A SURVEY ON IOT-BASED SMART-GRID OVERVIEW

Mehrdad Saffarie and Kheirollah Rahseparfard

Department of Computer Engineering, Qom University, Qom, Iran

ABSTRACT

The Internet of Things (IoT) has drawn significant research attention. IoT is considered as a part of the Internet of the future and will comprise billions of intelligent communicating 'things'. The future of the Internet will consist of heterogeneously connected devices that will further extend the borders of the world with physical entities and virtual components. The Internet of Things (IoT) will empower the connected things with new capabilities. The change of power sector is also guided by the growing penetration of renewable and Distributed Energy Resources (DER), as well as the increasing involvement of electricity consumers in the production and management of electricity, which in turn are expected to radically change the local electricity industry and markets, especially at distribution level, creating opportunities but also posing challenges to the reliability and efficiency of system operation. The trend is inline to the smart-grid concept, which represents an unprecedented opportunity to move the energy industry into a new era of reliability, availability, and efficiency that will contribute to our economic and environmental health. During the transition period, it is critical to carry out testing, technology improvements, consumer education, development of standards and regulations, and information sharing between projects to ensure that the benefits we envision from the smart grid become a reality.

KEYWORDS

Internet of things(IoT), smart-grid, applications, integration of IoT and SG

1. INTRODUCTION

Emergence of Internet-of-Things brings a whole new class of applications and higher efficiency for existing services. Application-specific requirements, as well as connectivity and communication ability of devices have introduced new challenges for IoT applications. [1].
The infrastructure of Internet of Things (IoT) relies on the communication between an enormous number of embedded devices with limited resources, i.e., constraint processing abilities, low data rates, restricted power supplies, in relatively harsh and dynamic environments. These employed embedded devices, which are typically equipped with sensors, actuators and wireless communication modules, are the key components of the IoT infrastructures[2].

Figure 1 illustrates the Gartner's estimation on the number of IoT devices by the year 2020 which is more than 20 billion in total [3]. It shows the prediction of IoT devices in different sectors: Consumer sector covers the devices that are purchased and used by the end user (e.g., personal gadgets, fitness bands, healthcare devices, etc). The cross-industry sector refers to the general devices and items that are deployed and used in industries such as smart home, smart city, etc. And finally, the industry-specific sector refers to the special devices and systems in the factories to increase the efficiency of other sectors. It includes infrastructures to improve the efficiency of production lines, monitoring the quality, etc. The smart grid falls into the cross-industry sector.

David C. Wyld et al. (Eds): NIAI, MoWiN, AIAP, SIGML, CNSA, ICCIoT - 2023
pp. 105-114, 2023. CS & IT - CSCP 2023 DOI: 10.5121/csit.2023.130309

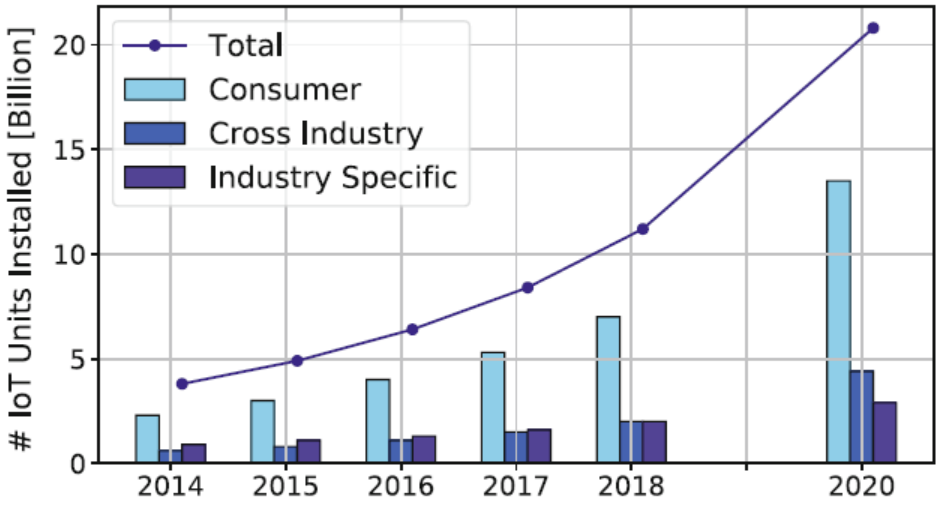

Figure 1. Gartner's estimation on the number of IoT devices in different sectors (The 2019 data is not available) [3].

2. SMART -GRID

[Smart grid is one of the main IoT application domains where generation, transportation, delivery and consumption of electricity is improved in terms of efficiency, reliability and safety] [4]. [The current power grid suffers from several issues such as unpredictable power disturbances and outages, undetectable consumer fraud, inflexible electricity prices, etc] [5]. These issues contribute to the cost of utility and ever-rising fossil fuel demand. For instance, to reduce the risk of an outage, the peak hour demand must be overestimated and more electricity must be generated.

The increasing electricity demand, together with the complex and nonlinear nature of the electric power distribution network, have caused serious network congestion issues. The network congestion and safety-related factors have become the main causes of several major blackouts that happened in recent years. In addition to the overstressed situation, the existing power grid also suffers from the lack of pervasive and effective communications, monitoring, fault diagnostics, and automation, which further increase the possibility of region-wide system breakdown due to the cascading effect initiated by a single fault. [6].

2.1. Traditional Power Grid

To address the lacking efficiency and reliability in traditional power grid, smart grid exploits the following concepts:

• Dynamic pricing: The main mechanism to manage the electricity demand during the peak hours is dynamic and real-time pricing. A dynamic pricing policy can be established based on the total available power supply, the dynamic demand, and Time of Use (ToU). During the peak hours when the load on power grid is high, the real-time price increases and vice-versa. The pricing policy considers historical demand and real-time demand data to estimate the total demand. It also requires to estimate the supply condition according to the predictive models for renewable energy sources and capacity of conventional power plants.

• Smart Meters: The installation of smart meters enables real-time information exchange between customers and providers. Smart meter can also control the smart appliances in a residential building, schedule their operations, and monitor their energy usage. It may receive the dynamic price information from the utility supplier and send back the information about the energy usage over time.

• Micro-grid: Interconnected subgroups of low-voltage electricity systems are known as micro-grid [7, 8]. Having self-generating and management mechanisms, micro-grid can increase the reliability of local distribution. A micro-grid can be connected to the power grid, but separate itself (go to the island mode) from it when there is a fault, failure, intrusion or other risks for the grid.

• Distributed generation: In the smart grid, consumers can generate power from renewable energy sources such as solar or wind. The excess generated power can be sold to the grid or to other customers within the micro-grid [4, 7]. The share of renewable sources in Germany's electricity is predicted to increase from 35% (in 2017) to more than 80% in 2050.

2.2. Components of Smart-Grid

Figure 2 illustrates the main components of smart grid [9]. The generation of electricity is not limited to the conventional power plants (e.g., fossil plants) anymore. The renewable energy sources such as wind and solar are included in the generation phase. To billing, real-time pricing, supply prediction, demand prediction and grid monitoring tasks require management systems. The generated electricity is then transported to the micro-grid for distribution among consumers including smart homes, smart buildings, data centers, factories and industries, electric vehicles, etc.

Micro-grids have local management systems and exchange information with other components in the smart grid such as utility suppliers.

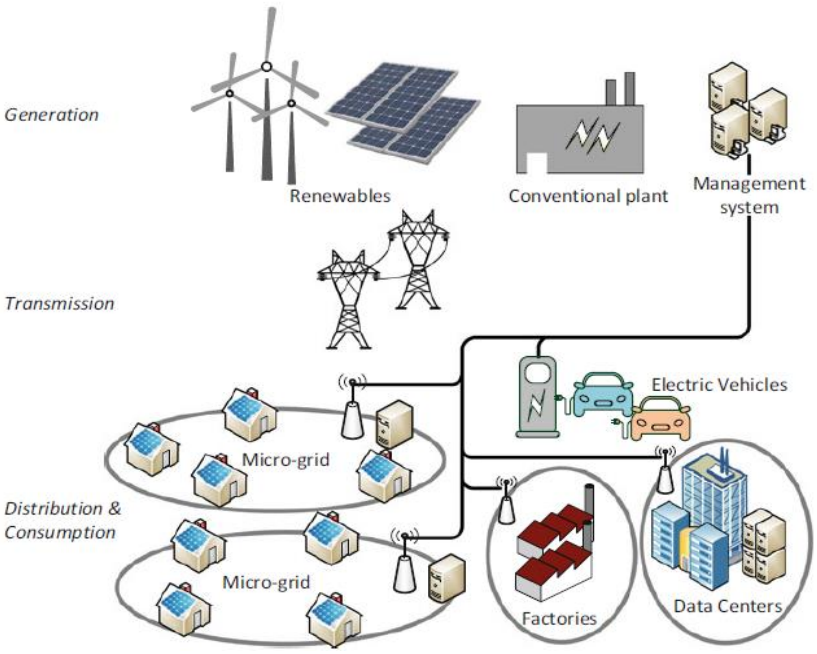

Figure 2.The main components future smart grid [9]

3. IOT APPLICATIONS TYPES

According to [10] the IoT applications can be classified in two categories the Massive IoT and the Critical IoT.

3.1. Massive IoT

Massive IoT refers to services that typically span over a very large number of devices, usually sensors and actuators. Sensors are extremely low cost and consume very low amounts of energy in order to sustain long battery life. Clearly, the amount of data generated by each sensor is normally very small, and very low latency is not a critical requirement. While actuators are similarly limited in cost, they will likely have varying energy footprints ranging from very low to moderate energy consumption (Table 1).

Sometimes, the mobile network may be used to bridge connectivity to the device by means of capillary networks. Here, local connectivity is provided by means of a short-range radio access technology, for example Wi-Fi, Bluetooth or 802.15.4/6LoWPAN. Wireless connectivity beyond the local area is then provided by the mobile network via a gateway node.

Table 1.Vertical markets for massive IoT technology [10]

Massive IoT
Transport and Logistics (Fleet management and Goods tracking)
Agriculture (Climate/agriculture monitoring, Livestock tracking)
Environment (Flood monitoring/alerts, Environmental monitoring)
Industrial (Process monitoring and control, Maintenance monitoring)
Consumers(Wearables kids/senior tracker, Medical monitoring
Utilities (Smart metering, Smart grid management)
Smart cities (Parking sensors, Smart bicycles, Waste management, Smart lightning)
Smart buildings (Smoke detectors, Alarm systems, Home automation)

3.2. Critical IoT

Critical IoT refers to applications such as traffic safety/control, control of critical infrastructure and wireless connectivity for industrial processes. Such applications require very high reliability and availability in terms of wireless connectivity, as well as very low latency [11]. On the other hand, Low Device cost and energy consumption is not as critical as for Massive IoT applications. While the average volume of data transported to and from devices may not be large, wide instantaneous bandwidths are useful in being able to meet capacity and latency requirements (Table 2).

Table 2.Vertical markets for critical IoT technology [10]

Critical IoT
Automotive (V2I, V2V, V2P, V2C, Car entertainment)
Industrial (Remote control, Automated fabrication, Collaborative robots)
Medical (E-Health, Remote surgery, Biomedical sensors)
Public sector (Smart grid, Video surveillance)

4. THE SMART-GRID APPLICATIONS

The SG consists of several groups of applications. These can classified according to [12] into the following application groups or domains.

• Smart home applications allow the use of sensors and actuators in devices and appliances. These devices may include smart TVs, smart refrigerators, temperature monitoring, lighting control, and home security systems. That group of devices together forms a Neighbour Area Network (NAN).

• The online monitoring of power lines is another useful application of SG. The IoT based smart grid will be able to improve the reliability of power lines by continuous status monitoring. Reports about faults will be send directly to the control units in order to resolve them in an instant way.
• The Demand-side energy management (DSM) is another critical point where the SG plays an important role. The user energy consumption profile is collected by IoT-nodes and then send to smart meters. Thus, the demand-response can be regulated in order to minimize the electrical consumption and the operation cost of the smart grid.

• The integration of distributed energy sources and especially renewable energy sources is another major issue. IoT nodes can collect data for the weather and therefore predictions about the availability of the renewable energy sources can be made.

• The integration of electric vehicles to the power grid is another application domain. The IoT technology helps in this way to collect information about the vehicles battery state and location in order to improve the charging and discharging scheduling algorithms.

5. SMART-GRID MODELLING AND SIMULATION

Modelling smart grids is an active area of research [13]. There are various proposals and techniques, which are based on various data, such as the type of the energy production, the power distribution network, the energy storage devices, the power consumption, the learning algorithm for energy costs reduction, the energy usage etc. Furthermore, each method presents a different objective. Examples include Distributed Online Algorithm for Optimal Energy [14, 15], Metering and optimal energy distribution [13], Optimal Storage management and Dimensioning [16], Learning algorithms for energy costs reduction and energy usage [17] and other. Here, we present some contributions to this field, based on an extensive survey of the literature. Specifically, we demonstrate an algorithm that accepts as input multiple types of energy production, such as solar, water and wind energy, as it occurs in a typical country, and we focus on modeling a distribution energy algorithm for simulation purposes.

5.1. Modelling of Smart-Grid Infrastructure

As it is evident from previous chapters, the traditional power grid is strictly one-way hierarchical, which means that the energy can only be distributed from the main power plant using traditional infrastructure; in contrast, the smart grid is characterized by the two-way flows of energy and real-time information, which offers tremendous benefits and flexibility to both users and energy providers. There are significant differences between them. The traditional power grid is centralized, which means all power must be generated from a central location, eliminating the possibility of easily incorporating alternative energy sources into the grid.

The renewable energy sources provide infinite energy, offering us the chance to use them continuously without polluting the environment, in contrast to non-renewable energy sources. It seems that renewable energy sources can easily replace the fossil energy sources, but it is not that easy, due to their influence from natural conditions [18-20]. For example, water, wind and solar energy depend on the weather; that's why the producers and consumers have to act in a more flexible way to meet the energy needs. Also, the generation cost of renewable power is high [21, 22] and for that the scientists are seeking new and more profitable methods. It is clear that the fluctuation in availability of using the renewable energy sources is depending on the weather and the cost, which are the main problems. From one hand we don't know the exact distribution power and it is also very difficult to predict the power consumption, because the consumers can change their needs at any time. To solve this issue between generation and consumption energy, suppliers may create a special offer, a motive model, such as offering energy at a reduced price during sunny days.

The consumers will benefit from this offer and for example will recharge their cars, use the washing machine etc. But this may lead to another problem: plenty of the consumers will react to the same time to benefit from the offer and there will be a spike on the demand. This may cause a blackout to the whole system. The only way to use the time variant prices is to use an energy management system.

It is widely understood that it is very complicated to keep the balance between the produced energy and the consumption. There are several approaches that depend on the perspective the researchers use to resolve the issues. The algorithms have different approaches. In [13] smart homes optimize the consumption of their own devices and share information about their consumption. Another approach is to control an entire power grid [23]. Besides the different approaches, there are also different goals that the algorithms try to reach, e.g. balance of supply and demand [14, 23], reduction of peak loads and energy losses, smoothing of power consumption through load shifting
[18] or minimization of micro grid costs [15].

All inserts, figures, diagrams, photographs and tables must be centre-aligned, clear and appropriate for black/white or greyscale reproduction.

Figures (e.g., Figure 1) must be numbered consecutively, 1, 2, etc., from start to finish of the paper, ignoring sections and subsections. Tables (e.g., Table 1) are also numbered consecutively, 1, 2, etc., from start to finish of the paper, ignoring sections and subsections, and independently from figures.

6. SMART-GRID HARDWARE SECURITY

Smart grids are vulnerable to a multitude of attacks, due to their cyberphysical nature. Such attacks can occur at their communication, networking, and physical entry points and can seriously affect the operation of a grid. Thus, the security factor of a smart grid is of an utmost importance. In order to properly secure a smart grid, we should be able to understand its underlying vulnerabilities and associated threats, as well as quantify their effects, and devise appropriate security solutions. In this chapter, we begin with an introduction to smart grids and Hardware Security. Then we continue to describe some grid architecture patterns, so that we can be able to understand a general picture of the grid functionality. In the next section, we discuss the basic and most important aspect of the security of the smart grid; the secure communication between the devices, providing some techniques for a secure device authentication scheme. We, then, discuss the confidentiality of the power usage, explaining various methods for metering data

anonymization. In the end, we present solutions related to the integrity of data, software and hardware.

According to a survey[24], Clearly describing the security goals the Smart Home/Smart Grid environment is expected to meet, serves as our first step in the effort for ensuring unfailing and consistent Smart Grid operation.

- Confidentiality, the assurance that data will be disclosed only to authorized individuals or systems. [24].
- Integrity, the assurance that the accuracy and consistency of data will be maintained. No unauthorized modifications, destruction or losses of data will go undetected. [24].
- Authenticity: authenticating the communicating parties. In this case, messages are sent by these parties themselves.
- Authorization: ensuring that each entity's access rights are legal and determined in the system, according to the level of access control of each entity.
- Non-repudiation: ensuring that there will be indisputable proof to ratify the honesty of any assertion of an entity. Generally, in the smart grid environment, threats continuously attempt to violate some or all of the above security objectives. Threats are categorized as shown below into two broad categories [25]:
- Passive attacks: attacks that do not affect system resources [26] and attempt to learn or make use of system information. Therefore, in passive attacks, the objective of the opponent is to obtain information that is transmitted rather than to modify it; therefore, seeking to gain any kind of knowledge. Passive attacks may formulate into a security disclosure problem, due to unauthorized monitoring of a continuous communication without the assents of the convey parties or motion analysis where the opponent monitors the traffic models to extract useful information from them.It is very difficult to detect these two types of attacks, since they do not alter any data. Our efforts to prevent such attacks focus only on prevention, not on their detection.
- Active attacks: attacks that attempt to modify a system's resources or disrupt it's operation [11]. active attacks that attempt to disrupt the normal functionality of a network such as denial-of-service (DoS) attacks and passive attacks such as eavesdropping attacks[27]. active attacks degrade reliability since Jimmy sends jamming signals to degrade the received signals at the legitimate receivers. passive attacks degrade the communication system's reliability since the legitimate transmitters will assign portions of their transmit powers to inject AN signals to secure their transmissions [27]. Finally, attacks with malware, are attacks for exploiting interior network vulnerabilities, modifying, destroying or stealing information, and gaining unauthorized access to system resources.

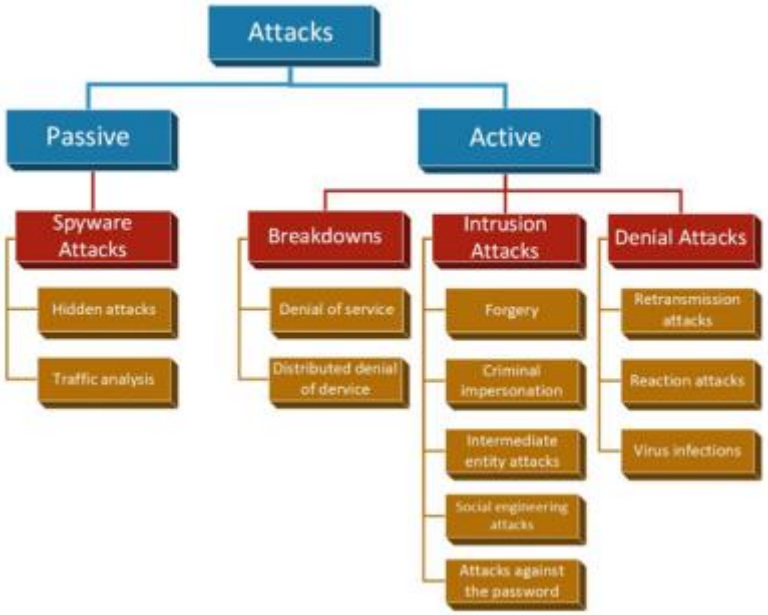

Figure 3. Categories of attacks on smart-Grid

7. RESULTS

The electric power infrastructure as we know it today has managed to serve our needs successfully, almost unchanged, for nearly a century; revolutionizing almost every aspect of our lives. However, as this infrastructure is inevitably aging it becomes increasingly less efficient, repeatedly running up against its limitations and constantly straining to keep up with our ever-increasing requirements. Needs for reliability, scalability, manageability, environmentally friendly energy generation, interoperability and cost effectiveness, bring forward the necessity for a modernized and intelligent grid for tomorrow; a new, reliable, efficient, flexible and secure energy infrastructure, known as the Smart Grid. Through the incorporation of advanced power system electronics, networking and communication technologies the Smart Grid is envisioned to significantly enhance the existing electric grid.

REFERENCES

[1] F. Samie, L. Bauer, and J. Henkel, "IoT technologies for embedded computing: A survey," in *2016 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ ISSS)*, 2016: IEEE, pp. 1-10.

[2] J. Henkel, S. Pagani, H. Amrouch, L. Bauer, and F. Samie, "Ultra-low power and dependability for IoT devices (Invited paper for IoT technologies)," in *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017*, 2017: IEEE, pp. 954-959.

[3] "Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016." Gartner. (accessed 2017).

[4] M. Erol-Kantarci and H. T. Mouftah, "Energy-efficient information and communication infrastructures in the smart grid: A survey on interactions and open issues," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 179-197, 2014.

[5] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE security & privacy*, vol. 7, no. 3, pp. 75-77, 2009.

[6] V. C. Gungor, B. Lu, and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," *IEEE transactions on industrial electronics*, vol. 57, no. 10, pp. 3557-3564, 2010.

[7] S. Bera, S. Misra, and J. J. Rodrigues, "Cloud computing applications for smart grid: A survey," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 5, pp. 1477-1494, 2014.
[8] H. Farhangi, "The path of the smart grid," *IEEE power and energy magazine*, vol. 8, no. 1, pp. 18-28, 2009.
[9] M. Godoy Simões *et al.*, "Comparison of smart grid technologies and progress in the USA and Europe," in *Smart Grid Applications and Developments*: Springer, 2014, pp. 221-238.
[10] "5G radio access," in *Ericsson Mobility Report* vol. 2017, ed: Ericsson, 2017.
[11] H. Hejazi, H. Rajab, T. Cinkler, and L. Lengyel, "Survey of platforms for massive IoT," in *2018 IEEE international conference on future IoT technologies (future IoT)*, 2018: IEEE, pp. 1-8.
[12] M. Jaradat, M. Jarrah, A. Bousselham, Y. Jararweh, and M. Al-Ayyoub, "The internet of energy: smart sensor networks and big data management for smart grid," *Procedia Computer Science*, vol. 56, pp. 592-597, 2015.
[13] Y. Zhang, H. Wang, and Y. Xie, "An intelligent hybrid model for power flow optimization in the cloud-IOT electrical distribution network," *Cluster Computing*, vol. 22, no. 6, pp. 13109-13118, 2019.
[14] K. Mets, M. Strobbe, T. Verschueren, T. Roelens, F. De Turck, and C. Develder, "Distributed multi-agent algorithm for residential energy management in smart grids," in *2012 IEEE Network Operations and Management Symposium*, 2012: IEEE, pp. 435-443.
[15] Y. Zhang, N. Gatsis, and G. B. Giannakis, "Robust distributed energy management for microgrids with renewables," in *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, 2012: IEEE, pp. 510-515.
[16] P. M. van de Ven, N. Hegde, L. Massoulié, and T. Salonidis, "Optimal control of end-user energy storage," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 789-797, 2013.
[17] J. S. Vardakas, N. Zorba, and C. V. Verikoukis, "A survey on demand response programs in smart grids: Pricing methods and optimization algorithms," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 152-178, 2014.
[18] M. Asif, "Growth and sustainability trends in the buildings sector in the GCC region with particular reference to the KSA and UAE," *Renewable and Sustainable Energy Reviews*, vol. 55, pp. 1267-1273, 2016.
[19] M. Malik, S. Abdallah, and M. Hussain, "Assessing supplier environmental performance: applying analytical hierarchical process in the United Arab Emirates healthcare chain," *Renewable and Sustainable Energy Reviews*, vol. 55, pp. 1313-1321, 2016.
[20] S. Barbosa and K. Ip, "Perspectives of double skin façades for naturally ventilated buildings: A review," *Renewable and Sustainable Energy Reviews*, vol. 40, pp. 1019-1029, 2014.
[21] D. Ziouzios, A. Sideris, D. Tsiktsiris, and M. Dasygenis, "Smart-Grid Modelling and Simulation," in *IoT for Smart Grids*: Springer, 2019, pp. 43-54.
[22] B. Zakeri and S. Syri, "Electrical energy storage systems: A comparative life cycle cost analysis," *Renewable and sustainable energy reviews*, vol. 42, pp. 569-596, 2015.
[23] A. Parisio and L. Glielmo, "A mixed integer linear formulation for microgrid economic scheduling," in *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2011: IEEE, pp. 505-510.
[24] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1933-1954, 2014.
[25] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, "Communication security for smart grid distribution networks," *IEEE Communications Magazine*, vol. 51, no. 1, pp. 42-49, 2013.
[26] S. Cui, Z. Han, S. Kar, T. T. Kim, H. V. Poor, and A. Tajer, "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions," *IEEE Signal Processing Magazine*, vol. 29, no. 5, pp. 106-115, 2012.
[27] A. El Shafie, H. Chihaoui, R. Hamila, N. Al-Dhahir, A. Gastli, and L. Ben-Brahim, "Impact of passive and active security attacks on MIMO smart grid communications," *IEEE Systems Journal*, vol. 13, no. 3, pp. 2873-2876, 2018.

AUTHORS

Mehrdad Saffarie, the 29 years old PhD student of Information Technology(E-Commerce) at University of Qom and his PhD thesis is "Migration Factors from smart-home to smart-city" .

He received his M.Sc. in Information Technology at K.N.Toosi University with the total GPA 16.52/20. Two papers derived from his thesis, and He has some work experience in Internet-of-Things, e-payments and mobile-banking.

Kheirollah Rahseparfard is a faculty staff of technological and engineering college of University of Qom. As a top researcher in University of Qom , he has some awards in applied Mathematics. His scientific honors include presenting several scientific and specialized articles in domestic and foreign conferences. Also, he has teaching experience in some subjects such as applied Mathematics and decision support systems.