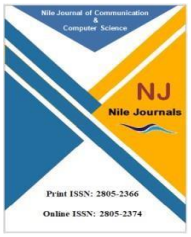
Nile Journal of Communication & Computer Science

Volume 6, December 2023

Journal Webpage: https://njccs.journals.ekb.eg



Security Issues and Challenges for IoT-based Smart Multi Energy Carrier Systems

Magda I. El Afifi[1], Hesham A. Sakr[2]

[1,2]Assistant Professor- ECE department-Nile Higher Institute for Engineering and Technology

Abstract

The Internet of Things (IoT) is revolutionizing the energy sector by providing a platform for energy hubs to connect and manage energy resources. IoT-enabled energy hubs allow energy providers to monitor, analyse, and optimize energy use across their networks. Smart energy hubs can measure energy consumption in real time, giving energy providers insight into how much energy is being used and when. This data can be used to adjust pricing and energy supply in order to maximize efficiency and cost savings. Moreover, the integration of IoT technology in energy hubs facilitates the implementation of automated energy management systems. These systems may be programmed to effectively address fluctuations in energy demand and supply, thereby ensuring a consistent and dependable energy supply. Finally, IoT-enabled energy hubs can be used to integrate renewable energy sources such as wind and solar into the energy grid, allowing energy providers to reduce their carbon footprint and meet sustainability goals.

Keywords: Internet of Things, Smart Energy hub, Security, Advanced Metering Infrastructure, Cyber Physical Systems.

1. Introduction

The concept of the Internet of Things (IoT) refers to a network of tangible entities, sometimes referred to as "things," which are equipped with sensors, software, and other technological components. These entities are designed to establish connections and facilitate the exchange of data with other devices and systems through the internet [1]. These gadgets encompass a wide spectrum, ranging from commonplace domestic products to highly advanced industrial instruments. According to Cisco [1], [2], the current number of interconnected IoT devices exceeds 7 billion. It is anticipated that this figure will increase to 10 billion by the year 2020 and further expand to 22 billion by 2025.

In recent years, the IoT has emerged as a highly significant technological advancement in the 21st century. With the advent of embedded devices, it has been feasible to establish internet connectivity for various daily objects such as kitchen appliances, cars, thermostats, and baby monitors. This technological advancement enables seamless communication among individuals, processes, and objects. The IoT seeks to establish connectivity among intelligent devices on a broad scale by utilizing IP-based technologies such as IP, TCP/UDP, and others. This connectivity can be established either by direct means or by utilizing gateways, in cases where implementing IP support is not practical. The ultimate goal is to enable these devices to engage in communication with any other participating entity over the Internet. In several applications, smart objects are now interconnected on a limited scale through the utilization of exclusive non-IP methods such as Zigbee, HART/Wireless HART, Z-Wave, and others.

In recent times, energy hub (EH) systems have emerged as viable strategies for fulfilling client requirements by utilizing diverse energy carriers such as electricity, natural gas, cooling, and heating systems [3], [4]. Due to the diverse range of energy resources available to EHs, they possess distinct advantages in terms of both economic and environmental considerations when compared to alternative energy networks. Hence, in numerous countries, the continuous advancement of these systems is regarded as their distinguishing feature, as they strive to fulfill energy requirements while minimizing emissions and pollution [5]. Moreover, the system operator has access to many resources that may be utilized as energy sources in order to achieve a balance between supply and demand within the network. This capability allows the operator to satisfy the demand at the most cost-effective level [5].

Numerous connectivity technologies, like as the IoT, have the potential to be seamlessly included into EHs, thereby augmenting their overall functionality. The sensors employed to monitor and modify an agent's physical or environmental conditions are encompassed under the IoT platform layer. The IoT encompasses a diverse range of challenges and an abundance of data and information. This encompasses the implementation of measures to limit access, the mitigation of security risks, and the establishment of a comprehensive infrastructure for the storage and processing of data across a wide geographic area. Hence, in order to enhance EH's capacity to utilize IoT technology for the purpose of information and data transmission, it is imperative to establish a dependable, expeditious, secure,

and intelligent communication network. When linked with EH, this approach transforms into a smart EH (SEH) possessing the aforementioned properties.

The utilization of the IoT holds considerable importance within the realm of EH; yet, it is crucial to acknowledge the potential for disasters that may arise as a consequence. Due to its reliance on industry-standard internet-based protocols and systems for monitoring and control, as well as its dependence on public communication infrastructure, the EH is susceptible to cyberattacks and might be considered a critical infrastructure. The potential consequences of an attacker's interference with the real-time equilibrium between energy generation and usage include financial losses for the utility and damage to the electric infrastructure. This interference can be achieved by processing data generated by smart devices or data received by the utility through manipulation [6].

This study aims to examine the security concerns and obstacles associated with the IoT-based EH systems. In the second section, a concise overview is provided about the IoT, EH, and the interconnectedness that exists between these two domains. Section 3 of this study delves into the examination of security concerns and obstacles within the context of the IoT-based environmental health. In this study, we examine the security services provided for the EH in part 4, and afterwards present our findings and conclusions in section 5.

2. Internet of Things and Smart Energy Hub

2.1. Internet of Things

The phenomenon of incorporating resource-constrained objects, including sensors, actuators, RFID tags, and other communication-enabled and computationally capable devices, into the Internet infrastructure is commonly known as the IoT. Nowadays, common household items such as refrigerators, windows, heaters, switches, and washing machines can be conveniently accessed, controlled, and interconnected through the Internet by utilizing protocols that operate over the internet such as HTTP, IPv6, UDP/TCP, and so on. The Internet Engineering Task Forces (IETF) has created several protocols specifically designed for devices with limited resources, notably those that comply with the IEEE 802.15.4 standard. These protocols aim to facilitate the seamless integration of such devices into the Internet infrastructure, operating at different tiers of the network stack.

- The 6LowPAN protocol, also known as IPv6 over Low Power Wireless Personal Area Networks, serves as an adaptation layer designed specifically for IEEE 802.15.4 networks. Its primary function is to facilitate the utilization of the IPv6 protocol within these networks [7].
- The topic of discussion is the Routing Protocol for Lossy and Low-Power Networks, commonly referred to as RPL [7].
- The Confined Application Protocol (CoAP) is a specialized web transfer protocol designed for usage with constrained nodes and networks [7]. The possibility of integrating into the global Internet network remains viable by utilizing gateways, which provide the translation of exclusive non-Internet Protocol (IP) stack protocols (such as Zigbee v1, HART, Z-Wave, etc.) to and regarding the protocols used in the IP stack. However, this integration comes at a considerable expense and does not fully achieve end-to-end communication. This assertion has validity even in the case of objects that have not yet achieved native support for IP or have been upgraded to accommodate it, primarily due to severe resource limitations or the need to maintain compatibility with previous systems.

2.2. Energy hub

The EH can be conceptualized as the traditional energy system enhanced by the extensive utilization of information and communication technologies (ICT), encompassing software, hardware, and networks. Furthermore, it entails the incorporation of dispersed renewable energy generation and storage capacities. As depicted in Fig. 1, the EH exhibits two distinct flows.

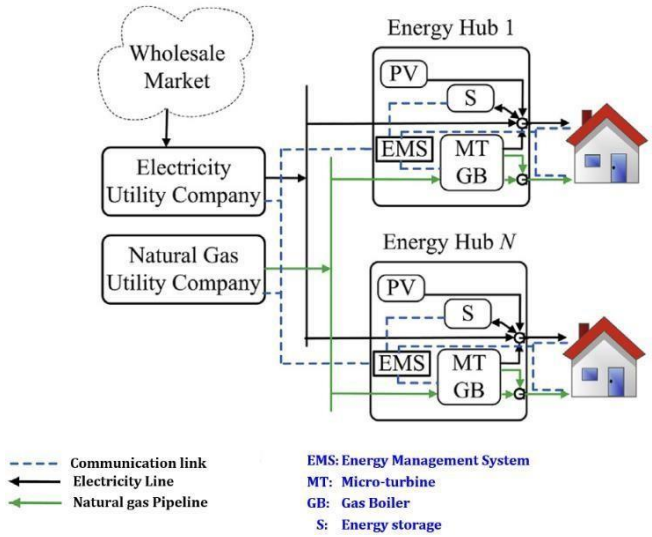


Fig. 1. Energy hub schematic [8]

 The primary flow (regular line) of the traditional energy system is the transmission of energy from the generation source at the plant to the ultimate consumer. However, according to the EH's perspective, the electric flow has the potential to be bidirectional, allowing the end-customer to both purchase and sell energy [9].

 Information flow (dashed lines): The exchange of information between the different stakeholders and components of EH serves as a crucial bidirectional communication channel. In conjunction with the utilization of smart meters and other intelligent devices such as smart appliances and electric vehicles, the predominant communication flow is attributed to the extensive deployment of sensors, actuators, and other intelligent entities in addition to the transmission and distribution sectors [10].

Two essential components of the EH are the Advanced Metering Infrastructure and Smart Meters:

 Smart/advanced meters (SMs) are installed in homes, businesses, and other structures. For billing or administration purposes, they keep track of information including energy consumption data. Due to their bidirectional communication capability, they are able to react to utility requests, such as software upgrades, real-time pricing, load shedding, and energy cut-off. and report data on a regular basis, upon request, or in response to specific events. By regulating or managing the energy usage of the smart gadgets in the home (fridge, oven, air conditioner, electric cars, etc.), they can optionally serve as a local energy management system.

 The Advanced Metering Infrastructure (AMI) [11] is in charge of gathering, processing, storing, and distributing the metering data sent by the SMs to the appropriate authorized parties so they can move forward with tasks like billing, outage management, demand forecasting, etc. Additionally, requests, directives, price data, and software upgrades from authorized parties must be transmitted to the SMs via the AMI. Figure 1 shows a condensed perspective of the AMI as a component of the entire EH.

2.3. IoT-based EH

The SEH, in contrast to the classical EH, incorporates a comprehensive integration of information and communication technology (ICT) throughout the entire energy chain, encompassing producers and end-consumers. This integration is achieved through the widespread deployment of diverse sensing, actuating, and embedded devices, along with the utilization of smart meters, smart appliances, and electric cars, all of which possess computing and communication capabilities.

The widespread popularity of the Internet can be attributed to the utilization of commonly used communication protocols, with a particular emphasis on the TCP/IP stack. Irrespective of the specific access method employed, it is possible for two computers situated in any geographical location throughout the globe to establish seamless end-to-end communication. The IoT facilitates the expansion of the Internet's coverage to encompass all entities capable of communication and individualized interaction, either through the utilization of standardized communication protocols or, in more extreme cases, via a gateway. The utilization of standardized communication protocols, specifically those depending on the TCP/IP stack, instead of proprietary solutions such as Zigbee v1 effectively tackles the challenge posed by the vast number of devices/objects installed on the SEH and the crucial requirement for timely and responsive interaction with these devices.

Assuming a hypothetical scenario, let us consider a nation's Sensor and Actuator-enabled Energy Harvesting system, comprising a substantial deployment of 40 million sensors and actuators. These devices are strategically positioned to effectively monitor the entirety of the power grid infrastructure. Additionally, the SEH system incorporates an additional 20 million smart meters, further enhancing its monitoring capabilities. The SEH operator may find it intriguing to have the capability to remotely monitor and alter smart meters, sensors, and actuators, independent of their manufacturer. Additionally, being able to get information on the current condition of the last mile grid would be of interest. To ensure accurate customer billing and mitigate the risk of manipulation, such as energy theft, energy companies may find it advantageous to implement remote monitoring of energy consumption through smart meters (SMs). To effectively regulate their usage, end users may find it beneficial to receive up-to-date pricing information (assuming a dynamic pricing model) and advance notifications regarding planned disconnections. Undoubtedly, the utilization of IP-based communication protocols and the inclusion of public communication infrastructures will yield significant advantages for bidirectional end-to-end interactions and communications. This is particularly true unless such implementation is deemed infeasible or socially unacceptable. The aforementioned measures will enhance scalability and effectively reduce associated expenses.

3. IoT-based Energy Hub's Concerns and Difficulties Related to Security

The traditional power grid's new ICT component created new security concerns and difficulties that weren't (or were only seldom) present there. These security concerns and difficulties may slow down the IoT-based EH's quick rollout and uptake by end users. Following, we quickly discuss the most significant security concerns and difficulties encountered on the IoT-based SEH.

3.1. Security Issues

The IoT-based SEH will encounter many security challenges in its capacity as a cyber-physical system.

- ***Impersonation*/Identity *Spoofing*:** The objective of this assault is to fraudulently utilize the identity of an authentic entity in order to engage in unauthorized communication on its behalf. In the realm of smart meter technology, it is conceivable for an individual with malicious intent to assume the identity of another person's smart meter, thereby compelling it to bear the financial burden of the energy it consumes.

- ***Eavesdropping*:** Since the objects/devices on the IoT-based SEH communicate, they frequently use open communication infrastructure, making it simple for an attacker to access the data they share. An attacker can quickly learn how much energy is used by families.
- ***Data tampering***: Exchanged data, such as dynamic prices supplied before peak times, can be altered by an attacker to make them lowest prices. In turn, this might lead to homes increasing their consumption (charging e-cars, etc.) rather than decreasing it, which would lead to an overcrowded power network.
- ***Authorization and Control Access issues*:** Given the remote monitoring and configuration capabilities of numerous devices, for example, technologies like smart meters and sensors and actuators installed in distribution substations., it is plausible for an unauthorized individual, including a malicious attacker or disgruntled employee, to attempt to gain illicit access to these devices. The objective of such unauthorized access would be to manipulate the devices and induce physical harm, such as damaging transformers, or disrupt the power supply by causing outages.
- ***Privacy issue*:** Smart appliances and meters installed in residential dwellings have the potential to offer a wider range of data beyond mere energy use. The fine-grained data created by the system has the potential to jeopardize the privacy of the end user. This is because it may reveal specific details about their daily routines, including wake-up, sleep, and meal times. Additionally, it may disclose if the user is at home or away, and even indicate if they are not at home.
- ***Compromising and Malicious code*:** Due to the inherent capabilities of SEH objects in terms of processing and communication, they are susceptible to intrusion from both local and remote sources. Furthermore, due to their utilization of diverse software applications, they may become susceptible to a range of software infections or malicious code infections with the intention of gaining control over and exerting influence on them. This could manifest in the form of targeted attacks on smart meters or smart home appliances, for instance. In addition, it is important to note that tamper-resistant technologies are generally not found in widely deployed objects that have limited electronic components, such as sensors. As a result, these objects are susceptible to physical compromise with relative ease.
- ***Availability and DoS issues*:** Targeting the availability of assets (electricity meters, substations, etc.) in the traditional power grid was challenging, if not impossible, especially on a large scale. ICT will be integrated into the essential components of the power grid in the SEH, making it feasible to target them and launch a DoS attack

that will render them partially or completely inaccessible. Furthermore, given that most gadgets/things are IP-enabled and do not run proprietary protocol stacks, it will be simpler for an experienced Internet attacker to carry out their attack.

- **Cyber-attack:** The SEH might be viewed as the greatest Cyber-Physical System, with ICT elements controlling and managing physical entities in physical systems that represent the EH's physical assets (transformers, circuit breakers, smart meters, cables, etc.) [12], [13].

3.2. Security Challenges

There are a number of problems to consider while dealing with security algorithms, protocols, and rules for the IoT-based EH:

- ***Scalability*:** The SEH involves many smart items and devices and may cover vast areas (such as numerous cities or the entire nation). Scalable security solutions, such as key management and authentication, will be challenging to imagine as a result [14], [15].
- ***Mobility*:** There will always be a requirement for authentication and secure connection with a changing environment (smart meters, electric charging stations, etc.) for mobile devices/objects like e-cars and on-the-field technical agents.
- ***Deployment***: Since the SEH might affect the entire nation, many items and gadgets are deployed, left to operate unattended, and put in remote locations with no physical boundary security, making them easily accessible. Any attempt to interfere with security systems should be recognized by their solutions.
- ***Legacy systems***: Due to their reliance on proprietary hardware and software, as well as their deployment in distant and isolated locations with limited communication infrastructure, existing systems and devices may exhibit inadequate security support. The integration of legacy systems into the IoT-based SEH poses a significant obstacle due to the lack of feasible options for replacement or update of existing systems to accommodate the required security solutions.
- ***Constrained Resources*:** Numerous SEH devices/objects, particularly those that have been deployed in large numbers, are resource restricted. When creating security solutions, extra attention must be taken to ensure that their constrained resources can support the solutions. This makes it difficult to deploy traditional security solutions, especially those relying on PKI.
- ***Heterogeneity*:** The task of establishing ensuring secure communications from start to finish is a difficult task that often requires modifying existing solutions or employing gateways. This is due to the disparity in resources between devices or objects on the secure end-to-end network, such as memory, computation power, bandwidth, energy autonomy, and time-sensitivity. Additionally, non-IP-based devices may have different protocols and communication stacks, further complicating the process.
- ***Interoperability*:** The heterogeneity of communication stacks and protocols among devices and objects in the EH may be considered as a contributing factor to this phenomenon. Legacy systems, devices, and objects that lacked support for the TCP/IP stack, such as Zigbee v1 and HART, faced challenges in achieving end-to-end secure communication. These systems were unable to directly communicate with IP-based systems, devices, and objects without the use of gateways. An additional illustration of interoperability arises when two devices employ identical protocols and communication stacks, however possess distinct feature capabilities. One device may provide complete support for a specific feature, whereas the second device may only offer partial support for the same feature. For instance, one device may support DTLS with certificate functionality, while the other device may lack this certificate support.
- ***Bootstrapping*:** What are the effective methods for securely initializing the cryptographic components (cryptographic keys, cryptographic functions, algorithms, parameters, etc.) of the numerous SEH devices and objects?
- ***Trust Management*:** Different organizations (end-users for smart appliances, EH's operator for smart metres and sensors, etc.) may be in charge of managing the objects and devices on the SEH. If a foundational degree of trust isn't built, objects and gadgets won't be able to communicate. Building trust among objects/devices owned/managed by various entities can be difficult, especially in such a vast network, whereas doing so for objects/devices owned/managed by the same entity is easy.
- ***Latency/Time Constraint***: Certain components of SEH necessitate real-time responses to events and messages. To ensure the security of assets and prevent the propagation of anomalies, it is imperative that electric SCADA systems employed in transmission and distribution sub-stations promptly respond to fluctuations in current, voltage, and frequency levels of electricity, as well as other meteorological factors that impact the functioning of

equipment. Activities that require a significant amount of time, such as public-key operations, are thus deemed unsuitable [16]–[21].

4. Services for The IoT-Based Smart EH's Security

Following, we provide a quick summary of the key security services that the IoT-based SEH should take into account:

- ***Authentication***: The capacity to identify and verify any communicating object or device in the SEH. For instance, in order to charge the appropriate user for each smart meter, the energy provider must authenticate each one [22]–[26].
- ***Data Integrity***: Ensures that any unauthorized changes to the (received) data have not been made. For instance, in addition to source origin, smart meters must guarantee the integrity of a software update.
- ***Confidentiality***: ensures that only the intended recipients have access to data (whether it is kept or transferred). For instance, only the energy provider and the SEH operator need to be aware of end-user consumption [27].
- ***User's Privacy***: provides assurances that no user (energy consumer end-user) data, whether raw, inferred, or computed, will be accessed without the user's express consent and will only be used for the specified objectives. Examples include the inability to use energy consumption data used for invoicing purposes for other purposes.
- ***Authorization and Control Access***: Ensures that an authenticated object or person has the requisite rights to access certain resources or is qualified to carry out certain duties. To manually configure a smart meter, for example, an on-the-field agent needs authorization and access control rights [28-30].

5. Conclusion

The IoT is the next step towards a universal and widespread connection to any object or device that is capable of communication and computation, regardless of access technology, resource availability, or location. The IoT vision, where smart items and devices are installed along the energy supply line from the generation facility to the final consumer, can be very advantageous for the SEH. But for the IoT and the widespread adoption and implementation of the SEH, security is the major issue.

The main security concerns and problems for the SEH were briefly covered in this article, along with the key security services that were needed. Future research will focus on how to safely incorporate energy-aware smart homes with smart meters and smart appliances into the SEH so that end users can participate actively and safely in the balance between energy consumption and output. This research will examine the security of the AMI, a key component of the SEH.

References

[1] C. Bekara, "Security issues and challenges for the IoT-based smart grid," *Procedia Comput. Sci.*, vol. 34, pp. 532–537, 2014, doi: 10.1016/j.procs.2014.07.064.

[2] A. A. Eladl, M. I. El-afifi, M. M. El-saadawi, and B. E. Sedhom, "Distributed Optimal Dispatch of Smart Multi-agent Energy Hubs Based on Consensus Algorithm Considering Lossy Communication Network and Uncertainty," 2023, doi: 10.17775/CSEEJPES.2023.00670.

[3] M. I. El-afifi and M. M. Saadawi, "Cogeneration Systems Performance Analysis as a Sustainable Clean Energy and Water Source Based on Energy Hubs Using the Archimedes Optimization Algorithm," 2022.

[4] A. A. Eladl, M. I. El-Afifi, M. M. El-Saadawi, and B. E. Sedhom, "A review on energy hubs: Models, methods, classification, applications, and future trends," *Alexandria Eng. J.*, vol. 68, pp. 315–342, 2023, doi: 10.1016/j.aej.2023.01.021.

[5] A. A. Eladl, M. I. El-Afifi, M. A. Saeed, and M. M. El-Saadawi, "Optimal operation of energy hubs integrated with renewable energy sources and storage devices considering CO2 emissions," *Int. J. Electr. Power Energy Syst.*, vol. 117, no. November 2019, p. 105719, 2020, doi: 10.1016/j.ijepes.2019.105719.

[6] A. A. Eladl, M. E. El-Afifi, and M. M. El-Saadawi, "Communication Technologies Requirement for Energy Hubs: A survey," *2019 21st Int. Middle East Power Syst. Conf. MEPCON 2019 - Proc.*, pp. 821–827, 2019, doi: 10.1109/MEPCON47431.2019.9008006.

[7] M. Eisenhauer, P. Rosengren, and P. Antolin, "An Overview of Privacy and Security Issues in the Internet of Things," *Sensor, Mesh Ad Hoc Commun. Networks Work. 2009. SECON Work. 09. 6th Annu. IEEE Commun. Soc. Conf.*, pp. 367–373, 2010, doi: 10.1007/978-1-4419-1674-7.

[8] F. Kamyab and S. Bahrami, "Efficient operation of energy hubs in time-of-use and dynamic pricing electricity markets," *Energy*, vol. 106, pp. 343–355, 2016, doi: 10.1016/j.energy.2016.03.074.

[9] A. A. Eladl, M. E. El-Afifi, and M. M. El-Saadawi, "Optimal power dispatch of multiple energy sources in energy hubs," *2017 19th Int. Middle-East Power Syst. Conf. MEPCON 2017 - Proc.*, vol. 2018-Febru, no. December, pp. 1053–1058, 2018, doi: 10.1109/MEPCON.2017.8301312.

[10] J. E. Dagle, “Cyber-physical system security of smart grids,” *2012 IEEE PES Innov. Smart Grid Technol. ISGT 2012*, pp. 1–2, 2012, doi: 10.1109/ISGT.2012.6175607.
[11] A. A. Sallam and O. P. Malik, “Scada Systems and Smart Grid Vision,” *Electr. Distrib. Syst.*, pp. 469–493, 2011, doi: 10.1002/9780470943854.ch13.
[12] R. Langner, “Stuxnet: Dissecting a cyberwarfare weapon,” *IEEE Secur. Priv.*, vol. 9, no. 3, pp. 49–51, 2011, doi: 10.1109/MSP.2011.67.
[13] M. Abdel-Azim, M., Awad, M. M., & Sakr, H. A.,” VoIP versus VoMPLS Performance Evaluation”, International Journal of Computer Science Issues (IJCSI), 11(1), 194, 2014.
[14] C. Bekara, T. Luckenbach, and K. Bekara, “A Privacy Preserving and Secure Authentication Protocol for the Advanced Metering Infrastructure with Non-Repudiation Service,” Proc. of ENERGY, no. c, pp. 60–68, 2012.
[15] M. A. Mohamed, H. Sakr, and R. Awards, “RSVP BASED MPLS VERSUS IP PERFORMANCE EVALUATION,” no. August, 2019.
[16] I. Prasad, “Smart Grid Technology: Application and Control,” *Int. J. Adv. Res. Electr. Electron. Instrum. Eng.*, vol. 3, no. May 2014, pp. 9533–9542, 2014.
[17] H. A. Sakr and M. A. Mohamed, “Performance Evaluation Using Smart: HARQ Versus HARQ Mechanisms Beyond 5G Networks,” *Wirel. Pers. Commun.*, vol. 109, no. 3, pp. 1503–1528, 2019, doi: 10.1007/s11277-019-06624-3.
[18] A. T. Khalil, A. I. Abdel-Fatah, and H. A. Sakr, “Rapidly IPv6 multimedia management schemes based LTE-A wireless networks,” *Int. J. Electr. Comput. Eng.*, vol. 9, no. 4, pp. 3077–3089, 2019, doi: 10.11591/ijece.v9i4.pp3077-3089.
[19] H. A. Sakr, A. I. Abdel-Fatah, and A. T. Khalil, “Performance evaluation of power efficient mechanisms on multimedia over LTE-A networks,” *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 9, no. 4, pp. 1096–1109, 2019, doi: 10.18517/ijaseit.9.4.7910.
[20] H. A. Sakr, H. M. Ibrahim, and A. T. Khalil, Impact of Smart Power Efficient Modes on Multimedia Streaming Data Beyond 5G Networks, vol. 125, no. 1. Springer US, 2022.
[21] H.A. Sakr and M.A. Mohamed, ‘Handover Management Optimization over LTE -A Network using S1 and X2 handover', Proc. of The Seventh International Conference on Advances in Computing, Electronics and Communication – ACEC 2018, ISBN: 978-1-63248-157-3 doi: 10.15224/978-1-63248-157-3-11, pp. 58–64, 2018.
[22] Soomro, A. M., Naeem, A. B., Senapati, B., Bashir, K., Pradhan, S., Maaliw, R. R., & Sakr, H. A. (2023, January). Constructor Development: Predicting Object Communication Errors. In 2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology (ICES&T) (pp. 1-7). IEEE.
[23] Soomro, A. M., Naeem, A. B., Senapati, B., Bashir, K., Pradhan, S., Ghafoor, M. I., & Sakr, H. A. (2023, January). In MANET: An Improved Hybrid Routing Approach for Disaster Management. In 2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology (ICES&T) (pp. 1- 6). IEEE.
[24] M. Ibrahim, I. S. Bajwa, N. Sarwar, F. Hajjej, and H. A. Sakr, “An Intelligent Hybrid Neural Collaborative Filtering Approach for True Recommendations,” IEEE Access, no. May, pp. 1–1, 2023, doi: 10.1109/access.2023.3289751.
[25] R. M. Ibrahim, M. M. Elkelany, A. Ake, and M. I. El-afifi, “Trends in Biometric Authentication : A review,” vol. 6, no. December, pp. 1–12, 2023.
[26] M. I. E.-A. Hesham. A. Sakr, PLVAR team, “Intelligent Traffic Management Systems: A review,” *Nile J. Commun. Comput. Sci.*, vol. 5, no. 1, pp. 42–56, 2023, doi: 10.21608/NJCCS.2023.321169.
[27] M. I. El-Afifi, M. M. El-Saadawi, B. E. Sedhom, and A. A. Eladl, “An IoT-fog-cloud consensus-based energy management algorithm of multi-agent smart energy hubs considering packet losses and uncertainty,” *Renew. Energy*, vol. 221, no. June 2023, p. 119716, 2024, doi: 10.1016/j.renene.2023.119716.
[28] N. A. Mansour, A. I. Saleh, M. Badawy, and H. A. Ali, *Accurate detection of Covid-19 patients based on Feature Correlated Naïve Bayes (FCNB) classification strategy*, vol. 13, no. 1. Springer Berlin Heidelberg, 2022.
[29] [A. H. Rabie, N. A. Mansour, A. I. Saleh, and A. E. Takieldeen, “Expecting individuals’ body reaction to Covid-19 based on statistical Naïve Bayes technique,” *Pattern Recognit.*, vol. 128, p. 108693, 2022, doi: 10.1016/j.patcog.2022.108693.
[30] A. H. Rabie, N. A. Mansour, and A. I. Saleh, “Leopard seal optimization (LSO): A natural inspired meta-heuristic algorithm,” *Commun. Nonlinear Sci. Numer. Simul.*, vol. 125, no. June, p. 107338, 2023, doi: 10.1016/j.cnsns.2023.107338.