

Open network structure and smart network to sharing cybersecurity within the 5G network

Aseel K. Ahmed¹, Abbas Akram Khorsheed²

¹Department of Computer Science, Al Rafidain University College, Baghdad, Iraq

²Department of Computer Science, college of science, Mustansiriyah University, Baghdad, Iraq

Article Info

Article history:

Received Mar 26, 2022

Revised May 14, 2022

Accepted Jun 8, 2022

Keywords:

5G

Cyber security

IoT

Machine learning

Smart network

ABSTRACT

The next-generation communication system incorporates information technology (IT) and operations technology (OT) for generating, delivering, and collecting, and obtaining communication power. We plan to include a brief outline of internet of thing (IoT) communication and its context, along with security concerns that arise for IoT data on the network and some methods for detecting and avoiding cyber security threats. With the rise of the 5G networks, we introduce the smart network's emergent technology and its opportunities and more cybersecurity issues. Whereas, finding or responding to a power outage is an essential part of system security That is why we will discuss the innumerable advantages of 5G networks and we must also cover the inevitable problems that we will encounter in power delivery. The use of smart IoT communication technologies is becoming more common in the energy sector, particularly with the network (5G). The smart network and energy flow integration Real-time data on generation, electricity distribution, and energy consumption is measured using computers and cutting-edge technologies. This information aids utility companies in managing electricity supply and demand, as well as price. While enhanced communication and information technologies are unquestionably crucial to the smart network.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Abbas Akram Khorsheed

Department of Computer Science, College of science, Mustansiriyah University

Baghdad, Iraq

Email: abbasarab2000@uomustansiriyah.edu.iq

1. INTRODUCTION

The use of internet of thing (IoT) increased in the new millennium. However, IoT has its origins in 'telemetry', which dates to the middle of the 19th century. Some notable developments in IoT [1] are depicted in Figure 1. Transmission, data processing, and tracking in the original form of telemetry, the first instance of live data exchange dates to 1850 when the information was broadcast in the middle of the army headquarters and the Tsar's Winter Palace. Further progress was made in telemetric data in 1910 when Edison [2] used land phone to relay running data for power plants and loads on the city. Telemetry has grown over the last century and is used in surgery, aerospace communications, climatology and conducting retail transactions these days. Such notable uses of data telemetry include smart homes [3]. A new business model emerged around the basis of telemetry in the 1990s, called IoT.

Although traditional telemetry was almost entirely limited to radio frequency signals, I transmitted and measured newer technology such as networks, mobile devices, sensors, and the Internet. Due to the progress of this decade, IoT communications has come to mean the IoT. The Internet of Things is a means of gathering data from sensors and intelligent electronic devices (IEDs) [4]. These intelligent appliances are

mounted at critical locations and transmitted to and received by gateways on the IoT network. IoT is employed in many sectors, including transportation and healthcare. Smart IoT communications technology increasingly appears in the energy field, specifically with the network (5G). Utility companies should take advantage of two-way IoT contact. Energy flow integration with the smart network computers and sophisticated technology measure real-time data on generation, power distribution, and power consumption [5], [6]. This data aids in utility operators' ability to control electricity supplies and demand as well as pricing. While these advanced communications and information systems are undoubtedly important to the smart network, their other disadvantages are too large to overlook. These include raising the vulnerability of the power network to malicious attacks [7]. Simultaneously, the country's power supply network must be protected from cyber-attack because it relies on the underlying technology.

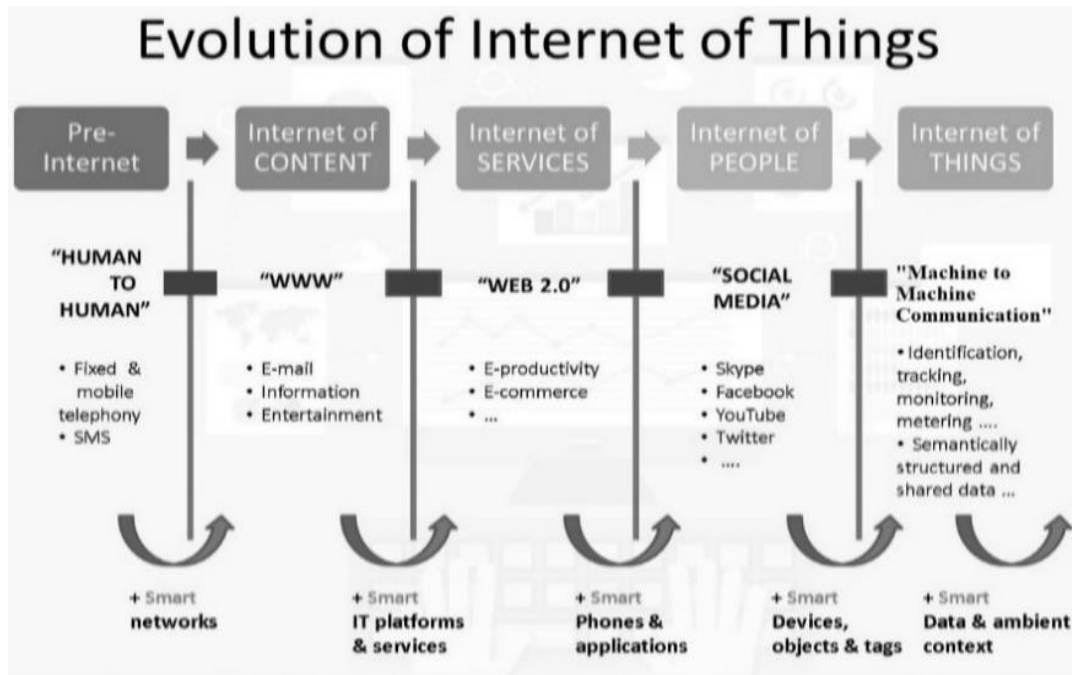


Figure 1. Evolution of IoT

2. INTERNET OF THING COMMUNICATION (IOT) ARCHITECTURE

Data from a computer to another device over a wireless network or wired network besides via a gateway, that can be evaluated, compiled, and the results used for informed choice-making and utilized to different services, is referred to as IoT communication [8]. IoT architecture [9], and this model considers three major domains: (i) IoT application field connects IoT gateways to intelligent IoT applications [10], (ii) IoT network field connects IoT applications to gateways and (iii) IoT application domain is a middleware framework that allows IoT data being used in business software [11].

A device may be as simple as a temperature sensor or as complicated as a complex as a machine. Data is extracted from an unavailable information collection device to a request or automatically to start the IoT communication. IoT architecture is depicted in Figure 2 as a basic visual representation. After the data is collected from the remote unit, it is sent to the IoT application for processing through a wired network or wireless network, cables, or communication satellites. From these results, valuable information is derived, which is then used by various business local services. While land phone [12] can use if one is available, and cables can be useful for tracking equipment in remote areas, in today's increasingly mobile world, cellular networks provide the safest, most cost-effective means of IoT communication. As the IoT ecosystem develops and more business leaders enter the IoT bandwagon, there is a raising need for standardization in this emerging region. IEEE [13], 3GPP [14], and ETSI [15] are only a few of the wireless standard organizations looking at the impact of IoT devices being used more commonly on existing networks.

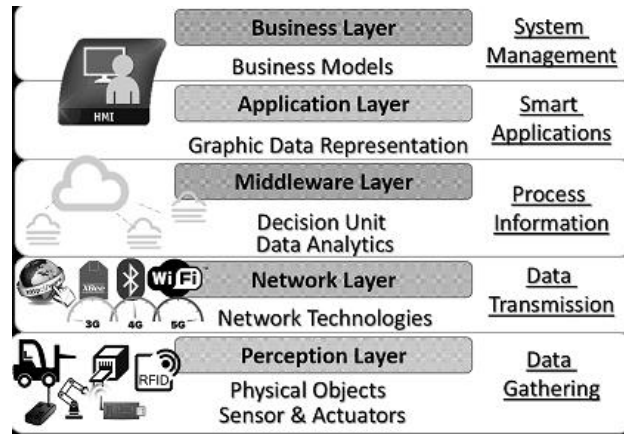


Figure 2. IoT architecture

3. SMART NETWORK CONCEPTUAL MODEL

The smart network is a common IoT communications application that combines OT (computers, power delivery, networks) and IT (computers, networks for business processes) into a next-generation electrical power system. The supervisory control and data acquisition (SCADA) architecture [16] bases information from various sources on, lets utilities to handle resources, and sustains communication bandwidth. Utilities use the IT platform to run their company and administrative processes. The enhanced use of networks and digital technologies in this integrated network infrastructure allows for decentralized, automated, consumer-interactive, but often environmentally friendly distribution, generation, and electrical energy consumption. The 5G is a more powerful energy distribution system in a nutshell [17].

The smart network conceptual model of NIST [18] divides the smart network into seven distinct domains: bulk operations, distribution, generation, customers, transmission, markets, and service providers. Storage, electricity generation, and distribution, as well as bidirectional flow, are among the four domains. Managing resources and supplying information to power providers is the final duty of the last three classifications in this hierarchy. Figure 3 shows how two domains are interconnected to make a complex and intelligent power network with a two-way data flow. For bulk generation, electricity comes from centralized and traditional sources like solar and wind and distributed sources like hydro and geothermal, as well as non-renewable coal and gas. With IoT devices like smart meters, consumers (domestic, private, and industrial) are all supplied with electricity. AMI [19] promotes the meter contact between customers and utilities. Incorporates can return power the power network, power systems use a dynamic two-way network. Every 2 to 5 seconds, the SCADA system maintains real-time data and remotely manages, monitors, and collects data from distributed substations. This expertise is then guiding the utility companies to ensure a constant supply of electricity.

Information obtained from customers, such as energy usage data, is processed further in the operations domain and provides essential business intelligence. A more effective power network has resulted from integrating the AMI with conventional distribution networks. Service providers by third-party, such as web portals, function in the service provider domain, allowing end-users to share information with their utility business and better control their energy usage. Utility companies worldwide have started analyzing, preparing, and implementing smart network technology by introducing AMI and other automated communication technologies since the first smart network was publicly implemented in the 1990s. The tool enables the utility to track and evaluate their allocation networks plus enabling them to provide consumers with an accessible, more reliable as well as effective control systems whether on the smart network or the micro-Network. The following are the data sources created by this intelligent smart network: (i) Smart meters-AMI, (ii) Automated distribution network, (iii) Data from third parties (information to networks) [20] and (iv) Asset administration (Firmware updates for the smart device or OS).

The "smart meter" is an important part of 5G. The metering application one of the IoT business applications that utilities employ to fully realize the smart network's potential. The smart meter is a system that stores data about electricity use and offers insight into trends in electricity use. Smart meter data is now obtained at 5-minute intervals rather than the weekly readings of the past [21]. As shown in Figure 4, this is just one factor contributing to the exponential growth of smart network data. Using this image, we are better able to understand how much data the utility must go through to fully appreciate smart network's capabilities [22].

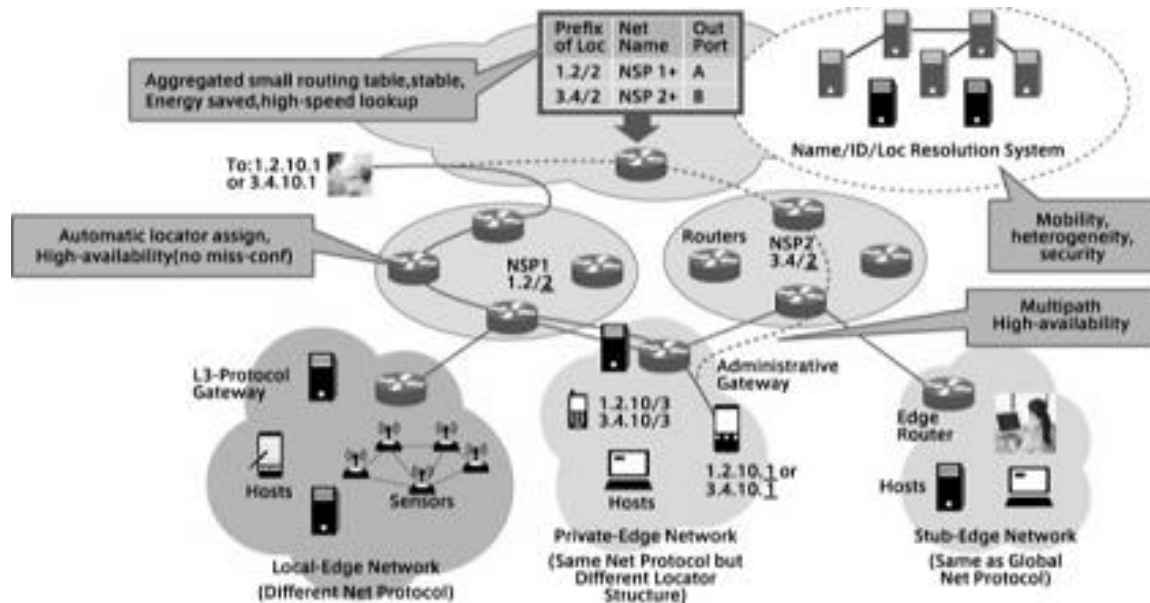


Figure 3. Smart network model

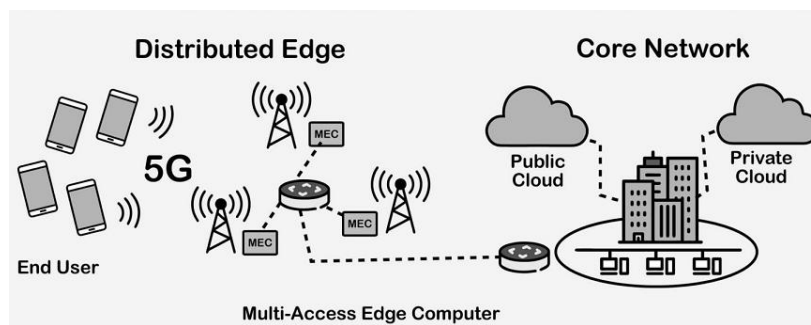


Figure 4. Sort of distributed "Mini-data centers"

4. SECURING THE SMART NETWORK

Although the United States attack in August 2003 did not originate in the cyber world, we have seen the impacts of that first attack in this country. In contrast to the legacy network, the smart network is more complex [23]. The very components that make it intelligent are some of which are shown in Figure 5. By strengthening cybersecurity [24], boosting network performance, and assuring consumer data protection reliability while limiting costs is a fine line that service providers will come up with to walk if they want to realize the complete ability of the smart network. Intelligent network such as IEDs, malware proliferation, SCADA, induced application denial of service, malicious network access, and manipulated data include purposes of connected devices. Customer privacy and data security, and protection are also played important considerations. As utilities extend their smart network activities, data security issues must be addressed to create customers with an efficient yet dependable power distribution system, and security controls must be implemented appropriately. These security controls must work for both the OT and IT platforms. The computing and communications networks OT/IT are increasingly overlapped as network deployment takes place worldwide, and corporations gather ever-larger quantities of network data [25]. Utilities will be able to discover cases of energy theft, cyber-related crime and forecast possible malicious outages using large data analytics.

Utility corporations are also occupied with organizations, and the Institute of Electrical and Electronics Engineers to develop a smart network security framework that includes privacy, authentication, meter data encryption, and data access security, among other features.



Figure 5. IoT 5G cybersecurity cycle

5. DATA MANAGEMENT ANALYTICS FOR SMART NETWORK

The amount of data generated by 5G will have to be captured, stored and managed to further improve utilities’ operations as well as improving their customer and stakeholder management that will be required utilities may employ the following network analysis software to assist in this investigation: (i) Computational modelling, (ii) Empirical modelling, (iv) Metric modelling and (iv) Other resources like wind, solar, and biomass resources

According to the cybersecurity market Figure 6, budgets will increase for smart network data analytics by \$38 billion, with Asia being the main driver of that expansion. Data of this volume and variety is now referred to as "big data." As opposed to the old, legacy electrical grid, the data generation model allows utilities to collect granular customer data. All market participants benefit from this information, including power suppliers and customers, who have a deeper understanding of energy trends and supply and demand. We will use the data-gathering capabilities of smart meters, sensor captures, and electric vehicles to fully utilize their ability to use them efficiently. If he lacks relevant statistical models, the Network Manager will not determine activity in the produced IoT data [26].

With smart network optimization, these analytical models can help utilities. Conventional and cloud-based data mining methods for processing and making intelligent decisions have yet to be applied extensively. Analytical tools can help work with data produced by the efficient network to perform at their peak. However, but also, data-mining techniques may be used to deter potential cyber-attacks in the future. The implementation of IoT protection for protecting the smart network is crucial. For example, the credibility of smart meters may be jeopardized if appropriate security measures are not implemented. Prominent technology firms, including ABB [27], NIKSUN [28], IBM [29], and GE [30], have seen the worldwide customer requirement for advanced network information security solutions and are making a name for themselves in the field. Each supplier is developing its technology to assist the smart network's various components in turning data into data that utilities can use to meet their requirements.

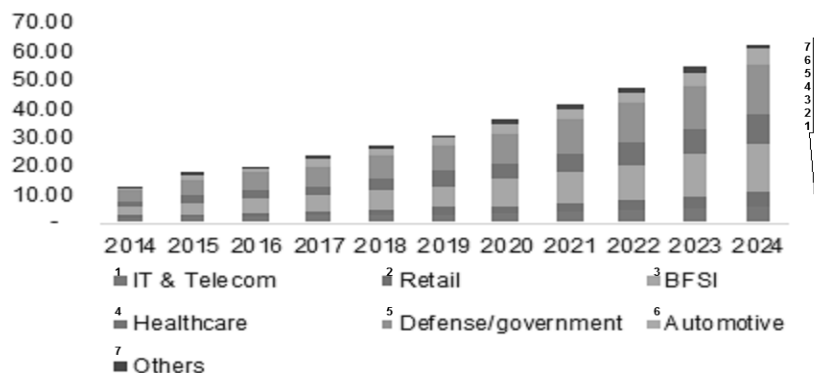


Figure 6. Cybersecurity market

It is worth remembering that the same techniques used to protect 5G also serve personal and illegal interests. Criminal activity can be identified by statistical models, such as energy use patterns, and accounted for in this way. Table 1 describes some of the instruments that are available from these vendors [31].

Table 1. IoT data analytics tools in the market

IoT analytics tools	Briefly description
AWS IoT analytics	A managed service such as AWS IoT automates the most challenging analysis tasks required to deal with IoT data. It is easy to use and construct analytics on edge for IoT deployments. Device metadata, including device type and location, can be stored in AWS IoT Analytics. IoT data analytics is handled and can handle petabytes of data. Such that you don't have to think about either the hardware or the infrastructure. Using AWS IoT Analytics, users can perform queries on real-time IoT data, cache and store data, and automate analyses using machine learning. It is possible to use a pay-as-as-you-you-go pricing model to experiment with AWS IoT, which charges you based on the amount of use.
Cisco data analytics	Cisco's data analytics platform makes it easy to use analytics across the entire network, both in the cloud and on-premises. Cisco provides companies with resources and tools for analysis of IoT data collection. Cisco IOx APIs allow businesses to streamline the data for enterprise applications to enhance operational performance. This Cisco has offered the following services: Real-time analytics, the cloud, and integrated analytics to security
IBM watson IoT platform	Analytics is a component of IBM's Internet of Things platform. Using this method, users can analyze and visualize IoT data and perform complicated analytics on the IoT data. Cognitive computing helps organizations extract useful knowledge from various kinds of data by processing structured and unstructured information. The organization can use Watson to incorporate natural linguistic processing, machine learning, and image and text analytics, as well as analytics functions like image and text analytics.
Microsoft azure stream analytics	To integrate with the microsoft azure stream analytics, you just need to have azure IoT hub and azure suite. azure stream analytics provides enterprises with the ability to implement real-time analytics and allows them to exploit their data's full potential. However, they also make building dashboards simple with power BI, as well as the resulting insight easy to find.
Oracle stream analytics and oracle edge analytics	Oracle has integrated IoT analytics with its oracle stream and oracle edge analytics offerings. Oracle's solutions allow you to create analytic applications that can read various sensors and devices and provide useful information. The capability of processing and analyzing large amounts of streaming data is built into stream analytics and edge analytics.
SAP analytics cloud	SAP analytics cloud can incorporate the internet of things (IoT) data and work with analytical applications to gain a deeper understanding of it. The SAP analytics cloud drives predictive analytics and machine learning. Also, SAP has a streaming lite component, a remote project deployment optimized for projects to the "to-the-edge" instances. If you wish to deploy projects on external gateway devices, you do not need to use streaming lite.

6. 5G GENERATIONS NETWORKS

The 'G' stands for the Generation of Cellular, which would benefit from ultra-reliable and low-latency communications. Previous generations of networks and cybersecurity Figure 7 have been characterized by their data transmission rates and their encoding methods. Table 2 lists some of the technologies on which the earlier networks are built on [32]. With regards to wireless networks, 5G network sectors are employed as well. They transmit information using orthogonal frequency division multiplexing. It supports high data capacity, has a strong rejection of multipath interference, and is capable of extremely high spectral performance.

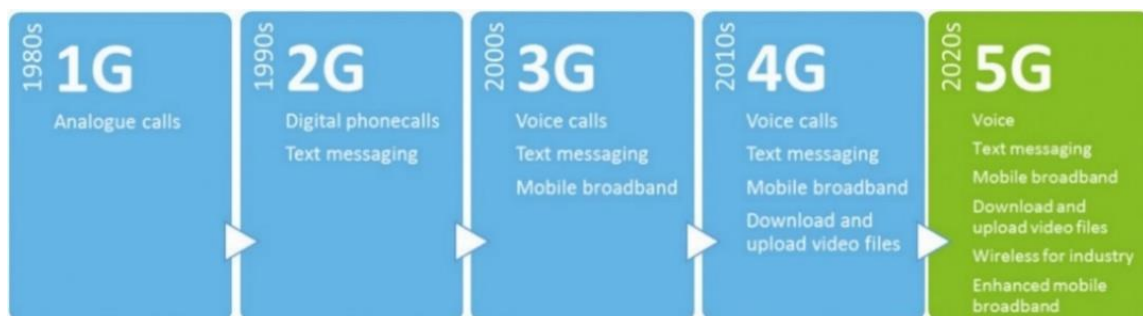


Figure 7. 5G generations networks

Table 2. History of wireless technologies generations

Generation	Speed	Technology	Period	Features
It is the began-1G	14.4 Kbps	NMT, AMPS, TACS	1970 to 1980	Wireless is used for voice only.
The cultural revolution-2G	9.6/14.4 Kbps	CDMA, TDMA	1990 to 2000	Multiplexing channels enables multiple users to exist on a single communication route. People use their cellular phones for both voice and data in the 2000s.
2.5G	171.2 Kbps 20-40 Kbps	GPRS	2001 to 2004	As the Internet has become more popular, data is more important Two and a 2.5G multimedia platforms and video streaming continue to show growth Support for web browsing is currently offered only via selected web browsers, and most phone models do not have yet installed the necessary software to enable it.
The 'packet-switching' revolution-3G	3.1 Mbps 500-700 Kbps	CDMA 200 (1xRTT, EVDO) UMTS, EDGE	2004 to 2005	In addition to Multimedia support, 3G provides for media streaming is becoming more common. portability and basic accessibility across various device types are built into 3G. televisions, mobile phones, PDAs, computers, etc.
3.5G	14.4 Mbps 1-3 Mbps	HSPA	2006 to 2010	3.5G provides higher bandwidth and faster speeds to support greater data demands for the users
The streaming era-4G	100-300 Mbps. 3-5 Mbps 100 Mbps (Wi-Fi)	WiMax, LTE, Wi-Fi	2010 to 2020	updates with increased to keep up with the and demand for various data services 4G HD support has been added Up-to-date mobile phones would have high-definition cameras. It gets chilly at night. You would have much more portability with 4G. It is just a matter of time before it becomes a reality. 5G is not yet in use.
IoT era-5G	Probably gigabits	Not yet	Lunched 2020 to2021	This will be greatly beneficial to the consumer public when it becomes affordable. In addition, it would maximize usable bandwidth

It is known as new radio" (NR) [33]. The 3rd Generation Partnership Project created the 5G NR standard (3GPP). Figure 8 illustrates some threats of the use cases for 5G networks. Due to millimeter waves and faster frequency bands, 5G networks are more suitable for building and internet of thing (IoT and smart device) connectivity.



Figure 8. Threats landscape of 5G

7. 5G NETWORKS AND SMART NETWORK

The 5G network will support machine type communication, SCADA applications as well as the huge amounts of data generated by the supervisory data acquisition and fault localization furthermore V2 RES integration. A collection of 5G networks would be used for continuous availability and fault localization, as well as self-healing. End-user technology will enjoy stronger 5G capability and better privacy controls. A 5G network must support the following machine communication requirements must be considered: (i) Ultra-high bandwidth is available on-demand and (ii) exceptional communication that provides immediate input with an extremely high level of trust.

In earlier versions of this document, electric power is delivered to residential or business customers who are part of the distributed generation network using AMI. The 5G network would make it possible for the consumer to communicate with their energy supplier and real-time and automated smart devices for system auto-configuration. 5G networks can provide network stability for distributed generation and delivery networks and increase the quality of experience (QoE) [34] for consumers. They cannot easily store energy and meet the demand for the most effective energy delivery. 5G networks can also support quicker response times from the network operations centers and smart meters.

8. SMART NETWORK AND THE CYBER SECURITY ISSUES IN 5G NETWORKS

Although 5G technology has its benefits, it also makes 5G networks more vulnerable to attacks from the Internet, as shown in Figure 9. As with the AMI deployment, the risk for blackouts and financial losses rises for the utility increases. a robust power supply is a critical part of a computer system's information protection and vulnerability to malicious attacks. Either finding or responding to a power supply failure is an essential part of system security (i.e., confidentiality, integrity, and availability).

5G uses message authentication, message integrity, and encryption. Problems mostly associated with corrupt data must be handled using low network latency. The protection must also include the risk of loss of contact plus unapproved login to the devices and network, the occurrence of network attacks distributed denial-of-service (DDoS) add to all MITM and signal scrambling must be addressed. Protection applications are required to have a low latency of less than 10ms when providing high reliability. If it does not, a correction can be applied in only one millisecond to ensure at least 99.99% of the messages arrive on time. Additionally, successful security applications will include time synchronization between substations and connected devices to operate efficiently in 5G.

Traditional and distributed energy resources (DER) [35] sources produce power-level balancing, voltage control, and frequency regulation. Applications would have the same security specifications as the same degree as defense applications but shall also meet the constraints in terms of latency (~ 200ms), performance (~ 99.9%), and time synchronization (i. = 99.9%).

Problems can be measured using current and voltage test tools for 5G networks these isobaric (sine wave) PMUs can be used for wide-region (stagnant) wave measurements of the large size and phase angle. Data transmission occurs often, but the overall standards are stricter (e.g., 500–1000ms latency, or less) in network monitoring. Consequently, essential technologies are concerned with synchronization and security in 5G networks. The large-scale rollout of the 5G smart meter deployment implies improved protection and compliance with privacy laws.



Figure 9. 5G network security challenges

9. CONCLUSION

This study has briefly covered the growth of IoT communication, the smart Network model abstract, and their implementation in the smart network, as well as showing the value of smart Network data analytics. In this age of 5G network rollout, we briefly describe wireless technologies' evolution before detailing 5G networks. On top of the innumerable advantages of 5G networks, we must also cover the unavoidable issues that we will face in power delivery.

ACKNOWLEDGEMENTS

The Authors would like to thank Mustansiriyah University (<https://uomustansiriyah.edu.iq>) Baghdad -Iraq for its support in the present work.




REFERENCES

- [1] A. Dash, C. Hegde, and S. Pal, "Ransomware auto-detection in IoT devices using machine learning," *Ransomware Auto-Detection In IoT Devices Using Machine Learning*, 2018.
- [2] M. OWA, "Thomas Edison," *Lecture 38: Nucleation and Spinodal Decomposition*, 2016.
- [3] B. Ravinder and K. S. Raju, "An application of internet of things for smart home," in *2016 National Conference on Computer Security, Image Processing, Graphics, Mobility and Analytics (NCCSIGMA)*, 2016, doi: 10.22161/ijaers/si.28.
- [4] T. H. Meen, W. Zhao, and C. F. Yang, "Special issue on intelligent electronic devices," *Electronics*, vol. 9, no. 4, 2020, doi: 10.3390/electronics9040645.
- [5] M. Kalinin and P. Zegzhda, "AI-based security for the smart networks," in *2020 13th International Conference on Security of Information and Networks*, 2020, pp. 1–4. doi: 10.1145/3433174.3433593.
- [6] T. H. Kim and S. J. Kim, "A study on facility maintenance information composition and sophisticated technology utilization measures," in *2015 2nd International Conference on Computer Science, Computer Engineering, and Social Media, CSCESM 2015*, 2015, pp. 23–26. doi: 10.1109/CSCESM.2015.7331822.
- [7] J. Jiang, S. Wen, B. Liu, S. Yu, Y. Xiang, and W. Zhou, *Malicious attack propagation and source identification*, vol. 73. 2019. doi: 10.1007/978-3-030-02179-5_1.
- [8] C. Bodei, S. Chessa, and L. Galletta, "Measuring security in IoT communications," *Theor. Comput. Sci.*, vol. 764, pp. 100–124, 2019, doi: 10.1016/j.tcs.2018.12.002.
- [9] F. M. Farahani, "IoT architecture models." 2020.
- [10] S. Goel and P. R. Kumar, "Fog, edge, and pervasive computing in intelligent IoT driven applications," in *Fog, Edge, and Pervasive Computing in Intelligent IoT Driven Applications*, 2020. doi: 10.1002/9781119670087.
- [11] B. Katole, V. Suresh, G. Gosavi, A. Kudale, G. Thakare, G. Yendargaye, and C. P. Kumar, "The integrated middleware framework for heterogeneous internet of things (IoT)," *International Journal of Engineering and Innovative Technology (IJEIT)*, vol. 4, no. 7, pp. 173–177, Jan. 2015.
- [12] N. Economides, "Quantifying the benefits of entry into local phone service," *SSRN Electron. J.*, 2012, doi: 10.2139/ssrn.2118271.
- [13] M. G. Perez, A. H. Celdran, F. Ippoliti, P. G. Giardina, and G. Bernini, "Dynamic reconfiguration in 5G mobile networks to proactively detect and mitigate botnets," *IEEE Internet Computing*, vol. 21, no. 5, pp. 28-3, 2017, doi: 10.1109/MIC.2017.3481345.
- [14] O. I. Oshin and A. A. Atayero, "3GPP LTE: An overview," in *Proceedings of the World Congress on Engineering*, 2015.
- [15] T. Kovacicova and S. P. Segec, "NGN standards activities in ETSI," *International Conference on Networking*, 2007, p. 76, doi: 10.1109/ICN.2007.60.
- [16] E. Wright, D. Reynnders, and S. Mackay, "Practical telecommunications and wireless communications," *For Business and Industry, Book*, 2004, doi: 10.1016/B978-0-7506-6271-0.X5000-8..
- [17] "23501-G20_5G_Architecture." www.viavisolutions.com. <https://www.viavisolutions.com/en-us/5g-architecture> (accessed Apr. 20, 2022).
- [18] S. Cockcroft, "What is the NIST framework?," *Itnow*, vol. 62, no. 4, pp. 48–49, 2020, doi: 10.1093/itnow/bwaa116.
- [19] M. A. Rahman, P. Bera, and E. Al-Shaer, "SmartAnalyzer: A noninvasive security threat analyzer for AMI smart grid," *Proc. - IEEE INFOCOM*, pp. 2255–2263, 2012, doi: 10.1109/INFOCOM.2012.6195611.
- [20] G. S. Misyris, A. Venzke, and S. Chatzivasileiadis, "Physics-informed neural networks for power systems," *IEEE Power Energy Soc. Gen. Meet.*, vol. 2020-Augus, 2020, doi: 10.1109/PESGM41954.2020.9282004.
- [21] I. Khorshed, A. Amer, and N. K. Khorshed, "Design an wireless sensing network by utilizing bit swarm enhancements," *IJCSNS International Journal of Computer Science and Network Security*, vol. 17, no. 6, Jun. 2017.
- [22] O. Martikainen, K. Raatikainen, and J. Hyvärinen, "Erratum to: Smart networks," *International Federation for Information Processing*, 2002, doi: 10.1007/978-0-387-35584-9_19.
- [23] S. Hasan and A. Amer, "Smart routing protocol algorithm using fuzzy artificial neural network OSPF," *Iraqi J. Sci.*, pp. 155–160, 2021, doi: 10.24996/ijcs.2021.si.1.21.
- [24] J. R. C. Nurse, "Cybersecurity Awareness," *Encycl. Cryptogr. Secur. Priv.*, pp. 1–4, 2021, doi: 10.1007/978-3-642-27739-9_1596-1.
- [25] A. A. Amer, "Improve the performance of the CNPV protocol in vanet networks," *Int. J. Civ. Eng. Technol.*, vol. 9, no. 11, pp. 304–314, 2018.
- [26] A. Chahal and P. Gulia, "Deep learning: A predictive Iot data analytics method," *SSRG Int. J. Eng. Trends Technol.*, vol. 68, no. 7, 2020, doi: 10.14445/22315381/IJETT-V68I7P205S.
- [27] Q. Chi, H. Yan, C. Zhang, Z. Pang, and L. Da Xu, "A reconfigurable smart sensor interface for industrial WSN in IoT environment," *IEEE Trans. Ind. Informatics*, vol. 10, no. 2, pp. 1417–1425, 2014, doi: 10.1109/TII.2014.2306798.
- [28] D. Hein, "Network security and performance monitoring: the basics." [solutionsreview.com](https://solutionsreview.com/networkmonitoring/network-security-and-performance-monitoring-the-basics/). <https://solutionsreview.com/networkmonitoring/network-security-and-performance-monitoring-the-basics/> (accessed Apr. 20, 2022).
- [29] J. Payne, K. Budhraja, and A. Kundu, "How secure is your IoT network," in *2019 IEEE International Congress on Internet of Things (ICIOT)*, 2019, pp. 181–188, doi: 10.1109/ICIOT.2019.00038.
- [30] C. Resnick, "GE's industrial internet of things journey." <https://www.ge.com/> (accessed Apr. 20, 2022).
- [31] L. Milic and P. Lotfian, "IoT data analytics report 2016." <http://ideya.eu.com>. <http://ideya.eu.com/publications/internet-of-things-data-analytics-report-2016.html> (accessed Apr. 20, 2022).




- [32] G. P. Kaur, J. Birla, and J. Ahlawat, "Generations of wireless technology," *Int. J. Comput. Sci. Manag. Stud.*, vol. 11, no. 02, pp. 176–180, 2011.
- [33] Y. Qi, M. Hunukumbure, H. Nam, H. Yoo, and S. Amuru, "On the phase tracking reference signal (PT-RS) design for 5G new radio (NR)," *IEEE Veh. Technol. Conf.*, vol. 2018-Augus, 2018, doi: 10.1109/VTCTFall.2018.8690852.
- [34] J. Antoniou, "Cloud computing: Considering trust as part of the user quality of experience," in *EAI/Springer Innovations in Communication and Computing*, 2021, pp. 37–53. doi: 10.1007/978-3-030-52559-0_4.
- [35] M. Mokhtari, G. B. Gharehpetian, and S. M. Mousavi Agah, "Distributed energy resources," *Distrib. Gener. Syst. Des. Oper. Grid Integr.*, pp. 1–19, 2017, doi: 10.1016/B978-0-12-804208-3.00001-7.

BIOGRAPHIES OF AUTHORS



Dr. Aseel K. Ahmed    is lecturer at Al Rafidain University College, computer science department, Baghdad-iraq since 2002 till now. She Holds a M. Sc. degree and Ph. D. degree in computer science from Iraqi authority for computers and informatics. She can be contacted at email: aseleelcom@gmail.com.



Dr. Abbas Akram Khorsheed    is lecturer at almustansiriyah university, college of science, computer science department, Baghdad-iraq since 2005 till now. He Holds a M. Sc. degree in Computer science from Iraq, and Ph. D. degree in computer science and informatics since 2015 from Lebanese university and university of Cagliari-Italy. He can be contacted at email: abbasarab2000@uomustansiriyah.edu.iq.