International Journal of
Science, Architecture, Technology and Environment

How 5G and Edge Computing Are Transforming Data Security

Taiwo Justice Olorunlana[1*]

[1] Lamar University, 10440 South Dr, Hoston Texas, USA, 77099

taiwojusticeo@gmail.com

*Corresponding author

Abstract

As 5G networks and edge computing expand, data security is being transformed, ultra-fast speeds are made possible, latency is lowered, and data processing is distributed quite far. Edge computing supports developing applications including driverless vehicles, telemedicine, and smart cities by processing data closer to the source, hence improving efficiency, network dependability, and These developments, meantime, also bring cybersecurity issues that must be resolved. The distributed character of 5G and edge computing expands attack surfaces, therefore exposing several avenues of access for cybercrime. Often lacking strong security mechanisms, edge devices become main targets for viruses, hacking and data leaks. To stop illegal access, safeguarding data transmission across remote networks also calls for sophisticated encryption, authentication systems and artificial intelligence-driven threat detection. This article displays the effect of age computing and 5G on the protection of data, eliminates major dangers and reduces measures, discovering difficulties and opportunities. Real world examples in the US look at the possible future and current threats of things like healthcare, finance, as well as core infrastructure. Topics include device authentication, regulatory compliance, data integrity, and DDoS attack resilience. If they want to lower the risk, then organizations must accept zero-trust systems, which are supported by tracking artificial intelligence and layer encryption for sensitive data. With machine learning technologies, automobile incident response and anomaly detection can significantly reduce the proactive strength of security. What's more, the assurance of data privacy and avoiding legal consequences hinge upon compliance with regulations including European General Data Protection Regulation (GDPR), Health Insurance Portability & Accountability Act (HIPAA), and California Consumer Privacy Act (CCPA). Adoption of 5G and edge computing quickens, hence cybersecurity policies must be strengthened. Businesses and governments may exploit the advantages of new technologies while protecting important data assets in an era of hyperconnectivity and scattered networks by tackling developing risks and improving network defenses.

Keywords: 5G and Edge Computing; Data Security; Data Transmission; Data Integrity and Privacy Challenges; IoT Vulnerabilities and Increased Entry Points; U.S. Government Initiatives on 5G Security; DDoS attack resilience

Chapter 1

1.0. Introduction

The advent of 5G networks has fundamentally transformed data processing, transmission and security. Thus, for edge computing, it is a new point of departure. Data handled in this way can now be given new media of development. The advances which 5G technology has now made possible—from smart cities and driverless cars to healthcare without borders—all rely on its radical new speed (how radically long it takes to get to the other end).

Data flows closer to enterprises. In earlier times, depending on a centralized cloud infrastructure made it impossible for enterprises to find their data when they needed it. New security issues crop up as data approaches people, also creating issues about just whose information it is (privacy), whether there are unauthorized sources trying to pick up your messages in transit, and weaknesses.

Complementing 5G technology, edge computing distributes data processing among several edge devices and nodes, therefore lowering network congestion and enhancing reaction times by means of which data processing is decentralized: This strategy reduces data exposure to outside cloud providers, therefore improving network security. Edge computing's distributed character, however, also increases the attack surface, hence increasing system vulnerability to cyberattacks. Edge devices—including IoT sensors and autonomous systems—often lack the strong security safeguards seen in conventional cloud environments, which makes them possible access sites for hostile actors (Singh et al., 2023).

The more connected devices, the harder managing security in richly dispersed networks gets (Patel et al., 2022). This technological marriage affords both opportunities and risks regarding data security. These technologies will inevitably suggest new security holes. At the same time, however, they also mean faster processing of data and networks that are sure to be more reliable (Gupta & Kumar, 2023). To do so, companies are turning to a range of measures linked to either artificial intelligence or blockchains and will keep running these defenses continuously as long as they can (Jones et al., 2022).

Furthermore, the mix of 5G and edge computing is poised to transform the IT scene and solve important problems that contemporary companies deal with. Amy Sara (2024) stated that, "This synergy increases the performance of applications in various fields." He even more underlined that, as "Gartner predicts, 75% of the venture data will be processed at the edge for a few years instead of centralized data centers, which highlights the immediate need for businesses to adopt these techniques.

Following Amy Sarah's observations (2024) combining 5G with edge computing not just improves present IT infrastructure, it even marks a transformation in what tasks enterprises must carry out and how they go about handling data processing, security, and efficiency. Businesses can perform real-time processing by placing the computation on the network edge, thus easing the pressure on centralized data centers. This is especially critical for sectors such as finance, healthcare, manufacturing, and autonomous transportation, where a difference of milliseconds equates to safety, production speed, or decision-making.

The prediction of Gartner that in five years 75% of corporate data would be moved to the edge heralds a total change in company IT strategy. Businesses that do not seize the opportunity of using 5G as well as edge computing will find themselves outmaneuvered by competitors taking advantage of less lag time, more bandwidth, and greater security to enrich customer satisfaction and innovation. 5G's ultra-reliable low-latency communications (URLLC) features added to edge computing will enable projects such as creating immersive virtual reality (VR) experiences for people, smart cities, or industrial automation. Real-time analytics at the edge, for example, enable manufacturers in smart factories to quickly find and correct production mistakes, therefore enhancing operational effectiveness. Edge computing combined with 5G can similarly improve telemedicine in healthcare by offering instant AI-driven diagnostics with low latency, hence ensuring improved patient outcomes.

Amy Sarah's point of view essentially emphasizes that in a digital-first economy companies must adopt 5G and edge computing if they are to remain competitive, safe, and agile. Integrating these techniques strategically will help companies manage exponential data expansion, promote cyber security rescue and provide innocent user experience in the growing world through technologies.

By highlighting the main risks, problems and reaction methods, it looks at the impact of 5G on paper edge computing and data security. The study of real -world case from the United States depicts both potential and dangers in areas such as healthcare, finance and significant infrastructure, as well as device authentication, regulatory compliance, data integrity and DDOS attacks also sees flexibility

Chapter 2

2.0. Understanding 5G and Edge Computing

When 5G and edge computing come together, the computerized terrain will see a substantial change in structure, and the methods of data transmission and processing will also be remodeled. Although individually strong, both have transformative power when used together. 5G is designed to provide ultra-fast data throughput, low latency, and enhanced connectivity.

This improves network performance, allowing real -time apps, innocent streaming and spreading the internet of things (IOT) nodes. Alone, 5G has tremendous strength. Nevertheless, if combined with edge computing, 5G is very promised in 5G. By processing the data close to the base, the age computing reduces the need to carry large versions of data for centralized data centers. The proximity means less bandwidth is required for real-time data processing, and lower latencies arise as well (Shi et al., 2016).

Edge computing guarantees faster answers and more effective data management by handling data at or near the source. While edge computing guarantees that this data is handled quickly at its source, 5G's high-speed connectivity helps to support the fast data transmission (Taleb et al., 2017). Augmented reality, smart city infrastructure, and self-driving cars in development are just some of the fields that need this mix.

In autonomous driving cars, for example, vast versions of real -time data are built and analyzed to keep the vehicle safe. With 5G and Edge Computing, this immediate data swapping and processing is possible, guarantees timely decisions (Satyanarayana, 2017). Moreover, businesses can use this connectivity to improve customer experiences. Companies now ought to spread edge computing on 5G networks so that premium, next-generation applications and services are available to a wider range of users. According to current statistics, this setup enables informed decision-making which sheds light on user behavior and developing market trends as well as gives deep user behavior insights. Edge computing and 5G come with questions, however. Processing is distributed among nodes across the system, meaning that the first concern here lies with data privacy and security.

In addendum, the infrastructure needed for widespread practical application is rather massive; Nevertheless, the combined forces of 5G and edge computing allowing faster, more reliable, and cheaper data handling transmission, this next generation of systems creation will penetrate fields ranging from healthcare through manufacturing. An amalgamation of edge computing with 5G marks a watershed change in data treatment. This potent mixture is poised to create new possibilities, lead to the next waves of technical revolutions, and remake user experience in our connected world.

2.1 What is 5G and Edge Computing

Indeed, Amy Sara (2024) mentioned that "5G edge computing is high speed, 5G high-bit network combined with decentralized computing. On the other hand, it can also send real-time data processing and decisions where it can also send. They need to be made. " There are both similarities and differences in the different views given on 5G edge computing by National Designated Personnel and the authors. Huang Xiaoguai (2021) also points out these tributaries of 5G.

It was he who stressed how "5G with edge computing actually uses 5G's faster data transmission, lower latency, and greater capacity than older technologies so that more information enters into users' hands instantaneously." Together with National Designated Personnel, Huang, a different author, observed that, "5G—or the fifth generation of wireless technology—is a new advance in mobile networks that offers ultra-high-speed transmissions, zero-delay connections, and high levels of wireless connectivity. This technology is changing the way we work, communicate, and harmonize our lives" (Andrews et al., 2021).

In this connection, it is necessary for academics to analyze his views and highlight important differences and parallels in 5G edge computing. First, Amy Sarah (2024) underlines how 5G integrated with edge computing optimizes the network's decision-making and real-time analysis of data at its edge. The author's description highlights another major gain derived from deploying edge computing: decentralized data processing. The closer we process data to its source, the less is the latency and the greater its benefit to inventive uses in sectors like intelligent manufacturing and driverless vehicles.

Where Andrews et al. (2021) differ is in their technological take on 5G: they describe it as a sweeping change that brings improvements in both engagement, connectivity and communications. While they do acknowledge the speed, low latency, and good device connectivity of 5G, their reasons do not touch on the vital element for real-time applications—edge computing. Though they emerge from diverse perspectives in 5G age computing, they have qualifications at these two areas. Amy Sara (2024) presented it for its functional mix with specific power in age computing and real-time data processing. Andrew' et, al (2021) Paint a large picture of 5G on a world scale, especially emphasizing its characteristics rather than connecting it with edge computing.

For autonomous driving, Sara (2024) definition is clearly applied. For traffic management, obstruction and navigation-All of them have data problems of the real world-Swar-drive cars should use 5G edge computing to ensure that there is no dependence on distant cloud servers, however, the reasoning would be more helpful in comprehending what part 5G plays to connect people regularly and communicate. The result is that while Andrews et al. (2021) provide an overall technical map, Sarah (2024) views this issue in more detail than anyone else today. In her point of view, which technical theory is a closer fit for economic practice?

In the context of 5G and edge computing, the reduction of total latency, but also bandwidth use, comes from local processing. Rather than transferring data to a central location, edge computing does this processing directly on the devices. Instead of centralized cloud data centers, edge computing places data closer to the source. This spreads processing power out at different places, accordingly, increasing security and reducing response times. 5G's combination with edge computing means that uses in areas such as manufacturing, robotics and AI, which were seen as highly difficult not long ago—now appear quite practical. Across several IoT scenarios, it paves the way both for near but quick changes from data and more effective operations.

2.1.1. Ultra-High Speed

The most obvious advantage of 5G is that it provides speed up to 10 GBPS, which is about 100 times faster than 4G. Mobile films can be downloaded in seconds, and full HD entertainment can be seen without any hindrance (Shafi et al., 2017). Increasing speeds also enable cloud computing and remote working to become more productive, reducing reliance on local storage.

2.1.2. Low Latency

The latency, or delay in data transmission, of 5G networks is far lower than in previous generations—down to a millisecond. Applications like self-driving cars, distant surgery, real-time gaming, and others where little latency can have a significant impact depend mainly on this (Dang et al., 2020).

2.1.3. Large -scale connectivity 5G network

Large -scale connectivity 5G networks can support billions of connections simultaneously. This is the backbone that will power the Internet of Things (IoT). With its ability to manage many connections, 5G will enhance smart homes, wearable devices, and industrial automation, both on an integrated level and as an extension to all levels of planning and control. Since smart cities are emerging, removing 5G boundaries, very quick real time to open capacity for large amounts of information (Osseiran et al., 2016).

2.1.4. Why 5G is important?

Why 5G is important, apart from just speed, 5G is expected to raise areas ranging from healthcare and transport to entertainment and construction systems, which are currently located in place (Bokardi et al., 2014). It will offer innovations like augmented reality (AR), virtual reality (VR), and AI-driven automation to bring the world closer together in a more connected and intelligent form of multi-core design. This technology integration also improves machine operation efficiency by moving processing power closer to the data source. Edge computing offloads data onto secure networks located near its origin, rather than risking privacy in remote locations without local storage. In areas with limited connectivity, 5G edge computing is an adaptive solution for backstage task processing.

Chapter 3

3.0 How 5G and Edge Computing Enhance Data Security

Faster and Secure Data Transmission lowers latency, decentralizes data processing, and improves real-time threat detection, therefore greatly enhancing data security by combining edge computing with 5G. Edge computing minimizes cyber danger exposure during transmission by data closer to the source.

Multi-factor authentication included in strong encryption, network slicing and 5G networks helps reduce illegal access hazards. Rapid discrepancy operated by artificial intelligence also helps in safety systems. A combination of these technologies helps companies improve cyber security, so the hyper connectivity era guarantees flexible, safe and efficient digital ecosystems in the era.

3.1. Faster and Secure Data Transmission

The 5G technology improves data security through rapid encryption. From end to end, 5G ensures that private data is encrypted when it is moving between devices and servers, sophisticated encryption techniques developed for connectivity of this new era (Sharma and Patel, 2023). Its ultra-fast connectivity reduces the vulnerabilities hackers can exploit that are suffered by conventional networks, in which congestion makes for delays and hence weaknesses.

3.1.1. Decentralized Data Processing

Edge computing increases security yet further by shifting data as close as possible to where it is generated and becoming less dependent on centralized cloud services for the job. In this way, through a distributed approach to data storage and computing, breaches and interception of data are minimized (thus also reducing all associated risks) (Williams et al., 2022). Keeping sensitive data at the edge allows businesses to keep their information under control and cut down the risks of cyber-attack.

3.1.2 Reduced Latency for Threat Detection

With edge computing and 5G, the actions of any line can be observed in near real-time. Real-time security systems with lower latency can faster discover and react to potential dangers, so they don't become more serious (Chen & Liu, 2021). For industries such as smart cities, banking, and healthcare, where data security is important, such a proactive approach serves to improve security. 5G and edge computing mean quicker, more secure data transmission, and network processing. So, in this digital age, it is guaranteed that security will improve!

3.2 Distributed Security Architecture

Edge computing is a method to distribute the processing of data among nodes, and unlike centralized cloud solutions, it avoids single points of failure. When data processing is moved away from the node, its security and resistance are improved. When the system works in this manner, if one node fails or is hijacked, the system is still able to continue operation with minimal interruption. This, in turn, has an impact on the speed at which possible security incidents can be noticed, thus both improving performance and enhancing security.

The basic goals of distributed computing systems include improving scalability, fault tolerance, and performance of an application. By distributing the task among several nodes, the system can handle different volumes of traffic and quantities of data without sacrificing speed or reliability. Monolithic designs often have difficulty with this because if one node fails, the others will continue to work—ensuring that processes unaffected by an outage or problem still go about their business as planned, thus minimizing the impact on overall operation.3.3 Reduced Risk of Centralized Breaches With data stored and processed at the edge, cybercriminals cannot target a single server to access all information.

Chapter 4

4.0. Emerging Security Threats with 5G and Edge Computing

With 5G and edge computing allowing more devices to access networks, the potential attack surface, or gateway for attack, naturally expands. By turning ordinary things into the Internet of Things, each of these devices becomes a potential exploit or tool for a hacker.

The robust and secure measures applied to traditional data centers are absent on these devices. Once they are hacked into, or the victim of malware hijacking, data is transmitted between breached servers or stolen all without much difficulty as in other industries.

Edge computing, moreover, lacks centralization. Its extreme dispersion of data sources and complex lines make it harder to monitor. Consequently, while individual services are protected, a greater overall risk exists (Tinglei Zhao and Jorge Li, 2024).

4.1. IoT Vulnerabilities and Increased Entry Points

The proliferation of IoT devices is now linked with 5G networks worldwide, opening billions of devices to potential cyber-attacks. Many of these devices, however, are ill-protected, without even the most basic cybersecurity measures such as strong encryption and authentication protocols.

In 2016, for example, the Mirai Botnet attack took advantage of IoT devices that were vulnerable and transformed them into zombie bots; it was one of the largest Distributed Denial-of-Service (DDoS) attacks ever recorded. This attack showed how vulnerable IoT devices are in a 5G environment and therefore also provided evidence for the urgency of stronger IoT network protection mechanisms. (Kassem & Ransford, 2023).

4.2. Data Integrity and Privacy Challenges

However, decentralization brings serious data integrity and privacy challenges. Without proper encryption and safety, edge devices become an easy goal for cyber-attack. Hackers can eavesdrop or tamper with data as it is being processed on the edge in real time. This not only distorts the accuracy of data, which can be catastrophic for analysis, but also potentially violates privacy laws. It is particularly impermeable standards like those shielding identities in healthcare and financial transactions which determine this problem (Zhang and Xu: 2013).

Chapter 5

5.0. How 5G and Edge Computing Secured Smart Cities

5G and edge computing have vastly improved the security and efficiency of running smart city projects, especially in New York City. For traffic management, the quick processing of camera feeds through edge devices helps ensure immediate responses to any incident that occurs.

With slow or rapid alert times, emergency response systems become burdensome on law enforcement and emergency services. An important security measure in the city's infrastructure is the use of encrypted communication between edge devices, effectively thwarting potential cyberattacks on public systems such as traffic lights or public transit networks. These technologies not only improve operational efficiency, however, also ensure that citywide data privacy and security are safeguarded (Smith & Taylor, 2024).

5.1 Cyberattack on 5G-Enabled Edge Devices

In 2021, an important cyberattack was launched, targeting 5G-connected security cameras on the grounds of an industrial estate. By taking advantage of vulnerable firmware in these cameras, the hackers obtained control over all of them. This compromised operations at the facility and posed a serious risk to the establishment itself. Fortunately, edge security firewalls installed contained the breach and isolated infected devices from other parts of the network. This attack is the best possible example of why firmware must be updated on a regular basis and how AI-driven security at the edge is needed to detect and neutralize threats in real-time. These measures will be vital if 5G-enabled edge devices are to be protected against future cyberattacks (Williams & Zhang, 2023).

5.2 Protecting Healthcare Data in Edge Computing Networks

Mayo Clinic has successfully integrated edge computing into its remote patient monitoring systems, particularly as regards the handling of sensitive health data like heart rate and blood pressure. By processing data at the edge, the clinic is now able to give real-time AI-powered alerts for any abnormal health conditions. With immediate response, potential emergencies are averted. To maintain patient privacy, all the data is encrypted before it goes up to Cloud storage to guard against unauthorized peeping and the potential for data leaks. This approach ensures the security of healthcare data—even though it is processed in a network of split nodes (Jones & Williams, 2023).

Mayo Clinic's use of edge computing technologies in remote patient monitoring delivers yet another milestone advances in healthcare technology. By processing such sensitive medical data as heart rate and blood pressure at the edge, the clinic thereby not only speeds up decisions in real time but also, with lower latency, reduces response time to critical changes in health levels. This will enable proactive intervention and, therefore, result in happier outcomes for patients too. Recently, before Cloud storage occurs, the data for transmitting usages of encryption is vital for information security. It ensures confidential patient personal data remains so, and that compliance with privacy rules, such as HIPAA, is enforced. For Instance, this is a case of using distributed computing and artificial intelligence to raise efficiency nevertheless keep security high.

Chapter 6

6.0. Regulatory and Compliance Considerations

6.1 U.S. Government Initiatives on 5G Security

The active stage of broadcasting content on YouTube is not as soon as you begin rolling, However, right away once ads are thrown in enroute to that target video stream. Forensics may be the best strategy when it comes to proving that these companies are not merely parasites skimming money off video content creators who do most of the work for nothing, or copyright law miscreants ripping off American livelihoods — nevertheless, too often, nobody has the time or resources for such workable strategies without cooperation from Hollywood (Cohen & Dupler, 2003).

Behavioral forensics videos by now are hiding ten zillion at a time. To empty out this kind of sickeningly large group of tourists pouring in from online videos uploaded, know how you laughed and made it available for all. They threw off their sheepskin vest before running you into the merest trickle on Terre Haute Communicator of someone trying to organize a speak-out.

So, one must continually report these gentlemanly requests to NLP and MSA have won some extreme victories in his love affair with just another colonel (believe that). Furthermore, the establishment of edge computing security rules by the National Institute of Standards and Technology (NIST) offers companies a disciplined framework to protect edge devices and networks, therefore mitigating dangers present in distributed computing systems. Both CISA and NIST serve to improve national cybersecurity resilience by providing these thorough criteria and best practices, thereby enabling firms to remain ahead of changing cyberthreats and guarantee compliance with federal laws. These initiatives are especially important as edge computing and 5G networks are revolutionizing sectors and allowing smart technologies necessary for the direction of digital security.

6.2 Edge Security Standards

Edge Security Standards have developed to protect distributed systems as edge computing grows more essential to contemporary networks. One such approach is Zero Trust Architecture (ZTA), which guarantees rigorous access control at the edge—where every device and user is handled as maybe untrusted. This not only would do away with the old idea of "trust but verify"—which means that there are recurring checks for validation required before certain information can be accessed privately by other spaces (Johnson, T., & Kumar, 2022).

Underpinning all our security efforts at the edge, the Secure Access Service Edge (SASE) architecture works in an integrated way across network security and cloud access management. Thus, it provides data protection no matter where the user is from home (Johnson, T., & Kumar, 2022). As we enter the 5G and x-nir era, ZTA and SASE together provide strong security for distributed networks. This reduces potential flaws as we safeguard the key data we need. Such services as the Zero Trust Architecture (ZTA) together with SASE edge computing networks are also effectively maintained with top-level security (Johnson, T., & Kumar, 2022). Those frameworks have visibility and control over the whole network, meaning it is important for maintenance of data privacy and security on a large scale in the 5G age (Johnson, T., & Kumar, 2022).

Chapter 7

7.0. Future Trends in 5G and Edge Security

Edge computing and 5G are growing more and more popular; their future developments will surely affect security. Threat detection based on artificial intelligence will rechange network security. Within 5G edge systems, it can operate high-efficiency monitoring and intrusion identification, therefore enabling faster reactions with less often erroneous outcomes (Patel & Roberts, 2023). This means there will have to be a new approach to data security and network reliability.

Quantum-safe encryption—in this way, as heralded by Patel and Roberts last year, future security trends will be 5G-resilient and edge-network-proof. In their AI and Quantum-Safe Encryption study, they explain how these technologies will strengthen protection against future forms of cyberattacks. In the future, AI will be able to automate threat detection, which is bound to result in more timely responses to cyberattacks added to fewer false alarms. This will become increasingly essential as real-time protection of sensitive data grows more important. Further down the road, as quantum computing becomes commercially available, traditional cryptographic methods will no longer offer any security. This emerging threat can be thwarted tomorrow by us adopting quantum-safe encryption to secure 5G networks and edge devices. Developed and put into practical use, these technologies will guarantee that tomorrow's 5G networks and edge computation secure indispensable industries such as healthcare and the intelligent urban concept goes ahead.

7.1. Best Practices for Securing 5G and Edge Computing

It takes a variety of ways to prevent both 5G and side networks from dissolving. This is his unique character as a network in decentralized and interconnected contexts. Multi-factor authentication (MFA) is important to prevent unauthorized access. It requires several verification methods before giving sensitive information or access to the system network (Patel and Roberts, 2023). Regular Security Patching is also important when deploying edge devices, which can form the basis for many future cyber weapons if they are not carefully guarded. Firmware updates help pick off bugs and vulnerabilities, meaning that attackers find it harder to successfully exploit flaws already well known not just by them but also others working in the field (Jones & Williams, 2023).

Encryption is still fundamental for security since it keeps sensitive information safeguarded as it passes through either within your network architecture or on its way to the cloud (Sullivan & Thomas, 2023). These best practices, once brought together, create a stronger posture of security for 5G and edge computing infrastructure. The researcher opined that these best practices—Multi-Factor Authentication (MFA), regular security patching, and data encryption—constitute the basics of trying to confront the security challenges inherent with 5G and edge computing.

MFA is important in containing unauthorized entry, which is more difficult in a connected internet where there are increasing numbers of devices joining the network. Applying patches regularly can prevent problems waiting to erupt as high edge suddenly threatens internal systems. Another point worth noting is that one can not only use in-transit security methods like data encryption, but also ensure confidence and compliance with privacy rules, especially for cases such as healthcare and banking where sensitive information must be exchanged. The combination of this adds up to a careful and solid security base, which can meet the demands of 5G edge computing. It's currently tackling threats while they're still in early stages.

Conclusion

Ultimately by increasing speed, lowering latency, and distributing data processing, 5G and edge computing have clearly transformed data security. Real-time decision-making made possible by these developments supports developing technologies such remote healthcare, smart cities, and autonomous vehicles as well as Still, as these technologies develop, they also bring fresh cybersecurity issues. As they grow, especially through IoT devices and edge networks, attack surfaces are enriched. While it enhances productivity, the decentralization of data processing raises the question of safeguarding private data as it approaches end-users.

Lacking robust protective mechanisms, edge devices then become potential attack points. When security is managed through wide-area networks, the risks of data breaches and cyber-attacks grow or are multiplied, as well as making their resulting negative fallout more difficult to manage. To tackle these problems, organizations and governments must establish complete security systems—data encryption, regular security patching, and multi-factor authentication are all essentials. By using quantum-safe encryption and AI-powered threat detection, we can even further strengthen defenses against the new risks. This approach will help companies ensure that the move to 5G and edge computing is safe, secure, and capable of safeguarding vital data in a world increasingly linked through connectivity.

Declaration of Conflicting Interests

The authors declare no potential conflicts of interest with respect to the research, authorship and publication of this article.

Funding

The author received no financial support for the research, authorship and publication of this article.

References

Akamai. (2023). Edge computing & 5G: Emerging technology shaping the future of IT. Retrieved from https://www.akamai.com

Amy Sarah (2024). 5G and Edge Computing: Empowering the Future of IT. Retrieved from https://www.znetlive.com/blog/5g-and-edge-computing-empowering-the-future-of-it/#:~:text=This%20integration%20leverages%205G%27s%20faster,by%20avoiding%20central%20data%20transmission.

Andrews, J. G., Buzzi, S., Choi, W., Hanly, S. V., Lozano, A., Soong, A. C., & Zhang, J. C. (2014). What will 5G be? IEEE Journal on Selected Areas in Communications, 32(6), 1065-1082.

Andrews, J. G., Buzzi, S., Choi, W., Hanly, S. V., Lozano, A., Soong, A. C., & Zhang, J. C. (2021). What will 5G be? IEEE Journal on Selected Areas in Communications, 32(6), 1065-1082.

Boccardi, F., Heath, R. W., Lozano, A., Marzetta, T. L., & Popovski, P. (2014). Five disruptive technology directions for 5G. IEEE Communications Magazine, 52(2), 74-80.

Chen, Y., & Liu, Z. (2021). Low-Latency Security in 5G Networks: Advancements and Challenges. International Journal of Wireless Security, 8(3), 102-118.

Dang, S., Amin, O., Shihada, B., & Alouini, M.-S. (2020). What should 6G be? Nature Electronics, 3(1), 20-29.

Gupta, P., & Kumar, S. (2023). Security threats in 5G and edge computing environments: A review. Journal of Cybersecurity, 18(2), 101-119.

Jones, M., & Williams, T. (2023). Securing healthcare data with edge computing: The Mayo Clinic case study. Healthcare Technology Journal, 29(2), 75-82.

Jones, R., et al. (2022). Zero-trust security models for 5G networks. Security & Privacy Journal, 11(1), 34-47.

Kassem, M., & Ransford, M. (2023). Security challenges and the IoT revolution in 5G networks. Journal of Cybersecurity, 30(4), 102-109.

Khan, S., & Singh, A. (2023). Security frameworks for edge computing: Zero Trust and SASE. International Journal of Cybersecurity, 19(4), 211-225.

Johnson, T., & Kumar, R. (2022). Advancing security with edge computing: A look into Zero Trust and SASE. Journal of Network Security and Privacy, 35(2), 80-90.

Lee, J., Kim, S., & Park, J. (2024). Enhancing security in 5G and edge computing environments. International Journal of Cybersecurity, 38(1), 24-33.

Li, X., et al. (2023). Enhancing data security through edge computing in 5G networks. Information Security Review, 22(5), 98-114.

Osseiran, A., Boccardi, F., Braun, V., Kusume, K., Marsch, P., Maternia, M., ... & Tullberg, H. (2016). Scenarios for 5G mobile and wireless communications: The vision of the METIS project. IEEE Communications Magazine, 52(5), 26-35.

Patel, V., & Roberts, L. (2023). Future trends in 5G and edge security: AI and quantum-safe encryption. Journal of Emerging Cybersecurity Technologies, 14(1), 45-53.

Patel, V., & Roberts, L. (2023). Future trends in 5G and edge security: AI and quantum-safe encryption. Journal of Emerging Cybersecurity Technologies, 14(1), 45-53.

Jones, T., & Williams, K. (2023). Securing the edge: Protecting sensitive data in 5G networks. Cybersecurity in Edge Computing, 18(2), 102-115.

Sullivan, D., & Thomas, M. (2023). Data encryption in distributed networks: A necessity for 5G security. Journal of Cybersecurity Standards, 21(3), 89-98.

Patel, V., et al. (2022). Authentication protocols for 5G security: A comparative study. IEEE Security & Privacy, 19(7), 56-72.

Satyanarayanan, M. (2017). The emergence of edge computing. Computer, 50(1), 30-39.

Shafi, M., Molisch, A. F., Smith, P. J., Haustein, T., Zhu, P., De Silva, P., ... & Tufvesson, F. (2017). 5G: A tutorial overview of standards, trials, challenges, deployment, and practice. IEEE Journal on Selected Areas in Communications, 35(6), 1201-1221.

Sharma, A., & Patel, R. (2023). Next-Gen Wireless Security: The Role of 5G Encryption. Cybersecurity Journal, 15(4), 78-92.

Sharma, D., & Chen, Y. (2022). Cybersecurity challenges in decentralized 5G networks. International Journal of Security Studies, 17(4), 67-83.

Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. IEEE Internet of Things Journal, 3(5), 637-646.

Singh, K., et al. (2023). IoT security vulnerabilities in edge computing environments. Journal of Information Security, 25(2), 112-128.

Smith, J., & Taylor, L. (2024). 5G and edge computing: Enhancing urban security in smart cities. Journal of Urban Technology, 22(1), 58-65.

Sullivan, R., & Thomas, G. (2023). U.S. government strategies for 5G and edge security. Journal of Cybersecurity Policy, 15(4), 45-52

Taleb, T., Samdanis, K., Mada, B., Flinck, H., Dutta, S., & Sabella, D. (2017). On multi-access edge computing: A survey of the emerging 5G network edge architecture and orchestration. IEEE Communications Surveys & Tutorials, 19(3), 1657-1681.

Williams, J., Brown, K., & Lee, M. (2022). Edge Computing and Cybersecurity: A New Era of Data Protection. Tech Security Review, 10(2), 45-61.

Williams, P., & Zhang, X. (2023). The role of edge security in defending 5G-connected devices. Cybersecurity and Privacy Journal, 18(3), 42-49.

Zhang, H., et al. (2021). The impact of 5G on real-time data processing and security. Future Networks Review, 9(3), 200-217.

Zhang, Y., & Xu, H. (2023). Data privacy and integrity in edge computing: Challenges and solutions. International Journal of Information Security, 42(2), 88-96.

Zhao, X., & Li, W. (2023). Cybersecurity challenges in edge computing and 5G networks. Journal of Network Security, 45(2), 56-65.