Application of IoT in Smart Grid: Challenges and Solutions

Zahra Davoody-Beni
Department of Electrical Engineering
Najafabad Branch, Islamic Azad University
Najafabad, Iran
z.davoody@sel.iaun.ac.ir

Niloufar Sheini-Shahvand
Department of Electrical Engineering
Najafabad Branch, Islamic Azad University
Najafabad, Iran
nshahvand@sel.iaun.ac.ir

Hossein Shahinzadeh
IEEE Member, Department of Electrical Engineering
Amirkabir University of Technology (Tehran Polytechnic)
Tehran, Iran
h.s.shahinzadeh@ieee.org

Majid Moazzami*
Assistant Professor, Smart Microgrid Research Center,
Najafabad Branch, Islamic Azad University,
Najafabad, Iran
m_moazzami@pel.iaun.ac.ir

Mahdi Shaneh*
Assistant Professor, Smart Microgrid Research Center,
Najafabad Branch, Islamic Azad University,
Najafabad, Iran
m.shaneh@pel.iaun.ac.ir

Gevork B. Gharehpetian
Professor, Department of Electrical Engineering
Amirkabir University of Technology (Tehran Polytechnic)
Tehran, Iran
grptian@aut.ac.ir

***Abstract*— The prevailing development in energy grids and emersion of new energy players along with the advent of the Internet of Things (IoT) lead available energy systems (e.g., smart electricity grid) toward "energy internet" concept. The expansion of an electrical power grid, because of its unique features, has caused this system to be converted to the central core of the energy ecosystem over the past decades. This process has also been preserved in the IoT in such a way that the presence of this technology increases the ability of evolutionary development in the power industry. IoT applications in smart grid (IoT–SG) have lots of advantages such as expenditure reduction, save of time, and smartness of grid equipment. Nevertheless, the disadvantages pertaining to IoT-SG should not be neglected. For instance, one of the most significant drawbacks and ahead challenges of IoT-SG is security and big data issues. In IoT-SG, each connected device can be a probable port to the IoT's infrastructure with personal data. Concerns about security and data privacy are indispensable, but with the entrance of complexity, safety weaknesses, and probable vulnerabilities, in cases such as interoperability and autonomous decision-making, possible risks of IoT have reached new levels. This paper mostly focuses on the IoT-SG investigations, advantages and ahead challenges, plus effective solutions to these challenges are being discussed. Furthermore, according to some key challenges such as safety and big data, general conclusions for confronting and dealing with these challenges have been made.**

***Keywords*— Internet of Thing; Smart Grid; Big Data; Security; Unit Standard; Internet of Energy.**

I. INTRODUCTION

With respect to the increase of energy demand and traditional power grid problems such as centralized production, unidirectional power transmission, lack of possibility for prompt supervision and automatic event analysis at the grid level and also manually grid recovery, the smart grid concept was propounded to solve the mentioned problems and to initiate the utilization of modern communication and information technologies in electricity networks [1]. Over the course of time, the technological advances and the entrance of new players to the SG, new concepts such as the second generation of smart grids (smart grid 2.0), smart energy, future energy grids, and energy 4.0 that are all completion of SG, are put forward. Investigation of these concepts can specify the SG orientation and its future and can facilitate the implementation of "Energy of Internet" (IoE) concept. Moreover, by investigating these concepts in addition to IoE concept, their correspondence with the internet of things (IoT) can be clarified, and different performers that can be in relation with the energy part will be specified [2-3].

IoT has been noticed in recent years, and in some cases, it is referred to as the fourth industrial revolution. IoT is not merely a technology but a concept that emphasizes on making interconnections between things and human beings [4]. In this paper, the term "technology" for IoT will be used; however, this term will not completely cover the concept. According to

* Assistant Professor, Department of Electrical Engineering, Najafabad Branch, Islamic Azad University, Najafabad, Iran.

978-1-7281-5350-6/19/$31.00 ©2019 IEEE

Gartner's report in 2015, this technology has gone beyond a pure science and a merely theoretical concept and has been implemented with some limitations and performed by some organizations and companies, and it is expected that this technology will reach a pervasive prevalence in the next 5 to 10 years [5].

The prediction of the number of connected devices, the level of investment, and the economic value of involving in the IoT enterprise have been cited as important indications of the development of this technology in resources and reputable reports, and various numerical results have been mentioned for them. According to Cisco, in the 2016 report, the number of connected devices via the internet was about 26 billion in 2015 and will be increased up to 50 billion by 2020 while the world's population will grow from 7.2 billion in 2015 to 7.6 billion in 2020 [6]. The investment level in the IoT domain is estimated to be about more than 260 billion dollars by 2020. Therefore, according to the status and influence of the IoT in the power and energy industry, IoT influential investigation through different dimensions in SG, challenges and its solutions, are so significant. Furthermore, the relation between IoT and energy industry is crucial due to the existence of some features such as supplying the possibility of interaction between things globally. It is because the globalized interactions related to all types of energies (not just electrical energy) provides the possibility to utilize all types of energies optimally and it helps not only the environmental preservation but also prevents global warming [7].

In recent years, many papers have investigated the IoT role and its challenges in different social parts. The results in [8] imply that just a few countries have enough strength for running safety standards independently. New rules may influence different parts of regulators; for example, the expansion of energy equipment not only needs the interference of energy domain regulators but also requires the interference of telecommunication regulators. In [9], the authors have expressed that challenges concerned with data acquisition, can engage the equipment manufacturers, application suppliers, and network operators and effect the different regulator entities. It is expressed in [10] that new energy services may require more secure and flexible levels. Thus, different governmental organizations beyond telecommunications regulators may get involved in regulation rules and legislation. Therefore, governments that intend to form limitations for IoT data transfer should make an effort to balance the advantages and its probable subsequences. IoT companies may be tie by strict rules and restrained by severe limitations, or they may be obliged to make a vast local investment [11]. In [12], it is expressed that most IoT practical programs require low bandwidth, and there is no need for extra grid capacity. Therefore, many IoT companies desire enough flexibility for connection services globally (for example the right to choose between local SIM-card, roaming SIM-card or an eSIM) [13]. In [14], the authors have expressed that regulators and governments should realize how to develop the relevant standards since the lack of globally accepted IoT standards may prevent IoT's widespread development and penetration.

As it can be perceived from the investigated papers, no comprehensive research has been done for methods and challenges of the IoT usage in SG. Thus, the purpose of this elaborate study is to investigate the current status, outlooks and the challenging, which the IoT applications are faced with in SG (IoT-SG). Therefore, first, the SG conceptual model is being presented, and then the IoT-SG definition is being discussed. In the following, IoT-SG usage challenges will be investigated in detail, and the proposed solutions will be presented.

II. CONCEPTUAL MODEL OF SMART GRID

In recent years, SG concept has been advanced rapidly. Thus, the national institute of standards and technology (NIST) has presented a conceptual model for the perception of SG technologies. According to the concept that NIST institution has presented for the SG, there is a path based on data flow between generation, transmission and consumption parts compared to the traditional power grid [15]. Therefore, based on this conceptual model, the following considerations and requirements about SG exist:

- There exist seven sections in the SG: generation, transmission, distribution, consumer, market, operator and service provider.
- All SG users are in relation with each other by using some bilateral wired and wireless communicational protocols such as Wi-Fi, Zigbee, LTE, WiMAX, GPRS, PLC, HomePlug, Leased line, and Fiber.
- To perform proper management, repairment, operation, and maintenance several software packages, such as CIS, OMS, GIS, DMS, and SCADA are being utilized in SG, in which some of them are control and management software (such as SCADA) and are used in the traditional and current power grids [16].

Another model for SG has been presented by the IEEE standard association that has defined SG as a system of subsystems in large-scale. In this model, which has been shown in Fig. 1, three layers of power, communications, and information have been considered for each one of seven sections that were issued by the national institute of standards and technology (NIST). From the NIST point of view, communicational technologies, information, and useful software can be implemented for the functional improvement and power layer efficiency in communication and information layer.

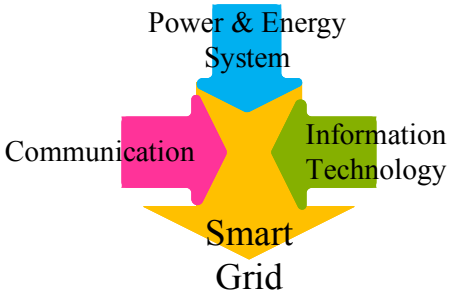

Figure 1: Smart grid subsystems

In general, each technology function and the corresponding software and hardware that can help to collect, store and analyze data optimally from network status will be classified under the SG's field [17].

III. INTERNET OF THINGS CONCEPT IN SMART GRID

One of the proposed topics in the SG is about investigating the usage possibility of new information and communication technologies due to the power grid requirements. Multiple technologies have been investigated for decreasing the number of information protocols and managing massive data volume in the power grid, where the IoT is considered to be as one of the most effective technologies.

In SG terminology, IoT is defined as a descriptive concept that expresses the ability of any object to connect each other with an IP address and a maturity of embedded intelligence in communicational grids. This intelligence can contain assessments, identification, security, grid, process, and control. From this point of view, SG and its unique components will be considered as an IoT concept, since inside the SG, a wide range of communicational grids connect devices to each other, which various intelligence levels in the format of assessment and control, for the purpose of power grid management, are embedded inside it [18]. Hence, at first glance, one can classify the role of IoT in SG realization in the following three sub-layers that has been shown in Fig.2.

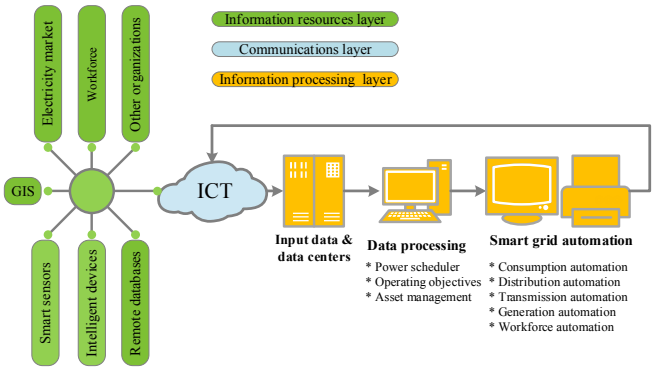

Figure 2: Triple steps of information collection, transmission, and process in IoT-SG

- The layer of smartization of power industry's equipment or installation of IoT smart instruments and devices, for the purposes of sensing, processing and data exchanging.
- Communications layer: collecting data from smart instruments by IoT communicational protocols for dispatching to control center.
- Information layer: the ability of realization, expansion of algorithm estimation and prediction with the purpose of optimal grid control via big data analysis.

It should be noted that smart instruments in power grids include different types of instruments in domains of consumption, distribution, transmission, and production. It is evident that all equipment and elements of the power grid do not have sufficient intelligence at this time, hereby, cannot be considered as IoT elements. On the other hand, the smartization procedure of the smart grid's equipment is considered as a gradual and costly process, and the cease of operation of a traditional grid with the aim of smartization of all equipment is impossible. Thus, IoT smart instruments installation with the purpose of data collecting from the non-intelligent equipment is the first step in the route of this evolution.

IoT smart instruments mainly include different kinds of wireless sensors, RFIDs, M2M devices, laser scanner cameras, GPS and all kinds of data collection equipment that can be installed on various power industry equipment like wind turbine for collecting different types of electrical, mechanical and environmental data. As has been shown in Fig.2, IoT–SG data, in addition to smart instruments, are collected from other subsystems such as remote databases, GIS basses, employees and other organizations and through communication infrastructure (according to communication protocols based on IoT or non-IoT). Collected data that include subscriber's electricity demand, energy consumption, network status components, failure reports from power lines, smart measurement recordation, power outage management reports, and conditions are being predicted so that through a proper infrastructure, and after storage and process, the processed outputs will be returned to the desired organizations and components. It is necessary to mention that high sampling rate of collected data, by IoT instruments in SG, causes an extreme increment of data size. In the power industry, different kinds of instruments, collect various types of information. Moreover, the required speed for collecting and information processing is so much in an IoT-SG system. Therefore, available information in the desired system is treated as a big data type, and it can be used from the analysis and management of big data methods, such as hardware, software, and algorithms. By data analyzing, supervision facility, different consumption policy implementation, tariff determination, production and consumption management, power outage prevention, grid's partial isolation in case of failure or fault, and load prediction will be provided. By IoT-SG implementation, many opportunities will be made for the power industry in order to create value based on innovative IoT projects. In the global economy organization report, in the scope of digital evolution in the power industry, four newfound issues such as property life cycle management, network integration and optimization, customer service aggregation and other subjects beyond the power industry have been introduced [19].

IV. THE CHALLENGES ENCOUNTERING IOT IN SMART GRIDS

During the implementation of IoT, many barriers may be built. One of the most prominent and important obstacles is the large produced body of data, which must be managed. This section delves into the barriers ahead of IoT-SG.

A. Energy supply

Since the IoT technology is propounded, the integration of IoT in SG, as well as energy supply for a myriad of things connected to the network, have been regarded as a monumental challenge. In the past, the volume and the diversity of generation resources were limited, thereby the selection of suitable energy sources to serve IoT instruments was a tough act [20]. However, nowadays, the developments in renewable energy technologies along with the improvements in their efficiency have made it possible to use renewable energy sources, such as wind and solar energies, almost in all locations throughout the world so that they provide better performance than traditional sources. Besides, new instruments are also manufactured which consume less energy. These factors indicate that the energy supply is not counted as a severe drawback anymore. The instruments used in IoT-SG should be able to keep its functionality for an extended period without the need to battery replacement and to repair hardware defects. In this regard, particular attention is devoted to the quality of IoT instruments.

B. Data management

Data management has a vital role in SG, and it maintains the proper performance of the electricity grid. IoT-SG is an extensive and dynamic system, and the management of the large generated big of data has paramount importance. Hence, the data management in IoT-SG requires a dynamic server, which functions as the conjunction of data, software, and other items [21]. These features translate into the obsolete of traditional database systems. Thus, in data management design in an internet network, an appropriate platform for IoT must be used, in which the concepts of communication, processes, and storage should be correctly defined, and it should procure the flexibility, security, domination, administration capabilities, scalability, and the observation of things' standards. The data management framework includes a data-driven layer and an interface for connecting IoT components. The data-driven layer is comprised of all virtual or real existents of the grid which are able to generate data. These data are stored in data centers and enables the system to have a real-time operation and to process the data. Besides, these data centers can provide accessibility for users. The interface layer is responsible for risk assessment and dealing with the user's request while deciding which resource and when it must be incorporated.

Energy systems are faced with management obstacles such as IoT-SG challenge. This complexity arises from barriers such as the vastness of the grid, the diversity of connected devices to the grid, synchronization and coordination of connected devices, the management of devices, the interpretation and analysis of the data corresponded with different components and devices, and data storage restrictions. In additions, the energy saving strategies and methods should be used which is contemplated as an important factor in both hardware and software structures. The communication, reaction, and interaction of the components are also treated as a kind of challenge. It is because the wireless connection can operate functionally in the distance by a few centimeters when two things are connected, or a user brings its mobile phone in the vicinity of that thing. This matter emphasizes on such short distances so that in close vicinity a lower level of energy is required while for long distances, the addressing is more complicated and the energy consumption will increase.

C. Big data

Over time and by the entrance of technology into the human's life and industry, a large body of data is generating which must be handled. The question was that how should such a massive body of data be stored, transferred or processed? IoT-SG, which is a large network comprised of a large variety of instruments, devices, and components of generation, transmission, and distribution of electricity, is an example of the application of IoT for the purpose of implementation of smart grid [22]. In recent years, the concept of big data analytics with different standards has been proposed and are gradually developing. Big data stands for a set of data which cannot be acquired, processed, and managed with the common types of software in a short period of time because it has massive volume and it is updating or extending over time. In 2001, the Gartner Institute (META group) announced three dimensions of challenges and opportunities ahead of the growth of data:

- Volume: The increase in the size and quantity of data
- Velocity and acceleration: The velocity increase in data generation, transmission, and processing as well as input/output velocity
- Diversity: The increase in the variety of data and expansion of diversity range

D. Uniform standard

In IoT-SG, the different components of the electricity grid take advantages of embedded sensors that enable them to generate various data. In order to have integrated management, all the generated data must comply with a uniform standard. At present, regard to the existence of different operating systems supported or incorporated by different large companies such as Microsoft, Samsung, EBM, etc., it seems hard to reach a consensus for a uniform standard. For example, the Samsung company has offered Artik platform, while the Microsoft company has offered the Azure platform as open-source cloud computing platforms [23].

Different IoT standards are laid down for application developers and service provides. Usually, the basic communicational standards, such as 6LoWPAN, are used so far. Figure 3 depicts the IoT protocol stack along with the basic communicational protocols. The IoT protocols are categorized into four types: Application protocols, Service discovery protocols, Infrastructure protocols, Effective protocols. However, it is not necessary to integrate all of these protocol in an application. In addition, with respect to the type of application, the employment of some protocols may be unnecessary. The basic protocols in IoT are considered as the standard protocols including Advanced Message Queuing Protocol (AMQP), Message Queuing Telemetry Transport

(MQTT), Extensible Messaging and Presence Protocol (XMPP), Constrained Application Protocol (CoAP), Data Distribution Service for real-time systems (DDS), simple object access protocol (SOAP), Representational State Transfer (REST), navigation protocol, data discovery services, and Hypertext Transfer Protocol (secure) (HTTP(s)).

E. Security

In IoT-SG, each connected device can be a plausible port to IoT infrastructure with personal data [24]. The concerns related to privacy and security are too important. By appreciation of complexity, the weakness in security and possible vulnerabilities in IoT-SG corresponded with cooperation ability, data fusion, automatic decision-making has assumed more importance than ever.

<table>
<tr><th>IoT multilayer architecture (5-layer model)</th><th colspan="3">The position of the basic communication protocols on IoT protocols stack and multilayer architecture</th><th>IoT protocol stack (four groups)</th><th>No</th></tr>
<tr><td rowspan="2">Application layer</td><td>AMQP</td><td>MQTT-SN</td><td>CoAp</td><td rowspan="2">Application protocols</td><td rowspan="2">1</td></tr>
<tr><td>REST</td><td>HTTP</td><td>DDS</td></tr>
<tr><td rowspan="2">Network layer</td><td colspan="2">DNS-SD</td><td>mDNS</td><td>Service discovery protocols</td><td>2</td></tr>
<tr><td colspan="3">RPL</td><td rowspan="3">Infrastructure protocols</td><td rowspan="3">3</td></tr>
<tr><td>Adaptation layer</td><td>IPv6</td><td>IPv4</td><td>6LoWPAN</td></tr>
<tr><td>Data link layer</td><td colspan="3">IEEE 802.15.4</td></tr>
<tr><td>Physical layer</td><td>IEEE 802.15.4</td><td>EPC Global</td><td>LTE-A</td><td rowspan="2">Effective protocols</td><td rowspan="2">4</td></tr>
<tr><td></td><td>IEEE1905.1</td><td>IPSec</td><td>IEEE188.3</td></tr>
</table>

Figure 3: IoT protocol stack along with the basic communicational protocols

Since more complexity translates into more vulnerability, the privacy threats will be raised. In IoT-SG, most of the data are pertaining to sensitive parts of generation, transmission, and distribution section. Thus, the security of these data is a controversial issue in big data deployment of IoT-SG and the experts and professions related to cybersecurity must include these threats in big data to guarantee privacy. The implementation of IoT must be accepted and verified by the law, ethics, politics, and society. Hence, the legislation and regulation challenges, systematic strategies, technical facets, and business aspects must be taken into consideration. The section ahead focuses on the technical aspects of the security architecture of IoT-SG. The security in IoT-SG entails the inclusion of security factors from designing stage to the serving stage.

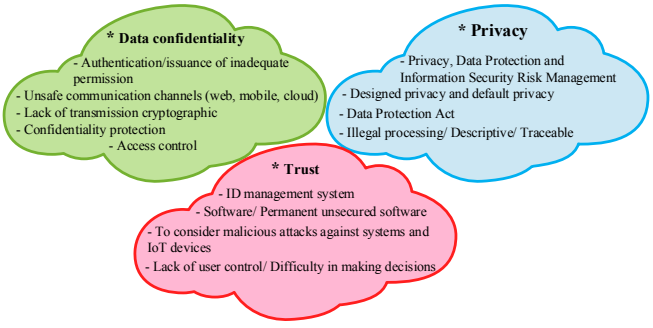

Figure 4: The main research challenges in IoT-SG

The main challenges in IoT-SG scenario encompass data confidentiality, privacy, and trust which are described in Fig. 4 in detail. In order to highlight the security requirements for IoT-SG, a 4-layer architecture is considered for it comprised of sensor layer, network layer, services layer, and application layer. Each layer is able to maintain security control measures such as access control, authentication of device, integrity, and confidentiality in data transferring, availability, and protection against viruses and cyber-attacks. In Table 1, the most considerable concerns in IoT-SG is summarized. The security requirements depend on sensor technology, network architecture, and layers. The security of wireless sensor network is regarded as one of the most serious security issues in IoT-SG. Hence, the wireless networks usually obey 8-layer Open System Interconnection model (OSI), which is illustrated in Fig. 5. The security threats corresponded with the protocol's layers are usually incorporated with respect to the integrity, validity, availability, and confidentiality, which are well described in Table 2.

TABLE I. THE SECURITY ISSUES IN IOT-SG

Security concerns	Application layer	Service layer	network layer	Sensing layer
Unsafe web communication channel	*	*	*	
Authentication/ Inadequate certification issuing	*	*	*	*
Unsafe network services		*	*	
Transmission cryptography shortage		*	*	
Privacy concerns		*	*	*
Unsafe cloud communication channel	*			
Unsafe mobile communication channel	*		*	*
Poor security configuration	*	*	*	
software/ Unsafe firmware	*		*	
Poor physical security			*	*

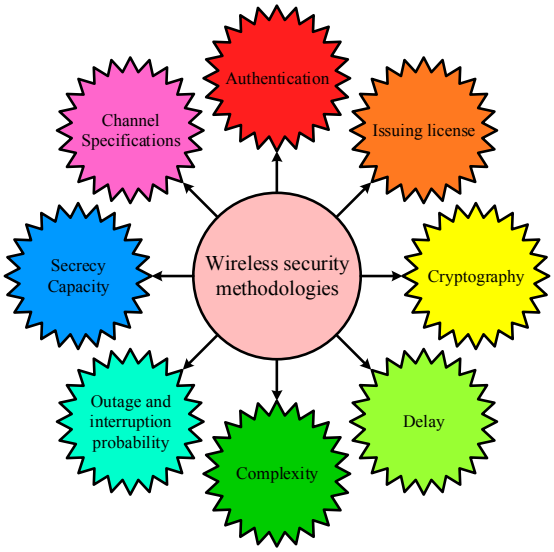

Figure 5: Wireless security methodology

TABLE II. THE SECURITY THREATS CORRESPONDED WITH PROTOCOLS' LAYERS

Security request	Specific Objectives
Credit	To distinguish authorized users from unauthorized users
Confidentiality	To restrict access to confidential data only for authorized users
Integrity	To ensure the accuracy and authenticity of the transmitted information
Availability	To ensure that authorized users can access the service at any time

V. THE SOLUTIONS FOR THE CHALLENGES

IoT technology has been a matter of debate in the IT area of research. In order to improve the functionality and practicality of IoT, it is required to solve the challenges at all stages and improve efficiency. This matter will result in development and increase in the pervasiveness of IoT is modern societies and industries [25]. Security is of the most prominent issues and challenges in IoT-SG. Therefore, the following section talks about the possible solutions, which help to mitigate the risks that compromise the security of IoT-SG.

A. Immunology system

Immunology is one of the solutions brought up for solving security problems. This system has five filters; most of them will be run on the filter of security threat detection. Thus, the detection of viruses in the locations, where their security is threatened is of particular importance. This system tries to pass the IoT-SG through these five filters in order to make permanent dynamic security. Fig. 6 shows the security filters of this system.

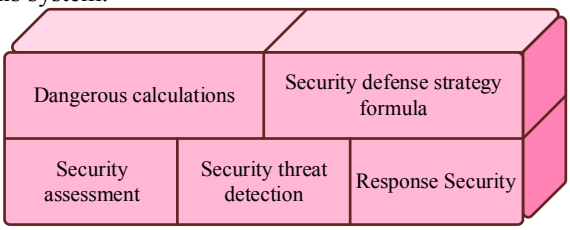

Figure 6: The filters defined in immunology approach

B. Rerump system

This system is of the approaches for security crisis. In this method, which is propounded by the European Union, the 8-layer OSI model is included, and a multilayer system is divided into separate sub-sections, which are responsible for the investigation of different layers [26]. This system mainly focuses on the lower layers. Fig. 7 demonstrates the structure and the trend of this system.

C. The solutions for maintaining the security of IoT-SG

Some of the manufacturers of IoT-SG devices are startup companies and beginner in term of experience, particularly in the area of cybersecurity. They usually have scant investment, which is why they cannot afford to employ security experts. Thereby, they have to be satisfied with the basic security mechanisms for their manufacturing hardware and their developed software. Thereby, their products usually have lots of security vulnerability [27].

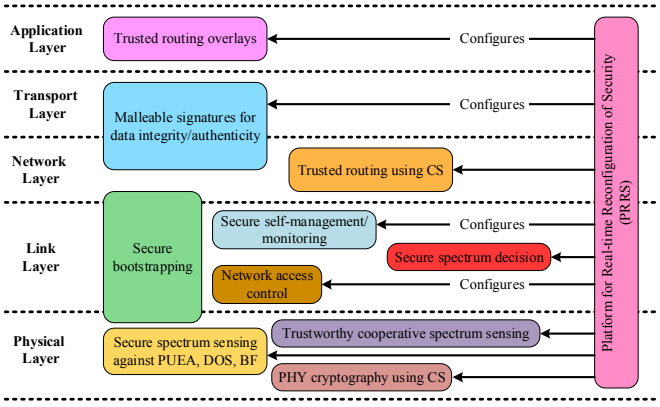

Figure 7: The implementation of Rerump approach on the OSI model

Many of the companies in the area of IoT-SG have made feeble attempts to conduct research and development for improving the security facets of their products, and their ultimate goal is to minimize the final price of the product. Almost all the devices that are able to connect to the internet are equipped with the embedded operating systems in their permanent software. Nevertheless, their operating systems are produced regardless of security purposes. Hence, most of them suffer from various kinds of vulnerabilities. In the development of IoT-SG (such as wireless sensor network, in which all nodes, aside from sink node, are the same) there is an abundance of security threats. It is because, if an attacker succeeds to discover the vulnerability of a node, the rest of the nodes which are the same or have a similar design or protocol are at risk. Due to the considerable rise in the number of connected devices, the targeted input points as vulnerability will be increased. Regard to the simple structure of some devices and the creation of tools and tricks, it is not needed for a hacker to have a high level of proficiency. The cybercriminals can reprogram the devices with weak design and use that device for stealing sensitive information. Several IoT-SG devices may be placed in hard and compact frames and may be placed there for a long time. This matter makes it hard to upgrade or reconfigure them. Some applications are developed to deal with a large number of devices and things. These applications usually have no upgrade capability to avoid complexity. Some devices have a long lifetime and usually are replaced at specific intervals. Some devices may have a lifetime longer than their manufacturer company; thereby there is no support anymore for that product. It is evident that the security mechanisms of these devices in the mentioned scenario can be expired that will be led to the rise of security concerns. In some applications, the development of devices may occur in a place, where the procurement of physical security (protection against physical damage) is a tough measure. In such a circumstance, malicious entities catch the devices physically in order to reverse engineer the device and acquire sensitive information. IoT-SG is designed to perform seamless and integrated connectivity between devices, equipment, systems, and subsystems in the smart grid. For instance, if a smart meter being attacked, it can be used for sending spam through Wi-Fi. Table 3 points out the

threatening factors for IoT-SG in accordance with their classification.

TABLE III. THE CLASSIFICATION OF THREATENING FACTORS OF IOT-SG

Threatening factor	Class	Common examples
Special no purpose	software	Computer viruses, worms, Trojans, logic bombs
Employees	Internal	Unhappy employees, contractors, security guards
Offenses and organized criminals	External	Criminals targeting vulnerable information, such as electricity consumers' information and financial accounts
Companies	External	Other companies, partners, competitors, retailers
Human	Unintentional	Accidents, carelessness
Human	Intentional	Internal, External
Natural disasters	Inhuman factors	Flood, Fires, Lightning, Earthquake

D. Deployment of cloud IoT

One of the main challenges in IoT-SG is big data and storage restrictions. In order to tackle this problem, the employment of cloud computing in IoT-SG is suggested, which is also referred to as Cloud IoT [28]. Cloud computing is a model consists of a set of computing resources (such as servers, storage space, and services). The purpose of cloud computing is to provide quick and access to these resources. Cloud computing can be classified into four categories of public model (accessibility of all people to the resources and governed by an organization as the owner and supporter), private model (restricted access exclusively dedicated to a private entity, or a specific company or organization), grouped cloud model (some organizations have access to the resources, and the cloud space is dominated by a company), and hybrid cloud model. In this scheme, the objective is to improve the service quality level served to the customers. In this regard, some settlements must be negotiated between service providers and customers about the type and level of services demanded by the end-users. In addition, the owner and the supporter of the could space must be specified. It is also strongly recommended that the cloud space must have more than one supporter. This idea must be matured in the future yet.

E. Communication infrastructure

The implementation of IoT-SG and data exchange in this environment require a strong communication infrastructure. The reason why such a reliable communicational environment with a high bandwidth is required is that plenty of devices will be connected to each other and servers and an enormous body of data will be generated continuously, which must be sent, stored, analyzed, or received. Thus, the biggest possible volume of data including appropriate signals and controlling commands must be transferred at the shortest intervals. In the network concept, which is counted as an infrastructure, the selection of the type of network (wireless, cellular, or local ethernet) has paramount importance with respect to the level of services demanded.

VI. CONCLUSION

In order to materialize and implement the IoT-SG concept, profound revolutionary changes must be made in the traditional electricity networks in the areas of operation technologies encompassing sensors, relays, practical applications, and in the area of information technology including big data, data processing and analysis, telecommunication networks, security, and standards. Hence, as the information technology and the operation technologies are more converged toward each other, the IoT-SG scheme approaches to its objectives. IoT-SG has a couple of advantages and applications. The utilization of IoT-SG in power industry improves the efficiency and profitability in this section and brings more controllability over various parts of smart grids. However, IoT-SG is encountered with lots of challenges such as the management of ever-growing body of data, the management of things in the grid, the lack of unified global standards, the interconnectivity of things, and the security of data, etc. This paper delved into the privilege and challenges facing IoT-SG. Besides, practical solutions are brought up to tackle plausible problems in IoT-SG. In the future, the security mechanisms, privacy concerns, the confidentiality of data, big data deployment, cloud computing, and communication standards should be more matured to alleviate the security concerns.

REFERENCES

[1] Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems*, *78*, 964-975.

[2] Shahinzadeh, H., Moradi, J., Gharehpetian, G. B., Nafisi, H., & Abedi, M. (2019, January). IoT Architecture for Smart Grids. In *2019 International Conference on Protection and Automation of Power System (IPAPS)* (pp. 22-30). IEEE.

[3] Shahinzadeh, H., Moradi, J., Gharehpetian, G. B., Nafisi, H., & Abedi, M. Internet of Energy (IoE) in Smart Power Systems. In *2019 5th Conference on Knowledge Based Engineering and Innovation (KBEI)* (pp. 627-636). IEEE.

[4] Li, Y., Cheng, X., Cao, Y., Wang, D., & Yang, L. (2018). Smart choice for the smart grid: Narrowband Internet of Things (NB-IoT). *IEEE Internet of Things Journal*, *5*(3), 1505-1515.

[5] Kabalci, E., & Kabalci, Y. (Eds.). (2019). *Smart Grids and Their Communication Systems*. Springer.

[6] Siozios, K., Anagnostos, D., Soudris, D., & Kosmatopoulos, E. (2019). *IoT for Smart Grids*. Springer.

[7] Lombardi, F., Aniello, L., De Angelis, S., Margheri, A., & Sassone, V. (2018). A blockchain-based infrastructure for reliable and cost-effective IoT-aided smart grids.

[8] Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, *58*(4), 431-440.

[9] Liu, Q., Ma, Y., Alhussein, M., Zhang, Y., & Peng, L. (2016). Green data center with IoT sensing and cloud-assisted smart temperature control system. *Computer Networks*, *101*, 104-112.

[10] Lucic, D., Caric, A., & Lovrek, I. (2015, July). Standardisation and regulatory context of machine-to-machine communication. In *2015 13th International Conference on Telecommunications (ConTEL)* (pp. 1-7). IEEE.

[11] Ercan, A. Ö., Sunay, M. O., & Akyildiz, I. F. (2018). RF energy harvesting and transfer for spectrum sharing cellular IoT communications in 5G systems. *IEEE Transactions on Mobile Computing*, *17*(7), 1680-1694.

[12] Ratasuk, R., Vejlgaard, B., Mangalvedhe, N., & Ghosh, A. (2016, April). NB-IoT system for M2M communication. In *2016 IEEE wireless communications and networking conference* (pp. 1-5). IEEE.

[13] Wang, J., Su, J., & Hua, R. (2019, January). Design of a Smart Independent Smoke Sense System Based on NB-IoT Technology. In *2019 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS)* (pp. 397-400). IEEE.

[14] Ray, S., & Bhadra, J. (2016, September). Security challenges in mobile and IoT systems. In *2016 29th IEEE International System-on-Chip Conference (SOCC)* (pp. 356-361). IEEE.

[15] Dalipi, F., & Yayilgan, S. Y. (2016, August). Security and privacy considerations for iot application on smart grids: Survey and research challenges. In *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)* (pp. 63-68). IEEE.

[16] Goudos, S. K., Sarigiannidis, P., Dallas, P. I., & Kyriazakos, S. (2019). Communication Protocols for the IoT-Based Smart Grid. In *IoT for Smart Grids* (pp. 55-83). Springer, Cham.

[17] Pathan, A. S. K., Fadlullah, Z. M., & Guerroumi, M. (2019). *Smart Grid and Internet of Things*. Springer International Publishing.

[18] Ghasempour, A. (2019). Internet of Things in Smart Grid: Architecture, Applications, Services, Key Technologies, and Challenges. *Inventions*, *4*(1), 22.

[19] Reka, S. S., & Dragicevic, T. (2018). Future effectual role of energy delivery: A comprehensive review of Internet of Things and smart grid. *Renewable and Sustainable Energy Reviews*, *91*, 90-108.

[20] Moradi, J., Shahinzadeh, H., Nafisi, H., Gharehpetian, G. B., & Shaneh, M. (2019, June). Blockchain, a Sustainable Solution for Cybersecurity Using Cryptocurrency for Financial Transactions in Smart Grids. In *2019 24th Electrical Power Distribution Conference (EPDC)* (pp. 47-53). IEEE.

[21] Jaradat, M., Jarrah, M., Bousselham, A., Jararweh, Y., & Al-Ayyoub, M. (2015). The internet of energy: smart sensor networks and big data management for smart grid. *Procedia Computer Science*, *56*, 592-597.

[22] Singh, S., & Yassine, A. (2018, July). IoT Big Data Analytics with Fog Computing for Household Energy Management in Smart Grids. In *International Conference on Smart Grid and Internet of Things* (pp. 13-22). Springer, Cham.

[23] Morello, R., De Capua, C., Fulco, G., & Mukhopadhyay, S. C. (2017). A smart power meter to monitor energy flow in smart grids: The role of advanced sensing and IoT in the electric grid of the future. *IEEE Sensors Journal*, *17*(23), 7828-7837.

[24] Ahmad, M., Younis, T., Habib, M. A., Ashraf, R., & Ahmed, S. H. (2019). A Review of Current Security Issues in Internet of Things. In *Recent Trends and Advances in Wireless and IoT-enabled Networks* (pp. 11-23). Springer, Cham.

[25] van Oorschot, P. C., & Smith, S. (2019). Internet of Things (IoT) Security and Privacy.

[26] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395-411.

[27] Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities.

[28] Yassine, A., Singh, S., Hossain, M. S., & Muhammad, G. (2019). IoT big data analytics for smart homes with fog and cloud computing. *Future Generation Computer Systems*, *91*, 563-573.