SPECIAL SECTION ON EMERGING TRENDS OF ENERGY AND SPECTRUM HARVESTING TECHNOLOGIES

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 19, 2020, accepted September 29, 2020, date of publication October 6, 2020, date of current version October 19, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3028764

Privacy Protection and Energy Optimization for 5G-Aided Industrial Internet of Things

MAMOONA HUMAYUN[1], NZ JHANJHI[2], MADALLAH ALRUWAILI[3], SAGAYA SABESTINAL AMALATHAS[2], VENKI BALASUBRAMANIAN[4], (Member, IEEE), AND BUVANA SELVARAJ[5]

[1]Department of Information Systems, College of Computer and Information Sciences, Jouf University, Sakakah 72388, Saudi Arabia
[2]School of Computer Science and Engineering (SCE), Taylor's University, Subang Jaya 47500, Malaysia
[3]College of Computer and Information Sciences, Jouf University, Sakakah 72388, Saudi Arabia
[4]School of Science, Engineering and Information Technology, Federation University, Mount Helen, VIC 3350, Australia
[5]School of Information Technology and Engineering, Melbourne Institute of Technology, Melbourne, VIC 3000, Australia

Corresponding authors: NZ Jhanjhi (noorzaman.jhanjhi@taylors.edu.my) and Mamoona Humayun (mahumayun@ju.edu.sa)

ABSTRACT The 5G is expected to revolutionize every sector of life by providing interconnectivity of everything everywhere at high speed. However, massively interconnected devices and fast data transmission will bring the challenge of privacy as well as energy deficiency. In today's fast-paced economy, almost every sector of the economy is dependent on energy resources. On the other hand, the energy sector is mainly dependent on fossil fuels and is constituting about 80% of energy globally. This massive extraction and combustion of fossil fuels lead to a lot of adverse impacts on health, environment, and economy. The newly emerging 5G technology has changed the existing phenomenon of life by connecting everything everywhere using IoT devices. 5G enabled IIoT devices has transformed everything from traditional to smart, e.g. smart city, smart healthcare, smart industry, smart manufacturing etc. However, massive I/O technologies for providing D2D connection has also created the issue of privacy that need to be addressed. Privacy is the fundamental right of every individual. 5G industries and organizations need to preserve it for their stability and competency. Therefore, privacy at all three levels (data, identity and location) need to be maintained. Further, energy optimization is a big challenge that needs to be addressed for leveraging the potential benefits of 5G and 5G aided IIoT. Billions of IIoT devices that are expected to communicate using the 5G network will consume a considerable amount of energy while energy resources are limited. Therefore, energy optimization is a future challenge faced by 5G industries that need to be addressed. To fill these gaps, we have provided a comprehensive framework that will help energy researchers and practitioners in better understanding of 5G aided industry 4.0 infrastructure and energy resource optimization by improving privacy. The proposed framework is evaluated using case studies and mathematical modelling.

INDEX TERMS 5G, energy optimization, industrial Internet of Things, privacy, security.

I. INTRODUCTION

The massive demand for high quality network services and increase of multimedia usage has triggered a significant change in the way network has been administered. To meet the increasing demands of internet customers; especially cellular users, organizations are embracing 5G as their future network. 5G will not only be just an advancement in its predecessors; instead, it aims to be a ground-breaking improvement in terms of bandwidth, massive connectivity, reliability, latency, and energy efficiency. It aims to connect everything everywhere by providing efficient and reliable services [1], [2]. It will allow Industrial internet of things (IIoT) devices to communicate and share data with very high speed and low latency as shown in Figure 1.

5G is designed with the protracted capacity to empower new deployment models by enabling next-generation users' expectations and delivering new services [3], [4]. It is mainly expected to expand the mobile network into new realms. It will impact every field of life, i.e. remote healthcare, safe transportation, digitized logistics, agriculture precision and much more. It will also affect the economy by creating new jobs, increasing global economic output and GDP [5], [6]. However, this massive connectivity of billions of devices will

The associate editor coordinating the review of this manuscript and approving it for publication was Guangjie Han.

FIGURE 1. Connecting everything everywhere using IoT devices.

FIGURE 2. How 5G works.

create various challenges, and most important of them are privacy and energy resource optimization. Working of 5G is shown in Figure 2.

5G will provide constant connectivity of IoT devices and is expected to transfer a huge volume of data. This massive transfer of data poses various challenges in terms of customer data privacy. For example, China is doing rapid advancement in technology, and it is expected that soon, it will install key elements of 5G network all around China. This will enable them to spy the traffic passing through them and thus is an alarming situation for the US government. Further, 5G will transfer a huge amount of sensitive personal data such as personal medical information, financial information, etc., this would also need privacy and protection from cyber breaches. Similarly, location and movement trial is another privacy issue in 5G due to large number of cellular towers [7], [8]. Some common factors that leads towards privacy issues in 5G network include: more privacy concerns due to excessive and fast transmission of data, new trust models, evolved threat landscape and new service delivery models [9]–[11] as shown in Figure 3.

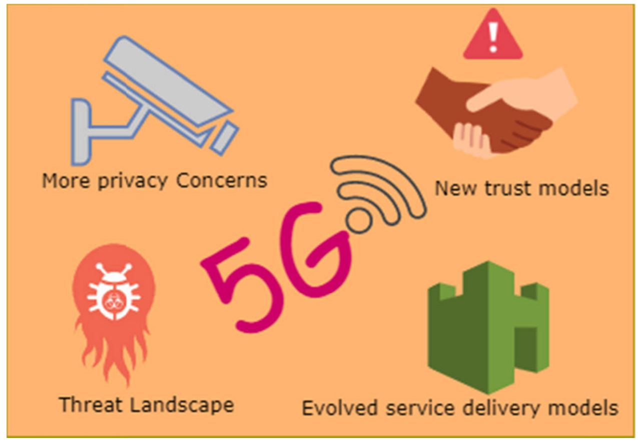


FIGURE 3. 5G privacy concerns.

The presence of evolved privacy issues in 5G network put more responsibilities on the developer as well as end-users. Developers need to implement reliable data encryption techniques to protect users' personal information. They also need to design user friendly privacy policies that are easy to understand by the customer. As far as the end-user is concerned, they need to make sure that the application they are downloading is from a reliable platform. Further, users need to protect their personal information from unnecessary disclosure. They need to read and comprehend the privacy policy of the application, where users' data will be stored [12]–[14].

Massive interconnected IoT devices will consume a huge amount of energy that can cause energy deficiency. To overcome this issue and to leverage the potential benefits of 5G, energy optimization is inevitable. Energy optimization means using energy in such a way that it could provide maximum services to the human and climate. The three key pillars of energy resource optimization are energy efficiency, demand response and fuel switching [15], [16]. Energy efficiency means saving maximum energy in existing infrastructure. This can be done by utilizing energy-saving equipment and proper management of energy resources. Demand response means facilitating energy customers by providing them with sufficient energy resources, and switching fuels refers to stop burning it indoors and shifting towards electricity [17]–[19]. Figure 4 provides a complete picture of an energy portfolio that need to be optimized for leveraging maximum benefits of 5G aided IIoT. According to figure 4, energy cycle is composed of various steps which include: energy demands in various sectors of life; this demand leads towards energy generation using resource-efficient ways, the generated energy is stored and delivered to various sectors of the economy for consumption. Finally, energy optimization for CapEx which include long term expenses and energy optimization for OpEx which include day-to-day energy expenses [20], [21].

IIoT is a system of heterogeneous interconnected devices that communicate and share information with each other without human interaction. It has brought great revolution in industrial sector by providing opportunities to leverage the potential of smart machines and getting benefits from

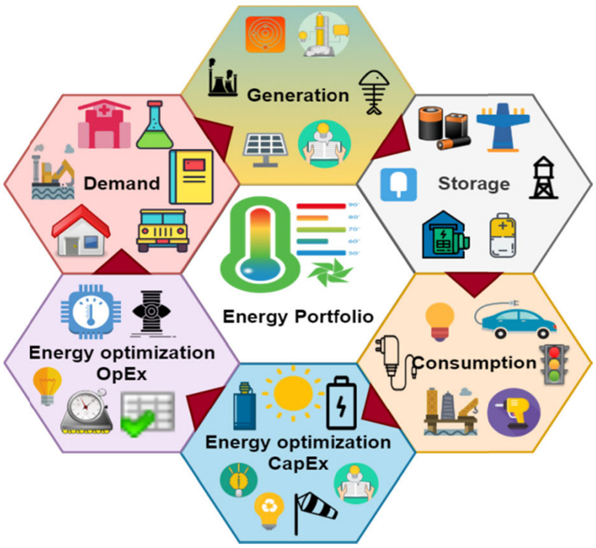


FIGURE 4. Energy portfolio.

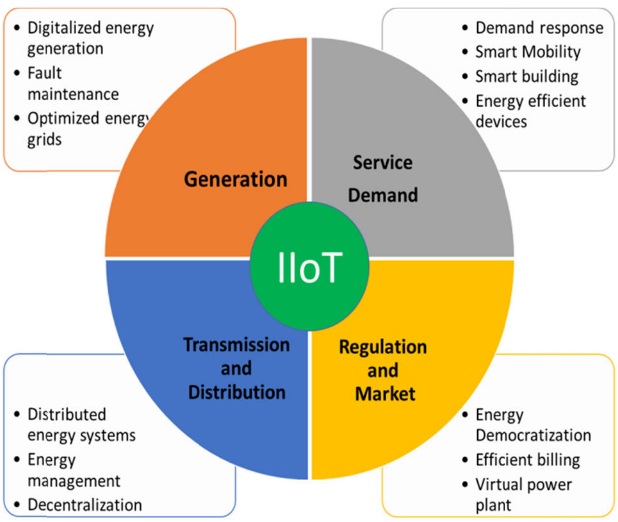


FIGURE 5. How IIoT benefits energy system.

real-time analysis of data in industrial settings [22], [23]. 5G technology has made these IIoT devices more useful by increasing communication speed and bandwidth [24].

IIoT devices enable smart energy systems by providing support in various dimensions of energy system including: demand services, regulations and marketing, generation, transmission and distribution [25]–[27] as shown in Figure 5.

5G and IIoT have benefited the field of energy and utilities the most. However, energy resources need to be optimized to leverage the potential benefits of 5G aided IIoT. For example, working hours need to be decided based on day-light strategy will save energy, as energy consumption is dependent on time and power as shown in equation 1

$$E = p * t \tag{1}$$

where E refers to the energy, p refers to power and t refers to the time

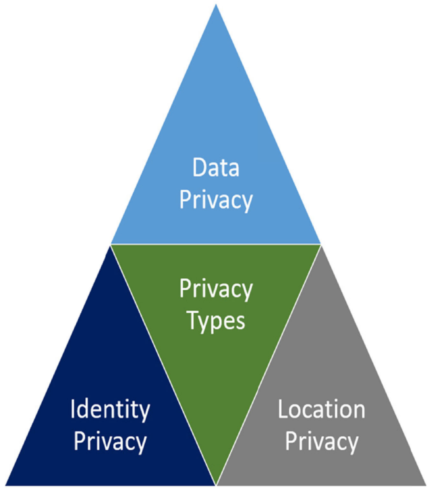


FIGURE 6. Dimension of privacy.

Keeping in mind the importance of privacy preservation and energy optimization in 5G network, this article aims to provide an effective solution for privacy and energy optimization. First privacy issues will be discussed in the light of existing literature, then energy related problems and solutions will be addressed. Next, we will provide a comprehensive framework that will not only address privacy concerns; rather, it will also provide energy optimization strategy. Further, both privacy preservation and energy optimization are modeled mathematically and evaluated using 2 case studies one for each. The remainder of the paper is organized into four sections; Section 2 will provide some related work for better understanding of the area under study. Section 3 will provide a novel privacy protection and energy resource optimization framework. Section 4 will use case studies and mathematical modeling to evaluate this framework, and finally, section 5 will conclude the paper by providing directions for future research. Before proceeding towards the next section, possible symbols used in our mathematical models are presented in Table 1, while table 2 list all possible abbreviations used in the paper.

II. LITERATURE REVIEW

This section will provide an overview of privacy protection and energy optimization in 5G context based on existing literature

A. PRIVACY PROTECTION IN 5G

Privacy is one of the important concerns in the 5G network that need to be addressed. Privacy is usually categorized into three parts, namely, data privacy, identity privacy and location privacy, as shown in Figure 6. In the section below, we provide some existing studies that have addressed the issue of privacy in 5G context

Paper [28] provided a detailed survey on the core technologies used in the 5G network and provided a 5G security model along with privacy concerns. This article considers privacy from user's perspective and identified core privacy

TABLE 1. Symbols and notations used.

Symbols	Used for
P	*Privacy*
X	*Identity privacy*
Y	*Location privacy*
Z	*Data privacy*
Aa	*Anonymous authentication*
Im	*Identity management*
Ka	*K-Anonymity*
Le	*Location encryption*
Dl	*Dummy location*
De	*Data encryption*
Dr	*Data rate*
Dp_t	*Data protection*
X_s	*Organizational set value for x*
Y_s	*Organizational set value for y*
Z_s	*Organizational set value for z*
E	*Energy*
EC	*Energy Consumption*
AEC	*Active energy consumption*
PEC	*Passive energy consumption*
X_1	*Energy consumption/Usage*
X_2	*Latency*
X_3	*Spectrum efficiency*
X_4	*Working time*
X_5	*Weather condition*
X_6	*Energy waste/leakages*
ε	*Standard error of estimation*
ES	*Energy supply*
DV	*Amount of data to be shared*
$a_1,a_2,a_3,\ldots a_6$	*Coefficient of* $X_1,X_2\ldots\ldots,X_6$ *respectively*
$P_1,p_2\ldots.p_6$	*Industry preferences for* $X_1,X_2\ldots\ldots,X_6$ *respectively*
$e_1,e_2,e_3\ldots e_6$	*Differences between optimized values and actual values*
$X_{1s}, X_{2s},\ldots.X_{6s}$	*Organizational values for* $X_1,X_2\ldots\ldots,X_6$ *respectively*

TABLE 2. List of abbreviations.

Abbreviation	Explanation
5G	Fifth generation
D2D	Device to device
I/O	Input Output
IIoT	Industrial internet of things
GDP	Gross domestic product
US	United State
CapEx	Capital Expenditure
OpEx	Operating Expenditures
E2E	Equipment to equipment
SDN	Software defined network
CPS	Cyber physical system
IAA	Industrial automation applications
RMA	Remote machine automation applications
RA	Robotic applications
SCA	Supply chain applications
HAM	Handover authentication mechanism
HetNets	Heterogeneous networks
QoS	Quality of Service
DLC	Development life cycle

challenges and also provided a few regulatory objectives. According to this research, privacy is categorized into 3 types including data privacy, location privacy and identity privacy. Some of the key privacy issues identified in this study include: E2E data privacy, shared environment, loss of ownership, varying trust objectives and third-party involvement. Finally, the paper proposed some key privacy properties that need to be incorporated in 5G, these properties include anonymity, unlikability, undetectability, unobservability and pseudonymity.

According to paper [12], privacy preservation is one of the key requirements of modern 5G network; it varies from application to application. However, there are generally three kinds of privacy concerns, namely, location privacy, identity privacy and data privacy. Location privacy can be preserved using three solutions, namely, k-anonymity, location encryption and dummy locations, while identity privacy can be maintained using anonymous authentication. The data privacy can be preserved using two solutions; using encryption and transmitting data at the rate, which is less than the secrecy capacity.

In paper [14], privacy issues in the 5G network have been identified along with the objective of privacy protection. It also aligned the identified issues with these objectives and proposed a technical and regulatory approach to address these issues. Some key issues identified in this article include E2E data confidentiality, loss of ownership, legal dispute, shared environment, loss of governance, hacking and providing information to the third party. The proposed solution is based on regulatory and technical approach. The regulatory process consists of applying proper regulation at three levels, namely, government, industry self-regulation and consumer/market regulation. The technical solution designed in this study includes privacy aware SDN based routing mechanism, design privacy, hybrid cloud and timely assessment of privacy and security.

According to [29], privacy preservation and balance between privacy requirements & offered services are the key requirements of 5G network that need to be taken into account from infrastructural as well as architectural perspectives. This article also discusses privacy from three perspectives, as mentioned in previous studies, namely, data privacy, location

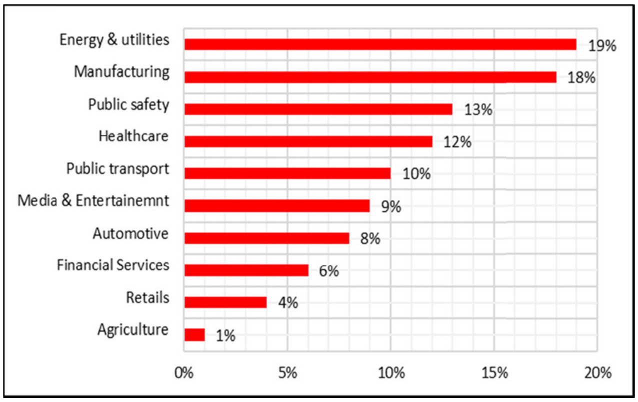


FIGURE 7. 5G enabled Industry expected revenues in 2026.

privacy and identity privacy. Data privacy can be addressed using strong data protection techniques and by following privacy regulations. The anonymity-based solution is suitable for preserving location privacy, and proper identity management is inevitable for maintaining identity privacy.

In paper [30], a novel HAM is proposed for 5G HetNets, and this mechanism ensures traceability and user anonymity using SDN technique and user capability integration. The proposed scheme doesn't involve the third party during authentication and key agreement between users' equipment and base stations in 5G HetNets. Thus it makes the handover process easy and also preserves privacy. According to study results, communication cost and computational overhead are low in the proposed scheme as compared to other existing schemes.

It is obvious from the above discussion that 5G will be the backbone for all future transactions. However, the massive, interconnected devices and fast data transmission will raise the problem of privacy. Various studies have discussed the issue of privacy by providing different practices that need to be adopted in 5G setting. Still, there exists no proper solution for it. To fill this gap, we will provide a framework in section 3 that will not only preserve privacy in 5G rather, it will also optimize energy efficiency in 5G.

B. ENERGY OPTIMIZATION IN 5G

5G has benefited various sectors of the economy, and energy & utilities are the sector that benefited from it the most. According to a report published by Ericson [31], the total revenue generated from 5G-enabled industries is expected to be 1.3 trillion USD in 2026 from which lion share will be generated through energy and utilities as shown in Figure 7. This indicates that energy is one of the key sectors that will get benefits from 5G. To leverage these potential benefits, energy resources need to be optimized. In this section, we will survey some existing studies on energy resources' optimization in 5G aided IIoT to get the state-of-the-art picture.

A 5G based network communication framework for Cyber-physical IoT is proposed in [32] with the aim to support full-duplex communication in a network having multiple sensors, actuators and a central controller. Based on the proposed framework, an algorithm was proposed for energy resource allocation efficiently. The framework was divided into two parts, namely power allocation and channel allocation, and separate algorithms were proposed for handling each issue. Proposed algorithms were tested using simulation and were also compared with existing algorithms. The simulation results validated proposed algorithms and proved that proposed algorithms outperform existing algorithms in term s of QoS and energy efficiency.

A detailed study on 5G and IoT is undertaken in [33] to explore the various approaches used for addressing resource problems. These approaches are categorized, weakness and strengths of each approach is discussed along with similarities and differences between these approaches and future directions for resource allocation in 5G and IoT is provided. Further, the issue of spectrum scarcity in 5G and IoT is addressed, and a solution model is proposed for it.

According to [34]; after IIoT and 5G emergence, a tremendous growth of smart devices is expected that will create substantial traffic shocks in the future network. To address this problem and to support computation intensive application on resource constrained users' devices, a joint resource optimization scheme is proposed in this study. The proposed scheme combines D2D communication technologies with edge computing for 5G edge network. Three processing modes are developed in this scheme for the processing of computationally intensive tasks which include local computing, edge node computing and fog computing along with corresponding energy consumption model, time delay model and task allocation model. The proposed optimization model was tested using simulation, and the results reveal better energy consumption and improved performance of 5G mobile communication.

According to [35], IoT is facing a spectrum shortage issue due to the tremendous growth of IoT terminals and the services of big data. On the other hand, 5G owns enough spectrum resources for handling big data. Therefore, combining IoT and 5G will expand communication resources. This article proposes power splitting and time switching model for simultaneous transfer of IoT and 5G information where IoT nodes handle both streams. Two joint optimization problems are formulated in this study: first, node power and allocation power for maximizing 5G transmission rates with minimal IoT transmission rate. Second, maximizing IoT transmission rate under 5G transmission constraints. Further, an energy efficient model is proposed to minimize IoT power consumption while guaranteeing transmission rates of both 5G and IoT. The proposed model was tested using simulation, and results reveal that the proposed model save IoT energy in 5G settings.

An energy efficient framework is proposed in [36] for managing and controlling data rate and transmission power of IoT devices and for minimizing energy consumption in 5G networks. According to the proposed framework, the consumption of energy can be optimized in three ways: 1) optimal power with fix rate given 2) optimal rate with fixed power is given and 3) an optimal combination of both power and rate. The proposed scheme was tested using simulation, and results reveal that the proposed scheme provides significant energy saving.

According to [37], IoT helps to improve energy efficiency, reduce negative environmental impacts and increasing renewable energy share. This article generally provides a detailed survey on IoT applications in energy and particularly in smart grid context. Various IoT enabling technologies are discussed along with associated challenges and solutions. The provided survey is helpful for energy policymakers, managers, and owners to better understand the role of IoT in optimization of energy system.

It is obvious that IIoT and 5G are most powerful technologies of the digitized world that will reshape the near future [38], [39]. However, privacy preservation and energy optimization are the problems in IoT and 5G realm that need to be addressed to leverage the potential benefits of these technologies. Most of the existing studies discuss privacy issues and provide some best practices that need to be followed, but a detailed framework for privacy preservation is missing. On the other hand, energy optimization is another problem in 5G that need to be addressed, but there exist only a few studies that discuss energy problem in IIoT and 5G realm, and their main focus is on energy efficiency rather than optimization [39], [40]. At the same time, a few more recent studies are focusing to the user privacy issues linked with their daily lives [41]–[43], while at home, using 5G based gadgets and while travelling. To fill these two gaps; in the upcoming section, we will provide a framework to address the issues of privacy preservation, and energy optimization in 5G aided IIoT.

III. PRIVACY PROTECTION AND ENERGY RESOURCE OPTIMIZATION FRAMEWORK

In this section, we have provided a 4-layered framework for privacy preservation, and energy optimization in 5G aided IIoT context. Layer 1 is the application layer which includes CPS, IAA, RMA, RA, and SCA etc. it is the top most layer that uses 5G technologies provided by 5G embedded telecommunication layer. Layer2 is 5G embedded technological layer that consists of 5G technologies such as 5G routers, base stations etc. Layer 3 of the model is the energy optimization layer; this is the most important layer of the framework. This layer aims to maximize users' comfort by minimizing power consumption. This layer will enable efficient use of energy through load balancing, energy saving, making energy equipment active when required, energy prioritization and various other best practices. Layer 4 is the industry 4.0 layer which aims to completely automate the data exchange using IIoT and 5G technologies and thus creating a smart industry. These 4 layers are interconnected virtually and strengthen each other as shown in figure 8. Privacy preservation is considered at all four layers by implementing the best practices which include: anonymity, unlinkability, undetectability, unobservability, pseudonymity, location encryption, dummy locations, proper identity management and transmitting data at the rate which is less than the secrecy capacity. Various privacy and security icons between layers of the framework highlights the importance of privacy and its preservation during overall data transmission periods.

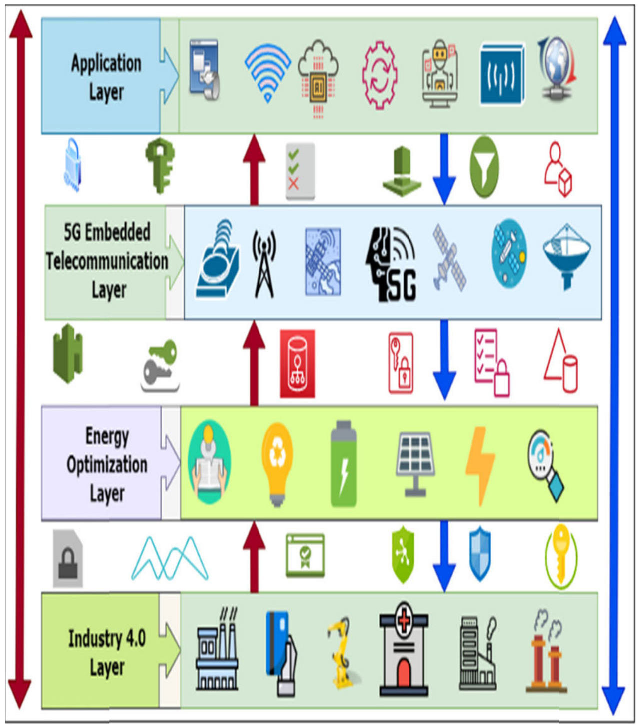


FIGURE 8. Proposed framework.

IV. FRAMEWORK EVALUATION

Industrial energy consumption is a major part of GDP globally. When it comes to 5G enabled industry 4.0, energy efficiency along with digitalization and production flexibility, become necessary to win. On the other hand, privacy preservation is inevitable for the success of any organization. Below we provide two separate mathematical models, one for privacy preservation and other for energy optimization in 5G aided IIoT.

A. MATHEMATICAL MODEL FOR PRIVACY PRESERVATION

This section will do the mathematical modeling of privacy preservation by using the symbols and notation mentioned in Table 1

$$P = f(x, y, z) \tag{2}$$

The objective function in our case will be privacy preservation that can be expressed mathematically as

$$\text{Objective function } \mathit{Maximize}\,(P) \tag{3}$$

where

$$x = f(Aa, Im) \tag{4}$$

According to equation 4, identity privacy is dependent on anonymous authentication and identity management.

If anonymous authentication and proper identity management are implemented, identity privacy preservation will be strong. There exists a proportional relationship between the dependent and independent variables as shown in equation 5

$$\therefore x \propto Aa \cap x \propto Im \quad (5)$$

Similarly

$$y = f\,(Ka, Le, Dl) \quad (6)$$

Equation 6 shows that location privacy is somehow dependent on implementing K-anonymity, location encryption and dummy location and there exist a proportional relationship between these variables as shown in equation 7

$$\therefore y \propto Ka \cap y \propto Le \cap y \propto Dl \quad (7)$$

In the same way

$$z = f\,(De, Dr, Dp_t) \quad (8)$$

According to equation 8, data privacy can be preserved through strong data encryption, transmitting data at the rate, which is less than the secrecy capacity and using strong data encryption techniques. Where

$$\therefore z \propto De \cap z \propto Dr \cap z \propto \frac{1}{Dp_t} \quad (9)$$

According to equation 9, data privacy is directly proportional to data encryption and data protection while it is inversely proportional to the data rate.

Let ρ_1, ρ_2, ρ_3 are the industry preferences for x, y *and* z then the comfort index of the user regarding privacy preservation will be

$$CI = \rho_1 1 - \left(\frac{e_1}{x_s}\right)^2 + \rho_2 1 - \left(\frac{e_2}{y_s}\right)^2 + \rho_3 1 - \left(\frac{e_3}{z_s}\right)^2 \quad (10)$$

where

$$\rho_1 + \rho_2 + \rho_3 = 1 \quad (11)$$

and e_1, e_2, e_3 are differences between optimized values of parameters and actual values of parameters

The variation in dependent variables x, y, z on the independent variable P can be calculated using the partial derivatives of equation one as shown below

$$f_x = \frac{\partial P}{\partial x} f\,(x, y, z) = P_x = \frac{\partial P}{\partial x} = D_x f \quad (12)$$

$$f_y = \frac{\partial P}{\partial y} f\,(x, y, z) = P_y = \frac{\partial P}{\partial y} = D_y f \quad (13)$$

$$f_z = \frac{\partial P}{\partial z} f\,(x, y, z) = P_z = \frac{\partial P}{\partial z} = D_z f \quad (14)$$

Equation 12-14 are the partial derivatives of equation 2. These equations provide an effect of change in independent variables on the dependent variable. To further illustrate our mathematical model, we have provided a privacy preservation algorithm below.

Proposed Algorithm 1 For Privacy Preservation

1. ***Begin***
2. *Set expected values for x, y and z as* x_i, y_i, z_i
3. *Set actual values for x, y and z as* X, Y and Z
4. ***if*** $X < x_i$
5. ***Then*** *Maximize* (Aa, Im)
6. ***else*** *if* $Y < y_i$
7. ***Then*** *Maximize* (Ka, La, Dl)
8. ***else*** *if* $Z < z_i$
9. ***then*** Max*imize* (De, Dpt) *and optimize* (Dr)
10. ***End if***
11. ***End***

Algorithm 1 compares the expected values and actual values for all identified parameters and compare them for any discrepancy. If the values of actual and expected parameters are same this means organizational privacy policy is strong. In case of variation between values of actual parameters and expected parameters, organization need to refine its policies by making changes in independent variables. Figure 9 shows the working of our algorithm.

According to figure 9, the organization set values for all three types of privacy, namely, identity privacy, location privacy and data privacy in the beginning. In case of any discrepancy in the set values, the organization need to optimize the corresponding values of independent variables.

B. MATHEMATICAL MODEL FOR ENERGY OPTIMIZATION

This section aimed to provide a mathematical model that will optimize energy in 5G context by following the symbols and notations mentioned in Table 1.

Energy consumption is usually a combination of active energy consumption and passive energy consumption, as shown in equation 15, where active energy consumption refers to the energy that is consumed during working hours. On the other hand, passive energy consumption refers to the energy that is consumed during non-working hours, e.g. holidays etc.

$$EC = AEC + PEC \quad (15)$$

where Objective Function is

$$Z = minimize\,(EC) \quad (16)$$

$$EC = f\,(X_1, X_2, X_3, X_4, X_5, X_6) \quad (17)$$

and

$$EC = \alpha_1 X_1 + \alpha_2 X_2 + \alpha_3 X_3 + \alpha_4 X_4 + \alpha_5 X_5 + \alpha_6 X_6 + \varepsilon \quad (18)$$

from the six variables identified in equation 18, we have to

$$Minimize\ \ (X_1, X_2, X_6) \quad (19)$$

$$Maximize\ \ (X_3) \quad (20)$$

$$Optimize\ \ (X_4, X_5) \quad (21)$$

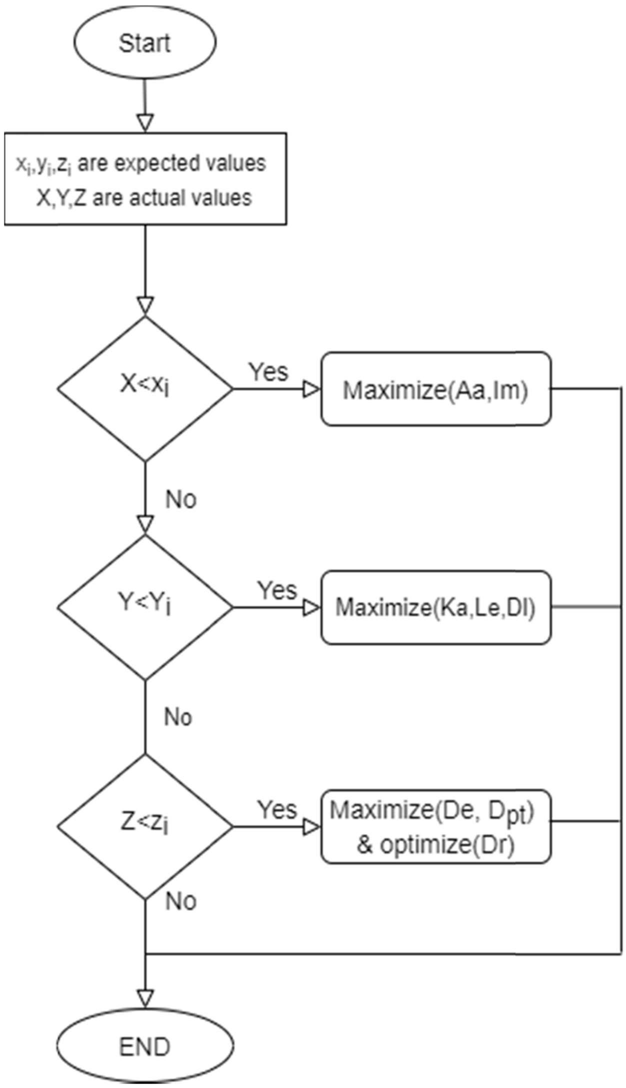


FIGURE 9. Privacy preservation flow chart.

According to equation 19, industry needs to minimize energy usage, latency and energy waste/leakages to get optimum energy results. On the other hand, improved spectrum efficiency will help in timely management and decision making and will accelerate the industry processes. While weather condition is somehow possible to control by prior prediction and to adopt suitable strategy according to that prediction. Working hours can also be optimized by taking maximum benefits from daylight working hours etc.

Hence, in our case

$X_1, X_2 \ldots X_6$ are decision variables.

Constraints

$$X_1 \leq ES \tag{22}$$

$$DV \approx X_3 \tag{23}$$

Suppose $p_1, p_2, p_3, p_4, p_5, p_6$ refers to a 4G industry preferences for $X_1, X_2, X_3, X_4, X_5, X_6$ then organizational comfort index regarding energy optimization will be

$$CI = p_1 1 - \left(\frac{e_1}{X_{1s}}\right)^2 + p_2 1 - \left(\frac{e_2}{X_{2s}}\right)^2 + p_3 1 - \left(\frac{e_3}{X_{3s}}\right)^2 + p_4 1 - \left(\frac{e_4}{X_{4s}}\right)^2 + p_5 1 - \left(\frac{e_5}{X_{5s}}\right)^2 + p_6 1 - \left(\frac{e_6}{X_{6s}}\right)^2 \tag{24}$$

where

$$p_1 + p_2 + p_3 + p_4 + p_5 + p_6 = 1 \tag{25}$$

According to proposed model

$$X_1 \propto X_6 \; and \; X_1 \propto X_4 \tag{26}$$

Equation 26 shows that energy usage is directly proportional to energy waste/leakages; this means when X_6 will increase X_1 will also increase. In the same way, energy usage is also proportional to working time which means that more time needs more energy resources to be consumed. Similarly

$$X_2 \propto \frac{1}{X_3} \; and \; X_3 \propto \frac{1}{X_5} \tag{27}$$

Equation 27, highlights that latency is inversely proportional to spectrum efficiency; if internet bandwidth is high, latency will be low. On the other hand, spectrum efficiency is inversely proportional to adverse weather condition, which means weather abnormalities will affect spectrum efficiency by creating distortion in 5G signals. In order to evaluate the individual effects of $X_1, X_2 \ldots X_6$ EC need to find the partial derivatives of equation 17 w.r.t. all six independent variables $X_1, X_2 \ldots X_6$ and these derivatives are shown in equation 28-33

$$f_{X_1} = \frac{\partial EC}{\partial X_1}(\alpha_1 X_1 + \alpha_2 X_2 + \alpha_3 X_3 + \alpha_4 X_4 + \alpha_5 X_5 + \alpha_6 X_6 + \varepsilon) = EC_{X_1} = \frac{\partial EC}{\partial X_1} = DX_1 \tag{28}$$

$$f_{X_2} = \frac{\partial EC}{\partial X_2}(\alpha_1 X_1 + \alpha_2 X_2 + \alpha_3 X_3 + \alpha_4 X_4 + \alpha_5 X_5 + \alpha_6 X_6 + \varepsilon) = EC_{X_2} = \frac{\partial EC}{\partial X_1} = DX_2 \tag{29}$$

$$f_{X_3} = \frac{\partial EC}{\partial X_3}(\alpha_1 X_1 + \alpha_2 X_2 + \alpha_3 X_3 + \alpha_4 X_4 + \alpha_5 X_5 + \alpha_6 X_6 + \varepsilon) = EC_{X_3} = \frac{\partial EC}{\partial X_1} = DX_3 \tag{30}$$

$$f_{X_4} = \frac{\partial EC}{\partial X_4}(\alpha_1 X_1 + \alpha_2 X_2 + \alpha_3 X_3 + \alpha_4 X_4 + \alpha_5 X_5 + \alpha_6 X_6 + \varepsilon) = EC_{X_4} = \frac{\partial EC}{\partial X_1} = DX_4 \tag{31}$$

$$f_{X_5} = \frac{\partial EC}{\partial X_5}(\alpha_1 X_1 + \alpha_2 X_2 + \alpha_3 X_3 + \alpha_4 X_4 + \alpha_5 X_5 + \alpha_6 X_6 + \varepsilon) = EC_{X_5} = \frac{\partial EC}{\partial X_1} = DX_5 \tag{32}$$

Proposed Algorithm 2 For Energy Optimization

1. ***Begin***
2. *Let* $P = \{P_1, P_2, P_3 \ldots\ldots P_n\}$ *is a set of processes in an industry*
3. ***For*** *all* P_i *if* $(p_1(X_1) \geq X_{1_s})$
4. ***Then*** *minimize* (X_6) *OR optimize* (X_4)
5. ***else if*** $(p_2(X_2) \geq X_{2_s})$
6. ***Then*** *improve* (X_3) *OR optimize* (X_5)
   else if $(p_3(X_3) \leq X_{3_s})$
7. *optimize* (X_5)
8. ***End if***
9. ***End***

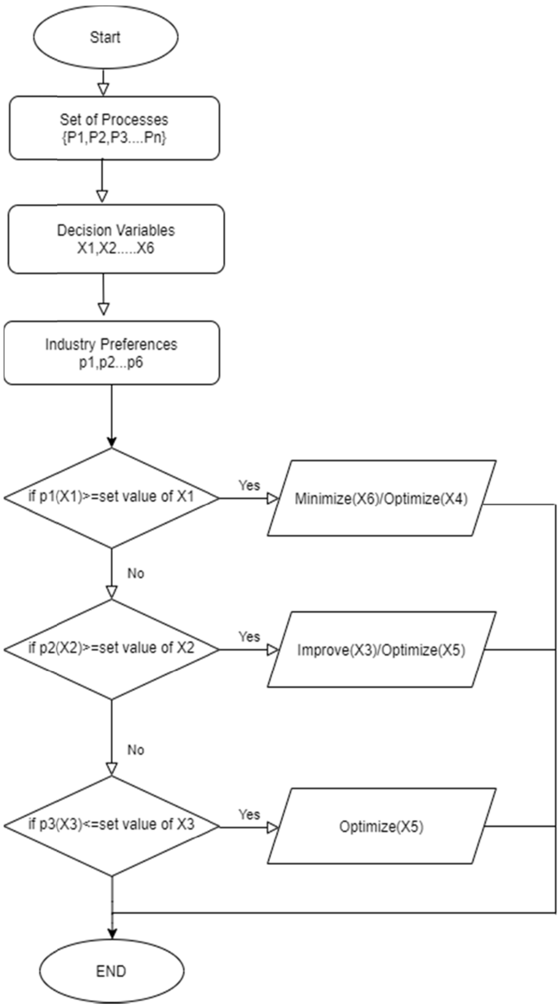


FIGURE 10. Energy optimization flow chart.

$$f_{X_6} = \frac{\partial EC}{\partial X_6}(\alpha_1 X_1 + \alpha_2 X_2 + \alpha_3 X_3 + \alpha_4 X_4 + \alpha_5 X_5 + \alpha_6 X_6 + \varepsilon) = EC_{X_6} = \frac{\partial EC}{\partial X_1} = DX_6 \quad (33)$$

The detailed working of the proposed model is shown in algorithm 2 and is also elaborated diagrammatically in Figure 10 According to Figure 10, the 5G aided IIoT based industry has a set of processes $P = \{P_1, P_2, P_3 \ldots .P_n\}$ these set of processes are executed according to organizational preferences. $X_1 \ldots X_6$ are decision variables that impact the energy level of the industry. The industry has its set preferences for each decision variable that is $p_1, p_2, p_3, p_4, p_5, p_6$ In the initial planning of the energy consumption/optimization, industry set its preferred values for all the decision variables that can be named as $X_{1s}, X_{2s}, X_{3s}, X_{4s}, X_{5s}, X_{6s}$ The industry compares its energy usage X_1 based on the reading it receives through smart meters and compare it with the set value of energy usage X_{1_s} If there is any discrepancy in the set value and the actual value of energy consumption, then it checks for energy waste/leakages X_6 and try to minimize it. If this is not the case, then it can modify working times to get benefits from sunlight and other renewable/natural sources of energy.

In the same way, if the latency is high as compared to the expected value, then industry need to improve spectrum efficiency or it may be caused by adverse weather effects. In such cases, the industry needs to find some alternatives such as prior weather forecasting might help in future planning. Similarly, if the spectrum efficiency is less than the expected value, it might also be due to adverse weather conditions. This problem can be addressed by taking proper measures on time.

C. CASE STUDY A (PRIVACY PRESERVATION)

ABC is an American based healthcare industry 4.0 which is using 5G services to improve its healthcare services. The industry is having a strong cyber-physical system consisting of massive interconnected IoT devices for performing various healthcare activities. Patients are monitored remotely through wearable IoT sensors, and privacy preservation is one of the important targets of this healthcare industry. The industry is using various best practices to address all three dimensions of privacy. Wearable sensors attached to patient's body monitor vital health parameters, and in case of any variation in actual parameters and set parameters, the values are sent to base station which is responsible for sending it to the caregiver so that timely action could be taken. Privacy of patients' data, location and identity is preserved using various techniques as mentioned below.

Patient identity is protected through anonymous authentication and by implementing proper identity management. The industry has given different privileges to its employee, and strict monitoring and control is implemented to assure the privacy of patients' data. In case of any privacy leakages, the identity management process is refined and monitored strictly. Patient location is also kept private through K-anonymity, location encryption and dummy location. Location encryption mechanism is strong and protected by using trusted security software. Patients' data privacy is preserved through strong encryption, applying data protection techniques and by sending data rate less than the expected secrecy capacity to avoid data breaches. The working of case study is shown in Figure 11.

The step-by-step working of ABC healthcare industry is shown below

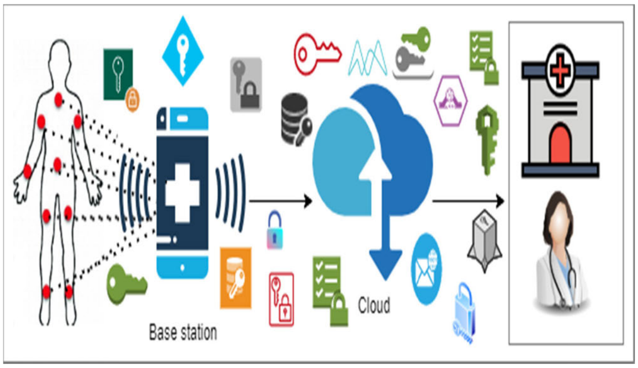


FIGURE 11. Case study a description.

1. Initialize the values of x, y, z and set preferred values for it
2. Identify the decision variables corresponding to x, y, z respectively
3. Calculate the partial derivative w.r.t. each decision variable to find the impact of change in decision variable on the corresponding privacy dimension
4. If there is any discrepancy in the actual and expected values of x, y, z then optimize decision variables as per the situation

D. CASE STUDY B (ENERGY OPTIMIZATION)

XYZ is a Japan based car manufacturing industry 4.0 which is using 5G services to accelerate its working. The company is having its own strong cyber physical system which include various smart machines. It is using modern control system (remote monitoring), and the whole system is automated using IIoT. All the products and the means of production are interconnected to achieve real-time optimization in terms of value creation and cost &, energy optimization. Information technology and operational technology is fully integrated at all levels starting from enterprise planning level to operation, production and up to field level.

The company is having a unified and fully digitalized operational platform which provides digital documentation instead of traditional blueprints. Data flow across the company through process chain and any modification in the data is also refreshed at other places. The digital documents are useful in building 3-D models and can also be used in training using virtual reality. An intelligent visualization platform helps in timely decision making. The whole development process starting from inception to construction is managed using a unified platform. XYZ Company is having a smart building, providing smart services, and is using smart DLC, as shown in figure 12. The company is using the latest IIoT technologies such as smart sensors, actuators, 5G enabled smart devices, smart meters, and various computing devices.

The company is using 4 types of energy resources to produce energy which include electricity, renewable energy, biofuels, and natural gas. Energy consumption is monitored through smart meters which calculate daily energy consumption. The steps used for energy consumptions and optimization are as follows

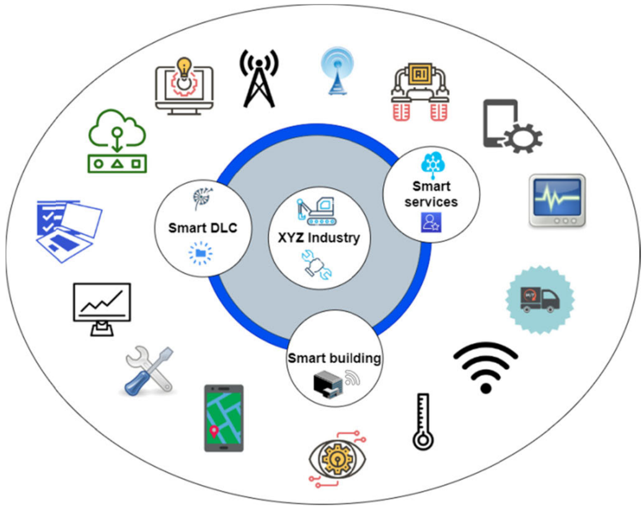


FIGURE 12. Conceptual working mechanism of XYZ industry 4.0.

1. Calculate daily energy usage/consumption which is equal to wattage multiplied by hours used per day and divide the answer by 1000 as shown in equation 34

$$DEC = \frac{w^*h}{1000} \tag{34}$$

   where DEC refers to daily energy consumption, w refers to energy wastage, and h refers to numbers of hours' energy is used
2. Calculate the monthly energy consumption by multiplying the daily energy usage with the number of days the devices are used as shown in equation 35

$$MEC = DEC^*D \tag{35}$$

   where MEC refers to monthly energy consumption, DEC refers to daily energy consumption while d refers to the number of days' energy is used
3. Multiply monthly energy consumption with the cost of energy as shown in equation 36

$$TEC = MEC^*Cost \tag{36}$$

4. Calculate energy waste by subtracting input power from output power as shown in equation 37

$$EW = IP - OP \tag{37}$$

   where EW refers to energy waste, IP is input power that is usually measured in AC and OP refers to output power that is measured in DC
5. Compare the calculated value with set values and take proper measures in case of discrepancies

The above discussion shows that the upcoming era is the 5G era in which most of the industries will be fully automated using 5G aided IIoT. It will provide huge benefits to the industry as well as the overall economy in terms of GDP growth. However, energy resources are limited, and there is a need to take maximum benefits from these resources through energy optimization. To do this, smart devices are there to calculate energy consumption and wastage. However, proper actions need to be taken to avoid energy waste. Various factors such as temperature, weather condition, latency, spectrum efficiency etc. impact energy usage in the industry. The need is to optimize energy consumption by minimizing the negative impacts of these factors and maximizing energy.

V. CONCLUSION AND FUTURE WORK

The objective of this research is to provide an optimal solution for privacy preservation, and energy optimization in 5G enabled IIoT based Industry 4.0. 5G has made a huge paradigm shift in almost every field of life. Industry 4.0 that is leveraging the potentials of IoT devices and 5G has now become a new industrial phenomenon. Industry 4.0 is using the concept of a smart building, smart services and small development lifecycle in which billions of devices will be interconnected. This massive interconnectivity of heterogeneous devices raises the issue of privacy that is one of the important users' concern. On the other hand, billions of interconnected devices and fast data transmission using the 5G network need many resources, and one of them is energy. To leverage the potential benefits from these massively interconnected devices, we need to improve the privacy as well as energy. To do this, we have provided a four-layered framework that will serve as a guide for Industry 4.0 researchers and practitioners in better understanding of the industry 4.0 infrastructure and the positive impact of privacy preservation and energy optimization. We have formulated a mathematical model to address the problem of privacy preservation and energy optimization quantitatively and also provided associated algorithms to elaborate the working of proposed models and framework. We have also provided two case studies to elaborate our framework/mathematical models and algorithms. In the future, we are planning to collect some real-world statistics from Industry4.0 for further analysis and validation of the proposed solution.

REFERENCES

[1] S. K. Tayyaba, H. A. Khattak, A. Almogren, M. A. Shah, I. Ud Din, I. Alkhalifa, and M. Guizani, "5G vehicular network resource management for improving radio access through machine learning," *IEEE Access*, vol. 8, pp. 6792–6800, 2020.

[2] M. Jaber, M. Ali Imran, R. Tafazolli, and A. Tukmanov, "5G backhaul challenges and emerging research directions: A survey," *IEEE Access*, vol. 4, pp. 1743–1766, 2016.

[3] F. Al-Turjman and S. Alturjman, "Context-sensitive access in industrial Internet of Things (IIoT) healthcare applications," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2736–2744, Jun. 2018.

[4] D. Kim, D., "A dynamic model for the evolution of the next generation Internet-implications for network policies': Towards a balanced perspective on the Internet's role in the 5G and industry 4.0 era," *Electron. Commerce Res. Appl.*, vol. 28, Mar./Apr. 2018, Art. no. 100966.

[5] S. Jacob, V. G. Menon, S. Joseph, V. P. G., A. Jolfaei, J. Lukose, and G. Raja, "A novel spectrum sharing scheme using dynamic long short-term memory with CP-OFDMA in 5G networks," *IEEE Trans. Cognit. Commun. Netw.*, vol. 6, no. 3, pp. 926–934, Sep. 2020.

[6] M. Abbasi, H. Rezaei, V. G. Menon, L. Qi, and M. R. Khosravi, "Enhancing the performance of flow classification in SDN-based intelligent vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, early access, Aug. 13, 2020, doi: 10.1109/TITS.2020.3014044.

[7] L. Z1hang, H. Zhao, S. Hou, Z. Zhao, H. Xu, X. Wu, Q. Wu, and R. Zhang, "A survey on 5G millimeter wave communications for UAV-assisted wireless networks," *IEEE Access*, vol. 7, pp. 117460–117504, 2019.

[8] W. Ejaz, A. Anpalagan, M. A. Imran, M. Jo, M. Naeem, S. B. Qaisar, W. Wang, "Internet of Things (IoT) in 5G wireless communications," *IEEE Access*, vol. 4, pp. 10310–10314, 2016.

[9] Y. Xu, M. Wang, H. Zhong, J. Cui, L. Liu, and V. N. L. Franqueira, "Verifiable public key encryption scheme with equality test in 5G networks," *IEEE Access*, vol. 5, pp. 12702–12713, 2017.

[10] X. Xu, X. Liu, Z. Xu, C. Wang, S. Wan, and X. Yang, "Joint optimization of resource utilization and load balance with privacy preservation for edge services in 5G networks," *Mobile Netw. Appl.*, vol. 25, pp. 713–724, Dec. 2019.

[11] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, "Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks," *IEEE Trans. Netw. Sci. Eng.*, early access, Aug. 28, 2019, doi: 10.1109/TNSE.2019.2937481.

[12] A. Zhang and X. Lin, "Security-aware and privacy-preserving D2D communications in 5G," *IEEE Netw.*, vol. 31, no. 4, pp. 70–77, Jul./Aug. 2017.

[13] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions," *IEEE Commun. Standards Mag.*, vol. 2, no. 1, pp. 36–43, Mar. 2018.

[14] M. Liyanage, J. Salo, A. Braeken, T. Kumar, S. Seneviratne, and M. Ylianttila, "5G privacy: Scenarios and solutions," in *Proc. IEEE 5G World Forum (5GWF)*, Jul. 2018, pp. 197–203.

[15] F. Al-Turjman and S. Alturjman, "5G/IoT-enabled UAVs for multimedia delivery in industry-oriented applications," *Multimedia Tools Appl.*, vol. 79, nos. 13–14, pp. 8627–8648, Apr. 2020.

[16] H. Park and Y. Lim, "Reinforcement learning for energy optimization with 5G communications in vehicular social networks," *Sensors*, vol. 20, no. 8, p. 2361, Apr. 2020.

[17] R. A. Abd-Alhameed and I. J. Elfergani Rodriguez, "Recent technical developments in energy-efficient 5G mobile cells: Present and future," *Electronics*, vol. 9, no. 4, p. 664, Apr. 2020, doi: 10.3390/electronics9040664.

[18] H. Hellaoui, M. Koudil, and A. Bouabdallah, "Energy efficiency in security of 5G-based IoT: An End-to-End adaptive approach," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6589–6602, Jul. 2020.

[19] C.-L. I, S. Han, and S. Bian, "Energy-efficient 5G for a greener future," *Nature Electron.*, vol. 3, no. 4, pp. 182–184, Apr. 2020.

[20] C. Bouras, P. Ntarzanos, and A. Papazois, "Cost modeling for SDN/NFV based mobile 5G networks," in *Proc. 8th Int. Congr. Ultra Modern Telecommun. Control Syst. Workshops (ICUMT)*, Oct. 2016, pp. 56–61.

[21] C. Bouras, S. Kokkalis, A. Kollia, and A. Papazois, "Techno-economic comparison of MIMO and DAS cost models in 5G networks," *Wireless Netw.*, vol. 26, no. 1, pp. 1–15, Jan. 2020.

[22] M. Humayun, N. Jhanjhi, B. Hamid, and G. Ahmed, "Emerging smart logistics and transportation using IoT and blockchain," *IEEE Internet Things Mag.*, vol. 3, no. 2, pp. 58–62, Jun. 2020.

[23] J. Cheng, W. Chen, F. Tao, and C.-L. Lin, "Industrial IoT in 5G environment towards smart manufacturing," *J. Ind. Inf. Integr.*, vol. 10, pp. 10–19, Jun. 2018.

[24] S. K. Rao and R. Prasad, "Impact of 5G technologies on industry 4.0," *Wireless Pers. Commun.*, vol. 100, no. 1, pp. 145–159, May 2018.

[25] H. N. Rafsanjani and A. Ghahramani, "Towards utilizing Internet of Things (IoT) devices for understanding individual occupants' energy usage of personal and shared appliances in office buildings," *J. Building Eng.*, vol. 27, Jan. 2020, Art. no. 100948.

[26] V. Marinakis and H. Doukas, "An advanced IoT-based system for intelligent energy management in buildings," *Sensors*, vol. 18, no. 2, p. 610, Feb. 2018.

[27] G. Bedi, G. K. Venayagamoorthy, R. Singh, R. R. Brooks, and K.-C. Wang, "Review of Internet of Things (IoT) in electric power and energy systems," *IEEE Internet hings J.*, vol. 5, no. 2, pp. 847–870, Apr. 2018.

[28] R. Khan, P. Kumar, D. Nalin K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 196–248, 1st Quart., 2020.

[29] T. Kumar, M. Liyanage, I. Ahmad, A. Braeken, and M. Ylianttila, "User privacy, identity and trust in 5G," in *A Comprehensive Guide to 5G Security*. Hoboken, NJ, USA: Wiley, 2018, pp. 267–279.

[30] J. Cao, "CPPHA: Capability-based privacy-protection handover authentication mechanism for SDN-based 5G HetNets," *IEEE Trans. Dielectr. Electr. Insul.*, early access, May 14, 2019, doi: 10.1109/TDSC.2019.2916593.

[31] *Top Uses of 5G in the Energy Sector*. Accessed: Sep. 2020. [Online]. Available: https://www.intellias.com/top-uses-of-5g-in-the-energy-sector/

[32] S. Li, Q. Ni, Y. Sun, G. Min, and S. Al-Rubaye, "Energy-efficient resource allocation for industrial cyber-physical IoT systems in 5G era," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2618–2628, Jun. 2018.

[33] B. S. Awoyemi, A. S. Alfa, and B. T. Maharaj, "Resource optimisation in 5G and Internet-of-Things networking," *Wireless Pers. Commun.*, vol. 111, pp. 2671–2702, Jan. 2020.

[34] Yang, S., "A joint optimization scheme for task offloading and resource allocation based on edge computing in 5G communication networks," Computer Communications, 2020.

[35] X. Liu and X. Zhang, "Rate and energy efficiency improvements for 5G-based IoT with simultaneous transfer," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 5971–5980, Aug. 2019.

[36] B. Al Homssi, A. Al-Hourani, K. G. Chavez, S. Chandrasekharan, and S. Kandeepan, "Energy-efficient IoT for 5G: A framework for adaptive power and rate control," in *Proc. 12th Int. Conf. Signal Process. Commun. Syst. (ICSPCS)*, Dec. 2018, pp. 1–6.

[37] N. Hossein Motlagh, M. Mohammadrezaei, J. Hunt, and B. Zakeri, "Internet of Things (IoT) and the energy sector," *Energies*, vol. 13, no. 2, p. 494, Jan. 2020.

[38] H. Zhang, M. Babar, M. U. Tariq, M. A. Jan, V. G. Menon, and X. Li, "SafeCity: Toward safe and secured data management design for IoT-enabled smart city planning," *IEEE Access*, vol. 8, pp. 145256–145267, 2020.

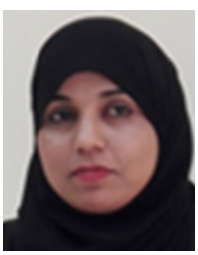
[39] S. Jacob, V. G. Menon, P. G. Shynu, S. K. S. Fathima, B. Mahapatra, and S. Joseph, "Bidirectional multi-tier cognitive swarm drone 5G network," in *Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Jul. 2020, pp. 1219–1224.

[40] M. Abbasi, A. Shokrollahi, M. R. Khosravi, and V. G. Menon, "High-performance flow classification using hybrid clusters in software defined mobile edge computing," *Comput. Commun.*, vol. 160, pp. 643–660, Jul. 2020.

[41] Z. A. Almusaylim, N. Zaman, and L. T. Jung, "Proposing a data privacy aware protocol for roadside accident video reporting service using 5G in vehicular cloud networks environment," in *Proc. 4th Int. Conf. Comput. Inf. Sci. (ICCOINS)*, Kuala Lumpur, Aug. 2018, pp. 1–5, doi: 10.1109/ICCOINS.2018.8510588.

[42] M. Saleh, N. Jhanjhi, A. Abdullah, and Fatima-tuz-Zahra, "Proposing a privacy protection model in case of civilian drone," in *Proc. 22nd Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2020, pp. 596–602, doi: 10.23919/ICACT48636.2020.9061508.

[43] Z. A. Almusaylim and N. Jhanjhi, "Comprehensive review: Privacy protection of user in location-aware services of mobile cloud computing," *Wireless Pers. Commun.*, vol. 111, no. 1, pp. 541–564, Mar. 2020, doi: 10.1007/s11277-019-06872-3.



MAMOONA HUMAYUN received the Ph.D. degree in computer architecture from the Harbin Institute of Technology, China. She has 12 years of teaching and administrative experience internationally. She is currently an active reviewer for a series of journals. She has supervised various master's and Ph.D. thesis. Her research interests include global software development, requirement engineering, knowledge management, cyber security, blockchain, the Internet of Things, healthcare security, and wireless sensor networks.

NZ JHANJHI received the Ph.D. degree in IT from Universiti Teknologi Petronas (UTP), Malaysia. He has 20 years of teaching and administrative experience internationally. He has an intensive background of academic quality accreditation in higher education related to ABET. He is currently an Associate Editor and an Editorial Assistant Board for several reputable journals, including IEEE ACCESS, the TPC Member for several IEEE conferences around the globe, and an active reviewer for a series of Q1 journals. He has authored several research articles in ISI indexed and impact factor research journals/IEEE international conferences, edited nine books in international reputed computer science area books, supervised a great number of postgraduate students, and an external thesis examiner to his credit. He has successfully completed more than 19 international funded research grants. He also served as a Keynote speaker for several conferences around the globe. He also chaired international conference sessions and presented session talks internationally. He has strong analytical, problem solving, interpersonal, and communication skills. His research interests include cyber security, wireless sensor networks (WSNs), the Internet of Things (IoT), mobile application development, *ad hoc* networks, cloud computing, big data, data sciences, and software engineering.

MADALLAH ALRUWAILI received the bachelor's degree (Hons.) from Jouf University, Sakakah, Saudi Arabia, in 2005, the M.S. degree from the University of Science Malaysia, in 2009, and the Ph.D. degree from Southern Illinois University, Carbondale, IL, USA, in 2015. His Ph.D. dissertation entitled enhancement and restoration of dust images. He is currently an Assistant Professor of Computer Engineering and Networks with Jouf University. He is also the Dean of the College of Computer and Information Sciences. His research interests include image processing, image quality analysis, pattern recognition, computer vision, and biomedical imaging.

SAGAYA SABESTINAL AMALATHAS has vast knowledge in big data analytics, business intelligence, and various disciplines of artificial intelligence. She has hands on experience in developing data analytics solution for various domains, including education, agriculture, telecommunication, and medical analytics. She also supervises research at the Ph.D. and master's levels in the area of big data analytics, business intelligence, and the Internet of Things (IoT).

VENKI BALASUBRAMANIAN (Member, IEEE) received the Ph.D. degree in body area wireless sensor network (BAWSN) for remote healthcare monitoring applications. He is the Pioneer in building (pilot) remote healthcare monitoring application (rHMA) for pregnant women at the New South Wales Healthcare Department. His research establishes a dependability measure to evaluate rHMA that uses BAWSN. His research opens up a new research area in measuring time-critical applications. He contributed immensely to eResearch, software research and development that uses cloud-based infrastructure. He is also a Core Member for the project sponsored by the Nectar Australian Research Cloud Provider. He contributed heavily in the field of healthcare informatics, sensor networks, and cloud computing. He also founded Anidra Tech Ventures Pty Ltd., a smart remote patient monitoring company.

BUVANA SELVARAJ received the master's degree in software science from Periyar University, India. She is currently an Academician with the School of Information Technology and Engineering, Melbourne Institute of Technology, Australia. Her research interests include Android programming, software engineering, and the Internet of Things (IoT).