International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

The Power of TaaS: Challenges and Considerations of TaaS Adoption

Rami Saied AlZaben *

School of Engineering and Applied Science, The George Washington University (GWU), USA.

International Journal of Science and Research Archive, 2024, 13(02), 227–239

Publication history: Received on 25 September 2024; revised on 04 November 2024; accepted on 06 November 2024

Article DOI: https://doi.org/10.30574/ijsra.2024.13.2.2141

Abstract

Telecom as a Service (TaaS) is an emerging model based upon cloud infrastructure supporting telecommunications functions more cost-effectively and flexibly. The growth of TaaS adoption is explored in this research, and the major benefits to its adoption by telecom operators, including reduced cost, scalability, and perfect service delivery, are identified. However, organizations have to face several challenges when adopting TaaS. Security, regulatory compliance, and data privacy are all key issues. TaaS is a security vulnerability and compliance that is particularly complex across different legal jurisdictions, as it runs in a cloud environment. Also, safeguarding user data on privacy regulations remains a big deal. We discuss these challenges and propose strategies to overcome them so that telecom customers can have secure, compliant, and private TaaS.

Keywords: TaaS; Telecom as a Service; Security Regulations; Compliance; Data Privacy; Cloud Telecom; Telecom Infrastructure

Graphical Abstract

https://gigs.com/blog/what-is-telecom-as-a-service

* Corresponding author: Rami Saied AlZaben

1. Introduction

1.1. Telecom as a Service (TaaS) Definition and Concept

Telecom as a Service (TaaS) is a cloud-based solution that enables businesses to develop new business models for telecommunications services. In a traditional telecom setup, companies must invest heavily in physical hardware like networking equipment and servers, cabling, and so on to manage communication. It does not require a lot of capital expenditure, but this entity has to be heavily consumed with operational costs for maintenance, upgrades, and troubleshooting. However, TaaS doesn't require businesses to maintain or have Telecom infrastructures. In place of telecom, functions, such as voice, messaging, and data services, are virtualized and delivered over the internet, ordinarily on a subscription or pay-per-use basis.

TWe offers telecom services via cloud computing in a manner that allows flexible, scalable, and on-demand. This saves companies the headache of dealing with hardware or complex systems. By virtualizing telecom functions, businesses can most effectively adjust their communications systems to the changing needs, optimizing bandwidth, connectivity, and response times. In addition, TaaS promotes greater agility of telecom features and functionalities for the market to call, so enterprises can quickly integrate new telecom features and functionalities as market demands change. Due to this capability, TaaS is a key enabler of businesses embarking on their digital transformation journey.

In today's business landscape, wherein companies seek to improve efficiency and lower costs, TaaS has become more relevant to the telecommunications industry. The cloud platform provides telecom providers with the opportunity to offer a broad range of services and the flexibility and convenience demanded by modern enterprises. TaaS delivers a more cost-effective and efficient telecoms lifestyle by scaling services up and down in real-time, only paying for what is used. Consequently, TaaS is not only changing the telecom scene but also a driving force of innovation and competition among providers as they race to provide the best, most innovative, and fastest solutions to customer demand.

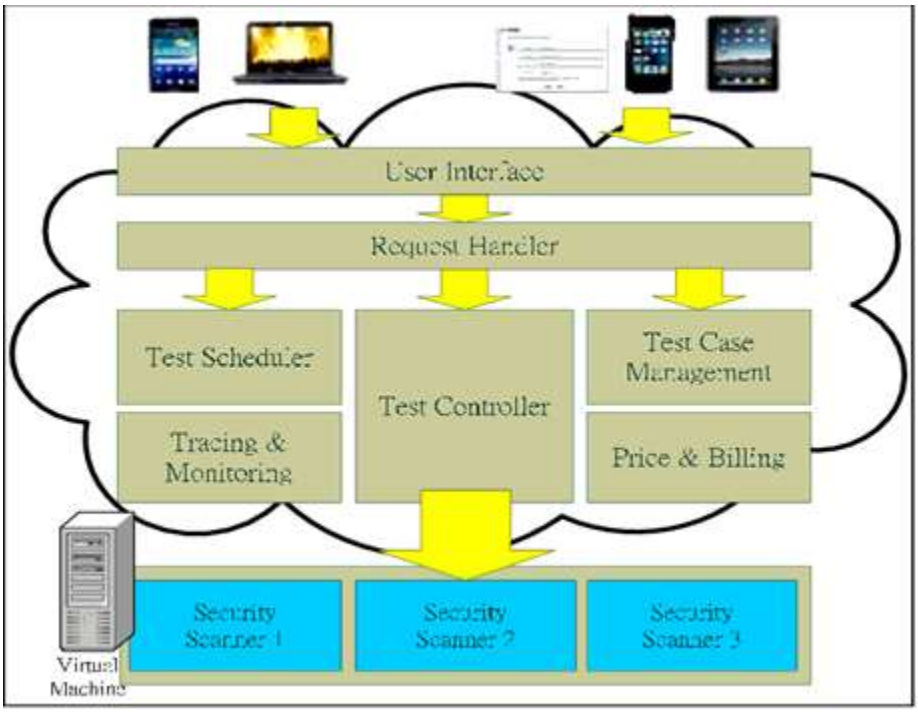

Figure 1 Taas Architecture Diagram

Source: Tung et al. (2014)

1.2. Scope of the Research

In this research, we take a closer look at the adoption of TaaS, looking at what it brings as an opportunity for business and telecom providers and its challenges. Specifically, it examines three critical factors that pose significant obstacles to the widespread adoption of TaaS: data privacy and regulatory compliance, all of which trade on security. Security concerns are introduced with TaaS as it is a cloud-based service, consequently making it a TaaS. Telecom environments

are vulnerable to cyberattacks, illegal access, and data breaches, which can falsify the communicative systems and violate the confidentiality of the information.

Organizations that adopt TaaS face another big challenge — regulatory compliance. Telecom services are heavily regulated and implemented with local and international laws. Even cloud-based services will not remove that complexity. Those regulations differ greatly within regions, particularly regarding data sovereignty, lawful intercept capabilities, and telecommunication infrastructure requirements. As more and more businesses go abroad, navigating this regulatory landscape becomes harder.

TaaS adoption is also dependent upon data privacy. Telecom services deal with sensitive and personal data, such as voice calls, messaging, and customer data. Since much of this data is stored and transmitted in cloud environments with TaaS, people have concerns about how data should be handled, stored, or shared. This research will examine how organizations can respond to these challenges to achieve secure, compliant, and privacy-focused communications.

This research on the scope intends to provide a holistic analysis of the challenges and considerations in adopting TaaS, particularly from the technical, legal, and privacy points of view necessary to bring the full benefits of cloud telecom services.

1.3. Importance of TaaS

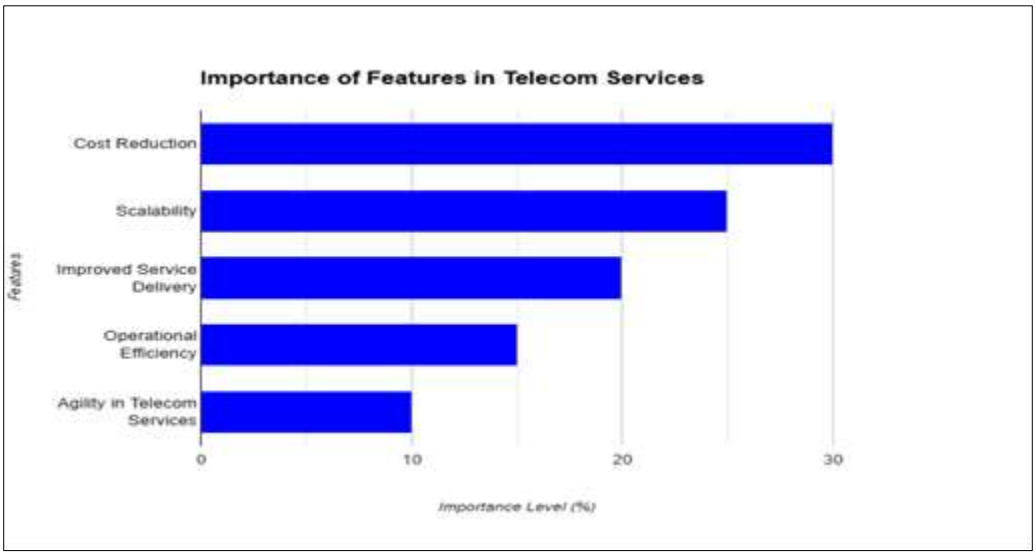

Figure 2 Importance of Telecom As Service

Table 1 Importance of TaaS Features for Telecom Operators

Feature	Importance Level (%)
Cost Reduction	30%
Scalability	25%
Improved Service Delivery	20%
Operational Efficiency	15%
Agility in Telecom Services	10%

Table 2 Challenges in Taas Adoption

Challenge	Impact Level (%)
Security	35%
Regulatory Compliance	30%
Data Privacy	25%
Customization and Flexibility	10%

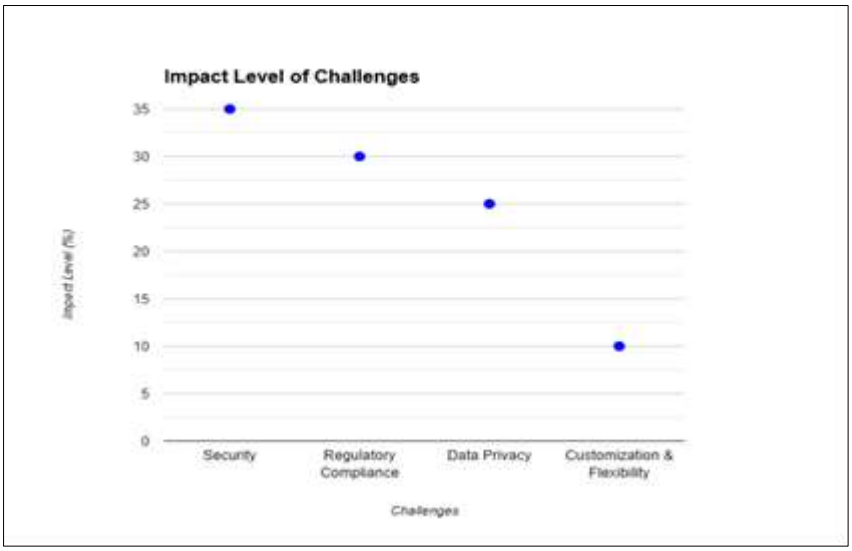

Figure 2 Impact level of challenges

TaaS is quickly expanding because corporations and organizations know the necessity for better, more efficient, and affordable telecom services. In traditional methodologies, telecom infrastructures are massive and complex structures that are costly to maintain, which is common since they need several staff and other resources. These systems also may need to be revised, meaning that the companies cannot grow and increase the telecommunication services offered to meet the changing internal needs or market peculiarities. On the other hand, TaaS is a flexible solution that frees users from these challenges because it outsources all telecom services to cloud providers.

Another striking advantage of TaaS is the degree of high operation cost saving. The markets have discovered that they can significantly cut initial costs through operational expenditure markets, cutting on expensive hardware and tools that would call for capital expenditure. Another advantage of TaaS is that it is responsible for only the consumption of the services availed, hence making telecommunication costs easier to manage and predict. In addition, since TaaS is scaleable, enterprises can flexibly change the telecom services they consume in real time to add or remove capacity, which means organizations benefit from improved utilization.

Besides cost reduction, TaaS also helps deliver and logistics telecom services. Businesses no longer have to pay attention to the details of actual telecommunications equipment, the maintenance of physical hardware, or telecommunication disruption. However, telecom providers manage all technicalities related to the service, thus guaranteeing that involved businesses get an unbroken and consistent communication service. This is especially beneficial for firms with branches in different regions or are forced to cater to a remote working environment, as TaaS can deliver access without regard for location.

TaaS also promotes innovation as it provides firms a means to use the best available telecom technology without long development drains or DandO. Thus, as delivery service advances, players can readily implement new services and solutions, including 5G networks, VoIP, and other improved instruments without long-lasting upgrading processes. This makes it possible for the business to compete effectively in an era characterized by the high use of telecommunications technologies.

2. Telecom as a Service Overview

2.1. Evolution of Telecom Services

In recent decades, the telecommunications sector has experienced a major transformation from old hardware-intensive models to cloud IoT services. As a result, telecom companies are placed to satisfy diverse and fluctuating market requirements in an affordable, adaptable, and customized way. Voice over Internet Protocol (VoIP), introduced in the middle of the 1990s, realized voice transmission over the Internet, which set the ball rolling for following innovations that formed the basis for nascent cloud solutions like Telecom as a Service (TaaS).

TaaS is the next generation of Telecom in which services and functions are hosted on the cloud to be delivered through the Internet. This model has allowed them to divorce themselves from the dependency on the physical infrastructure to operate, lower costs, and access flexible, scalable telecom solutions. Mobile Virtual Network Operators (MVNOs) have come to dominate the telecommunications landscape, and they lease wireless network capacity from major operators rather than own physical infrastructure. Most of their offerings tend to include mobile voice and data plans, IoT connectivity, customizable plans and niche services.

Organizations are turning to private 5G networks as their customizable solution for connectivity. High speed, low latency connection and improved security are what these networks offer, enabling organizations to control data flow seamlessly and reduce risks of privacy of the data and unauthorized access. Real-time data processing systems are ideal for applications such as autonomous vehicles, smart manufacturing, and industrial automation. With private 5G networks, large-scale and high-density IoT deployment can be enabled, and they are deployed in smart cities, automated factories, and remote monitoring. The telecommunications sector is evolving from old hardware-intensive heavy telecom models towards cloud services due to 5G, MVNOs, and private 5G networks. The result is more versatile, flexible, and friendly communication solutions for telecom companies to satisfy a wide range of different and varying market needs.

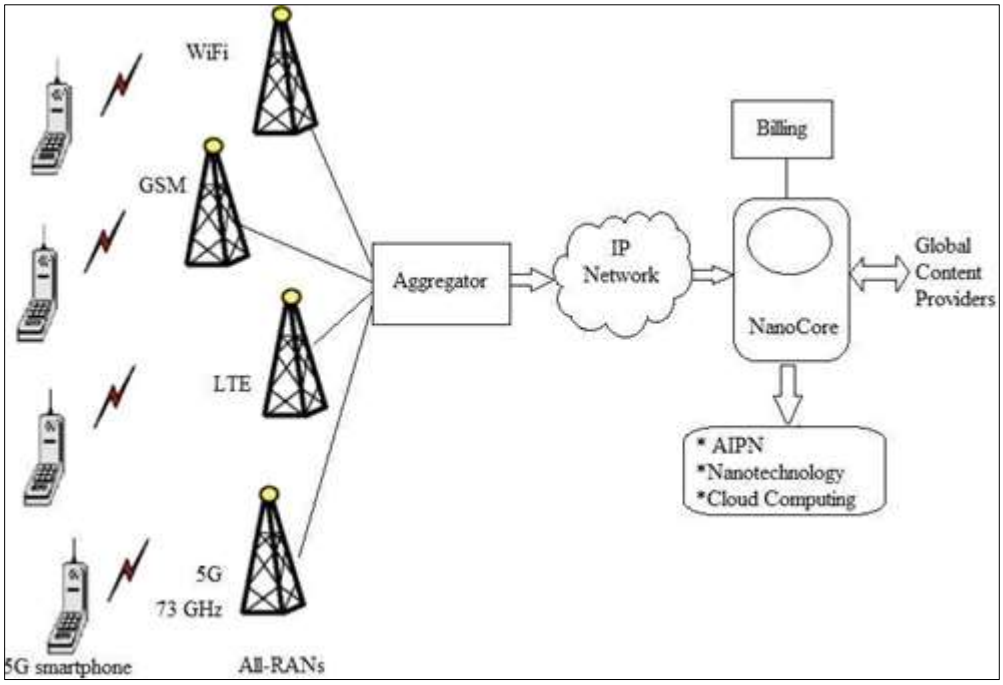

Figure 3 5G Network Architecture Diagram

Source: Arunachalam et al., (2018).

Two prime examples of Telecom as a Service (TaaS) in the industry are private 5G networks and Mobile Virtual Network Operators (MVNOs). Private 5G networks serve to create customized secure high speed connectivity solutions particularly useful for industrial applications such as smart manufacturing and automated factories within the enterprises. They take out the infrastructure management, lower the operational overhead, and maintain control over how the data flows, is private and has low latency performance. MVNOs are basically independent companies that lease

space from established service providers to offer voice, messaging and data services without owning network infrastructure. Under TaaS, MVNOs utilize cloud-based telecom functions to provide fast, low-cost services with features that are customizable across different customer segments/niche markets. Private 5G and an MVNO a good examples of how TaaS enables flexible, scalable, cloud-managed telecom services to respond to technological advances and market demands.

2.2. How TaaS Works

Telecom as a service works on the virtualization of traditional telecom functions with the help of a physical network. TaaS specifically deals with the cellular operating model, where voice, messaging, data, and networking services are delivered on cloud servers and managed by third parties. Businesses can access these services through the Internet, allowing companies to benefit from telecom functions without owning telecom infrastructure.

As with other cloud services, TaaS's provision is similar, allowing businesses to use telecom services based on their current requirements. The service is normally invoked either on a subscription or an on-demand basis, allowing organizations to choose their working models based on the cost they want to incur. For example, a business may see a spike in the call traffic it receives; based on this increase, the company can increase its telecom resources by simply managing its TaaS provider. On the other hand, during low activity, the business can use the service at a minimum level to correspond to this expensed amount only**.**

2.3. Key components of TaaS include

- Virtualized Telecom Functions: Legacy services, which are voice communication, messaging, data, etc, are strived and offered as software-based services on a remote cloud.
- Cloud-Based Infrastructure: TaaS providers are solely responsible for the underlying fabric of the data infrastructure comprising data centers, servers, and other network gear. Industry players acquire these solutions electronically without owning or installing physical telecom facilities.
- 3.Service Models: TaaS is generally provided under several forms /models that comprise Infrastructure as a Service (IaaS), with the provider owning, managing, and maintaining the network infrastructure; Platform as a Service (PaaS), in which businesses can build or code their telecommunication solutions based on the TaaS provider platform; and Software as a Service (SaaS) models where the telecom solutions are pre-developed and the business directly consume/s use the solutions over the internet.

TaaS is fully based on cloud infrastructure, providing better flexibility than traditional services because companies can easily deploy, expand, and control their telecom services. Thirdly, by taking full charge of the telecom infrastructure, maintenance, enhancements, and security, TaaS providers allow businesses to continue with operations and reap extended telecom advantages.

Current Market Adoption

3. TaaS Challenges and Considerations

Worldwide, Telecommunications as a Service (TaaS) has been gradually gaining implementation, mainly led by the increasing adoption of cloud-based telecom services in all business areas. Need for Faster and More Efficient Communication Solutions to Meet Enterprise’s Needs, Digital Transformation Initiatives, and Thus the Ongoing Migration to Cloud Infrastructure in Organizations are all driving factors contributing to the market growth at a CAGR rate of more than 13%, which is expected to reach $50 billion by 2026 are thus based on these factors. Entering the TaaS market are many years of experience across the telecommunications and cloud services sectors with an array of offerings geared towards both small and large enterprises. Here is an example: Telecom giants such as ATandT, Verizon and Google have launched TaaS platforms in Silicon Valley, using cloud infrastructure to provide telecom services that businesses can smoothly adopt. Furthermore, the market is further diversified by emerging global null-scale telecom startups, which compete in the TaaS arena.

The case of TaaS shows its benefits in practical applications. A good example is a multinational retail firm that struggled to control the way it communicated to different locations. Through the TaaS model, the company was able to reduce telecom costs by 30%, raise communication standards, and extend those services to international operations. TaaS was fed by a financial services company, which in turn provided telecom-related services to its remote employees. TaaS was driven seamlessly between multiple locations without any physical infrastructure commitment.

Moreover, the growing enthusiasm for TaaS is also tied to the increasing demand for 5 G services, which requires Wireless Internet Providers (WiPs) to help provide higher-speed data flow and networking. As 5G networks become available globally, enterprises will be able to utilize the potential of next-generation telecom solutions and be strategically positioned to meet this demand with TaaS.

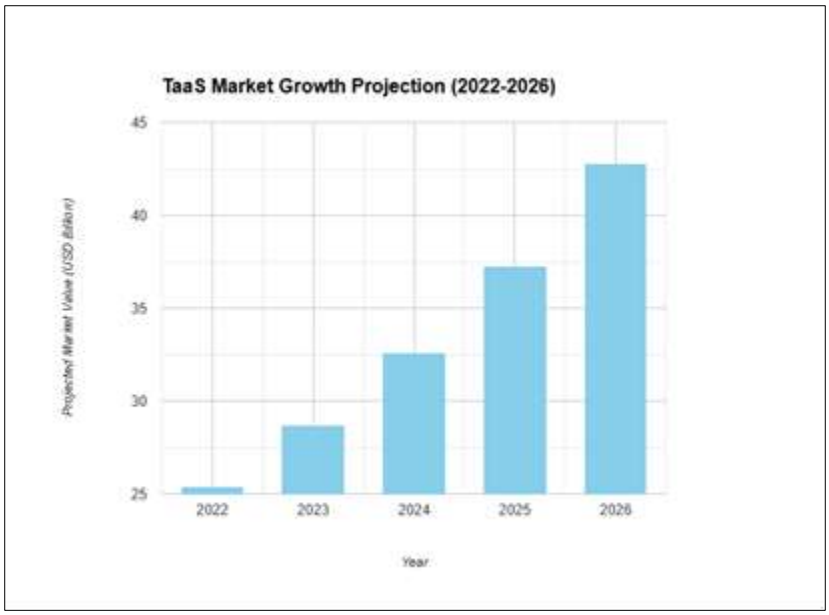

Figure 3 A bar graph illustrating the projected CAGR of the TaaS market from 2022 to 2026, showcasing the anticipated increase in market value over the years.

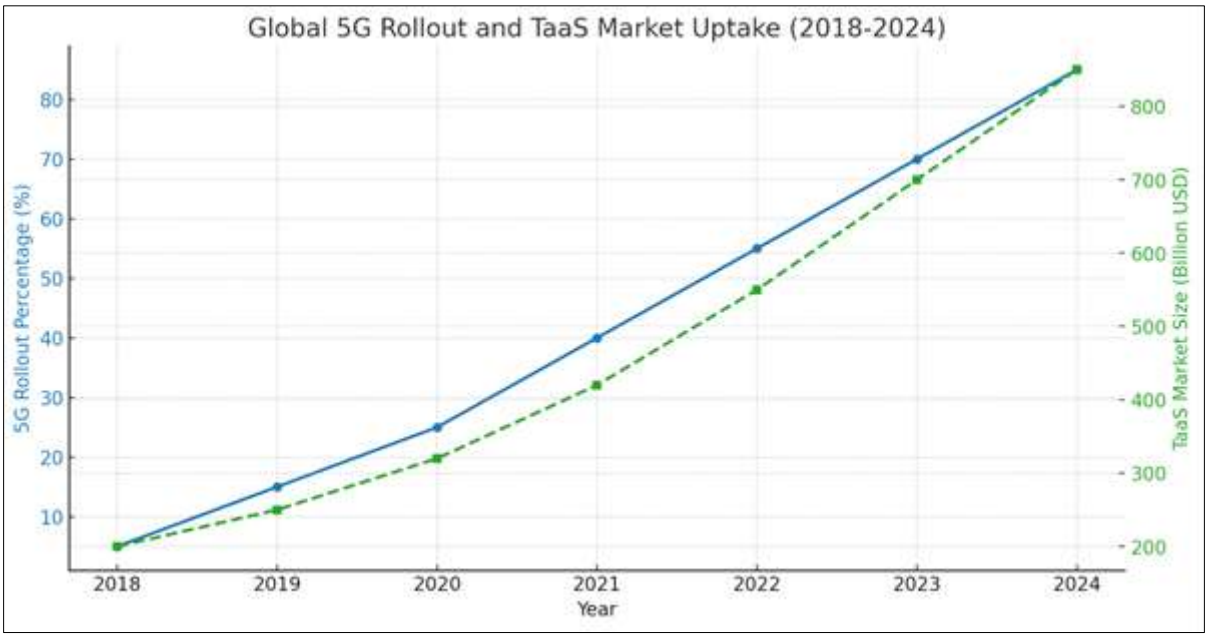

Figure 4 A timeline graph highlighting the rollout of 5G services globally, correlating with the growth of TaaS and its market uptake by businesse

4. TaaS Issues and Implications

4.1. Cost and Scalability

Implementing TaaS TM profoundly changes the cost model for telecoms and firms as follows: Earlier, telecom services were capital-intensive investments in terms of switches, routers, the networking fabric, and so on. When talking about TaaS, there needs to be more CapEx involved since turning to a more OpEx approach is more feasible for businesses. This entails that companies purchase telecom services on a pay-as-you-use basis, not requiring them to install expensive infrastructure.

Nonetheless, concerning cost perspectives, TaaS submitting is useful since it eliminates initial costs; at the same time, we cannot deny that cost issues also affect the aspect of scale. Companies that undergo rapid growth or have high demand during certain months can easily adjust their telecom services through TaaS platforms. Pay The use model thus offers the businesses flexibility benefits; they can easily scale up or scale-down the use of telecom resources. Of course, the costs accompanying the growth rate increase, and profits become unpredictable if not controlled properly.

Amid growth, scalability poses its own set of issues for telecom operators. With the increase in the adoption of TaaS among customers, operators in the cloud environment must design networks that can accommodate many users without causing service disruptions. The demand for resources can spike significantly, especially as firms move to new platforms such as data-intensive services such as video conferencing, large-scale messaging, or those supported by 5G technologies. Hence, operators are always stuck in a game of having to develop and improve their infrastructure to address increased demand while ensuring that costs are balanced.

An important research domain that has proved useful for evaluating **service quality and reliability is SERVQUAL.**

Another major issue with TaaS is achieving high service availability and quality for critical operations, which businesses rely on once they leave the transport layer to the application layer to a TaaS provider. In conventional telecom arrangements, firms have infrastructure power and can guarantee constant performance as they perpetrate their management. In The Case of TaaS, the telecommunication services are outsourced and provided by a third party; hence, the business is limited by the ability of the provider to provide uninterrupted quality service.

Service quality can be difficult to maintain, whether for companies operating within the telecommunications industry or businesses that rely on telecom services for basic needs such as communication with clients, employees, or partners or making payments. A power outage or having to perform repairs or updates can cost businesses a lot of money, reputation, and customer trust. Further, telecommunication services that demand high bandwidth or low latency, for example, real-time video conferences or financial trading, may be impacted if the actual infrastructure possessed by the TaaS provider does not adequately support the particular business demands.

4.2. Customization and Flexibility

The TaaS model also provides flexibility in terms of scalability and cost, but the main problem is to provide flexibility in satisfying specific customer requirements. The corporate world specifically has specific telecom needs not catered to by the structural offerings of a TaaS platform. For example, a particular enterprise in financial services might need to integrate highly developed security and compliance solutions. At the same time, commercial retailing companies might focus more on the prospects of large-scale and efficient communication with customer centers.

It is challenging for providers to deliver highly customized telecom services in a cloud-based model such as TaaS. Telecom solutions are innovative, flexible, and extremely customized to meet the needs of every buyer, although cloud environments are organized to deliver large numbers of standardized services. To tailor the telecom services to an individual industry or a certain application, changes to the platform design may be needed, or implementation of external applications that would complicate the process and add costs to the system for both the provider and the customer.

Additionally, many business concerns regarding flexibility are needed to adopt the TaaS solution in conjunction with the company's current software and hardware environment. For instance, a company may already have fixed telecom equipment in-house and prefer a hybrid model in which TaaS would accompany the installation. A major issue often faced while adopting TaaS is the integration between TaaS and current on-premises systems; this can be a daunting task if the implemented telecom provider's TaaS platform does not have the hybrid implementation capability. Specialization

and integration solutions must be compatible with the providers' platforms and ready to accommodate various scenarios.

However, customization and flexibility must remain key success factors in adopting TaaS. There is also a need for more flexibility and differentiation in the delivery of telecom services as other operational requirements are emerging, and businesses request more telecom solutions and service configurations. This might require the creation of modules of telecom solutions that can be easily extended or offering application programming interfaces and instruments that will enable businesses to develop and include their very own telecom features to the TaaS platform.

5. Potential Obstacles in TaaS Adoption

5.1. Security Challenges

From a business perspective, the biggest hurdle to adopting Telecom as a Service (TaaS) is due to the complicacy and different nature of security when it comes to technology. TaaS services run primarily in virtualized environments, leaving them open to an especially high likelihood of cyber threats. Distributed Denial of Service (DDoS) attacks are one big risk: Telecom networks are flooded with excessive traffic from adversaries, which causes network disruptions. Further, the TaaS network is vulnerable to evolving threats such as malware, ransomware and phishing attacks. A major challenge in TaaS virtualized networks is the fact that they are multitenant, where they have many users and service instances running on identical physical infrastructure. However, this architecture could be too unfavourable if not properly secured, as attackers can breach the virtualization layer, reach sensitive telecom data and even disrupt the service operation. In addition, since voice, messaging, and data transmission are fundamental for the operation of business, the telecommunications market is a prospective target for hackers aiming to undermine organizations.

Additionally, questions surrounding end-user data protection during TaaS are a crucial issue. Telecom data is sensitive and requires strict data privacy measures to preclude unauthorized access and Confidentiality of telecom data. Yet the security of data privacy in virtualized TaaS environments is difficult in part because of the shared infrastructure. In this context, the division of security responsibility between the cloud customer and the cloud provider is critical to assessing risks and managing security in this context. However, cloud providers usually handle the security around the underlying infrastructure, such as physical security and the bottom layer network protections. As a TaaS customer, rather than being responsible for securing data, applications and configurations ‘inside’ the TaaS environment, cloud customers bear the responsibility. In the shared responsibility model you bring with you both have to have clearly defined roles so that you do not occupy security gaps and you protect the data. However, TaaS is not as secure as it appears, and internal threats perpetuate it as much as external threats. Telcom system information can be lost or compromised by employees who have access to it, intentionally or unintentionally. The more that TaaS services are built globally, the trickier it becomes to manage access rights to telecom infrastructure when many people are accessing the network and many devices are accessing the network, too. To mitigate these insider risks you want to have robust access controls, regular audits, and your employee training.

5.2. Regulatory Compliance

Another factor is the issue of regulatory compliance, as relations between the participants of the transport network are rather intricate. As a necessity for global communication, telecom services are bound by many legal requirements that differ from country to country, and it is often a challenge to facilitate legal compliance across borders. For instance, in the European Union (EU), subordinate regulations and rules under the General Data Protection Regulation (GDPR) prescribe the handling, storing, and processing of personal and sensitive data. The nonadherence of these regulations makes big penalties and harm to the company possible.

Another of TaaS's critical issues is the flow of telecom data across borders. Whereby cloud-based telecom services can be accessed from anywhere with an online connection, corporate organizations are legally bound by data sovereignty policies: the policies demand that telecom data must be hosted and handled within certain places. These laws are even more rigorous in areas like the EU and Asia Pacific due to the regulator's high regard for data protection and consumer privacy.

However, the telecom industry is highly governed in some sectors of its operations, including emergency services, management of the networks or telecom spectrum, and data retention issues. They need to ensure that their services are legal according to these regulations, but the legal aspect keeps them from changing over time. This challenge is made worse because rules also vary depending on the type of sectors; therefore, companies operating in heavily regulated industries such as health or finance must adhere to extra rules.

5.3. Data Privacy Concerns

One of the biggest concerns of TaaS is data privacy, as telecom services deal with huge amounts of personal and private information such as phone numbers, call details, messages, and user locations. In cloud-based TaaS contexts, this data is stored, processed, and transmitted over the Internet. There is always a great risk of unauthorized access, data breaches, or misuse of personal information.

The first threat that exists with data privacy in the context of TaaS is when there is an ability of other people or a third party to gain unauthorized access. When security in the TaaS provider is low, hackers could get in between and steal telecom data or get their hands on it, which would cause a violation of users' privacy and several cases of identity theft. When the data is shared with third-party service providers or subcontractors, the risks appear as these companies may not adequately protect personal data.

However, the important aspect that raises questions is how telecom service providers collect, manage, and use customer data in light of the growing service usage of analytics and AI technologies. For instance, using these technologies to render superior service deliveries and foster near-perfect client experience also presents certain risks associated with the utilization of data and disclosure. Customers must fully understand how their data is harvested, utilized, or shared. So, potential privacy risks exist when telecom providers fail to provide sufficient and clear data handling policies.

5.4. 5G SA(Standalone) Core and Service-Based Architecture (SBA)

Several threats attack the 5G SA Core and SBA. If not secured properly, these open, standardized APIs are attack vectors that the SBA relies upon for communication between network functions. Attackers can exploit these APIs to inject malicious requests, intercept data, or disrupt service continuity. Network slicing allows them to create multiple, isolated, virtual networks on top of the same infrastructure, but this can also expose vulnerabilities as one slice might be attacked, and the attack could spread to others. A DoS attack can be particularly important (i.e., particularly vulnerable) on the architecture, and especially on the architecture's use of sharing of resources to perform different network functions. Now, when exploiting data exchange in 5G networks, we not only encounter an increased number of independent exposure risks but also the exposure risk arising from compromised data integrity; being able to compromise data integrity is sufficient to compromise users' access or to manipulate the exchanged data. In the case of weak authentication mechanisms for internal users or devices, insider threats are a risk to the sensitive data and the network segments the outsiders may have access to.

6. Overcoming the Obstacles

6.1. Security Best Practices

In the modern context of TaaS implementation, new risks and threats emerge as security issues that require certain security standards and procedures from businesses and TaaS providers. One of these strategies is using multiple layers of protection, such as firewalls, intrusion detection systems (IDS), and encryption. The security of telecom data at rest and in transit can also discourage the action of third parties from accessing it. Maintaining confidentiality and integrity of the data during transit requires end-to-end encryption in the voice and the messaging service.

Another important step is to adopt a so-called zero-trust security model. This approach entails that no organization or individual on the other end of the supply chain can be trusted. Telecom services are made available after the identity of users, devices, and applications has been authenticated through several checking procedures. MFA and RBAC can also add layers of security that would limit access to huge volumes of data and allow only needed personnel to interact with critical telecommunication systems.

Security check-ups and penetration tests are also important to determine possible loopholes in the TaaS platforms. Such approaches make it possible for organizations to identify the areas of weakness that might be exploited by the wrong end and prevent them. TaaS providers should also have response plans prepared to guarantee THEM the capacity for quick reaction to cyberattacks and simultaneous impact on their services.

Network slicing security concerns strong isolation of slices, tightly micro-segmented in order to eliminate cross-slice attacks, and traffic flow monitoring to detect and/or respond to unauthorized access cases. Security policies are developed and regularly audited on a slice basis in order to be able to establish trained sanity checks. End-to-end encryption and integrity are achieved by means of hashing algorithms. Network functions are mutually authenticated preventing access from compromised or rogue functions. Where Access privilege is restricted by the user's Role and Responsibility (Role Based Access Control) and super sensitive/administrative access requires MFA (Multi-Factor

Authentication). The core of zero trust security principles is trust no one, continuous verification, least privilege access, threat detection and response, and regular penetration testing. Although anomaly detection is used in real-time to detect unusual behaviors and potential threats across the network, it sustains itself throughout the various parameters. Security Orchestration, Automation, and Response (SOAR) software systems automate the processes associated with detecting and responding to threats, thereby reducing or even eliminating response time and human error. An exposed interface or APIs are regularly subjected to penetration testing to find and resolve possible vulnerabilities.

6.2. Ensuring Compliance

Adherence to regulatory compliance, hence, has to be pre-emptive, which has translated to adopting international telecom standards and practices. Most legal requirements match standards like ISO/IEC 27001, which guides information security management systems (ISMS). Thus, referring to globally identified standards, TaaS providers can prove to conform with the various regulations required to secure and develop adequate security and privacy controls.

Having automated tools for complying with such rules can greatly reduce the challenges arising from their enactment. These tools run in the background and constantly check telecom services and data management practices against certain legal requirements. They either alert an administrator or auto-correct the process if necessary. Automated compliance systems are especially effective when there is a need to report on data privacy laws, including GDPR, because of their ability to enforce data policies like data retention, data encryption, and consent management.

In addition, telecom and data privacy regulatory legal changes require business input from legal consultants to ensure compliance. Due to challenges in transferring data across national boundaries, the TaaS providers also have to develop data localization policies pointing to where the telecom data is stored and processed in a way consistent with the laws of the countries in which they operate.

6.3. Data Privacy Protections

In the case of TaaS, both the TaaS provider and the business require data encryption, user privacy control, and disclosure. It is good practice to encrypt personal and sensitive data in motion and at rest in the system so that in the unlikely event that sensitive data is compromised, what is in the hands of a third party will be fairly useless to that particular party. Encryption is a critical component of security, and for protecting telecom data specifically, using strong encryption algorithms is mandatory to fend off motivated adversaries.

It is necessary to utilize strict access control measures that are also an effective way to protect data privacy. With role-based access, it becomes difficult for some users to view or tweak certain information when it becomes sensitive. Access logs and audits can provide visibility into the handling of telecom data and identify who has worked with the data.

However, the technical changes require complement with additional non-technical measures that TaaS providers must adopt to make customer data collection, storage, and processing transparent. For such data to be trusted, it must be accompanied by clear policies on how it will be used for the user's benefit. Consumers have to be given the choice of whether or not they wish to participate in data collection and for what purpose; organizations also have to be clear when collecting data about the use of the collected data. By applying privacy throughout the process of functioning as a telecom service provider, a privacy-by-design approach is essential to minimize the risks that threaten customers' privacy.

7. Future of TaaS

7.1. Technological Advancements

TaaS is on the cusp of becoming a mature industry as it addresses security, compliance and flexibility. Detection, protection, and management of cybersecurity threats in telecom services is revolutionized by Artificial Intelligence (AI) and Machine Learning (ML). This potential for prediction reinforces the resilience of a virtualized telecom environment and guarantees uninterrupted service as cyber threats evolve. Isolated, secure, and high-speed connections from private 5G networks make it possible for enterprises to have custom applications tailored for them. Today, leading cloud providers such as AWS, Microsoft Azure, and Google Cloud have brought private 5G solutions to the market which allow businesses to reap the 5G advantage of lower latency and higher bandwidth without depending on legacy public telecom infrastructure.

Mobile Virtual Network Enabler (MVNE) offers infrastructure and operational support for Mobile Virtual Network Operators (MVNOs) to operate on a user experience and specialized services basis rather than having worries about

physical infrastructure. Private 5G is already becoming a reality. Now is a particularly valuable time as the service grows, allowing MVNOs to shine by offering superior services while the technicalities get outsourced. Blockchain technology is the key to TaaS, where secure and tamper-resistant data is transferred to/from users and providers. The international telecom industry, with its complex legislation and privacy standards, could benefit from this type of decentralized record-keeping. Advances in TaaS potential aided by 5G technology provide faster, more available connectivity to services such as IoT integration and real-time video streaming. As 5G progresses further and turns to the commercial stage, TaaS (telecom as a Service) providers will be enabled to provide scalable and low-cost solutions to satisfy telecom demand in the cloud.

7.2. Industry Collaboration

To achieve the maximum impact of TaaS, a collaboration with telecom operators, regulatory bodies and cloud service providers is required. Cooperation in this regard includes the implementation and development of standardized security and privacy measures. Stakeholders can establish industry-wide guidelines by working together, which will incline TaaS providers to give priority to the protection of telecom and client data. This collaborative approach also simplifies compliance, although there are obvious regulatory challenges as the TaaS is deployed across various regions. At the same time, there is consistent adherence to security initiatives across the industry.

8. Conclusion

TaaS is a revolutionary idea that can benefit business companies and telecom operators. It provides prospects to apply effectively balanced telecom services, potentially creating massive savings in overhead expenses, simplifying corporate functioning, and improving its services. However, with this potential also come several issues and questions, such as security, regulation, and data protection. The above barriers should be addressed to achieve success in TaaS implementations.

Advancements in technology provide great solutions to the challenges experienced in the network through artificial intelligence security, blockchain, 5G connectivity, and many more. Telecom operators, cloud service providers, and regulators must coordinate their efforts to produce a better, safer, and more effective TaaS market. By resolving these critical questions, TaaS is positioned to redefine the space of the telecom industry and promote further advancement and popularity of cloud telecom services for years to come.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Gomes, C. (2012). Estudo do Paradigma Computação em Nuvem [Master project, ISEL, in Portuguese].

[2] GAO. (2003). AIRLINE TICKETING - Impact of Changes in the Airline Ticket Distribution Industry. Retrieved from http://www.gao.gov/assets/240/239237.pdf

[3] GlobalPlatform. (2009). GlobalPlatform's Value Proposition for the Public Transportation Industry: Seamless, Secure Travel Throughout Multiple Transportation Networks. Retrieved from http://www.globalplatform.org/documents/whitepapers/GP_Value_Proposition_for_Public_Transportation_whitepaper.pdf

[4] Mut-Puigserver, M. M., Payeras-Capellà, M. M., Ferrer-Gomila, J.-L., Vives-Guasch, A., and Castellà-Roca, J. (2012). A survey of electronic ticketing applied to transport. Computers and Security, 31(8), 925-939. https://doi.org/10.1016/j.cose.2012.04.002

[5] Smart Card Alliance. (2006). Transit and Contactless Financial Payments: New Opportunities for Collaboration and Convergence.

[6] Transit Cooperative Research Program (TCRP) Report 115. (2006). Smartcard Interoperability Issues for the Transit Industry.

[7] Vilanova, E. V., Endsuleit, R., Calmet, J., and Bericht, I. (2002). State of the Art in Electronic Ticketing. Universität Karlsruhe, Fakultät für Informatik.

[8] Meier, K. J., and O'Toole, L. J. (2002). Public management and organizational performance: The effect of managerial quality. Journal of Policy Analysis and Management, 21(4), 629–643. https://doi.org/10.1002/pam.10078

[9] Autor, D. H., Dorn, D., and Hanson, G. H. (2016). The China Shock: Learning from Labor-Market Adjustment to Large Changes in Trade. Annual Review of Economics, 8(1), 205–240. https://doi.org/10.1146/annurev-economics-080315-015041

[10] Atzori, L., Iera, A., and Morabito, G. (2016). Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm. Ad Hoc Networks, 56, 122–140. https://doi.org/10.1016/j.adhoc.2016.12.004

[11] Hu, H., Wen, Y., Chua, T., and Li, X. (2014). Toward Scalable Systems for Big Data Analytics: A Technology Tutorial. IEEE Access, 2, 652–687. https://doi.org/10.1109/access.2014.2332453

[12] MarketsandMarkets. (2023). *Telecommunications as a Service (TaaS) Market - Global Forecast to 2026*. https://www.marketsandmarkets.com/Market-Reports/telecommunications-as-a-service-market-215387798.html

[13] Deloitte. (2023). *Digital Transformation: The New Business Imperative*. https://www2.deloitte.com/global/en/pages/technology/articles/digital-transformation.html

[14] Telecoms.com. (2023). *How Major Telecom Players Are Adapting to TaaS*. https://telecoms.com/news/how-major-telecom-players-are-adapting-to-taas/

[15] Gartner. (2023). *Emerging Telecom Startups and Their Impact on the TaaS Market*. https://www.gartner.com/en/newsroom/press-releases/2023-telecom-startups

[16] Business Insider. (2023). *Case Study: TaaS Implementation in Retail*. https://www.businessinsider.com/taas-implementation-in-retail-case-study

[17] Harvard Business Review. (2023). *Connecting Remote Teams: The Role of TaaS in Finance*. https://hbr.org/2023/05/connecting-remote-teams-role-of-taas

[18] Cisco. (2023). *5G and the Future of Telecommunications as a Service*. https://www.cisco.com/c/en/us/solutions/service-provider/5g/overview.html

[19] Tung, Yuan-Hsin and Lin, Chen-Chiu and Shan, Hwai-Ling. (2014). Test as a Service: A Framework for Web Security TaaS Service in Cloud Environment. Proceedings - IEEE 8th International Symposium on Service Oriented System Engineering, SOSE 2014. 212-217. 10.1109/SOSE.2014.36.

[20] Arunachalam, Siddhika and Kumar, Shruti and Kshatriya, Harsh and Patil, Mahendra. (2018). Analyzing 5G: Prospects of Future Technological Advancements in Mobile.