ONLINE ISSN: 3007-3197 | PRINT ISSN: 3007-3189

http://amresearchreview.com/index.php/Journal/about

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 7 (2025)

Cybersecurity Risks and Mitigation Strategies in 5G IoT: Identify and Analyze Cybersecurity Risks in 5G IoT Systems and Propose Mitigation Strategies

[1]Sara Abbas, [2]Abdulrehman Arif, [3]Amna Asif

Article Details

Keywords:: Data Breaches, Unauthorized Access, Device Spoofing, Privacy Invasion, Supply Chain Attacks, Insider Threats

Sara Abbas
MS in Software Engineering, Islamia University of Bahawalpur, Pakistan
Email: sarahrajpoot47@gmail.com
https://orcid.org/0009-0003-9117-0194
Abdulrehman Arif
Department of Computer Science and Information Technology , University of Southern Punjab , Multan
Email: khanabdulrehman026@gmail.com
https://orcid.org/0009-0009-6757-2293
Amna Asif
Lecturer University of Education Multan
Email: amnaasif326@gmail.com

ABSTRACT

The emergence of 5G networks not only becomes a significant advance in the field of communicational technology but also guarantees a previously unheard-of connection, the rapid exchange of information, and a low indicator of delay time, allowing for the work with an enormous amount of Internet of Things (IoT) devices. Such an emerging technology has many cybersecurity issues that must urgently be solved so that the safe implementation and operation of the same may be realized. The 5G outcomes of cybersecurity are the result of its complicated architecture, varieties of applications, and an amalgamation of various heterogeneous networks. This paper explains the hazards and problems related to the 5G networks, such as the supply chain vulnerability, software-defined networking (SDN), network slicing, and integration of IoT. It even indicates the significant channels of attack, including denial-of-service attacks, data exfiltration, and advanced persistent attacks, utilizing flaws of a simple nature in 5G networks. The solutions to such challenges need to include extensive security systems, which would consist of strict regulatory policies, encryption, and real-time monitoring of threats. The paper ends by making practical recommendations that the stakeholders, such as governments, network operators, and corporations, can take in order to maintain the secure deployment and operation of 5G networks and encourage innovation and resilience.

INTRODUCTION

With the introduction of fifth-generation (5G) networks, the world is now witnessing a paradigm change in communications that allows unprecedented abilities to change many industries. 5G is truly a leap forward compared to all other technologies, primarily because of an increase in speed, latency, and the ability to connect such devices (Akyildiz et al., 2020). This development facilitates the remarkable advances in such areas as healthcare, where telemedicine and tele-procedures become more real, transportation, where autonomous on-ground vehicles and traffic management run through intelligent traffic control systems are only possible with near-zero-time data transfer. The manufacturing industry is no exception and also enjoys a smooth integration of the Internet of Things (IoT) gadgets and equipment, which allows production lines to be more automated and efficient (Gill et al., 2022). Moreover, 5G is instrumental in the realization of smart cities, which are a key aspect of current urban development, as it enables the management of utilities, the safety of the masses, and infrastructure. Despite these benefits, however, the additional capabilities and complex architecture of 5G pose a significant cybersecurity concern, presenting fears about the security of the network in terms of new threats. Extremely high speed and low latency of 5G networks are also essential to their appeal, with data rates far higher than 4G and with latencies that enable real-time usage (Geraci et al., 2022). But it is but obvious that along with such technological achievements, the target area of bad guys also rises.

The 5G ecosystem is a dynamic network comprising a number of elements that are susceptible to maneuver including virtualized infrastructure, edge computing as well as massive machine-type communication (mMTC). The huge segment of the virtualized infrastructure is much dependent on the attainment of software-defined networking (SDN) and network function virtualization (NFV) to be more flexible and less costly (Amin et al., 2021). Whenever there is efficiency in operations using those technologies, there are potential risks due to the existence of a bug in software applications, misconfigured engines, and unlawful access. Likewise, edge computing, designed to operate on decentralized data processing to minimize latency, provides multiple point of access potentially exploited by cyberattacks. The large scale of the mMTC, containing billions of interconnected devices. The sheer scale of interconnected devices in mMTC adds to the security situation by providing attackers with nearly an infinite variety of targets to attack. Another weakness introduced by the 5G networks relates to the use of global supply chains, which leaves the critical infrastructure vulnerable to potential interference by state-sponsored actors and supply chain attacks (Khorsandroo et al., 2021). The manufacturing, deployment, and

maintenance of 5G elements occasionally involve many vendors in various countries that are subject to varying levels of regulatory requirements.

The ultimate globalization of the supply chain elevates the threat of the spoiled hardware or software into the network, both via intentional manipulation and insufficient quality control. State-sponsored spying is a significant vulnerability, as it is possible to suppose that governments can enter international networks through the weak links of supply chains and obtain valuable information (Singh et al., 2021). The nature of these operations not only infringes on the security of national networks but also has a serious impact on national security and international relationships. There is also a danger of extensive damage and data theft when unverified or insecure aspects are introduced to the critical infrastructure. These challenges are worsened by the lack of uniform cybersecurity guidelines on how to install 5G networks. The global deployment of 5G prompts unequal security standards across regions and vendors, which creates an inconsistent picture to be utilized by hackers (Cammers-Goodwin, 2023). Other governments might value deploying their networks quickly as opposed to instituting strict security measures, thus making the networks more susceptible to attacks.

The fact is that vendors having different cybersecurity approaches can cause unintentional vulnerabilities in the network, particularly in the case that their parts are connected without any attention to compatibility testing. This is worsened with the rapid development of technologies that often overtake the growth and development of regulatory mechanisms (J & Majid, 2020). Unless there is a very concerted effort to establish and implement rigid security standards across the world, there is a likelihood that the weaknesses associated with 5G networks would continue, which could hurt their adoption, given the trust and reliability required in their uptake. Security challenges of the 5G networks do not only refer to vulnerabilities in technical systems but also human and organizational factors in the deployment and operation of 5G networks (Liu et al., 2022). Human error due to a misalignment of the settings, lack of education, or malicious intent remains one of the greatest. It carries quite a complicated 5G architecture, which requires an experienced staff skilled in the ability to identify and mitigate potential risks, but the need often exceeds the supply. In addition, integration of 5G into the systems that are already outdated, of whose most have not been created with modern best cybersecurity practices compliances in mind, obliterates the security circumstances (Gill et al., 2022b).

Among the problems which organizations may have fallen into, there is the search of an effective mechanism of 5G transition, whereas risks are to be minimized within the framework of existing

infrastructure. Although it is clear that 5G networks can be a source of innovative purposes and economic growth, there are high risks on cybersecurity that come with their introduction (Quach et al., 2022). Speed at a significant rate, low latency rates, and the ultimate connected state are the features that render 5G transformative but also compose a very broad surface of a target where corrupted organizations can operate. Threats of this sort may be added to the dependence on global supply chains and the general unavailability of cross-industry lines of cybersecurity which is why the unity and holistic approach to maintain the 5G networks secure can be all the more important. Such issues concern the collaboration by the government, industry members and cybersecurity professionals in creating security standards that are high, creating universal requirements and enacting and realizing the benefits of 5G, without impairing the security of critical infrastructure (Dwivedi et al., 2022).

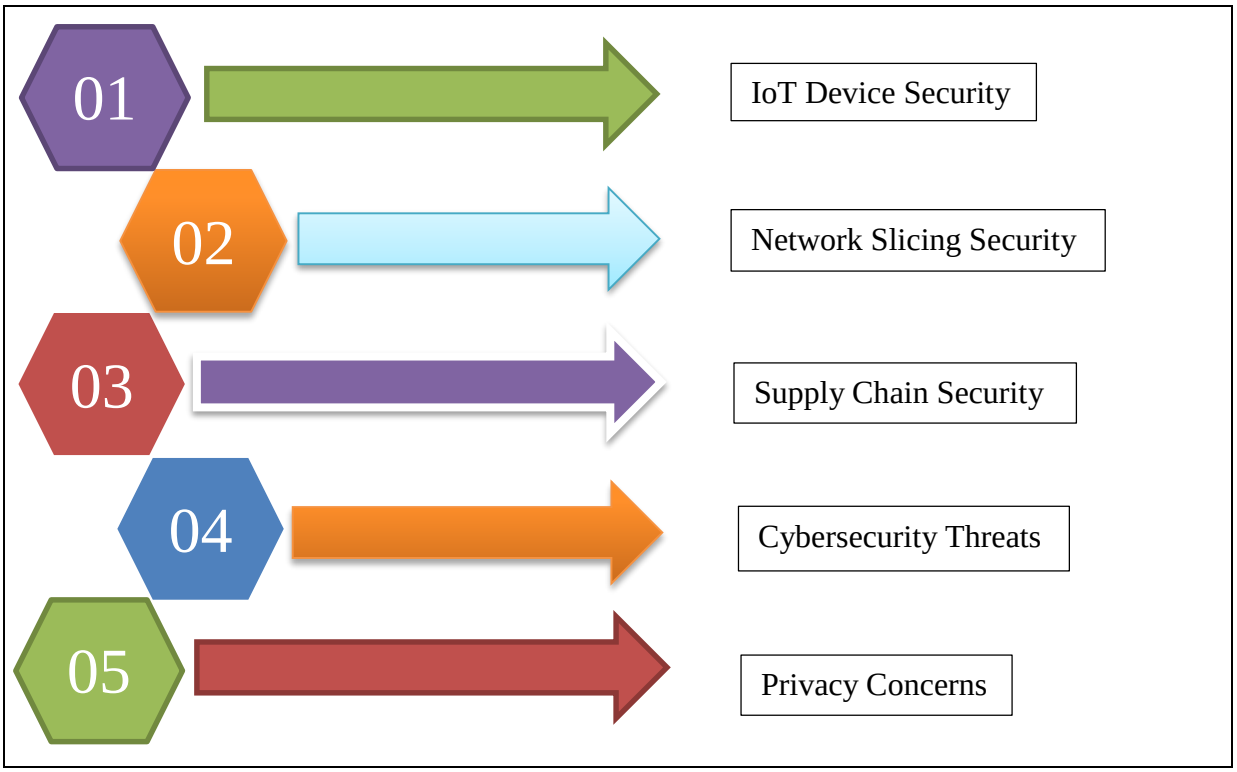
CYBERSECURITY VULNERABILITIES OF 5G NETWORKS

The newness of 5G networks has transformed the digital communication system, which is characterized by unmatched speed and decreased latency as well as being able to serve an unmatched number of connected devices. The technological innovation also poses several major cybersecurity threats whose impact is devastating to people and organizations (Wanasinghe et al., 2020). The most significant issue with the 5G networks is enlarging the targets attack surface since these 5G networks interact closely with IoT devices as well as edge units that form networks. The use of IoT devices together with 5G radio elicits a lot of questions because the number of devices that have accessibility to the network is relatively large. Although IoT solutions are very useful when it comes to increasing connectivity and the creation of innovative solutions in a diverse number of industries, quite a lot of pieces of the equipment do not have some basic security features available. Such risk has occurred due to several factors, such as financial constraints in the development, as well as the lack of computing power to facilitate the use of enhanced security protocols, and the inconsistency of manufacturers in adhering to cybersecurity regulations (Gann et al., 2019).

Accordingly, any IoT gadget that has been connected to a 5G network can be a source of vulnerability to cyberattacks that can increase vulnerability to the network and users. An Internet of Things device, like a smart thermostat or a body-worn health sensor system, can be hacked into and used as a gateway by attackers to gain access to a network at large and cause a significant impact (Paul et al., 2023). Besides, the decentralized structure of the 5G networks, particularly through Edge Computing, enhances these vulnerabilities. Edge computing moves data processing

facilities closer to the customer or device, thus reducing latency and boosting efficiency. Another strategy will provide more access points that can be compromised. Unlike typical centralized data centers, the edge computing systems are distributed and often lack physical as well as cyber-security mechanisms. Using such entry points, malefactors can crack confidential data, perform distributed denial-of-service (DDoS) attacks, or affect critical processes (Tlili et al., 2022). Although desirable in performance, the decentralized nature of edge computing gives rise to high-security issues that have to be addressed in order to ensure that 5G networks are secure.

FIGURE 1: CYBERSECURITY RISKS AND MITIGATION STRATEGIES



One of the major cybersecurity risks associated with 5G networks is weakness in the supply chain. The establishment and implementation of 5G infrastructure rely substantially on third-party components, which numerous world manufacturers deliver. This is a fast, low-cost approach that increases the chances of damaged equipment intruding on the network (Ploetz et al., 2020). Criminals can take advantage of these weaknesses: mainly, the state-sponsored businesses will add backdoors or other malicious features in the manufacturing or supply process. The purposes of such backdoors are gaining unauthorized access into the network; data exfiltration with the essential operations; impairments with vital functions. Global supply chains are relatively complicated and opaque, thus the difficulty to identify and respond to such threats, putting the

networks at great risk. State sponsored espionage comprises the supply chain susceptibility. Their power to influence manufacturers or a supplier can be utilized by the hostile governments to implant weaknesses in the 5G infrastructure to spy or demolish (Nowak et al., 2021). This risk is especially threatening to national security as well as critical infrastructure as the disturbances in problem and services in the 5G networks may lead to the domino effect of the vital services such as healthcare, transport and power.

The opportunity of the state-sponsored actors to capitalize the vulnerabilities of the supply chains underlines the importance to proceed with the effective screening of the vendors, open up manufacturing processes, and collaborate globally to create and implement stringent yet globally acceptable rules and regulations that concern cybersecurity. The cybersecurity threats that 5G networks create also indicate that it is not a smooth ebb and flow between technological development and safety concerns (Delimatsis et al., 2023). The occurrence of these threats requires a holistic approach, which would involve the adoption of stringent security measures in IoT devices, strengthening hardware infrastructures connected through edge computing, and developing secure and traceable supply chains. Without such controls, the benefits of 5G networks can be overshadowed by the significant threat they pose to people, companies, and states. Software-Defined Networking (SDN) has significant risks because data and control planes are separated in its inherent design. A major weakness of SDN is that its centralized control system can be attacked, and this is actually referred to as a control plane attack (Nguyen et al., 2020). In this way, by hijacking the control plane, the attackers gain access to the centralized SDN controller, which coordinates the entire network. A successful attack would create challenges to the integrity, confidentiality, and availability of the network, and it would enable the attackers to modify network traffic, bring a disturbance in terms of service interruption, or extract crucial information.

Relying on the SDN controller creates a single point of failure that makes the effects of an attack even more drastic and recovery more challenging. In addition to direct attacks, the SDN networks face vulnerability due to setup errors. SDN controller misconfigurations may create unwanted vulnerabilities that allow third parties to gain unauthorized access or obstruct normal operations (Ranaweera et al., 2021). Such weak points, which often appear due to human monitoring or bugs in the code, may be employed by malefactors to gain access to the network or change its operation. The programmability and flexibility of SDN, which is also its advantage in terms of flexibility and scalability, also increases the possibility of introducing security vulnerabilities by mistake. With this, securing SDN systems would require the development of a

stringent process of testing, monitoring, and incident reporting so that these vulnerabilities can be minimized effectively (Kodheli et al., 2020). The field of network slicing represents a crucial part of the 5G technology, and certain vulnerabilities are central to that specific entity, given the architecture of the feature. Network slicing allows multiple virtualized and conceptually isolated networks to operate together on a common physical platform.

The inter-slice attacks are also potentiated in this very environment. The break being in one slice can maybe spread to the other slices, this is especially possible when there is poor isolation between the slices, or when the isolation systems are adversely penetrated. This may also be of deadly consequence to critical applications that use network slicing, healthcare systems, driverless cars and industrial internet of things in which network integrity and performances are important (Dyson, 2022). The ability to ensure that slices are well isolated adds to these risks as it makes it difficult to guard. Isolation process involves involved operations to separate assets and avoid unknown relationship between the slices. The absence of these processes may result in breach of data, breach of security, hacking, and downtimes. In addition, the shared infrastructure of the community might help the hackers to move horizontally between the slices, thereby increasing the menace even more (Zawish et al., 2024). Their security issues involve a mix of sophisticated security technologies, including end-to-end security and zero-trust with active monitoring to identify and mitigate the threats before such they become rather serious.

Among the most dangerous threats to contemporary networks and, in particular, with 5G infrastructure, there exist those referred to as Advanced Persistent Threats (APTs). What are outstanding about these supremely covert threats is that they are highly advanced and forward-thinking, coupled with being extremely persistent therefore it becomes a highly desirable mode of operation by the actors leading the nation state and organized cyber-criminal consortia. Generally, Advanced Persistent Threats (APTs) are a prolonged attempt to infiltrate networks, remain concealed, and attain access to some valuable data or cause havoc (Djenna et al., 2021). The necessity of the 5G infrastructure with its numerous technologies like massive IoT, edge computing, and networks over the virtualization, itself gives APT a broad target area. Any weakness in any of these components may provide criminals with an opportunity to enter the network and manipulate its work through connectivity. In addition, the current threat landscape of 5G networks reveals that it is challenging to foresee and hinder the emergence of new malicious schemes. Because technology and method of attack keeps evolving, the users and attackers should not be behind and should install the proper proactive threat intelligence and dynamic security.

Their impact on the 5G network is enormous and can entail the loss of critical confidential information, shutdown of essential services and erosion of the confidence of the majority towards telecommunication infrastructure ("Delivering Quality Education and Health Care to All," 2021). To diminish all these risks, businesses are advised to establish comprehensive defense mechanisms that include technical prevention, procedural prevention, and organizational prevention and integration of threat hunting, incident response, and liaison with global cybersecurity networks. The lack of regulatory and legislative tools continues to augment the cybersecurity issues associated with SDN, network slicing, and 5G networks (Rashid et al., 2023). One area of concern is that there are as yet no internationally standardized cybersecurity guidelines for 5 5G. When norms are not established, there is a considerable number of discrepancies in the security practices across the regions, leading to variable levels of protection and presenting vulnerabilities that attackers can potentially exploit.

An example would be that in one area, more stringent security measures are put in place, and in another location, because of a lack of resources, a slow pace in legislation, or the different goals and methodologies, it lags. This inconsistency will be a setback to the effort of protecting telecommunications networks in the world, which are inherently interconnected and interdependent (Boylan et al., 2020). Absence of standardization is a barrier to harmonization of stakeholders that include network operators, equipment makers, and regulators, hindering the formation of a united response to cyber threats. This issue has another complexity in the existence of jurisdictional difficulties. These legal and functional issues arise due to the cross-border dimension of the 5G networks and data transmissions in terms of carrying out cybersecurity. Differences in institutions, national laws, privacy standards and action tactics spur confusion and snags, which delay solutions to security issues. Cyberattack, which originated in a jurisdiction, and had the target in another jurisdiction, needs long-term negotiations and collaboration between the governments, which on the one hand makes it longer to respond to the attack itself, and on the other hand worsens the effects of such an attack (Radu, 2019). These gaps can be only overcome through international coordinated measures to create universal systems of cybersecurity, enhance information transfer, and regulate regulatory approaches to achieve a safe and safe international 5G ecosystem.

OBSTACLES IN SAFEGUARDING 5G NETWORKS

The entry of 5G network is a revolution that has taken place and is being introduced into the field by the telecommunications where 5G provides an unprecedented speed, latencies that are very low

and the ability to connect many connected devices. This rise of technology comes with its challenges especially security of the networks against various threats and weaknesses (Dwivedi et al., 2022b). This is one of the central concerns, which is dictated by complicated technical nature of 5G architectures. 5G is different, with the use of such technologies like software-defined networking (SDN), network slicing, and virtualization. Even though this kind of development is more flexible and efficient, there also exists a configuration of weak points, and it is on this basis that there is the necessity that security requires special remedies. One such thing is SDN where the control of the network is centralized meaning that in case of a hack there is likely to be a single point of failure (Hussain et al., 2020). Due to the capacity of creating and sharing numerous virtual networks on a sole physical infrastructure through the usage of network slicing, cross-slice attacks can arise, as no isolation mechanisms are installed. Whereas virtualization does help to achieve a high level of scalability and cost efficiency, it also presents additional attack surfaces by means of the hypervisor and virtual machines.

The disparate weaknesses demand strong adaptive security solutions that could safeguard the integrity, privacy, and availability of the network. One of the problems associated with the development of 5G networks is the large cost related to the introduction of intensive security mechanisms (Khan et al., 2020). Defending 5G infrastructure requires a large investment in emerging technologies, such as artificial intelligence-driven threat detection systems, sophisticated encryption systems, and safe hardware. Such investments are not only costly but also require ceaseless commitment and effort to upgrade and modernize the systems to counter new threats. To many companies, especially telecommunication companies in small markets or those in developing regions, this is too much to spend. Besides, processes of establishing secure 5G networks usually require collaboration of assorted stakeholders, such as governmental agencies, commercial enterprises, and technical standards bodies, to converge resources and align security goals (Das et al., 2023). Inadequate funding level compromises the ability to apply sophisticated service protection, making the networks susceptible to cyberattacks and other undesired actions. The coming of 5G networks has brought with it powers of transformation, especially high-speed data transfer and ultra-low end-to-end delay. These characteristics are, however, innovative and result in huge complexities in the area of network security.

The real-time capabilities inherent in 5G communications demand a matching degree of swift and high-protection security assurances to secure the integrity, confidentiality, and availability of data being passed over such networks. Unlike traditional networks, which, as a rule, allowed the analysis

of the situation after the incident and other actions with its correction, 5G obliges the implementation of preventive solutions to identify and combat threats. Approaches to security that are traditional, such as batch processing or occasional system scans, are inherently inadequate in this respect due to their slowness and to the fact that they cannot handle the high-volume continuous data flows that characterize 5G systems (Martínez-Plumed et al., 2020). The 5G application latency tolerance, namely the ones that support critical infrastructure, or services of special needs, where the risk of latency must be addressed promptly, demands that the potential risks should be identified and eliminated immediately.

To realize these strict requirements, there is a need to implement potent machine learning algorithms. These technologies are very essential in real-time threat prevention, whereby systems are able to scour large amounts of data within milliseconds and identify anomalous trends that are indicative of devious activity and automatically initiate appropriate corrective action. Machine learning is naturally skilled in the ability to analyze large volumes of data, discover subtle abnormalities in common behavior, and adapt to a fluctuating threat landscape (Bethel et al., 2021). Such skills are required in the world of 5G since the network is prone to new and sophisticated cyber-attacks. Such vulnerability is worsened by the introduction of the Internet of Things (IoT), where the spread of devices connected in this system is primarily preconditioned by 5G, significantly increasing the area of attack.

The security mechanism should be capable of operating at record-high speeds and be economically scalable to protect billions of networked devices that relay information in real-time. AI-based response systems form one of the major building blocks of security in 5G networks. Human-related processes and human decision-making, which remain one of the defining characteristics of manual intervention, do not match the rapid pace of 5G communications (Fuller et al., 2020). Security systems should automatically take defensive actions such as isolating malicious network nodes, blocking malicious traffic, or updating software patches without operator or expert knowledge. Such automation not only makes the reaction times much faster but also reduces the likelihood of human error, which the opponents can exploit. These capabilities are crucial, particularly when deployed in scenarios undertaken by distributed denial-of-service (DDoS) attacks that can clog up network resources within a few seconds. By pairing automated answers with machine learning, it will allow 5G networks to achieve resilience that is proactive and flexible, and essentially avert the threat before it can develop into a larger-scale breach (Bariah et al., 2020). Moreover, the introduction of 5G networks brings new architectural principles

involved, including network slicing and edge computing, and, despite the fact that they enhance the effectiveness and adaptability of networks, they may also add to the marginalization of security-related issues.

Network slicing allows the operator to partition one physical network into a series of logical networks, tailored to support specific applications or user groups. This is used to increase resource distribution and service provisions, though strict division of slices is necessary in order to prevent cross-slice attacks. To realize this isolation, dynamic and granular security policies would be required, able to match themselves to each slice's individual needs and threat profiles (Kreutz et al., 2014). By bringing data processing closer to its origin (therefore reducing latency), edge computing can decentralize data; however, it also increases potential sources of attack because, by distributing critical information and computation among multiple edge nodes, more attack surfaces are exposed. These nodes should be highly encrypted, authenticated, and must have an intrusion detection system, which has to be running in real-time because of the heightened risks of decentralized systems. Emphasis on real-time security in 5G does not seem to be only a technical demand but also a manifestation of a significant growth in risks associated with the introduction of the technology (Mansell, 2021). Many applications of 5G are crucial to the important sectors, such as healthcare, transportation, and PSD, where even minor delays can present catastrophic results. Self-driving cars will rely on the effective transfer of data on a 5G network to make judgments in real-time. Lapses or jitters in this communication can be a cause of accidents or loss of lives. Similarly, smart grids aiming to connect 5G-based real-time monitoring and control of the resource supply may be vulnerable to a hacker attack that can seriously disrupt the power supply.

The potential implications of those accidents emphasize the strong need for powerful, real-time security tools capable of safeguarding not only the network but also the whole socio-economic systems that operate on its stability. The stakeholders must work together in this setting. The safety concerns of 5G require close cooperation between network operators, technology providers, legislators, and cybersecurity experts (Nguyen et al., 2021). The development of a secure 5G environment is essential as standardization of security standards, sharing of threat intelligence, and investment in research and development are significant. Furthermore, as a network security aspect, implementing the 5G service security thinking into the overall design and implementation of the 5G infrastructure (usually referred to as a security-by-design strategy) will also help significantly enhance the resilience of the respective network. Such a proactive stance involves incorporating security functions into the very structure of 5G systems, instead of treating it as an

added layer to them or an afterthought (Calderaro & Blumfelde, 2022). The stakeholders can mitigate risk and inculcate a sense of trust and dependability in 5G networks by identifying potential weaknesses and fixing them before they become a problem. Summing up, the instantaneous nature of 5G communication systems essentially changes the situation with network security, and it has to be met with a paradigm change in the approach to the identification and prevention of attacks.

The speed and complexity of 5G require security techniques that not only have to be fast and efficient but also need to be smart and adjustable. These challenges can be easily addressed, as it can be done with a set of advanced machine learning algorithms, automation of response mechanisms, and well-engineered architectures with advanced security guards that will help them to ensure overall security and stable functioning of 5G networks. In order to achieve this extent of security, the approach must be integrative and collaborative hence the reason proactive planning, active innovation, and coordinated vigilance in the continuously changing threat environment is critical (Dwivedi et al., 2023). Nevertheless, development of such real-time features is technically demanding and resourceful. Furthermore, the use of automated facilities would carry some thorns because hackers might target their weaknesses in AI programs or simply bombard them with highly sophisticated attacks that do not trigger the protection systems. It will be important to guarantee the reliability, accuracy of real-time systems of detecting threats, which is a tedious process in the protection of 5G networks.

Privacy is a concern in 5G security. The general functionality related to 5G allows generating and transfer an enormous volume of data and keeping much of it extremely sensitive. The risks of the abuse of information are huge, and they will comprise both life and money data that will be exchanged by interconnected medical gadgets, and funds data that will be used by intelligent payment devices. The predicament is further escalated considering the maintenance of the user privacy since they are exposed to the strong data protection policies, such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States (Swain et al., 2022). The technologies responsible of data encryption have an essential part in flexibility of data during transmission, but this does not imply that they are hack-proof and can be decrypted using complex decryption tools or even by trusted staff members.

Besides, the necessity to find a balance between the right to privacy and other interests, such as the interest in performance enhanced by network or interest by the government to access data, results in the activation of potential upheavals which may be only skillfully controlled. The

matter of being related to the protection of privacy is even more questionable when it comes to international networks of 5G because of a high rate of data migration between several countries and different legal frameworks and protection measures. Both policymakers and network operators would find it an insurmountable task to construct and come up with effective privacy policies that would work in this complicated model (Bibri, 2023). Lack of skilled labor is also another critical issue hindering the growth of the 5G platforms. Talented people with skills on designing, implementing, and managing the 5G structure are rare and desired in handling cybersecurity. 5G deployment is tricky and demands a profound acquaintance with numerous disciplines most of which are included under the network design, cryptography, threat intelligence, and incident response domains.

The rapid development of technology has made the level of educational programs and training initiatives inadequate, which is why the demand and supply of organized and skilled specialists are uneven. The shortage is further aggravated by the fact that it is of a global nature, with the flow of talent becoming highly competitive even between countries and industries. The firms can contract with security agencies or implement automated systems which may in some way offset the experience shortfall of human operators (Ibn-Mohammed et al., 2020). The probability of exploits of the vulnerabilities is also a bigger threat because lack of qualified professionals capable of monitoring and securing 5G infrastructure can ruin the potential of giving way to a paradigm shift in the 5G technology. Despite a significant potential impact of 5G networks on communication and enabling many novel applications, they present a significant threat to security.

The technological complexity of 5G systems will require the assistance of experts to control various risks. This task is more challenging to complete in the context of these networks due to a high price at which the deployment should be carried and the impossibility of real-time threat detection. The prerequisite of the privacy and adherence to the regulations provides additional challenges, and the pressure of the lack of reliably qualified cybersecurity specialists develops the necessity to invest in the human resources growth (Petersson et al., 2022). It demands a comprehensive strategy involving technological advancement, financial investment, policy formulation and capacity which would counter these issues. The total 5G potential can be fully delivered only in the union with the stakeholders and without the concessions to the security and confidence.

CONCLUSION AND RECOMMENDATIONS

There should be a multistage strategy implemented to deal with all the numerous, and

compounding problems of this disruptive technology, with regard to 5G implementation of safe networks. The most important of them is the enhancement of the supply chain security. This would be done by introducing highly demanding vetting services of the third-party providers so that reliability and integrity of the whole network components could be guaranteed. Considering critical components, people should start with valid suppliers and reduce the chance of penetration of the vulnerabilities in the network structure. It is also necessary to promote foreign collaboration in the establishment of global standards in supply chain security because of interdependence of 5G networks, which is represented by single way of addressing transnational risks. Collaborative spirit in the region may be realized on a collective basis through trust and creation of ideal practices that would improve the whole security framework of 5G systems. Zero-trust architecture is one of the core concepts of safe introduction of 5G. The zero-trust concept is driven by the assumption that neither a person nor a device must be trusted, not even on the inside network perimeter. It involves constant identification of users and gadgets and permission to resources. This makes such an active security system highly restrictive to the site of attack and reduces the probability of break-ins. Other measures in this approach include comprehensive endpoint protection and multi-factor authentication (MFA) which further adds layer of protection covering hacked credentials and vulnerability of endpoints.

The prevalence of interconnected devices offered by a 5G network demands implementing a zero-trust-based approach that will address access controls problems besides protecting valuable data. The improvement of encryption is an important measure in 5G network security. E2E encryption will be required to safeguard integrity and privacy of data instructions as data is retransmitted through the network. Encryption of the data sent and stored will assist the network operators to be sure that vital information is not intercepted, altered or destroyed. Along with this, one should also pay much attention to the idea of investing into the quantum-resistant encryption technology in order to secure the future of the entire network, as there also lies a certain threat to the conventional encryption tool due to the development of the quantum computing idea. This kind of proactive investment unburdens the system of the emerging threats in addition to enhancing the confidence of the users and stakeholders to the security of the network in the 5G network. Machine learning (ML) and artificial intelligence (AI) would be an undeniable method of enhancing the security of the 5G network. The application of AI-powered systems enables real-time monitoring of threats and anomalies in the system, which enables the network operators to detect and deal with possible security issues before they develop into major problems. Predictive analytics,

provided through AI, enhances the ability to anticipate and counteract issues ahead of time. Moreover, automation of the process of responding to incidents through AI also significantly reduces the duration of downtimes and reduces the impact of attacks, therefore, increasing the resilience of 5G networks. The new challenges caused by the dynamically evolving threat landscape associated with 5G make AI solutions particularly effective due to their flexible and modular nature. Setting up robust regulation mechanisms would be a critical element in the secure application of 5G.

To achieve harmony in the global cybersecurity setting, international collaboration is needed to come up with universally acceptable guidelines of cybersecurity, which would ensure homogeneity and interoperability of most jurisdictions. Governments can come up with a common regulatory system in collaboration with international agencies that enables the delivery of safe 5G systems. Additionally, proper compliance with the data protection law and transparency on how the networks are being run creates accountability and gives confidence to the masses. The 5G ecosystem is complex and extremely interconnected, with a good regulatory framework supporting it. The development of workers is essential in negotiating the complexity of 5G networks. The advent of these networks introduces new challenges and chances, which makes cybersecurity experts in high demand. The point is the introduction of more specialized training and upskilling, which supplies the staff with the acumen needed to address the unique 5G security issues. This cooperation with academics, as well as industry and government, can achieve more in the creation of special training programs, which would align with the current and forthcoming needs. Through the manufacture of a pool of skilled professionals, the stakeholders can ensure that the 5G networks are managed and in a secure state. Finally, the promotion of the idea of public-private partnerships is a key policy that needs to be adopted to enhance 5G security. Problems of 5G implementation are complex, and each government, a company based in the private sector, and research organizations have their role in solving them. Through collaboration, the sharing of threat intelligence and best practices can be harmonized among the different stakeholders, resulting in an overall protective activity against cyber-attacks.

The provision of the incentive to innovation in 5G security technology stimulates the development of state-of-the-art solutions. The positive features of the two sectors are combined through public-private cooperation, and the overall and coordinated approach to the protection of 5G networks is provided. The safe deployment of 5G networks should include a multi-angle approach that deals with supply chain protection, zero-trust structure, stronger encryption, artificial intelligence, and

machine learning, legislative system development, workforce training, and partnerships between the government and industry. All these are important when it comes to risk management, protection of sensitive data, and strengthening the resilience of 5G networks. Through these precautions, the stakeholders can enhance the prowess of the 5g technology and secure its users and infrastructure against the arising threats.

REFERENCES

Akyildiz, I. F., Kak, A., & Nie, S. (2020). 6G and Beyond: The Future of Wireless Communications Systems. *IEEE Access*, *8*, 133995–134030. https://doi.org/10.1109/access.2020.3010896

Amin, R., Rojas, E., Aqdus, A., Ramzan, S., Casillas-Perez, D., & Arco, J. M. (2021). A survey on Machine Learning Techniques for Routing Optimization in SDN. *IEEE Access*, *9*, 104582–104611. https://doi.org/10.1109/access.2021.3099092

Bariah, L., Mohjazi, L., Muhaidat, S., Sofotasios, P. C., Kurt, G. K., Yanikomeroglu, H., & Dobre, O. A. (2020). A prospective look: key enabling technologies, applications and open research topics in 6G networks. *IEEE Access*, *8*, 174792–174820. https://doi.org/10.1109/access.2020.3019590

Bethel, B. J., Buravleva, Y., & Tang, D. (2021). Blue Economy and Blue Activities: Opportunities, Challenges, and recommendations for the Bahamas. *Water*, *13*(10), 1399. https://doi.org/10.3390/w13101399

Bibri, S. E. (2023). The metaverse as a virtual model of platform urbanism: its converging AIOT, XReality, Neurotech, and nanobiotech and their applications, challenges, and risks. *Smart Cities*, *6*(3), 1345–1384. https://doi.org/10.3390/smartcities6030065

Boylan, B. M., McBeath, J., & Wang, B. (2020). US–China relations: nationalism, the trade war, and COVID-19. *Fudan Journal of the Humanities and Social Sciences*, *14*(1), 23–40. https://doi.org/10.1007/s40647-020-00302-6

Calderaro, A., & Blumfelde, S. (2022). Artificial intelligence and EU security: the false promise of digital sovereignty. *European Security*, *31*(3), 415–434. https://doi.org/10.1080/09662839.2022.2101885

Cammers-Goodwin, S. I. (2023). *Bridging the gaps between humans and their infrastructure: what are the challenges for citizen engagement introduced by increasing smart urban infrastructure and how might those challenges be mitigated?* https://doi.org/10.3990/1.9789036556101

Das, S. K., Benkhelifa, F., Sun, Y., Abumarshoud, H., Abbasi, Q. H., Imran, M. A., & Mohjazi, L. (2023). Comprehensive review on ML-based RIS-enhanced IoT systems: basics, research

progress and future challenges. *Computer Networks*, *224*, 109581. https://doi.org/10.1016/j.comnet.2023.109581

Delimatsis, P., Bijlmakers, S., Borowicz, M. K., Cerny, P., Belmonte, R., Randall, T., Nield, M., & Judkins, R. (2023). The Evolution of Transnational Rule-Makers through Crises. In *Cambridge University Press eBooks*. https://doi.org/10.1017/9781009329408

Delivering quality education and health care to all. (2021). In *OECD rural studies*. https://doi.org/10.1787/83025c02-en

Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of Things meet Internet of Threats: New concern Cyber security Issues of critical cyber infrastructure. *Applied Sciences*, *11*(10), 4580. https://doi.org/10.3390/app11104580

Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., Dennehy, D., Metri, B., Buhalis, D., Cheung, C. M., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D., Gustafsson, A., Hinsch, C., Jebabli, I., . . . Wamba, S. F. (2022a). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, *66*, 102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542

Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., Dennehy, D., Metri, B., Buhalis, D., Cheung, C. M., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D., Gustafsson, A., Hinsch, C., Jebabli, I., . . . Wamba, S. F. (2022b). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, *66*, 102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542

Dwivedi, Y. K., Kshetri, N., Hughes, L., Slade, E. L., Jeyaraj, A., Kar, A. K., Baabdullah, A. M., Koohang, A., Raghavan, V., Ahuja, M., Albanna, H., Albashrawi, M. A., Al-Busaidi, A. S., Balakrishnan, J., Barlette, Y., Basu, S., Bose, I., Brooks, L., Buhalis, D., . . . Wright, R. (2023). Opinion Paper: "So what if ChatGPT wrote it?" Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. *International Journal of Information Management*, *71*, 102642. https://doi.org/10.1016/j.ijinfomgt.2023.102642

Dyson, M. R. (2022). Combatting AI's Protectionism & Totalitarian-Coded Hypnosis: The Case for AI Reparations & Antitrust Remedies in the Ecology of Collective Self-Determination. *SMU Law Review*, *75*(3), 625. https://doi.org/10.25172/smulr.75.3.7

Fuller, A., Fan, Z., Day, C., & Barlow, C. (2020). Digital Twin: enabling technologies, challenges and open research. *IEEE Access*, *8*, 108952–108971. https://doi.org/10.1109/access.2020.2998358

Gann, G. D., McDonald, T., Walder, B., Aronson, J., Nelson, C. R., Jonson, J., Hallett, J. G., Eisenberg, C., Guariguata, M. R., Liu, J., Hua, F., Echeverría, C., Gonzales, E., Shaw, N., Decleer, K., & Dixon, K. W. (2019). International principles and standards for the practice of ecological restoration. Second edition. *Restoration Ecology*, *27*(S1). https://doi.org/10.1111/rec.13035

Geraci, G., Garcia-Rodriguez, A., Azari, M. M., Lozano, A., Mezzavilla, M., Chatzinotas, S., Chen, Y., Rangan, S., & Di Renzo, M. (2022). What will the future of UAV cellular communications be? A flight from 5G to 6G. *IEEE Communications Surveys & Tutorials*, *24*(3), 1304–1335. https://doi.org/10.1109/comst.2022.3171135

Gill, S. S., Xu, M., Ottaviani, C., Patros, P., Bahsoon, R., Shaghaghi, A., Golec, M., Stankovski, V., Wu, H., Abraham, A., Singh, M., Mehta, H., Ghosh, S. K., Baker, T., Parlikad, A. K., Lutfiyya, H., Kanhere, S. S., Sakellariou, R., Dustdar, S., . . . Uhlig, S. (2022a). AI for next generation computing: Emerging trends and future directions. *Internet of Things*, *19*, 100514. https://doi.org/10.1016/j.iot.2022.100514

Gill, S. S., Xu, M., Ottaviani, C., Patros, P., Bahsoon, R., Shaghaghi, A., Golec, M., Stankovski, V., Wu, H., Abraham, A., Singh, M., Mehta, H., Ghosh, S. K., Baker, T., Parlikad, A. K., Lutfiyya, H., Kanhere, S. S., Sakellariou, R., Dustdar, S., . . . Uhlig, S. (2022b). AI for next generation computing: Emerging trends and future directions. *Internet of Things*, *19*, 100514. https://doi.org/10.1016/j.iot.2022.100514

Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2020). Machine learning in IoT Security: current solutions and future challenges. *IEEE Communications Surveys & Tutorials*, *22*(3), 1686–1721. https://doi.org/10.1109/comst.2020.2986444

Ibn-Mohammed, T., Mustapha, K., Godsell, J., Adamu, Z., Babatunde, K., Akintade, D., Acquaye, A., Fujii, H., Ndiaye, M., Yamoah, F., & Koh, S. (2020). A critical analysis of the impacts of COVID-19 on the global economy and ecosystems and opportunities for circular economy strategies. *Resources Conservation and Recycling*, *164*, 105169. https://doi.org/10.1016/j.resconrec.2020.105169

J, C. R. K., & Majid, M. A. (2020). Renewable energy for sustainable development in India: current status, future prospects, challenges, employment, and investment opportunities. *Energy Sustainability and Society*, *10*(1). https://doi.org/10.1186/s13705-019-0232-1

Khan, A., Sohail, A., Zahoora, U., & Qureshi, A. S. (2020). A survey of the recent architectures of deep convolutional neural networks. *Artificial Intelligence Review*, *53*(8), 5455–5516. https://doi.org/10.1007/s10462-020-09825-6

Khorsandroo, S., Sánchez, A. G., Tosun, A. S., Arco, J., & Doriguzzi-Corin, R. (2021). Hybrid SDN evolution: A comprehensive survey of the state-of-the-art. *Computer Networks*, *192*, 107981. https://doi.org/10.1016/j.comnet.2021.107981

Kodheli, O., Lagunas, E., Maturo, N., Sharma, S. K., Shankar, B., Montoya, J. F. M., Duncan, J. C. M., Spano, D., Chatzinotas, S., Kisseleff, S., Querol, J., Lei, L., Vu, T. X., & Goussetis, G. (2020). Satellite Communications in the New Space Era: A survey and future challenges. *IEEE Communications Surveys & Tutorials*, *23*(1), 70–109. https://doi.org/10.1109/comst.2020.3028247

Kreutz, D., Ramos, F. M. V., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2014). Software-Defined Networking: A Comprehensive survey. *Proceedings of the IEEE*, *103*(1), 14–76. https://doi.org/10.1109/jproc.2014.2371999

Liu, F., Cui, Y., Masouros, C., Xu, J., Han, T. X., Eldar, Y. C., & Buzzi, S. (2022). Integrated Sensing and Communications: Toward Dual-Functional Wireless Networks for 6G and beyond. *IEEE Journal on Selected Areas in Communications*, *40*(6), 1728–1767. https://doi.org/10.1109/jsac.2022.3156632

Mansell, R. (2021). Adjusting to the digital: Societal outcomes and consequences. *Research Policy*, *50*(9), 104296. https://doi.org/10.1016/j.respol.2021.104296

Martínez-Plumed, F., Gómez, E., & Hernández-Orallo, J. (2020). Futures of artificial intelligence through technology readiness levels. *Telematics and Informatics*, *58*, 101525. https://doi.org/10.1016/j.tele.2020.101525

Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., & Poor, H. V. (2021). Federated Learning for Internet of Things: A Comprehensive survey. *IEEE Communications Surveys & Tutorials*, *23*(3), 1622–1658. https://doi.org/10.1109/comst.2021.3075439

Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2020). Blockchain for 5G and beyond networks: A state of the art survey. *Journal of Network and Computer Applications*, *166*, 102693. https://doi.org/10.1016/j.jnca.2020.102693

Nowak, T. W., Sepczuk, M., Kotulski, Z., Niewolski, W., Artych, R., Bocianiak, K., Osko, T., & Wary, J. (2021). Verticals in 5G MEC-Use cases and security challenges. *IEEE Access*, *9*, 87251–87298. https://doi.org/10.1109/access.2021.3088374

Paul, M., Maglaras, L., Ferrag, M. A., & Almomani, I. (2023). Digitization of healthcare sector: A study on privacy and security concerns. *ICT Express*, *9*(4), 571–588. https://doi.org/10.1016/j.icte.2023.02.007

Petersson, L., Larsson, I., Nygren, J. M., Nilsen, P., Neher, M., Reed, J. E., Tyskbo, D., & Svedberg, P. (2022). Challenges to implementing artificial intelligence in healthcare: a qualitative interview study with healthcare leaders in Sweden. *BMC Health Services Research*, *22*(1). https://doi.org/10.1186/s12913-022-08215-8

Ploetz, E., Engelke, H., Lächelt, U., & Wuttke, S. (2020). The chemistry of reticular framework nanoparticles: MOF, ZIF, and COF materials. *Advanced Functional Materials*, *30*(41). https://doi.org/10.1002/adfm.201909062

Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: tensions in privacy and data. *Journal of the Academy of Marketing Science*, *50*(6), 1299–1323. https://doi.org/10.1007/s11747-022-00845-y

Radu, R. (2019). Negotiating internet governance. In *Oxford University Press eBooks*. https://doi.org/10.1093/oso/9780198833079.001.0001

Ranaweera, P., Jurcut, A. D., & Liyanage, M. (2021). Survey on Multi-Access Edge Computing Security and Privacy. *IEEE Communications Surveys & Tutorials*, *23*(2), 1078–1124. https://doi.org/10.1109/comst.2021.3062546

Rashid, A. B., Kausik, A. K., Sunny, A. a. H., & Bappy, M. H. (2023). Artificial intelligence in the military: An overview of the capabilities, applications, and challenges. *International Journal of Intelligent Systems*, *2023*, 1–31. https://doi.org/10.1155/2023/8676366

Singh, A., Dev, K., Siljak, H., Joshi, H. D., & Magarini, M. (2021). Quantum Internet—Applications, functionalities, enabling technologies, challenges, and research directions. *IEEE Communications Surveys & Tutorials*, *23*(4), 2218–2247. https://doi.org/10.1109/comst.2021.3109944

Swain, S., Bhushan, B., Dhiman, G., & Viriyasitavat, W. (2022). Appositeness of optimized and reliable machine learning for healthcare: a survey. *Archives of Computational Methods in Engineering*, *29*(6), 3981–4003. https://doi.org/10.1007/s11831-022-09733-8

Tlili, F., Fourati, L. C., Ayed, S., & Ouni, B. (2022). Investigation on vulnerabilities, threats and attacks prohibiting UAVs charging and depleting UAVs batteries: Assessments & countermeasures. *Ad Hoc Networks*, *129*, 102805. https://doi.org/10.1016/j.adhoc.2022.102805

Wanasinghe, T. R., Wroblewski, L., Petersen, B. K., Gosine, R. G., James, L. A., De Silva, O., Mann, G. K. I., & Warrian, P. J. (2020). Digital Twin for the oil and gas industry: Overview, research trends, opportunities, and challenges. *IEEE Access*, *8*, 104175–104197. https://doi.org/10.1109/access.2020.2998723

Zawish, M., Dharejo, F. A., Khowaja, S. A., Raza, S., Davy, S., Dev, K., & Bellavista, P. (2024). AI and 6G Into the Metaverse: Fundamentals, Challenges and Future Research Trends. *IEEE Open Journal of the Communications Society*, *5*, 730–778. https://doi.org/10.1109/ojcoms.2024.3349465