IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

Bio-Inspired Network Security for 5G-enabled IoT Applications

Kashif Saleem[1], Ghadah Alabduljabbar[2,3], Nouf Alrowais[2,3], Jalal Al-Muhtadi[1,2], Member, IEEE, Muhammad Imran[4], Member, IEEE, and Joel J. P. C. Rodrigues[1,5,6], Fellow, IEEE

[1]Center of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh, 12372, Saudi Arabia
[2]College of Computer and Information Sciences (CCIS), King Saud University, Riyadh, 11653, Saudi Arabia
[3]King Abdulaziz City for Science and Technology (KACST), Riyadh, Saudi Arabia
[4]College of Applied Computer Science, King Saud University, Riyadh, Saudi Arabia
[5]Federal University of Piauí (UFPI), Teresina-PI, Brazil
[6]Instituto de Telecomunicações, Portugal

Corresponding author: Kashif Saleem (e-mail: ksaleem@ksu.edu.sa).

The authors extend their appreciation to the Deputyship for Research and Innovation, "Ministry of Education" in Saudi Arabia for funding this research work through Project no. (IFKSURP-109).

ABSTRACT Every IPv6-enabled device connected and communicating over the Internet forms the Internet of things (IoT) that is prevalent in society and is used in daily life. This IoT platform will quickly grow to be populated with billions or more objects by making every electrical appliance, car, and even items of furniture smart and connected. The 5th generation (5G) and beyond networks will further boost these IoT systems. The massive utilization of these systems over gigabits per second generates numerous issues. Owing to the huge complexity in large-scale deployment of IoT, data privacy and security are the most prominent challenges, especially for critical applications such as Industry 4.0, e-healthcare, and military. Threat agents persistently strive to find new vulnerabilities and exploit them. Therefore, including promising security measures to support the running systems, not to harm or collapse them, is essential. Nature-inspired algorithms have the capability to provide autonomous and sustainable defense and healing mechanisms. This paper first surveys the 5G network layer security for IoT applications and lists the network layer security vulnerabilities and requirements in wireless sensor networks, IoT, and 5G-enabled IoT. Second, a detailed literature review is conducted with the current network layer security methods and the bio-inspired techniques for IoT applications exchanging data packets over 5G. Finally, the bio-inspired algorithms are analyzed in the context of providing a secure network layer for IoT applications connected over 5G and beyond networks.

INDEX TERMS 5th Generation Network; Artificial Intelligence; Biological; Internet of Things; Network layer; Security; Wireless Sensor Networks;

I. INTRODUCTION

With rapid global development, new applications and technologies emerge to meet ever-increasing needs. Technologies have an important effect on personal interactions, governments, and businesses. The Internet of Things (IoT) is a computing paradigm that has a major role in modern data communication, mobility, and monitoring technologies [1]. IoT enables everyday objects to connect with the Internet and communicate with each other. By using IoT, a huge number of devices and applications can be interoperable [2]. Over time, IoT requires new performance criteria such as large-scale connectivity, security, ultra-reliability, and throughput [3]. To meet these requirements, the evolving 5G technology is expected to provide a new platform for IoT applications and to handle IoT system requirements. 5G technologies aim to provide a high data rate, extensive coverage, efficient capability of networking, and improved quality of service [4]. In supporting IoT, 5G plays a vital role in connecting and facilitating communication of the massive number of objects over the Internet [5].

According to a 2018 McNamee report, IoT faces security concerns due to its rapid growth and evolution [6, 7]. Although security is the most important challenge for IoT system and with the evolution of 5G and beyond [8], other enormous challenges need to be addressed to provide an

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3046325, IEEE Access

interoperable and reliable architecture for the data packet exchange between heterogeneous devices in a 5G environment. According to [9, 10], several factors multiply the security issues in 5G networks, including the IP-based open architecture, the diversity of the underlying access network technologies, the huge number of interconnected mobiles, the dynamic heterogeneity device types, and the cloud, which uses information exchange and data preprocessing [9, 11].

IoT data routing security over 5G is the biggest challenge that must be addressed before the massive utilization of IoT. The large number of users and the data transfer speed over gigabits per second in 5G leads to a high number of threats in transferring malicious files [5]. Before the formal use of these IoT systems over 5G that are meant to transfer enormous data every minute, 5G must ensure data reliability and security [12-14]. Billions of IoT entities communicating over 5G make the system vulnerable and opens for attackers to launch denial-of-service (DoS) or man-in-the-middle (MITM) attacks [3]. Furthermore, 5G and beyond networks change the way of transmitting data by the significant reduction in latency that requires massive updates in network protocols security meant for 4G networks to protect data routing between IoT devices over 5G networks. Figure 1 present the threat landscape at the network layer 5G enabled IoT applications [15-19].

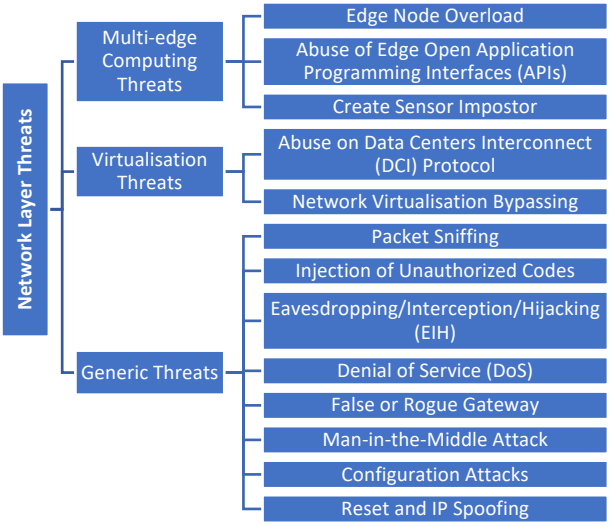

FIGURE 1. Threats on the Network Layer of 5G enabled IoT Applications.

The challenges encountered by IoT applications increase the need for new algorithms that are able to provide efficient data routing. The authors in [4] conducted a comparative study between bio-inspired and classical solutions to address IoT challenges and found bio-inspired techniques promising. These bio-inspired algorithms are rare because to build these solutions, a researcher needs to have a detailed background in the relevant biology field. Bio-inspired solutions can solve complex problems in a reliable manner and with high accuracy; such solutions include ant-colony optimization, artificial immune systems, swarm optimization, bee-colony optimization, and genetic algorithms. These intelligent algorithms use techniques that mimic the behavior of biological organisms to solve computer science problems. In particular, in computer network security, the word "virus" was adapted from life sciences to emphasize their similar behavior [20, 21].

Several published studies have dealt with IoT challenges for 5G using biologically inspired algorithms. These studies focus on various aspects such as flexibility, reliability, mobility, scalability, and availability. However, very few studies concentrate on data routing security in 5G networks. Many cybersecurity projects can gain from implementing diverse nature-inspired solutions such as genetic algorithms, increasing the prevention of cybercrime [22]. Furthermore, the use of genetic algorithms can help in detecting cyberattacks and anomalies [22].

The performance improvement for 5G networks attained by the Autonomous Distributed Mobile Management Entity solves selection problems. The bio-inspired solution is based on the attractor-selection mechanism in the biological systems gene expression; a computer simulation shows the solution's positive effect in the system performance, load distribution, decreasing overhead, and achieving load balance [23]. Other research targets the IoT communications in 5G networks by developing a bio-inspired resource allocation scheme that considers a group of users who share similar social characteristics including their relationship and behavior using a cellular automaton-based model in which the best features of the biological systems are imitated; this process simplifies the complexity in the large-size sliced network and support resource allocation optimization [24]. A new bio-inspired solution based on the genetic algorithm is designed to solve the Physical Cell Identifier configuration problems in 5G ultra-dense networks; the new algorithm is automated, efficient, and has computationally feasible time [25]. In addition to a highly efficient and reliable platform designed for 5G mobile communication, the platform based on the bacterial communication concept mimics three bacterial behaviors, namely, perception, infection, and diffusion [26].

The recent literature indicates that the nature-inspired algorithms provide better outcomes compared with traditional ones when facing IoT challenges. From 2010 to 2018, approximately 75% of bio-inspired studies focused on gateway problems in IoT applications, and 20% focused on interoperability challenges. By contrast, essential and important IoT challenges need to be studied such as security, privacy, reliability, flexibility, and mobility [4]. Therefore, more research should focus on these aspects using nature-inspired solutions. Given that few studies concentrate on the security aspect, this paper focuses on bio-inspired network

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3046325, IEEE Access

security in 5G networks for IoT applications.

The main contributions of this paper are as follows.

i. Thoroughly investigates the security of 5G-enabled IoT applications to discover the main challenges and solutions.

ii. Describes and reiterates the security vulnerabilities and requirements for WSNs, IoT, and 5G-enabled IoT applications.

iii. The viability of bio-inspired approaches is reviewed and analyzed for security of 5G-enabled IoT applications.

Section II provides an IoT application scenario of data routing in 5G networks, then discusses the security requirements and loopholes in IoT technology, and explores network layer security issues in IoT–5G systems. Section III reviews current approaches to provide network security in 5G-enabled IoT applications. Section IV studies the bio-inspired techniques that can address the network security issues in 5G-enabled IoT applications. Section V demonstrates the analysis of bio-inspired network security algorithms for 5G-enabled IoT applications. Section VI concludes.

II. SECURITY REQUIREMENTS IN THE NETWORK LAYER OF IoT OVER 5G

IoT has a significant role in several important fields such as education, healthcare, business, transportation, and agriculture, as shown in Fig. 1 [27]. Therefore, addressing and analyzing network layer security issues in IoT applications is critically important, helping developers and corporations to design and propose appropriate solutions to provide the most reliable IoT-based services. A mobile gateway-based remote eHealthcare solution was given in [28] that acts as a router for the Body Sensor Network (BSN). The body sensors autonomously collect vital sign data such as patient location using GPS sensor, heart rate using optical heart rate sensor, and possible fall detection using accelerometer sensor. The data are sent in real-time to the intelligent personal assistants (IPAs) platform called AMBRO (storage side) for further analysis and appropriate actions in case of emergency. Therefore, in the given scenario, data routing security is an essential requirement to protect sensitive information against malicious behavior. To secure the data routing security between BSN and AMBRO, authors in [29] propose using ECG based Multiple Fiducial-points based Binary Sequence Generation (MFBSG) algorithm for data encryption.

The security architectures for previous generations (3G [30] and 4G [31]) are not adequate for 5G because of the security challenges that originated in 5G technologies. Therefore, researchers in [32] presented a security architecture for 5G networks that consider the dynamic environment, new services, and technologies in 5G. The architecture is divided into four main components: domains, strata, security realms, and security control classes. First, domains are the core of 5G security architecture and represent a set of network physical and logical entities, various services, and different functionalities in 5G. Then, the strata offer a high-level view of data, protocol, and functions related to domain services. Next is the security realm (SR). Unlike the previous two components at a high abstraction level, SR is the main tool in 5G security architecture that captures all security threats from strata and domains by focusing on security assessment for different network functionality and areas. The relevant security realms for 5G networks are access network, core network, and management SRs. Some of the security requirements under the access network security realm are data storage protection, false selection detection, illegitimate data injection prevention, and radio control message protection. In the core network security realm, the requirements are authentication, authorization, privacy protection, secure mobility, key distribution, and algorithm negotiations. The security requirements for the management security realm are access monitoring and management, secure orchestrations, and key management. The final component is the Security Control Classes, which provides a set of needed security functions and mechanisms [32].

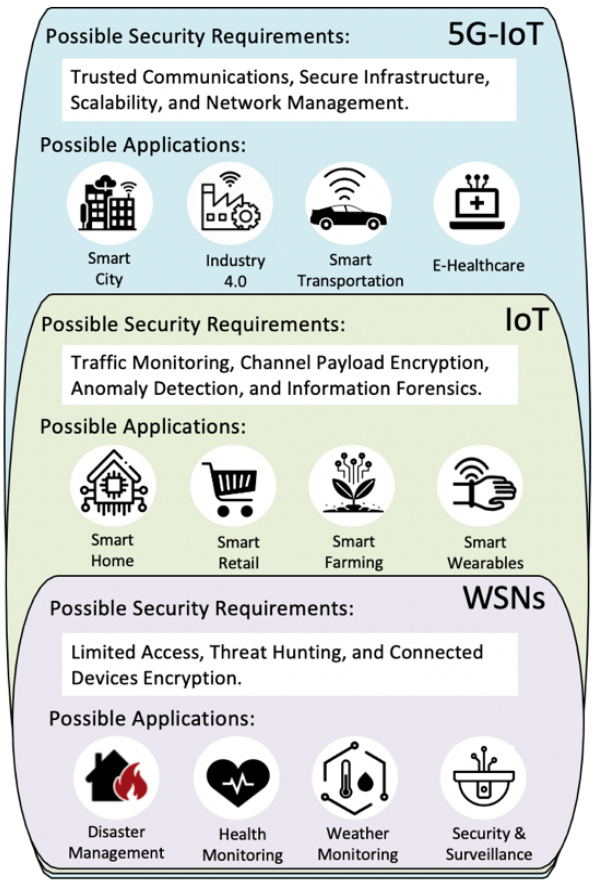

FIGURE 2. WSN, IoT, and 5G–IoT Applications with Security Requirements.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3046325, IEEE Access

With the advancement in IoT services and 5G technologies, studying the security requirements and accordingly addressing the vulnerabilities in IoT applications are important. The security requirements and loopholes based on IoT architecture layers (Application, Network, and Edge layers) are classified in [33]. The application layer provides a range of services and functions, usually performing functionalities using APIs in which mostly the least level of security is enabled. Moreover, current IoT devices by default trust the third-party service providers that are found to have potential flaws, such as weak authentication and misbehaving service. Thus, the application layer required to include a secure API, application verification, and information forensics. Next, the network layer maintains data transmission and supports IoT applications in collecting massive amounts of data. Therefore, the network layer requires on the security side, at minimum, traffic monitoring, channel encryption, anomaly detection, and traffic shaping. On the edge layer that is related to performing the interaction between the IoT environment and end-point devices, it requires at least authentication, limited access, threat hunting, and data encryption. The generated data from the edge are valuable, critical, and sensitive.

Thus, confidential data should be protected and can only be accessed by authorized persons. Moreover, one of the edge layer applications is the wireless sensor network (WSN) that includes a set of sensor nodes that is controlled and managed by a coordinator [34]. WSN is an enabler of technology and one of the main components in IoT environments [35]. Figure 2 shows a graphical abstract of possible applications and security requirements of WSN, IoT, and 5G–IoT systems. The research community recently began to notice the enormous security issues that arise with the integration of IoT-based systems and 5G networks and its massive effects on global data communication [36].

5G-based IoT systems bring extensive improvements in several critical domains such as security monitoring, mHealth care systems, traffic safety, and e-Banking [36], as shown in Fig. 1. Therefore, applying extreme levels of security is essential to avoid problems and provide reliable data routing. Crucial security issues in 5G include DoS and distributed denial of service (DDoS) attacks caused by the massive number of connected devices; these attacks are the result of vulnerabilities on both sides of the system, namely, the infrastructure and the edge devices [36]. In addition, the high diversity of IoT devices, functionalities, and routing protocols that can lead to security issues need to be addressed by using authentication mechanism such as cryptographic algorithms, considering the computational overhead that accompanies it and attempting to find a balance between robustness, performance, and efficiency [33].

Generally, data attacks can be made by unauthorized access to data in a repository or attacking this data while in transit by launching on data routing using eavesdropping, message modification, MITM, authentication, and replay attacks [5]. The assurance of data packets' security and privacy will always be a key issue for 5G–IoT systems until it is given full consideration at every step, mainly in the development stage [37]. In addition to common concerns that involve device access control, authentication, authorization, and privacy preservation, new issues are recently highlighted, such as the building of trusted communications over 5G networks with early threat detection and quick response mechanisms [37]. Mainly, known or even zero knowledge-based threats can be addressed by designing a scalable security architecture and a highly energy-efficient security solution that can handle billions of resource-constrained devices [38]. Table 1 summarizes the security requirements and vulnerabilities of network layers in WSN, IoT, and 5G–IoT systems.

TABLE I
NETWORK LAYER VULNERABILITIES AND SECURITY REQUIREMENTS

	Vulnerabilities	Security Requirements
WSN [33, 39-42]	Weak physical security, Insecure interfaces, Spoofing attack, Deprivation attack, Insufficient energy harvesting.	Limited authorized access, Threat hunting, Mobile Application Framework (MAF) authentication, Connected devices encryption.
IoT [33, 43-47]	Weak programming practices, Inadequate authentication, Insecure interfaces, Software and OS misconfiguration, Algorithm computational overhead, Privacy violation on the cloud, Buffer overflow, Replay attack, RPL routing attack.	Traffic monitoring, Channel payload encryption, Anomaly detection, Traffic shaping, Secure API, Application verification, Information forensics.
5GIoT [37, 38, 48-52]	Several attacks (DoS, MITM, Sybil, Flooding, and Jamming), Misconfiguration, Hacking, Data manipulation, Node subversion, Node failure and outage, Message corruption, Managing massive number devices, Interruption interception.	Trusted communication over 5G networks, Flexible and scalable security architecture, Energy-efficient security, Secure infrastructure, Scalability, Hardware and software security, Network management.

III. CURRENT 5G NETWORK SECURITY APPROACHES FOR IOT APPLICATIONS AND THE CHALLENGES THEREOF

The network layer security and privacy is the most critical aspect that needs to be addressed with the development of 5G–IoT systems. This advancement affects users' social trust, personal safety, and confidence [52]. Recently, some

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3046325, IEEE Access

of the research has attempted to address the issues by introducing different approaches to leverage network layer security and the protection of consumer privacy.

A service-oriented authentication framework that supports network slicing in 5G–IoT systems (ES^3A) is given in [53]. Network slicing allows the network core infrastructure to share resources efficiently across different services by using the privacy-preserving slice selection mechanism that enables anonymous access to IoT services by users, without exposing slice/service types. Moreover, to guarantee secure access to service data, a three-party session key negotiation mechanism was introduced among IoT servers, local fog nodes, and end-users. However, the given authentication framework is lacking in a proper design of the security algorithm and a valid simulated result that is required to build secure communication between end-users and IoT servers.

Authors in [54] focused on the IoT edge devices communication security in 5G networks. They propose techniques using crowdsourcing in that a reward is given to participants for their participation to mitigate security threats and cyberattacks in 5G networks. All sharing is at high speed due to 5G-amplified power. The authors presented a set of use cases, such as sharing information on attacks and known vulnerabilities among service providers and malware information and sharing platform where organizations can share critical information related to recent attacks and threats that allows the development of countermeasures and the implementation of the digital witness concept. However, concerns arise on how IoT devices will adapt to the resource sharing of network slicing, which is a major aspect of 5G networks. Additionally, using the crowdsourcing technique in some cases is not feasible, especially when privacy and trust need to be considered.

In [55], the authors propose a new control strategy by using statistical channel state information to investigate intelligent secure communication for IoT networks. This strategy is based on Q-learning. This learning uses game theory, in which the transmit power of the sender changed according to the attack mode, and the attacker changes their mode according to the current transmit power. Then, the sender adjusts the transmit power based on the current attacker mode to prevent attacks. Afterward, the best strategy is learned by using Q-function that uses Q-function that uses statistical information of the sender and attacker to obtain the optimal value of transmitter power.

The authors in [56] protect 5G–IoT technologies by an encryption method. This method involves a block cipher technique by using s-box. This mechanism is constructed by using features of quantum walks. S-box is based on one-dimensional one-particle quantum walks on circle 1D1PQWs. The authors in [56] found that the quantum walk features were not used to encrypt videos. Thus, the s-box mechanism is used to encrypt videos and other sensitive data before sending over 5G networks. The data are encrypted with the key sequence generated from controlled alternate quantum walks (CAQWs) that is a two-dimensional single walker and is controlled by a binary string with the keys used to substitute the original and then permutate the generated by using s-box.

In [57], a secure and efficient routing system between nodes in Cloud-MANET-IoT integrated framework used mobile ad hoc network (MANET) to construct a network between neighbor devices without using a centralized point. The IoT devices can interact with each other using MANET and is able to communicate to share information. One of the MANET smart devices should be tied to a Wi-Fi network and independently enrolled on the cloud. Accordingly, the cloud provider will provide its services to the MANET device/network in real time. Communicating with the cloud over 5G offers efficient connectivity with smart devices; on the other end, smart devices are able to submit required data on the cloud for the complete session. The approach specifically addresses the security issues that arise because of the ubiquity, the increase in cloud consumption, and cloud performance.

Given that complex security could lower the lifetime of IoT, the authors in [58] propose an D2D communication system is designed based on lightweight cryptography. The adaption is first done at the D2D token generation step. Second, by using 5G-AKA the SUSI is verified. Furthermore, the gNB avails the outcome and based on that generates D2D token. This D2D token is then transmitted to the UE that requests for token. The approach helps in increasing the security of 5G–IoT while maintaining energy consumption.

TABLE II
BIO-INSPIRED NETWORK SECURITY MECHANISMS COMPARISON

	Methods Utilized	Performance Evaluation
[53]	privacy-preserving slice selection mechanism	theoretical and simulation analysis in terms of computational and communication overheads
[54]	Crowdsourcing mechanism	OMNET+ + in terms VoIP service
[55]	Q-learning	Simulation results obtained based on game theory and in terms of eavesdropping rate, jamming rate and spoofing rate
[56]	s-box based encryption method with key sequence generated from controlled alternate quantum walks (CAQWs)	MATLAB software R2017a to simulate the evolution of 1D1PQWs in terms of nonlinearity, bit independence (BIC), strict avalanche (SAC), linear (LP) and differential (DP)
[57]	Cloud-MANET-IoT framework	Simulated and analyzed in terms of Data Transmission
[58]	elliptic curve cryptography (ECC) and lightweight authenticated encryption	Simulated in terms of processing time and energy consumption. Perform security analysis theoretically

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3046325, IEEE Access

IV. BIO-INSPIRED TECHNIQUES TO ADDRESS 5G NETWORK LAYER SECURITY FOR IOT APPLICATIONS

Bio-inspired cybersecurity plays a very important role and provides promising mechanisms in securing the network layer from different threats [21]. Acquiring and enhancing these bio-inspired mechanisms for securing 5G–IoT is a vital requirement. The cybersecurity infrastructure has many limitations, such as the absence of self-awareness, lack of interactions between network devices, and the absence of self-correcting mechanisms [59]. Thus, bio-inspired intelligent algorithms that can handle these limitations in cyberspace are needed [21], as is supporting networks and communications systems to protect against attacks, cybercriminals, hackers, and anomalies efficiently.

Biologically inspired systems have many appealing characteristics, such as adapting to various environmental conditions and self-resiliency toward damages [59]. Thus, defense algorithms that are inspired by natural organisms can be effective to deal with complexities in cybersecurity. Some examples of cybersecurity technologies that include bio-inspired techniques are anti-virus, honeypots, attribution, intrusion detection, counterattacks, and threat behavior analysis [21]. Several studies have contributed to the improvement of cybersecurity using bio-inspired techniques for communications and networking systems.

In [60], authors developed a distributed, self-organized, honeybee-inspired algorithm for early anomaly detection in a connected system over a wireless network. The algorithm is derived by observing the colonies of honeybees and imitates the way that honeybees use to forage efficiently. Similarly, the participants defined the target (resources such as computer networks) and encountered them based on decision making and information extraction methods to detect and mitigate attacks such as SYN flooding attacks. The proposed approach uses a distributed coordination framework (DIAMoN) to dynamically and automatically detect distributed attacks using a feedback mechanism. Even though they succeeded in mitigating the attacks by improving the early intrusion detection, the limitation of this approach is it does not support the scalability and the heterogeneity that comes with 5G–IoT systems.

With the fast development of WSNs, studies used intelligent features to handle security issues. For example, in [61], the authors focused on the routing where the attacker can easily perform sniffing, tamper with the data, induce path loss, or overtake all over the network. They proposed a trust routing algorithm (BiTRS) inspired by ant colony activities to prevent and detect attacks without interrupting the data routing between network devices. The proposed algorithm adapts the ant colony optimizations (ACO) and the physarum autonomic optimization (PAO) to handle the dynamical node changes in the network. Every node in the network will define the target node route. Then, all neighbor node behavior is monitored to gather trust-based information and send it as feedback for trust assessment. The proposed algorithm provided a solution for addressing routing problems while combining the features of ACO and PAO. However, it does not consider energy conservation, which is a crucial part of IoT.

A new approach proposed by the authors in [62] was named Bio-Inspired Secure IPv6 Communication Protocol. This approach improves routing protocols for low-power and lossy networks with classification algorithms supported by an artificial immune system, which classifies the node as self or non-self-based on the behavior using a correlation coefficient algorithm and according to the given threshold. Node energy, link throughput, latency, and quality are used as metrics to detect misbehavior. This approach improves the performance of the routing protocol and the security against most common attacks. However, the authors did not consider all security parameters.

The authors in [63], propose Swarm Intelligence for Wireless Sensors Networks Cybersecurity,(SIWC) which is a generic bio-inspired model. Periodically, each node calculates critical parameters such as collision rate and arrival rate and sends them to the protector node as a control packet. Then, the weights assigned to each parameter are based on the importance of the parameter to define the attack. The node is categorized as a protector, using the weight parameter maximum likelihood estimation that is trained based on the swarm intelligence optimization algorithm to find the highest probability of cyberattack. The parameter is then detected and compared with a prefixed threshold beyond which is the cyberattack risk. Afterward, appropriate action to the malicious node is taken by the base station. SWIC checks authentication and integration at the local level as one of the protector's responsibilities. In this approach, the sensor nodes are highly dependent on the protector node. Figure 3 demonstrates the taxonomy of bio-inspired techniques that can address 5G network layer security for IoT applications.

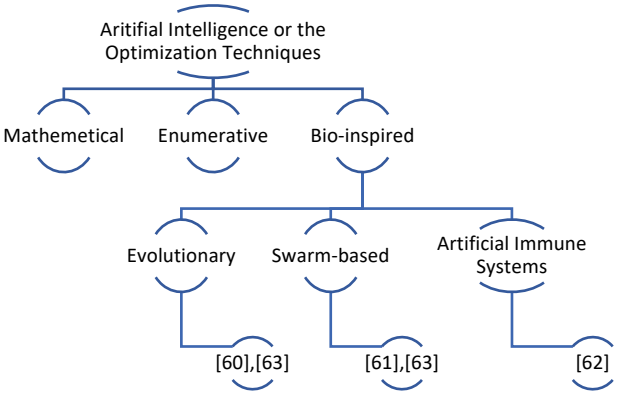

FIGURE 3. Taxonomy of Bio-Inspired Network Security Techniques.

Recently, most studies addressing security issues and enhancing network layer security are based on bio-inspired

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3046325, IEEE Access

techniques. In [22], Choraś et al. show different bio-inspired techniques with their applications and how these techniques useful in detecting cyberattacks and how they can improve computer network protection. Moreover, researchers are led by different reasons for bio-inspired techniques for cybersecurity. These reasons include adjusting to different environmental circumstances, robustness, resilience with failures, fault tolerance, complex behaviors with limited basic rules, and ability to self-evolve [59].

V. ANALYSIS AND FUTURE PROSPECTS

In this section, the biologically inspired mechanisms that can address the issues of 5G-enabled IoT network layer security, as discussed in Section IV, are further compared in terms of methods utilized and the performance criteria as shown in Table 2.

The gained improvement by these biological security methods, and how they can help in securing the network layer of 5G-enabled IoT applications is discussed and presented in Figure 4.

The heterogeneity in 5G requires distributed security solutions and [60] can help in providing distributed cyber defense systems, especially to address DDoS attacks. Moreover, the trusted routing scheme given in [61] can assist 5G-enabled IoT applications for reliable and efficient data delivery. [62] secured the network layer of 5G-enabled IoT from different routing attacks autonomously and was able to enhance the data routing reliability. Cyberattacks on the side of cyber-physical systems, which play a major part in 5G-enabled IoT applications are studied and addressed in [63]. Many other weak points remain in the network layer of 5G-enabled IoT applications that require in-depth consideration.

TABLE II
BIO-INSPIRED NETWORK SECURITY MECHANISMS COMPARISON

	Methods Utilized	Performance Evaluation
[60]	Colonies of honeybees	Mininet 2.0 network emulator BLID in terms of sensitivity and accuracy
[61]	Ant colony optimization (ACO) and Physarum autonomic optimization (PAO)	Network Simulator ns-2 (version 2.34) AODV, AntHocNet, and TGRP in terms of delay, delivery ratio, and traffic overhead
[62]	Artificial immune system (AIS).	Contiki OS RPL in terms of power consumption
[63]	Swarm intelligence algorithm and neural network	Theoretically

VI. CONCLUSION

This paper performs an in-depth review of the recent literature on network layer security in 5G&IoT systems, including future challenges. Additionally, the network layer vulnerability and security requirements in WSN, IoT, and 5G&IoT are investigated and compared. Moreover, the scholarly literature on current approaches and the bio-inspired mechanisms that provide secure routing in 5G networks for IoT applications is thoroughly reviewed. The bio-inspired techniques are more promising in addressing challenges in 5G&IoT and providing secure and reliable data transfer. Furthermore, this paper conducts a detailed comparative analysis to identify open research topics.

In the future, this survey will help researchers adopt the best possible solution for their studies and to address the issue in 5G network layer security for IoT applications.

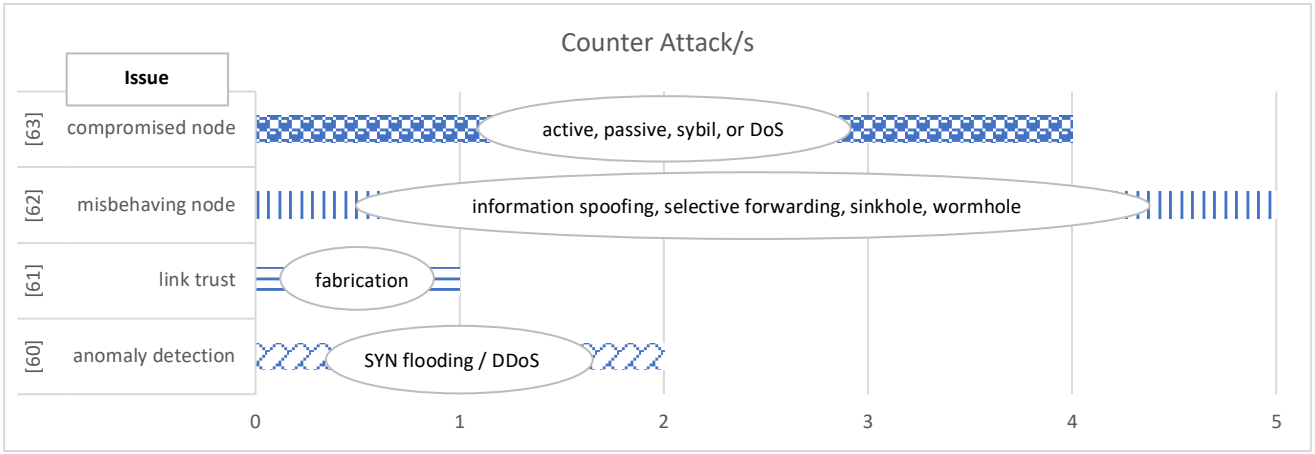

FIGURE 4. **The Issues and Attack/s Counter by the Biological Network Security Mechanisms.**

REFERENCES

[1] R. Alonso-Sanz, "Cellular automata and other discrete dynamical systems with memory," in *2012 International Conference on High Performance Computing & Simulation (HPCS)*, 2012: IEEE, pp. 215-215.

[2] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for internet of things: a survey," *IEEE Internet of things journal,* vol. 3, no. 1, pp. 70-95, 2015.

[3] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges," *IEEE Access,* vol. 6, pp. 3619-3647, 2018, doi: 10.1109/ACCESS.2017.2779844.

[4] R. Hamidouche, Z. Aliouat, and A. M. Gueroui, "Bio-inspired vs classical solutions to overcome the IoT challenges," in *2018 3rd Cloudification of the Internet of Things (CIoT)*, 2018: IEEE, pp. 1-7.

[5] R. T. Tiburski, L. A. Amaral, and F. Hessel, "Security Challenges in 5G-Based IoT Middleware Systems," in *Internet of Things (IoT) in 5G Mobile Technologies*: Springer, 2016, pp. 399-418.

[6] T. Poulos. "IoT and 5G security threats could have network operators reeling." disruptive. (accessed 28-03-2020, 2020).

[7] M. A. Amanullah *et al.*, "Deep learning and big data technologies for IoT security," *Computer Communications,* vol. 151, pp. 495-517, 2020/02/01/ 2020.

[8] L. U. Khan, I. Yaqoob, M. Imran, Z. Han, and C. S. Hong, "6G Wireless Systems: A Vision, Architectural Elements, and Future Directions," *IEEE Access,* vol. 8, pp. 147029-147044, 2020, doi: 10.1109/ACCESS.2020.3015289.

[9] J. Rodriguez, *Fundamentals of 5G mobile networks*. John Wiley & Sons, 2015.

[10] Y. Liu, H.-N. Dai, Q. Wang, M. K. Shukla, and M. Imran, "Unmanned aerial vehicle for internet of everything: Opportunities and challenges," *Computer Communications,* vol. 155, pp. 66-83, 2020/04/01/ 2020.

[11] W. Rafique, L. Qi, I. Yaqoob, M. Imran, R. U. Rasool, and W. Dou, "Complementing IoT Services Through Software Defined Networking and Edge Computing: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials,* vol. 22, no. 3, pp. 1761-1804, 2020, doi: 10.1109/COMST.2020.2997475.

[12] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," *Wireless Networks,* vol. 20, no. 8, pp. 2481-2501, 2014.

[13] M. Abomhara and G. M. Køien, "Security and privacy in the Internet of Things: Current status and open issues," in *2014 International Conference on Privacy and Security in Mobile Systems (PRISMS)*, 11-14 May 2014 2014, pp. 1-8, doi: 10.1109/PRISMS.2014.6970594.

[14] J. M. Batalla *et al.*, "Security Risk Assessment for 5G Networks: National Perspective," *IEEE Wireless Communications,* vol. 27, no. 4, pp. 16-22, 2020, doi: 10.1109/MWC.001.1900524.

[15] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "5G security: Analysis of threats and solutions," in *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, 18-20 Sept. 2017 2017, pp. 193-199, doi: 10.1109/CSCN.2017.8088621.

[16] N. Javaid, A. Sher, H. Nasir, and N. Guizani, "Intelligence in IoT-Based 5G Networks: Opportunities and Challenges," *IEEE Communications Magazine,* vol. 56, no. 10, pp. 94-100, 2018, doi: 10.1109/MCOM.2018.1800036.

[17] M. Lourenço and L. Marinos, "ENISA Threat Landscape for 5G Networks," *European Union Agency for Cybersecurity (ENISA),* no. 2019, p. 87, 21/11/2019 2019, doi: 10.2824/49299.

[18] G. Millar *et al.*, "INtelligent Security and PervasIve tRust for 5G and Beyond," 2019.

[19] Y. Shah, N. Chelvachandran, S. Kendzierskyj, H. Jahankhani, and R. Janoso, "5G Cybersecurity Vulnerabilities with IoT and Smart Societies," in *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity*, H. Jahankhani, S. Kendzierskyj, N. Chelvachandran, and J. Ibarra Eds. Cham: Springer International Publishing, 2020, pp. 159-176.

[20] W. Mazurczyk and E. Rzeszutko, "Security--A Perpetual War: Lessons from Nature," *IT Professional,* vol. 17, no. 1, pp. 16-22, 2015.

[21] W. Mazurczyk, S. Moore, E. W. Fulp, H. Wada, and K. Leibnitz, "Bio-inspired cyber security for communications and networking," *IEEE Communications Magazine,* vol. 54, no. 6, pp. 58-59, 2016, doi: 10.1109/MCOM.2016.7497767.

[22] M. Choraś, R. Kozik, and I. Maciejewska, "Emerging cyber security: Bio-inspired techniques and MITM detection in IoT," in *Combatting Cybercrime and Cyberterrorism*: Springer, 2016, pp. 193-207.

[23] D. Kominami, T. Iwai, H. Shimonishi, and M. Murata, "A control method for autonomous mobility management systems toward 5G mobile networks," in *2017 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2017: IEEE, pp. 498-503.

[24] D. Wu, Z. Zhang, S. Wu, J. Yang, and R. Wang, "Biologically inspired resource allocation for network slices in 5G-enabled Internet of Things," *IEEE Internet of Things Journal,* vol. 6, no. 6, pp. 9266-9279, 2018.

[25] A. Roy, N. Saxena, B. J. Sahu, and S. Singh, "BISON: A bioinspired self-organizing network for dynamic auto-configuration in 5G wireless," *Wireless Communications and Mobile Computing,* vol. 2018, 2018.

[26] H.-C. Chao, H.-H. Cho, T. K. Shih, and C.-Y. Chen, "Bacteria-Inspired Network for 5G Mobile Communication," *IEEE Network,* vol. 33, no. 4, pp. 138-145, 2019.

[27] Z. AjazMoharkan, T. Choudhury, S. C. Gupta, and G. Raj, "Internet of Things and its applications in E-learning," in *2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT)*, 2017: IEEE, pp. 1-5.

[28] J. Santos, J. J. Rodrigues, B. M. Silva, J. Casal, K. Saleem, and V. Denisov, "An IoT-based mobile gateway for intelligent personal assistants on mobile health environments," *Journal of Network and Computer Applications,* vol. 71, pp. 194-204, 2016.

[29] G. Zheng *et al.*, "Multiple ECG fiducial points-based random binary sequence generation for securing wireless body area networks," *IEEE journal of biomedical and health informatics,* vol. 21, no. 3, pp. 655-663, 2016.

[30] 3GPP. "TS 33.102: 3G Security; Security Architecture.".

[31] ITU-T. "X.805: Security Architecture for Systems Providing end-toend Communications. ."

[32] G. Arfaoui *et al.*, "A security architecture for 5G networks," *IEEE Access,* vol. 6, pp. 22466-22479, 2018.

[33] H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, and H. Karimipour, "A survey on internet of things security: Requirements, challenges, and solutions," *Internet of Things,* p. 100129, 2019.

[34] K. Saleem, N. Fisal, and J. Al-Muhtadi, "Empirical studies of bio-inspired self-organized secure autonomous routing protocol," *IEEE Sensors Journal,* vol. 14, no. 7, pp. 2232-2239, 2014.

[35] T. M. Behera, S. K. Mohapatra, U. C. Samal, M. S. Khan, M. Daneshmand, and A. H. Gandomi, "I-SEP: An Improved Routing Protocol for Heterogeneous WSN for IoT based Environmental Monitoring," *IEEE Internet of Things Journal,* 2019.

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

[37] S. Li, L. Da Xu, and S. Zhao, "5G Internet of Things: A survey," *Journal of Industrial Information Integration,* vol. 10, pp. 1-9, 2018.

[38] D. Zhang, Z. Zhou, S. Mumtaz, J. Rodriguez, and T. Sato, "One integrated energy efficiency proposal for 5G IoT communications," *IEEE Internet of Things Journal,* vol. 3, no. 6, pp. 1346-1354, 2016.

[39] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in *2015 IEEE Symposium on Computers and Communication (ISCC)*, 2015: IEEE, pp. 180-187.

[40] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based detection of sybil attacks in wireless networks," *IEEE Transactions on Information Forensics and Security,* vol. 4, no. 3, pp. 492-503, 2009.

[41] H. Xie, Z. Yan, Z. Yao, and M. Atiquzzaman, "Data collection for security measurement in wireless sensor networks: a survey," *IEEE Internet of Things Journal,* vol. 6, no. 2, pp. 2205-2224, 2018.

[42] O. A. Osanaiye, A. S. Alfa, and G. P. Hancke, "Denial of service defence for resource availability in wireless sensor networks," *IEEE Access,* vol. 6, pp. 6975-7004, 2018.

[43] M. Zolanvari and R. Jain, "IoT security: a survey," *Computer Scientists & Computer Engineers at WashU,* 2015.

[44] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, and K. Wehrle, "6LoWPAN fragmentation attacks and mitigation mechanisms," in *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*, 2013, pp. 55-66.

[45] A. Dvir and L. Buttyan, "VeRA-version number and rank authentication in rpl," in *2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems*, 2011: IEEE, pp. 709-714.

[46] S. Raza, S. Duquennoy, J. Höglund, U. Roedig, and T. Voigt, "Secure communication for the Internet of Things—a comparison of link-layer security and IPsec for 6LoWPAN," *Security and Communication Networks,* vol. 7, no. 12, pp. 2654-2668, 2014.
[47] J. Granjal, E. Monteiro, and J. S. Silva, "Application-layer security for the WoT: Extending CoAP to support end-to-end message security for Internet-integrated sensing applications," in *International Conference on Wired/Wireless Internet Communication*, 2013: Springer, pp. 140-153.
[48] A. Girson, "IoT has a security problem-will 5G solve it," *Available on line,* vol. 15, 2018.
[49] M. Ndiaye, G. P. Hancke, and A. M. Abu-Mahfouz, "Software defined networking for improved wireless sensor network management: A survey," *Sensors,* vol. 17, no. 5, p. 1031, 2017.
[50] H. Rahimi, A. Zibaeenejad, P. Rajabzadeh, and A. A. Safavi, "on the Security of the 5G-IoT Architecture," in *Proceedings of the international conference on smart cities and internet of things*, 2018, pp. 1-8.
[51] K. M. Modieginyane, B. B. Letswamotse, R. Malekian, and A. M. Abu-Mahfouz, "Software defined wireless sensor networks application opportunities for efficient network management: A survey," *Computers & Electrical Engineering,* vol. 66, pp. 274-287, 2018.
[52] L. Liu and M. Han, "Privacy and Security Issues in the 5G-Enabled Internet of Things," *5G-Enabled Internet of Things,* p. 241, 2019.
[53] J. Ni, X. Lin, and X. S. Shen, "Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT," *IEEE Journal on Selected Areas in Communications,* vol. 36, no. 3, pp. 644-657, 2018.
[54] A. Nieto, A. Acien, and G. Fernandez, "Crowdsourcing analysis in 5g iot: Cybersecurity threats and mitigation," *Mobile Networks and Applications,* vol. 24, no. 3, pp. 881-889, 2019.
[55] J. Xia, Y. Xu, D. Deng, Q. Zhou, and L. Fan, "Intelligent secure communication for internet of things with statistical channel state information of attacker," *IEEE Access,* vol. 7, pp. 144481-144488, 2019.
[56] A. A. Abd El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung, and S. E. Venegas-Andraca, "Secure data encryption based on quantum walks for 5G Internet of Things scenario," *IEEE Transactions on Network and Service Management,* vol. 17, no. 1, pp. 118-131, 2020.
[57] T. Alam, "Efficient and Secure Data Transmission Approach in Cloud-MANET-IoT integrated Framework," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC),* vol. 12, no. 1, 2020.
[58] B. Seok, J. C. S. Sicato, T. Erzhena, C. Xuan, Y. Pan, and J. H. Park, "Secure D2D Communication for 5G IoT Network Based on Lightweight Cryptography," *Applied Sciences,* vol. 10, no. 1, p. 217, 2020.
[59] U. Rauf, "A taxonomy of bio-inspired cyber security approaches: existing techniques and future directions," *Arabian Journal for Science and Engineering,* vol. 43, no. 12, pp. 6693-6708, 2018.
[60] M. Korczynski, A. Hamieh, J. H. Huh, H. Holm, S. R. Rajagopalan, and N. H. Fefferman, "Hive oversight for network intrusion early warning using DIAMoND: a bee-inspired method for fully distributed cyber defense," *IEEE Communications Magazine,* vol. 54, no. 6, pp. 60-67, 2016.
[61] M. Zhang, R. Zheng, Q. Wu, W. Wei, X. Bai, and H. Zhao, "B-iTRS: a bio-inspired trusted routing scheme for wireless sensor networks," *Journal of sensors,* vol. 2015, 2015.
[62] K. Saleem, J. Chaudhry, M. A. Orgun, and J. Al-Muhtadi, "A bio-inspired secure IPv6 communication protocol for Internet of Things," in *2017 Eleventh International Conference on Sensing Technology (ICST)*, 2017: IEEE, pp. 1-6.
[63] S. Bitam, S. Zeadally, and A. Mellouk, "Bio-inspired cybersecurity for wireless sensor networks," *IEEE Communications Magazine,* vol. 54, no. 6, pp. 68-74, 2016, doi: 10.1109/MCOM.2016.7497769.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3046325, IEEE Access

Kashif Saleem is with the Center of Excellence in Information Assurance (CoEIA), King Saud University, Saudi Arabia, since 2012 and currently, working as an Associate Professor. He received his Master of Engineering (M.E.) in Electrical Engineering - Electronics & Telecommunication, and Doctor of Philosophy (Ph.D.) in Electrical Engineering from University Technology Malaysia in 2007 and 2011, respectively. The Post Graduate Diploma (PGD) in Computer Technology & Communication from Government College University, Lahore, Pakistan in 2004 and B.Sc. (Computer Science) from Allama Iqbal Open University, Islamabad, Pakistan in 2002. He is trained and certified by the Massachusetts Institute of Technology (MIT) in Cybersecurity, University of the Aegean in Information & Communication Security, Institut Mines-Télécom in Queuing Theory, IBM in Security Intelligence Analyst, Microsoft and Cisco in Computer Networks. Dr. Saleem has authored and coauthored over 100 papers in refereed international journals and conferences. Dr. Saleem is an Associate Editor of Journal of Multimedia Information System (JMIS), IEEE Access, International Journal of Ehealth and Medical Communications (IJEHMC), The International Journal of Cyber-Security and Digital Forensics (IJCSDF). He served as a technical program committee member plus organized numerous international workshops and the conferences. Dr. Saleem acquired several research grants in KSA, EU, and the other parts of the world. His research interests are Ubiquitous Computing, Mobile Computing, Internet of Things (IoT), Machine to Machine (M2M) Communication, Wireless Mesh Networks (WMNs), Wireless Sensor Networks (WSNs) & Mobile Adhoc Networks (MANETs), Intelligent Autonomous Systems, Information Security, bioinformatics.

Ghadah Majid Alabduljabbar is a researcher at the National Center for Robotics Technology and Autonomous Systems, King Abdulaziz City for Science and Technology (KACST) in Saudi Arabia, since 2018. She received a Bachelor of science degree in Information Technology - Data Management, and a Master of science degree in Computer Science from King Saud University (Saudi Arabia) in 2016 and 2020, respectively. From 2016 to 2017, she was an Assistant Systems Engineer at TATA Consultancy Services (TCS). Her research interests include data mining, computer vision, artificial intelligence, and image processing.

Nouf Alrowais received the B.S. degree in information technology from King Saud University, Saudi Arabia, in 2016. She is currently pursuing the M.S. degree in Computer Science Department, King Saud University, Saudi Arabia. Since 2017, she is a Researcher at the National Center for Robotics Technology and Autonomous Systems, King Abdulaziz City for Science and Technology (KACST) in Saudi Arabia. Her research interest includes artificial inelegance, machine leaning and data mining.

Jalal Al-Muhtadi is the Director of the Center of Excellence in Information Assurance (CoEIA) at King Saud University, and an Associate Professor at the Department of Computer Science, King Saud University. His areas of expertise include cybersecurity, information assurance, privacy, and Internet of Things. He received his PhD and MS degrees in Computer Science from the University of Illinois at Urbana-Champaign, USA. He has published over 50 scientific papers in the areas of cybersecurity and internet of things.

Muhammad Imran is an Associate Professor in the College of Applied Computer Science at King Saud University, Saudi Arabia. He received a Ph. D in Information Technology from the University Teknologi PETRONAS, Malaysia in 2011. His research interest includes Internet of Things, Mobile and Wireless Networks, Big Data Analytics, Cloud computing, and Information Security. His research is financially supported by several grants. He has completed a number of international collaborative research projects with reputable universities. He has published more than 250 research articles in peer-reviewed, well-recognized international conferences and journals. Many of his research articles are among the highly cited and most downloaded. He served as an Editor in Chief for European Alliance for Innovation (EAI) Transactions on Pervasive Health and Technology. He is serving as an associate editor for top ranked international journals such as IEEE Communications Magazine, IEEE Network, Future Generation Computer Systems, and IEEE Access. He served/serving as a guest editor for about two dozen special issues in journals such as IEEE Communications Magazine, IEEE Wireless Communications Magazine, Future Generation Computer Systems, IEEE Access, and Computer Networks. He has been involved in about one hundred peer-reviewed international conferences and workshops in various capacities such as a chair, co-chair and technical program committee member. He has been consecutively awarded with Outstanding Associate Editor of IEEE Access in 2018 and 2019 besides many others.

Joel J. P. C. Rodrigues [S'01, M'06, SM'06, F'20] is a professor at the Federal University of Piauí, Brazil; senior researcher at the Instituto de Telecomunicações, Portugal; and collaborator of the Post-Graduation Program on Teleinformatics Engineering at the Federal University of Ceará (UFC), Brazil. Prof. Rodrigues is the leader of the Next Generation Networks and Applications (NetGNA) research group (CNPq), an IEEE Distinguished Lecturer, Member Representative of the IEEE Communications Society on the IEEE Biometrics Council, and the President of the scientific council at ParkUrbis – Covilhã Science and Technology Park. He was Director for Conference Development - IEEE ComSoc Board of Governors, Technical Activities Committee Chair of the IEEE ComSoc Latin America Region Board, a Past-Chair of the IEEE ComSoc Technical Committee on eHealth, a Past-chair of the IEEE ComSoc Technical Committee on Communications Software, a Steering Committee member of the IEEE Life Sciences Tech- nical Community and Publications co-Chair. He is the editor-in-chief of the International Journal on Ehealth and Medical Communications and editorial board member of several high-reputed journals. He has been general chair and TPC Chair of many international conferences, including IEEE ICC, IEEE GLOBECOM, IEEE HEALTHCOM, and IEEE LatinCom. He has authored or coauthored over 900 papers in refereed international journals and conferences, three books, two patents, and one ITU-T Recommendation. He had been awarded several Outstanding Leadership and Outstanding Service Awards by IEEE Communications Society and several best papers awards. Prof. Rodrigues is a member of the Internet Society, a senior member ACM, and Fellow of IEEE.