Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 1, No. 5, January : 2024

FRAMEWORK OF NETWORK SECURITY FOR ENERGY INTERNET

Dr. Chetan Khemraj Lanjewar Director, Mangalmay Institute of Engineering & Technology, Greater Noida, U.P., India, Email: chetan.khemraj@gmail.com
Sushma Vinayak Barahate Assistant Professor, Sri Balaji College of Engineering, Jaipur, Rajasthan.

Abstract
This study proposes that energy Internet is the power system's future development direction, since it addresses the issues of clean energy compatibility and deep and efficient power system control. The energy sector faces information security challenges. The Internet classifies flaws and investigates information security. Protection of distributed energy stations in an energy Internet context. This paper presents the system architecture of distributed energy stations in the context of the energy Internet, analyses the information security protection countermeasures of distributed energy stations, and analyses by constructing the network security framework of distributed energy stations, in order to provide assurance for distributed energy station information security.
Keywords: Energy Internet, Network Security Framework, Internet of Things.

Introduction

The development and implementation of the Internet of Energy has gotten a lot of attention lately, thanks to the rapid expansion of renewable energy and the increasing wave of mobile applications. The term "Energy Internet" was coined by Jeremy Rifkin, a well-known American researcher. He stressed the following point of view in his book "The Third Industrial Revolution": fossil fuels, such as petroleum, play an indispensable role in modern society, but its faults, such as non-renewability and pollution generated by their usage, are equally fatal. The current industrial paradigm based on fossil fuels is increasingly fading as civilization progresses. Rifkin forecasts that a new energy system called "Energy Internet" will emerge and grow in the near future in his other writings. He is built on a new energy system and is heavily reliant on power information technologies. Rifkin's suggested energy Internet has following characteristics:

1. The primary energy consumed is converted to renewable energy;
2. Distributed power generation and small-scale energy storage systems will continue to be linked in the future energy development process. Connected to the power grid, its access modes and ways are gradually diversifying;
3. Different forms of energy at various locations may be networked and shared using the newest Internet technology;
4. It can promote the development and progress of electrification.

Renewable energy, particularly distributed renewable energy, will increasingly become dominant in the energy Internet's composition in the near future. Information technology is constantly being utilised in new industries as modern computing, network, and remote control technology advance, and power system information technology is also rapidly growing, gradually integrating with energy technology. New technologies are continually being developed as part of the integration process . The field of smart energy entails the application of sophisticated power information technology to improve power energy management and completely realise energy connectivity and precision regulation in various places. The regional energy Internet concept is primarily based on the continuous expansion of unit scenarios in the energy Internet, which include integrating photovoltaic power generation, distributed energy, electric vehicles, energy storage, integrated energy, and other power system components, as well as combining scheduling transactions and information interaction business scenarios. The regional energy network has advanced at a remarkable place[1].

The main difference between the energy Internet information communication and the traditional energy information network, in terms of the composition of the energy Internet and its business

scenarios, is in the aspects of renewable energy automation data access and business application mobilisation. For large-scale centralised new energy stations, automated data communication methods mostly follow traditional thermal power plants, hydropower plants, and other power plant automation access methods and security strategies, that is, the remote control device passes through the dispatch data network Access to the dispatching SCADA system. There are still a considerable number of examples where the automated connection to the grid dispatching and monitoring has not been realised for dispersed energy stations connected to the distribution network. The challenge of automatic data communication remains unsolved, and the grid's secure and stable operation poses some security hazards. In terms of business application mobilisation, another pressing issue in the energy Internet information communication is the security of mobile application information interaction. Information security, such as mobile terminal electrical bill payment, information query, distributed power transaction, demand response, smart home control, and so on, is a major concern in terms of equipment functioning and transaction funds security. As a result, information security has grown in importance, and information security protection technology has emerged as a critical technical assurance for a new generation of energy and power systems. The energy Internet information communication scenario is depicted schematically in Figure 1:

There may be some potential security flaws in data gathering, communication, authentication, and other areas of the energy Internet, which will undoubtedly cause a certain number of information security difficulties. Because the control of all infrastructure in a distributed energy station is dependent on the Internet, an attack on the network system can directly lead to the breakdown of the information system, and the security of the information system has a direct impact on the security of the entire system. The information security of the distributed energy station control system is a complicated problem, and relying solely on security technology solutions may not be able to realise the overall security protection system. Instead, comprehensive prevention and control of a variety of means, as well as compliance with national standards and regulations, 2.0 points domain and layered various relatively mature security protection measures, are required to improve the defensibility[2].This paper investigates the information security depth defence architecture of distributed energy station control systems and researches and analyses the information security of distributed energy stations in the energy Internet environment, based on threats to the information security of distributed energy station control systems in the energy Internet environment.

The second chapter of this paper primarily introduces major threats of the energy Internet system, the third chapter primarily introduces distributed energy station architecture in the context of the energy Internet, the fourth chapter primarily discusses the application of information security protection for distributed energy stations, and chapter 5 is the conclusion.

Energy Internet system and its major threats

Several power information system sub-modules are currently included in the existing power grid information system: power information network, power dispatching automation network, DMS(“distribution network management system”),WAMS(“wide area monitoring system”) and EMS(energy Management system). The key components of the energy management system are: “data acquisition and monitoring system (SCADA)”, “power state estimation system” and “AGC(automatic generation control system)”.DMS generally includes distribution system and DAS(distribution automation system).PMU(“synchronous Angle measurement unit”), DMS and GIS(Geographic information system) are the primary elements of a WAMS.

Real-time capture of diverse power grid data is possible thanks to PMU control. To ensure timely data gathering, both DMS and EMS systems require a remote control unit and a “supervisory control and data acquisition system(SCADA)”. The demands on power grid construction are increasing as the smart power grid evolves, and they are unable to match the high real time needs of powergrid broad area control and energy scheduling. The WAMS has a response time of roughly 100 milliseconds, but it has a number of drawbacks, including expensive power grid building costs and p

oor repeatabilit-y. In China, only PMU nodes are used to adjust the Main system voltage above 110 kV, and smaller substations cannot be developed due to a shortage of funds. The existing power grid information system can only collect and control data from 110 kV power stations and high-power equipment due to construction limits, and cannot receive power load information in real time[3]. It can only allocate energy based on off-line predictions of future power consumption. The power information network has the following major issues based on the features of the aforesaid information systems:

1. Important power system parameters, such as power amount and peak value, are timevarying and realtime, and cannot be predicted in real time, making prediction extremely difficult and dispatchi-ng with the help of the power information system.
2. For the purpose of ensure the safety of power lines and the transmission lines' actual capacity is frequently sacrificed, resulting in waste of resources and repetitive building.
3. At the moment, the power system is unable to assess the situation in a timely manner. The location and severity of the flaws. The use of a single detection method results in construction repetition, which wastes a lot of man power and material resources.
4. Electric energy storage on a large scale is not possible achieved, resulting in a dynamic load balancing of reactive power, which has an impact on the grid's efficiency. To tackle the aforementioned issues, a significant amount of capital expenditure is required to continuously build monitoring equipment. However, a considerable amount of data arrives at the same time, causing the power grid information system's processing efficiency to fall shorty of meeting demand. To meet the appropriate needs, advanced information network technology and big data processing technology can be applied. At the moment, this is the issue that the smart gris system must address. At the same time, various factors can have an impact on the energy internet cintinuum.

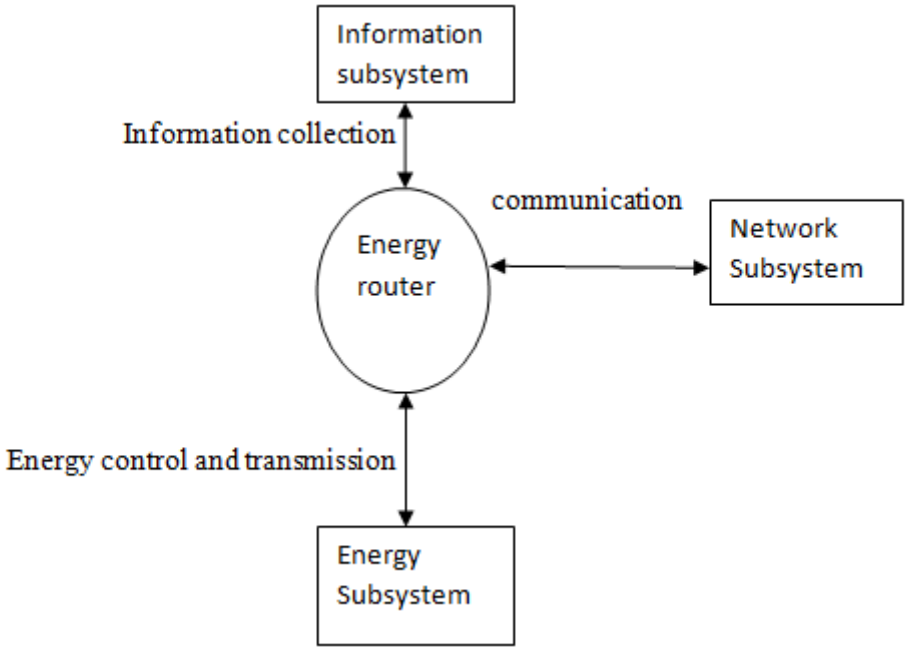

Fig. 1 Energy Internet Communication.

2.1 Cyber Attacks

Denial of service-

A DoS attack paralyses a system by faking a large number of connection requests, causing the user's request to fail to respond normally.Smart metres, for example, which are commonly used in power pl ants, enable only a limited number of connections and are subject to denial-of-serviceassaults[4]. The attacker can fabricate bogus data and report it to the control centre whenever the device stops responding after a particular amount of time.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 1, No. 5, January : 2024

Network intrusion-
It exploits a flaw in the industry control system to get access to the actual physical system, gaining ac cess to the user's personal information, crucial system operational parameters, and even paralysing th e entire distributed energy system with forged control commands. A huge number of intelligent devic es are widely deployed in energy stations, and the related protection measures are very inadequate, m aking them easy targets for invasion and attack. When an attacker uses intelligent gadgets to break in to an enterprise's private communication network, the control system of the energy station, for exam ple, may be harmed.

Password cracking-
This type of attack aims to get device access rights. By using traffic monitoring or brute force cracki ng, illegal users can gain access to a password system and collect passwords, access rights, and user personal information.

4. Malware attack-This form of assault entails scanning network traffic for flaws, installing malicious programmes or adware, and attacking key electrical infrastructure. In Ukraine, malicious code attacked the power sector's monitoring and control system in December 2015, resulting in the destruction of a substation control system, power monitoring management system also malicious invasion, power generation equipment malfunction, and power blackouts in a matter of hours. At the same time, the power line repair system was targeted by malicious automatic dialling software , causing the system to become unresponsive and preventing normal maintenance work[5]. Malware attacks have increased in quantity, volume, and complexity in recent years. Such attacks will have a greater impact on the energy Internet as it continues to expand.

Architecture of distributed energy station under the environment of energy internet
In the future, the development of new smart grid information systems will be a major research focus. Following the preceding explanation, Fig. 2 depicts the suggested smart grid information system arch itecture.It is divided into three sections. To begin, smart grid information system infrastructure prima rily refers to the building of smart grid hardware foundations, which are registered for various compu ter rooms, servers, and communication connections, among other things[6]. The building of smart gri d software infrastructure, includes all types of software toplevel design; Smart grid information syste m application system to meet the smart grid construction objectives of various applications, primarily for users of various information systems[7].The physical model and information model, in general, c an be used to explain the information front end. The former describes the information front end's syst em node position, while the latter displays its dynamic and static data.

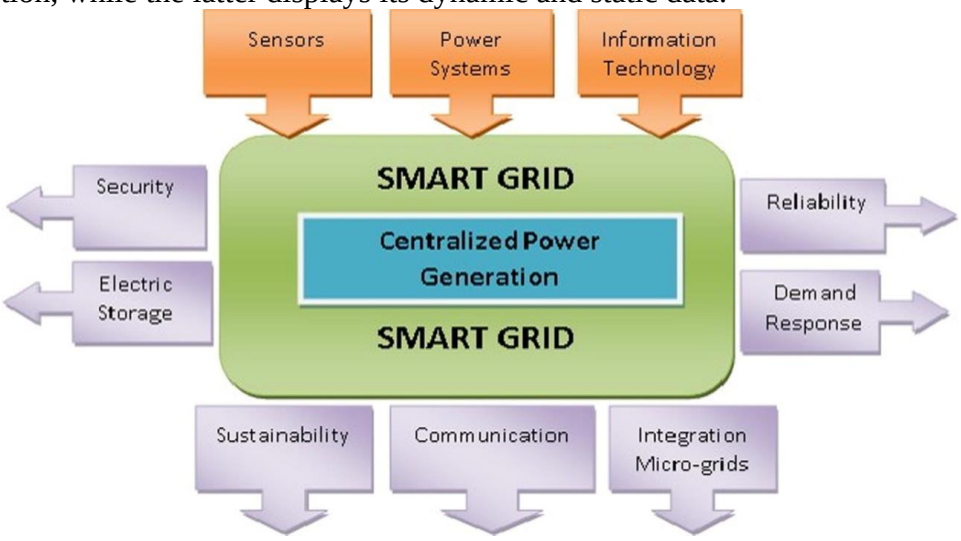

Fig.2 Architecture of Smart grid
[Source:20]

3.1 Distributed Energy Architecture

Under the Internet power environment, the distributed power station control system is mainly composed of a measurement element, a controller and an actuator, among which the controller is made up of a hardware platform and an application software platform. Since distributed power involves various industries, such as power and construction, the hardware control system platform is based on the creation of an automated control system based on a precise digital controller.It also refers to the energy industry using the SCADA-based PLC system or the DCS system.This paper introduces a distributed power station in East China as an example[8]. The power station is a three-way system, cooling and natural gas-based, which aims to provide cooling / heating of air-conditioning and domestic hot water in each building in the region, effectively improving energy efficiency and low carbon emissions. to get out. Project construction includes a set of internal gas generator, gas turbine, refrigerator / hot potassium unit, air source heat pump unit, medium cold water unit (heat pump), electric centrifugal chiller, heating equipment and storage tank system power.

Distributed energy station control system in gas internal combustion engines, gas turbines, gas smell k units, the main material such as centrifugal water chillers, air source heat pump pump is usually each manufacturer sets an integrated control system, bus communication monitoring system[9]. The mode is adopted to improve one-way communication, read the parameters of the machine state, in addition to the virtual connection between the monitoring system and the underlying system using a small amount of complete hardwire first-stop operation and important parameter settings. Depending on the software software and control system control system, firstly, due to the lack of platform hardware integration, the application software control strategy is in a state of combat, as well as a control function. remains only at the level of process control and first hand operation of the suspension and repair of power supply equipment[10]. A few software applications have been installed to monitor energy efficiency and efficiency, but the need for a separate user load changes frequently and significantly, network / cooling distance is longer, slower, and testing and research in this field is much shorter, so it is very necessary to do research by security protection of distributed power stations.

3.2 Countermeasures of information security protection of energy stations:

3.2.1 Components for protective security-

(1) Whitelist protection: a whitelisted defense system using pre-defined rules for a specific agreement to limit network data exchange, flexible behavior in control network controls based on analysis of network transfer protocol features. and a hole-in-the-line approach, from the source control network to the emergence and spread of anonymous malicious behavior. Authorization protection system is used not only in the rules for setting up security technologies, but also on the principles to be followed in actual network management[11]. For example, when performing appropriate tasks on a control computer or computer, you need to use a custom computer terminal with a USB flash drive, disk, etc. Managers rely only on visible ownership in performance, and unauthorized actions will be prohibited. Check the security of the goods. Authorized listing technology includes protocol authorization, white device list, white instruction list, white host list, white software list and white mobile media list, etc.

(2) Industrial firewall: This is an advanced firewall product designed for industrial control system. Analyzes the in-depth message of communication protocols (such as Modbus, OPC, Siemens S7, etc.) used in the industrial network[12]. Currently a firewall-based firewall only works on a Windows or UniX platform, only on embedded type control devices in a network (such as PLC, DCS, etc.) for specific traffic management, and industrial control is a special type. firewall hardware or software and hardware solutions, through a series of rules, to transfer information flow control to allow or deny network performance.Industrial firefighters, for example, include ip-free segregation, distributed distribution distribution, dual-layer protocol protection, industrial protocol configuration, and alarm log management to prevent unnecessary communication and reduce potential intrusion threats[13]. The information security strategy is shown in Fig. 3

3.2.2 Components for detection class security-

1. Risk scanning software: With compromised scanning software, the risk of power stations distributed under the Internet power station is constantly monitored, and vulnerable mining software is used to install vulnerable mines and early warning in the area without - use industrial control equipment, and identify security threats for advanced industry control equipment. Vulnerable scanning systems work to control[14].
2. Security monitoring and evaluation system: Security monitoringand the research program is rapidly developing on the basis of the signs of “no depth”, “no surveillance” and “insecurity” of the Chinese industrial management system[15]. Accept how to create a data screen to collect data for a large monitoring network, then performs a series of analyzes, and ultimately detects various security threats such as network confusion and hacker attacks. In addition, the system will use the "pass" method to connect people to it industrial control network, will not have negative effects on production performance, so it is easy to move and promote[16].

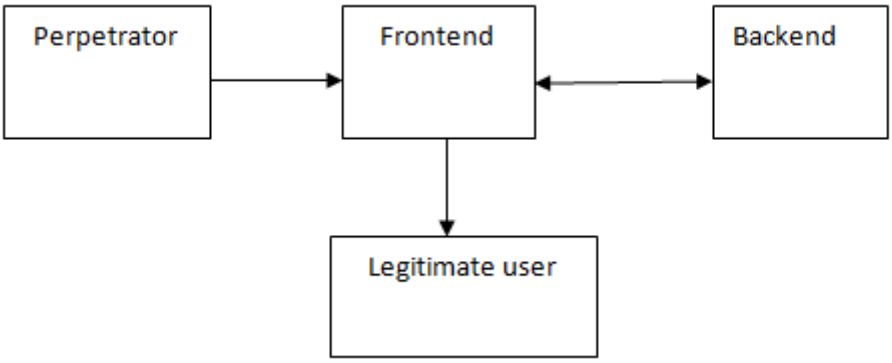

Fig.3 Frontend security

Application of the information security

The program has provided an integrated security management center, with a focus on integrated management of used security products and security incidents in the industrial network. Its highly efficient software and hardware hardware can integrate security configurations, policy outsourcing, security monitoring and trusted gateway alarms, security guards and an industry-controlled security monitoring system and research system installed in the entire power station control network. Measures of segregation and protection of the boundaries of the industrial control system are welcome. Blockage and border protection are used between the internal network and the external network, and border protection measures such as firewall, VPN and access control are adopted to ensure the security of the internal network[12]. The management system in the system is similar to the traditional IT system, which focuses on content information security and adopts common information security measures such as authority management and access control, while an industrial firewall and segmentation equipment is adopted between the control layer andIndustrialcommunication protocol is tested on a white list[17]. Trusted gateway is an important management element of a management center. All configurations are directed at a particular gate, and firewall safety policy rules should be issued to a particular gate to play a role, to facilitate the management of multiple gates with the same business. Grouping is an integrated problem with the control of the configuration gateway of the same service. When working in a group, all the online gates under that group are affected, so that the gateway to the same group can be set up in the same way. The distributed power architecture is shown in Fig. 4[18].Through security guards' security guards, industrial control traffic detection and unusual acquisition of security monitoring and research system, reliable gateway protection, security management including power station termination, network overload and network boundary built.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 1, No. 5, January : 2024

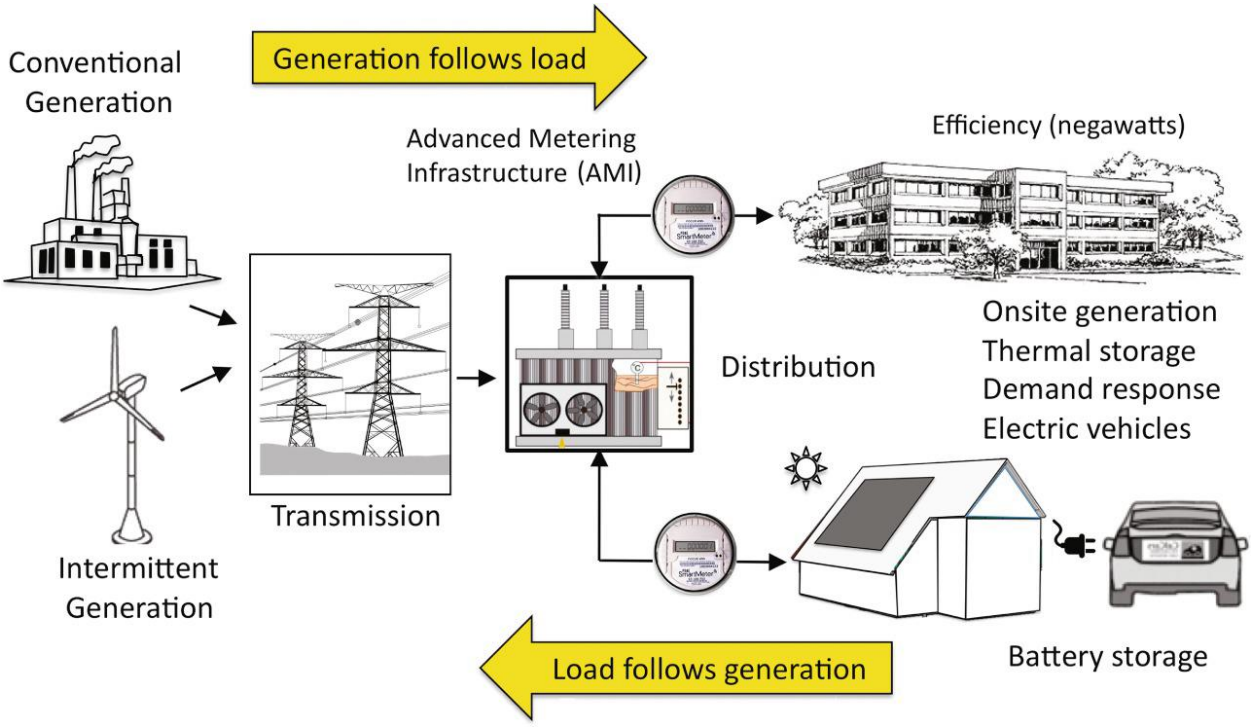

Fig.4 Architecture of distributed energy
[Source:19]

Conclusion

With the development of power communications and information security, information security for distributed power channels under the power internet site is a field of experimental research with a promising application potential. On the other hand, the development of distributed power stations presents significant opportunities for economic development in the industrial energy sector. On the other hand, it brings many new security issues. Power under an Internet site based on security analysis of distributed power information, this paper analyzes distributed power management system. With the continuous development of the energy industry, the smart energy grid has become a key driver for future energy grid development. The regional power network read in this paper is an integral part of future development, and the problem of access to end-to-end protection information will be an important guide to future development of power communications. The smart energy grid has become the subject of research and guidance at home and abroad. Therefore, the new intelligent and efficient design of the power network can continue to be built to improve the construction and use of a complete power network. Advanced capabilities may include the following technical features, the Internet from cloud computing, the Internet of Things, big data and mobile internet and other advanced concepts, integrated use of intelligent terminology, data collection and processing, forecasting analysis, control editing and other advanced technologies , a concept and a real secret combination, be aware of the flow of two forms of power and knowledge and sharing. Currently, the Chinese State Grid Corporation has prioritized a strategy to build a global power network and established its own policies and activities. Many provincial companies have done the work of building and using internet power.

References

1. KhaleghnasabR,BagherifardK,NejatianS,etal.Anewenergy-efficientmultipathroutingininternetofthingsbasedongraytheory.IntJInfTechnolDecisMaking2020;1(1):1–15
2. BorgesV.SurveyofcontextinformationfusionforubiquitousInternet-of-Things(IoT)systems.OpenComputerSci,2016;6(1).
3. HuanW.Researchandimplementationofsecuritymechanismsforinternetofthingsforresidentiale

nergybasedonZSEprofilestandard.ModernArchitElectr2016.
4. Cost of a Data Breach Report 2019 (2019). URL: https://www.all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf (accessed by 04.03.2021)
5. Website hacking statistics of 2020 (2020). URL: https://www.webarxsecurity.com/website-hacking-statistics-2018-february/ (accessed by 04.03.2021).
6. Security Orchestration, Automation And Response (SOAR) (2017). URL: https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-response-soar (accessed by 04.03.2021).
7. KoudaiHatakeyama, Daisuke Kotani, Yasuo Okabe, Zero trust federation: Sharing context under user control towards zero trust in identity federation, in: IEEE international conference on pervasive computing and communications, 2021.
8. Jinghui Li, Bifei Mao, Zhizhang Liang, Zeqi Zhang, Qiushi Lin, Trust, and trustworthiness: What they are and how to achieve them, in: IEEE international conference on pervasive computing and communications, 2021.
9. NirBitansky, AkshayDegwekar, VinodVaikuntanathan, Structure vs. hardness through the obfuscation lens, in: International cryptology conference, 2021.
10. W. Roh, J. Seol, J. Park, B. Lee, J. Lee, Y. Kim, J. Cho, K. Cheun, F. Aryanfar, Millimeter-wave beamforming as an enabling technology for 5G cellular communications: theoretical feasibility and prototype results, IEEE Commun. Mag. 52 (2) (2014) 106–113.

A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of Things: A survey on enabling technologies, protocols, and applications, IEEE Commun. Surv. Tutor. 17 (4) (2015) 2347–2376

11. August, T., Dao, D., & Kim, K. (2019). Market segmentation and software security: pricing patching rights. Manag. Sci., 65(10), 4575e4597.
12. August, T., Niculescu, M. F., & Shin, H. (2014). Cloud implications on software network structure and security risks. Inf. Syst. Res., 25(3), 489e510.
13. Meng, W., Zhu, L., Li, W., Han, J., & Li, Y. (2019). Enhancing the security of FinTech applications with map-based graphical password authentication. FutureGenerat. Comput. Syst., 101, 1018e1027.
14. Yang, W., Li, J., Zhang, Y., &Gu, D. (2019). Security analysis of third-party in-app payment in mobile applications. Journal of Information Security and Applications, 48, 74e87.
15. Abbasi, M., Mohammadi-Pasand, E., &Khosravi, M. R. (2021). Intelligent workload allocation in iot-fog-cloud architecture towards mobile edge computing. Computer Communications, 169, 71–80.
16. Abouzakhar, N. S., Jones, A., &Angelopoulou, O. (2017). Internet of things security: A review of risks and threats to healthcare sector. In 2017 IEEE international conference on internet of things (ithings) and IEEE green computing and communications (greencom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (smartdata) (pp. 373-378).
17. Adil, M. (2021). Congestion free opportunistic multipath routing load balancing schemefor internet of things (iot). Computer Networks, 184, 107707.
18. Randolph and G. Masters, "Distributed Energy Resources", *Energy for Sustainability*, pp. 313-339, 2018. Available: 10.5822/978-1-61091-821-3_10 [Accessed 30 March 2022].
19. H. Bhatti and M. Danilovic, "Making the World More Sustainable: Enabling Localized Energy Generation and Distribution on Decentralized Smart Grid Systems", World Journal of Engineering and Technology, vol. 06, no. 02, pp. 350-382, 2018. Available: 10.4236/wjet.2018.62022.