy (IoE) in smart power systems. In: 5th Conference on Knowledge-Based Engineering and Innovation (KBEI), Tehran, Iran, 2019, pp. 627−636 (2019). https://doi.org/10.1109/KBEI.2019.8735086.
44. Andoni, M., et al.: Blockchain technology in the energy sector: a systematic review of challenges and opportunities. Renew. Sustain. Energy Rev. **100**, 143–174 (2019)