Cyberattack Measures in Smart Cities and Grids

Cevat Özarpa, İsa Avci, and Bahadır Furkan Kinaci

1 Introduction

With the development of information and communication technologies, cybersecurity problems in smart cities and networks are increasing rapidly. For this reason, increasing population, construction and mega investments, increasing energy needs in cities, and the need for smart grids come to the fore. However, this shows that the smart grid concept needs to be invested in and developed. With the frequent use of advanced network technologies used in smart cities, cyber risks and security vulnerabilities have come to the fore. Smart grids cover the areas of use of electricity, water, and natural gas networks, which are critical infrastructures of smart cities.

Anonymity and deniability are the facts that cyberattacks present an opportunity. It is also very difficult to identify the states and individuals behind these attacks. In such an environment, it is not possible to protect systems without mentioning absolute cybersecurity. For this reason, it is aimed to keep cybersecurity risks at a manageable and acceptable level. It is important to protect data in smart systems and to use them continuously. Cyberattack incidents should be handled with a holistic approach in smart grids and cities.

C. Özarpa
Engineering Faculty, Mechanical Engineering, Karabuk University, Karabuk, Turkey
e-mail: cevatozarpa@karabuk.edu.tr

İ. Avci (✉)
Engineering Faculty, Computer Engineering, Karabuk University, Karabuk, Turkey
e-mail: isaavci@karabuk.edu.tr

B. F. Kinaci
Engineering Faculty, Railway System Engineering, Karabuk University, Karabuk, Turkey
e-mail: furkankinaci@karabuk.edu.tr

G. Marques, A. González-Briones (eds.), *Internet of Things for Smart Environments*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-031-09729-4_7

Intelligent buildings are often part of a smart city project. Sensors can detect the deterioration of the building and can notify the authorities if necessary. Sensors can also be used to detect leaks in water mains and other piping systems, reduce costs, and help increase network efficiency. Also, smart city technology, in addition to job creation, energy efficiency, and sustainable use of space, increases the production and productivity of urban agriculture, including more fresh food for urban consumers.

While continuing to increase the population in cities, urban areas and infrastructure of these assets need to adapt to the increasing population by using them more efficiently. Smart city applications can enable these improvements, and cities can improve their operations and improve the quality of life of residents. From traffic lights to bus stops and even roads, all the elements that make up smart cities are interconnected, so they need to be protected from hackers. While cybersecurity techniques are designed to make it harder for hackers to work, those who run smart cities should always be on the alert. In this chapter, we will talk about what we need to do to prevent smart city software from being hacked by data thieves.

The process starts with smart grid and city applications, improving existing grids and making them smart. It enables to find and create new value from the existing infrastructure of networks and cities. This study aims to give general information about smart grids and cities and to explain the concept of systems. First of all, the concepts of smart city, smart grid, Internet of Things (IoT), and cybersecurity attacks in smart cities and networks are defined. The most common cyberattacks are given in smart grids and cities.

2 Smart Cities

Smart cities are human and nature-oriented and redesigned to provide maximum efficiency. In addition, smart cities have a framework that focuses on change, strategy, development and change, humans, and the environment in the management approach. For these reasons, smart cities are urban structures that have improved living standards by raising the living standards of society. These structures aim to use innovative and sustainable methods that reduce environmental problems. Moreover, it is based on creating new living spaces where the resources used are consumed efficiently and wisely. The smart city and grid, in other words, should provide human and social capital, sustainable economic support, and high lifetime value in classical and modern communication infrastructure. In addition, natural resources must be reasonably managed through competent management [1] (Fig. 1).

With the development of technology in recent years, smart grids have gained great importance by being widely adopted in many countries and cities. However, these new technologies have security disadvantages. Systems such as open data, education, IoT devices, smart agriculture, and smart energy form the basis of smart grids. However, it is very important to control and manage the structures in these smart grids (Fig. 2).

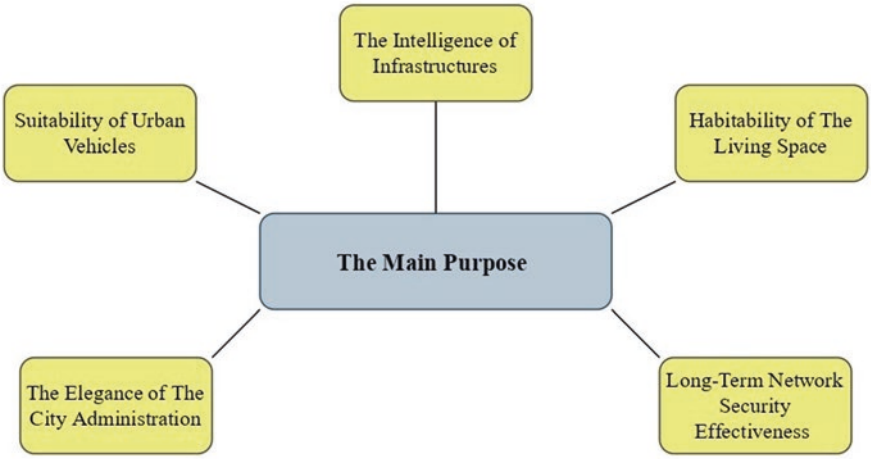

Fig. 1 The main purpose of developing and popularizing smart cities [2]

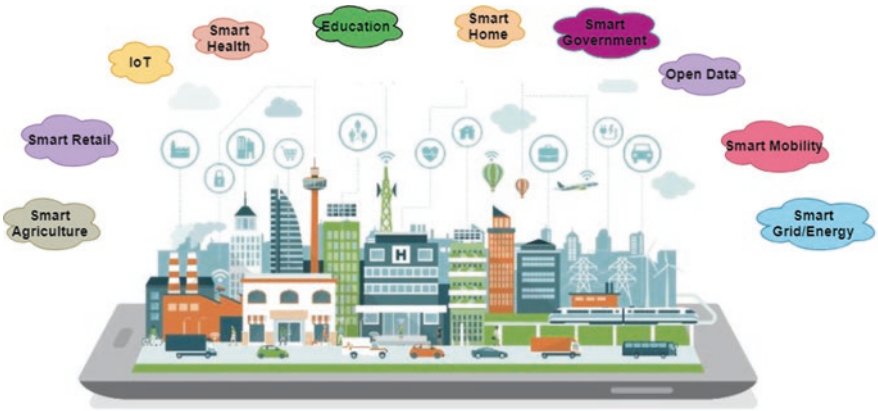

Fig. 2 Smart city overview [3]

The development of smart grids and cities and the prevention of security vulnerabilities that may arise in them is one of the most important issues. This study details the cybersecurity vulnerabilities of applications in smart grids and cities and the measures to be taken against them. These must necessarily require minimal precautions to be taken. It will be inevitable that there will be material and data losses in the face of measures not taken.

In addition to the emergence of new hardware and applications due to the changes in cyberattack methods and the development of technologies, an increase in security vulnerabilities is observed. In recent years, malware, distributed denial of service (DDoS), and advanced persistent threats have increased, especially among cyberattack methods. This study tried to determine the cyberattack methods that were detected and frequently used.

The continuity of all smart systems used in smart grids in terms of their operation and the availability of data, confidentiality, and integrity are the main components of information security. Furthermore, experienced personnel will be needed for the best management of these systems. The main components of success in the field of information security are people, technology, and the company. These are critical to the successful management of smart grids.

3 Smart Grids

Smart grids are an energy system that integrates the supply and consumption behavior of all market participants connected to them and aims to reduce loss and leakage, continuity in use, economic efficiency, and continuous data flow. Infrastructure services play an important role as an indispensable element of urban life. Control over these utilities became vital as the urban population grew. Population increases make it difficult to manage the use of information technology (IT) infrastructure, without software applications and made it impossible to manage [5].

ISO (which deals with the best management of physical assets by the International Organization for Standardization) argues that the management of infrastructure, as a whole should be systematic, risk-based, optimal and sustainable. Organization of systematic and interrelated movements manages assets and systems to achieve success and performance through a structure that is needed to control the risk and cost of organizational life cycle plans [4]. This requires intelligent networks for systematic monitoring.

The scope of the IEC 61850 (International Electrotechnical Commission) communication standard is based on the intelligent network protocol transformer. Otherwise, the same or different manufacturers use such non-parallel multiple protocols and interfaces [6]. The smart grid concept covers the use of information technology and communication systems, storage and consumption for the distribution and transmission system, and efficient, reliable supply of energy and materials through flexible management. In addition, the operating company has networks and wastewater systems designed for processes similar to information technology and electricity distribution in this sector, as well as processes for natural gas and water distribution [7].

In the classical network systems used today, problems such as power cuts, meter failures, low efficiency, and energy leaks can be detected by the subscribers by sending them to certain centers or by the work of distribution companies. In smart grids, on the other hand, these problems can be detected instantly and automatically resolved remotely without any interruption in service. Thanks to its real-time communication infrastructure, smart grids detect overloads, regulate energy flow directions, and contribute to preventing energy loss and leakage. At the same time, they manage the energy supply–demand balance and energy distribution, providing a fairer consumption price and more balanced resource use. Smart grids are more

resilient to natural disasters and offer energy systems to distribution companies and consumers, which are quickly reactivated in the case of any natural disaster.

The working principle of the smart grid is based on the principle of managing the entire energy production and consumption infrastructure from a single center. Each of the natural gas, electricity, water, and telecommunication systems is managed from a single center within itself, and infrastructure management is carried out by ensuring the efficient operation of the systems. From this point of view, smart grids are the integration of computer and network technology into today's networks through geographic information systems. They process and interpret the data intelligently and manage the needs according to the data analysis they receive [8].

Smart grids, an essential component for smart cities, play a major role in bringing reliability, availability, and efficiency into the era. Testing, technology improvements, consumer education, standards, legislation development, and information sharing between projects will be critical in the transition from conventional grid systems to smart grids (Fig. 3).

In particular, the electrical grid, natural gas distribution is also very critical in a smart grid. The necessity to supply natural gas sustainably and efficiently requires smart network systems. The gas distribution network is a system that supplies

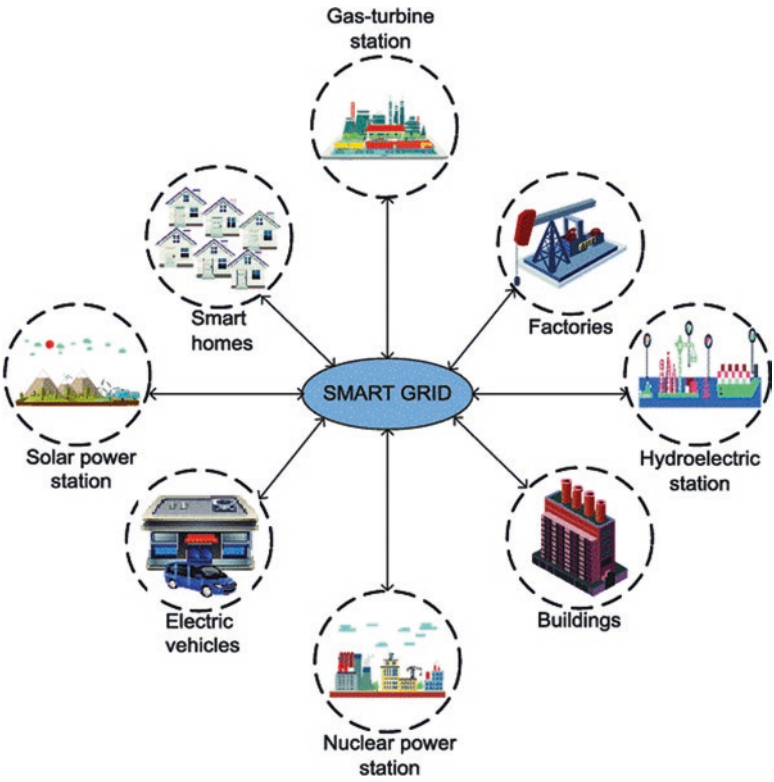

Fig. 3 Smart grid overview [7]

low-pressure gas from city gates to industrial, commercial, and residential buildings through pipelines of steel and polyethylene (PE) pipes at different pressure levels. Natural gas distribution networks consist of (i) Regulation and Metering Stations (RMS), (ii) mainline (steel) communication lines, (iii) regional stations and distribution lines, and (iv) service boxes and service lines. Due to critical safety issues in these systems, there can occur several cyberattacks. For instance, the set pressure and temperature levels of heating units can be altered remotely in the case of a cyberattack. This can damage the customer stations as well as the entire natural gas network [8].

An important element that effectively recognizes the full value of the smart grid process is its performance and capabilities to implement integrated, scalable, and interoperable engineering activities. In this new and more intelligent world, the customer's energy consumption of mobile devices, which can be watched via the Internet or a private home monitor, does the same things as meter data management systems. The counter also detects power surges and power outages, and the service will serve as a network sensor that can be used to connect or disconnect the remote connection [9].

The smart grid provides the integration of two-way communication between utilities and consumers through smart meters using Advanced Measurement Infrastructure (AMI). Thus, AMI is designed to provide real-time information on energy parameters such as prices, demand, capacity, and quality. If so, it would be surprising if the service company is properly navigating in terms of return on investment in an already deployed technology. Like all technological advances in energy efficiency, the smart grid has an important advantage to be noted and is highlighted in Fig. 4 [10].

Cybersecurity attacks are at the forefront of the difficulties experienced in smart grid deployment. Systems are protected against these attacks by using independent interfaces. It also provides energy efficiency and significant cost savings as an energy management tool called CISCO Energy Wise [11]. A smart grid system should have the following features.

Digitization means having a secure and fast digital platform for smart systems. Also, to be smart is to have good technology. Resilience, on the other hand, means that the developed intelligent systems can provide continuity without being affected by cyberattacks in the case of any abnormality. Personalization means tailoring customers to their needs. Finally, flexibility means that the smart grid is extensible, adaptable, and can work harmoniously within itself [12].

4 IoT in Smart Grids and Cities

In general, referring to the smart grid concept and the field of smart infrastructure, IoT applications in cities, transportation, industry, health, and other sectors are widely used. With the technologies that develop according to IoT application areas, its use has gained importance and provides significant convenience to human life.

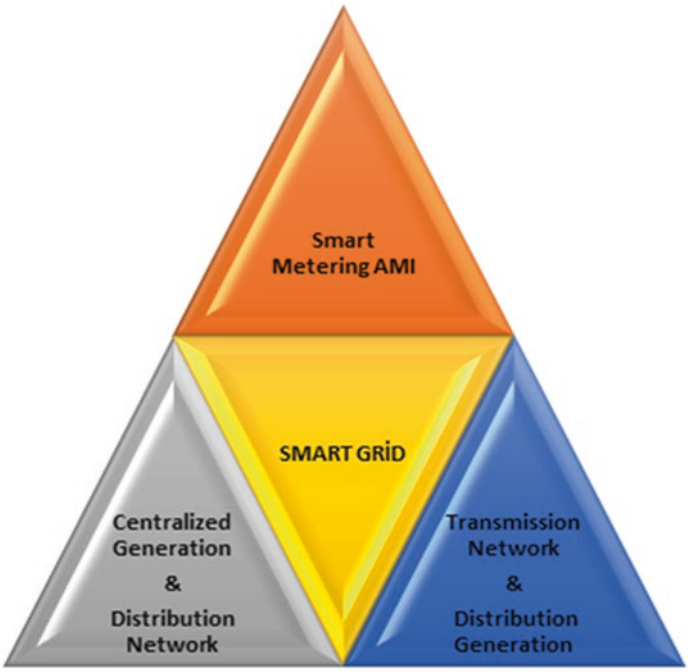

Fig. 4 The fundamental building block of the smart grid [10]

With the use of IoT devices, the security risks that will occur in the communication of data come to the fore. Studies in this area must be carried out and developments in this direction must be followed. All sectors and fields are given in detail in Fig. 5.

Smart cities use a combination of applications developed and interfaces created for the user to use devices, the IoT, and communication networks. The data collected by the communication of these devices with each other is stored in the cloud or on the server. With the development of these technologies, people's lives are getting easier. At the same time, the efficiency of both the public and private sectors is at the highest level.

5 Cybersecurity in Smart Grids and Cities

With advancing information technologies, cybersecurity threats have been an ever-increasing trend in recent years. From this point of view, it is clear that institutions strengthen their internal information security dynamics and place their strategic targets in the first place in terms of cybersecurity. In the field of cybersecurity, countries aim to protect computer networks in public and private sectors by following and adapting to international standards.

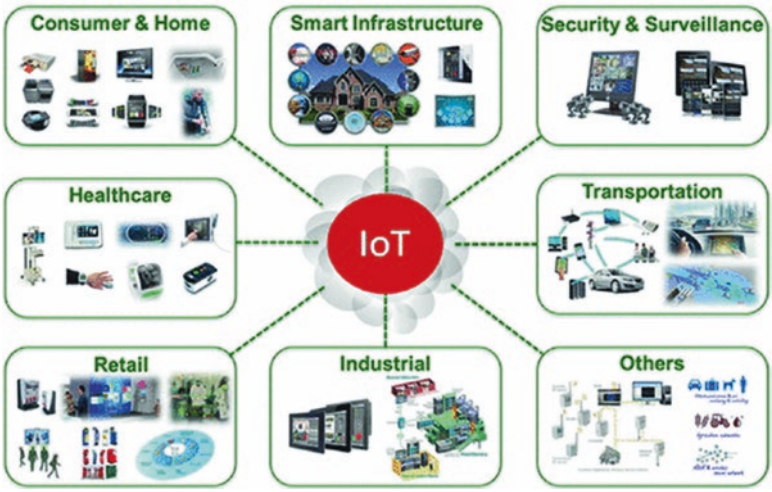

Fig. 5 Fields of application of IoT [13]

In terms of cybersecurity, no software application can guarantee companies a hundred percent security. For this reason, each institution should take its security measures, namely, technological, managerial, and education. Significant measures should be taken. For instance, employee information security awareness training should be done every year, the institution must have competent and senior experts in the field, and employment of cybersecurity experts to train the personnel, user, and system access logs should be kept: Cyber Incidents Response Team (CIRT), Cyber Security Center (CSC), Cyber Intelligence Center (CIC), and Software Security Testing Laboratory (Pentest Lab.) In order to respond immediately to cyber incidents, a Cyber Fusion Center (CFC) should be established, a corporate cybersecurity policy should be established, and the top management should support implementing them.

There are many sectors covered by smart grids and cities in Fig. 6. The exposure to cyberattacks against these sectors is shown as a percentage. Considering the impact of these cyberattacks, it is seen that the sector that has the highest risk and attacks with 26% is the energy sector [14].

5.1 Most Common Cyberattack Methods in Smart Grids and Cities

First of all, it is possible to define the subject threat in smart grids and cities, especially electricity, water, and natural gas. Looking at the smart city concept in general, it covers health, transportation, water supply, energy infrastructure, traffic management, waste management, and other services. A smart city can interoperate

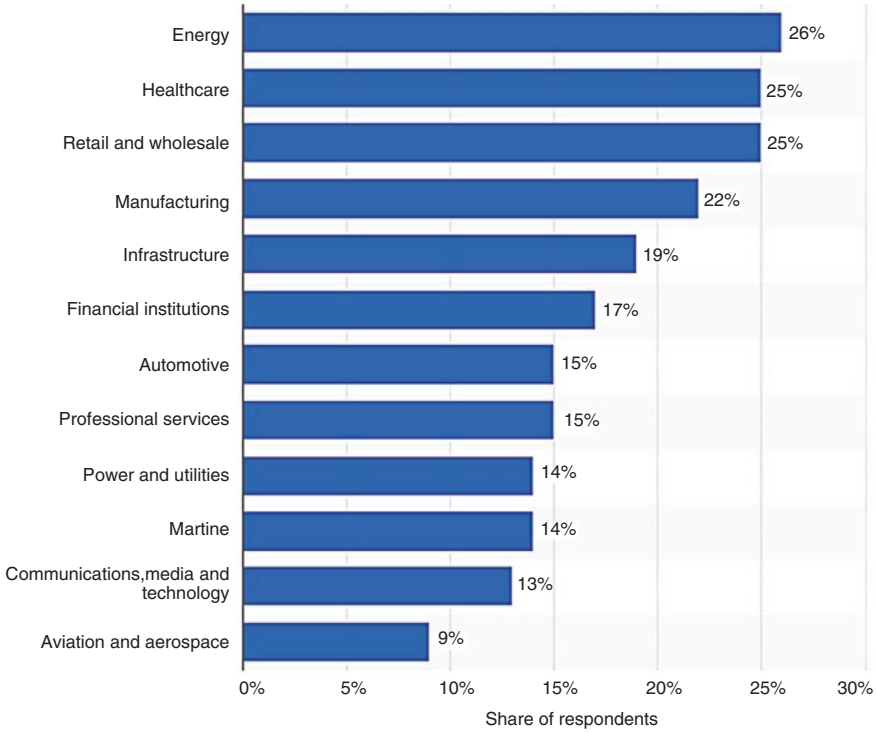

Fig. 6 Cyberattacks by sectors worldwide between 2016 and 2017 [14]

systems by establishing a mutual interaction between service providers and citizens. In this context, there are many concepts/methods such as cyber terrorism, cybercrime, cyber warfare, and cyber intelligence, each with different motivations, and different types of attacks. In this study, cyberattacks will be used for all of these methods. Cybersecurity violations intended to damage these structures are all functionally considered cyberattacks. In particular, this study investigates cyberattacks in smart grids and cities [15].

Cybersecurity aims to protect from external harmful applications, viruses infecting personal computers, advertisements from e-mails, and antivirus programs that need to be updated. In addition, when it comes to cybersecurity, one of the first things that come to mind is smart cities and grids. Because in terms of national security, loss of services in smart grids and cities can cause loss of life, large-scale economic damage, or weakening of national security. In particular, these systems are the most important assets to be protected in terms of cyberattacks. The main cyberattack methods are listed against smart grids and cities ([15–24]) (Fig. 7).

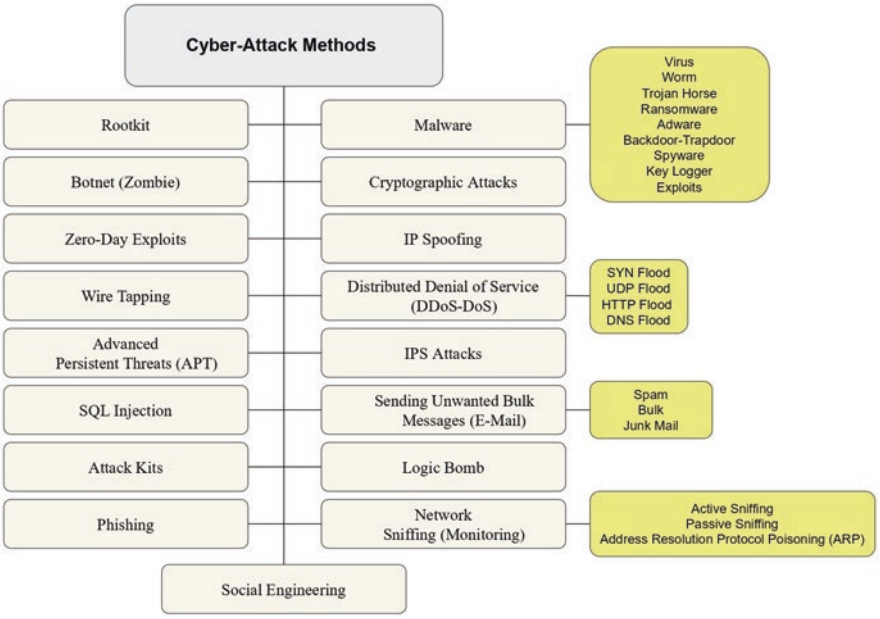

Fig. 7 The main cyberattack methods in smart cities and grids [2]

5.2 Measures Against Cyberattacks in Smart Grids and Cities

Some of the measures to be taken against cyberattacks in the smart networks and the main group of actions are shown in Fig. 8. The main groups given here have been determined based on the previous studies examined in the literature. In subsequent academic studies, these articles can be further expanded, and this chapter can motivate the studies to be carried out in this area.

The measures mentioned here must be given importance and attention in the critical infrastructures of state institutions and private companies. In addition, the mentioned cybersecurity measures motivated the creation of this article as a result of the studies and academic studies examined.

When building smart cities, they must take responsibility for understanding the systems they use and establish transparent relationships with the companies they support, from system construction to maintenance. In addition, every smart city should have trained cybersecurity emergency response teams to counter possible cyberattacks and their negative effects. Not knowing how to react to attacks can cause great confusion and stop normal city traffic. Therefore, serious cybersecurity strategies should be developed. But just as bacteria become resistant to antibiotics, threats can emerge with greater force to counter a change in strategy. Thus, each heightened security strategy often faces a new security threat. Therefore, security measures need to be constantly updated and monitored. For this reason, those who

Fig. 8 Overview of measures against cyberattacks smart grids and cities

want to be protected from attacks should always be one step ahead of hackers (Table 1).

Considering most of the identified attacks in general, they are among the most important issues that every institution should pay attention to. Because institutions and organizations do not want to be exposed to a cyber incident by experiencing a cyberattack, smart grids and cities can become more resistant to cyberattacks with technology.

Data that can be easily captured by taking advantage of vulnerabilities in smart systems such as face recognition over security cameras are used to threaten society. In particular, a system with a security vulnerability can be captured more easily than other systems. But, it is difficult to add a new system because all systems in smart cities work in an integrated manner. For this reason, the security strategy should be considered as a whole and at the same time, all security vulnerabilities should be minimized or even eliminated for each system. A security system is also required for the protection, monitoring, and control of smart grid and systems network traffic in cities. Firewalls aim to make systems more secure by preventing attackers from accessing data without authorization.

Table 1 Most common cyberattacks methods and measures [15–24]

	Most common cyberattacks methods	Most common measures
1	Distributed denial of service (DDoS-DoS) [14]	Determining cybersecurity performance targeted by top management and keeping performance records of all individuals.
	SYN flood	Determining the mode of action of the system to prevent unintentional disclosure of sensitive information related to the design, operations, and safety of the system.
	UDP flood	For third-party applications, patch management should be followed and a procedure or instruction should be prepared and followed up periodically.
	HTTP flood	The configuration controls and management of the software and hardware should be fully performed and monitored.
	DNS flood	It requires awareness to be resistant to cyber risks at all levels, from employees to senior management levels.
2	Botnet (zombie) [15]	The institutions should always keep risk management regulations against cyberattacks.
3	Zero-Day Exploits [16]	The institutions should always keep their inventory lists of information technologies against cyberattacks.
4	Advanced persistent threats (APT) [16]	Organizations should conduct personal access management on computers and servers.
5	Attack Kits [16]	Wired and wireless networks should be protected by strong authentication systems.
6	Sending unwanted bulk messages (E-mail) [17]	Institutions should perform event and log management.
	Spam	The institutions should conduct 24/7 emergency incidents and monitor management against cyberattacks.
	Bulk	Modem connections, local networks, connections with partners, internet, wireless networks, and satellite connections should be considered separately.
	Junk mail	To ensure a high level of cybersecurity, unnecessary network connections and unnecessary ports must be closed.
7	Network sniffing (monitoring) [18]	Institutions should use corporate networks and operational networks separately.
	Active sniffing	The security of SCADA systems used in smart grids and cities is mostly provided by the protection levels of the protocols produced specifically to communicate with the field vehicles and servers.
	Passive sniffing	Organizations should apply multiple access controls for user access to the internet and the applications in their network.
	Address resolution protocol poisoning (ARP)	Institutions should clearly define policies and procedures for cybersecurity and information security.
8	Malware [19]	Institutions should set up intervention teams against cyber incidents.
	Virus	The institutions should take the expert training of information security personnel and this training should be repeated periodically.

(continued)

Table 1 (continued)

	Most common cyberattacks methods	Most common measures
	Worm	Institutions should have penetration testing at regular intervals and keep their reports regularly.
	Trojan horse	In smart networks, standards on cybersecurity should be prepared and legally audited.
	Ransomware	Collaborative work should be done with universities, government, and private institutions on cybersecurity in smart grids and cities.
	Adware	Native and national software on cybersecurity should be developed in smart grids and the government should encourage this process.
	Backdoor-trapdoor	
	Spyware	
	Key logger	
	Exploits	
9	Rootkit [20]	
10	Cryptographic Attacks [21]	
11	IP Spoofing [20]	
12	Wire Tapping [22]	
13	IPS Attacks [21]	
14	SQL Injection [21]	
15	Logic Bomb [21]	
16	Phishing [21]	
17	Social Engineering [21]	

6 Conclusion

Cyber threats in smart grids and cities continue to grow day by day in an organized manner. Especially in terms of cyber incidents, the rate of attacks against the energy sector in the world is very high. Approximately 26% of cyberattacks worldwide are against the energy sector. Cyber threats and attacks have been detected in the energy sector, especially in natural gas, electricity, and water networks. Such attacks are expected to increase further in the coming years. However, the increase in the number of devices used in the concept of smart cities causes an increase in big data and wireless communication. The increase in the size of this data carries a high risk to ensure data security in terms of cyberattacks. Necessary security measures should be taken to reduce the risks of these cyberattacks, and cities should be made livable. Precautions to be taken should be preferred in terms of cybersecurity and newly developed hybrid prevention methods. Especially artificial intelligence and machine learning applications developed against new attack dimensions should be preferred.

Smart city leaders should be alerted, stating that many cities are not planning cyberattacks, although cities have plans for natural disasters such as floods and earthquakes as a result of research done by security research companies. Since the

target of cyberattacks is a human-centered system, it is necessary to consider that they can lead to major events and to develop reasonable strategies against cyberattacks. As technologies improve in smart grids and cities, cyberattacks and vulnerabilities are also increasing. Therefore, in this study, cyber threat methods and solution suggestions are discussed in detail. It is shown that cybersecurity and information security are in every aspect of our lives, and it is recommended that institutions pay attention to the solutions given here. For this reason, the communication of the systems must be secure, the use of secure models, the protection of data, etc. In cases, the safety precautions given in this study should be taken into consideration. Finally, 17 cyberattacks were detected in smart cities, grids, and IoT systems used. However, measures that can be taken in these systems against cyberattacks have been given. Along with these measures, all stakeholders should cooperate among themselves and make suggestions for the measures to be taken against these cyberattacks. All countries should develop secure maturity models against cyberattacks for smart cities and grids. Moreover, investments should be made in this field, and joint work should be carried out by leading the way on these issues.

References

1. T. Nam, T.A. Pardo, Conceptualizing smart city with dimensions of technology, people, and institutions, in *Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times*, (ACM, 2011), pp. 282–291
2. ISO, https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/smart_cities_report-jtc1.pdf. Accessed date:25.05.2021
3. C. Özarpa, M.A. Aydın, İ. Avcı, *International Security Standards for Critical Oil, Gas, and Electricity Infrastructures in Smart Cities: A Survey Study, SCA2020* (Karabuk, Turkey, 2020)
4. J.R. Minnaar, W. Basson, P.J. Vlok, Quantitative methods required for implementing pas 55 or the ISO 55000 series for asset management. South Afr. J. Indus. Eng. **24**(3), 98–111 (2013)
5. Baigent, D., Adamiak, M. and Mackiewicz, R., IEC 61850 Communication Networks and Systems in Substations: An Overview for Users, (2004)
6. M. Dönmez, Smart grids, and integration. BTC Bus. Technol. (2013)
7. F. Feroze, N. Javaid, Towards Enhancing Demand Side Management Using Evolutionary Techniques in Smart 17 Grid. (2017). https://doi.org/10.13140/RG.2.2.34456.49920
8. H. Bıyıkcı, C. Özarpa, Smart grid maturity analysis and roadmap for natural gas networks in metropolitan cities: A case study for İstanbul/Turkey. IGRC Rio **2017** (2018)
9. S. Borlase, *Smart Grids: Infrastructure, Technology, and Solutions* (CRC Press, 2016)
10. S. Goel, A. Jindal, Evolving cyber security challenges to the smart grid landscape, international journal of advance research, ideas and innovations in technology (2017)
11. Cisco Energy Optimization Service., http://www.cisco.com/web/strategy/docs/energy/energy_optimization_service_aag.pdf. Retrieved from CISCO. Accessed date: 21.01.2019
12. S. Iyer, *2011, Cyber Security for Smart Grid, Cryptography, and Privacy* (Int. J. Digit. Multimed. Broadcast., USA, 2011)
13. S. Tanwar, S. Tyagi, S. Kumar, *The Role of Internet of Things and Smart Grid for the Development of a Smart City, Intelligent Communication and Computational Technologies*, vol 19 (Springer, Singapore, 2018), pp. 23–33. https://doi.org/10.1007/978-981-10-5523-2_3
14. Statista, https://www.statista.com/statistics/784590/cyber-attacks-on-industriesworldwide-2017. Accessed date: 21.01.2019

15. C. Özarpa, M.A. Aydın, İ. Avcı, Chapter 89: International security standards for critical oil, gas, and electricity infrastructures in smart cities: A survey study, in *Innovations in Smart Cities Applications*, vol. 4, (Springer, 2021)
16. M. Yıldız, *Cybercrime and Institution Security, Maritime Specialization Thesis* (T.C. Ministry of Transportation, Maritime Affairs and Communication, 2014)
17. S. Samtani et al., *Identifying SCADA Vulnerabilities Using Passive and Active Vulnerability Assessment Techniques, Management Information Systems*., https://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=7739307 (The University of Arizona Tucson, 2016)
18. Ö. Alp, *Cyber Security in Smart Grids, Master Thesis* (Institute of Social Sciences, Istanbul Bilgi University, 2018)
19. A. Ashok et al., Cyber-physical security of wide-area monitoring, protection and control in a smart grid environment. J. Adv. Res., Cairo University (2014)
20. Drias, Z., et al., Analysis of Cyber Security for Industrial Control Systems, International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), (2015)
21. S. Saini et al., Modelling for improved cyber security in smart distribution system. Int. J. Future Revol. Comput. Sci. Commun. Eng. **4**(2), 56–59 (2018)
22. A. Anwar, A.N. Mahmood, *Cybersecurity of Smart Grid Infrastructure, the State of the Art in Intrusion Prevention and Detection* (CRC Press, Taylor & Francis Group, 2014), pp. 449–472
23. L.A. Maglaras et al., Cybersecurity of critical infrastructures. ICT Express **4**(1), 42–45 (2018)
24. M. Koca, İ. Avcı, *A Survey of Optical Networks Vulnerabilities and Solutions (IATS'17, 8th International Advanced Technologies Symposium), October 19–22* (Fırat University, Elazıg, Turkey, 2017)