2021 21st International Conference on Computational Science and Its Applications (ICCSA) | 978-1-6654-5843-6/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICCSA54496.2021.00034

Secure Access Service Edge: A Multivocal Literature Review

Mohammed Nurul Islam
Department of Computer Science
Østfold University College
Halden, Norway
mohammni@hiof.no

Ricardo Colomo-Palacios
Department of Computer Science
Østfold University College
Halden, Norway
ricardo.colomo-palacios@hiof.no

Sabarathinam Chockalingam
Department of Risk,Safety and Security
Institute for Energy Technology
Halden, Norway
Sabarathinam.Chockalingam@ife.no

***Abstract*- Over the last decade, corporate networks have undergone significant changes and have been increasingly reliant on cloud-based services to run their businesses. The Covid-19 pandemic has expedited this pattern. In this scenario, there is a need to provide security to infrastructures in an advanced and integrated way. Gartner invented the term *"Secure Access Service Edge (SASE)"* to meet the above-mentioned goal. SASE is a single framework cloud-native architecture that integrates various network and security functions. SASE is seen as a new cybersecurity solution that impacted established vendors but has received little academic attention. Therefore, in this paper, we present a Multivocal Literature Review (MVLR) aiming to gather an illustration of SASE, including definition, key characteristics, reported benefits and challenges and, finally, critiques of this new term. SASE is adopting the benefits of cloud approaches adding security to the service, however, challenges remain in several setups, including legacy systems.**

Keywords- Secure Access Service Edge, SASE, Multivocal Literature Review

I. INTRODUCTION

Modern society increasingly depends on network infrastructure. This dependence is even more evident after the Covid-19 pandemic, an event that has impacted almost all aspects of our life. Nearly all organizations and individuals are looking for new technologies to continue their operations flawlessly [1]; Networks are among the cornerstones in this seek. So, network providers face challenges to meet the demand of end-users during these times [2]. The Covid-19 pandemic leads to a global transformation accelerating digitalization processes. However, on the other hand, this also results in some negative consequences like new cybersecurity threats and unexpected workload leading to performance issues [3].

With the rapid growth in telecommunications' core network infrastructure, there is a substantial increase in user service requirements and new security threat management issues [4]. Also, digital corporate transformation inverts architecture patterns of the network and security services, from a central data center to remote users and/or computers. That raises the burden on safety and risk managers to hit the converged protected access service edge offered by the cloud for this transition [5], [6].

Even before the pandemic, many topics were pivotal challenges for IT professionals, including the cloud and secure remote network access. Nowadays, these challenges are even more important due to the new working landscape. Consequently, Software-Defined Wide Area Network (SD-WAN) is getting more popularity. SD-WAN enables companies to securely link users with applications using any combination of transport services, e.g., Multiprotocol Label Switching (MPLS), Long-Term Evolution (LTE) and broadband internet services. In the current times, SD-WAN is aimed to provide better security features [6], [7].

With increasing numbers of users, organizational units, data, remote services, organizations realize and fight to keep momentum and maintain network stability, privacy and honesty [8]. Current network and technology solutions available on the market cannot handle all sorts of traffic and ever-changing security risks that a modern enterprise needs to contend with [8]. No company can function effectively without adopting and utilizing multiple point products, such as secure web gateways, firewalls, secure remote access by a Virtual Private Network (VPN) and SD-WAN [8]. This need increases the difficulty of deploying multiple architectures with each product, configuring a series of rules, infrastructure to maintain and its own set of logs causing a burden for institutions by increasing safety costs, complexity and security holes [8].

Existing network methods and technologies are struggling to provide the standard of protection and access control that digital businesses need. It is now a primary necessity for organizations to demand immediate, uninterrupted access for their users, regardless of where they are located [8], [9]. Besides, more traffic from the public cloud to a branch office creates an urgency for a new and protected network architecture approach [8], [10].

Any remote user is now operating as a WAN edge, so protection must synchronize with the network more often. Before the pandemic, cloud firewalls were the primary security mechanism used for any SD-WAN implementation, but current circumstances require improved robustness. While connecting to the internet, firewalls are still necessary, but additional security functions are critical for data protection. For example, take the Cloud Access Security Broker (CASB), endpoint safety and ID WAN analysis, and uninterrupted security

978-1-6654-5843-6/21/$31.00 ©2021 IEEE
DOI 10.1109/ICCSA54496.2021.00034

threats and response services. These security features usually go outside of SD-standard WAN's domain, explaining why a new wave of technologies resonates with difficulties back in 2020 [7].

SASE is a new approach aimed to tackle these challenges. SASE is a solution that Gartner proposed to support organizations using cloud and connectivity by offering safety networks and services. SASE was designed to serve organizations in leveraging a standard cloud-based architecture to support cloud and mobility by delivering security services for networks and the network. It was developed to ensure that all cloud systems are equipped with reliable security services by means of a common framework. The elimination of multiple point items and using the SASE solution offered in the cloud will minimize complexity while saving substantial technological, human and financial resources [8]. SASE integrates networking and security technologies into a single cloud-delivered system. SASE provides a solution by combining security as a service and network as a Service (NaaS). SASE presents three component levels: Core, Recommended and Optional [5]. SASE core component consists of SD-WAN, Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Zero Trust Network Access (ZTNA) and Firewall as a Service (FWaaS), consistently monitoring the threats with the capability of detecting sensitive data/malware and also encrypting/deciphering the information on a line-speed basis [5]. Here Web applications and API security, remote window isolation, recursive DNS and network sandboxing are among the SASE recommended practices. This API-based security as a service access provides data sense as well as support for both checked and unchecked devices. Finally, given that WLAN and VPN services are still required for the customer; these parts are optional in SASE environments [5].

According to Gartner, SASE is a modern paradigm for providing security and network access across a single cloud security framework [5]. However, SASE has received criticism from a variety of outlets, including IDC and IHS Markit. Both analyst firms questioned that it is not a revolutionary product but rather a technical development [11]. SASE is a Gartner concept that refers to incorporating current technology with a single point of control rather than a new item or technology on the market [12]. Clifford Grossner of IHS Markit forecasted that enterprises would not recommend using a single provider for both SD-WAN and security features [12].

SASE can significantly assist businesses by allowing security teams to provide a diverse spectrum of fast network security services that are reliable and incorporated to meet the needs of digital business transformation, edge computing and workforce mobility. Gartner conjectures that at least 40% of enterprises will have SASE adoption strategies in place by 2024, up from 1% in 2018 [5], [6].

SASE is such a new technology and to the best of authors´ knowledge, there is no literature review on this topic. To fill this gap, we conducted a multivocal literature review (MVLR) to investigate SASE. Because of the subject's novelty, finding scientific literature for academic articles that deal with specific aspects of SASE does not provide comprehensive results. As a result of this observation, an MVLR is needed and was the method adopted.

The rest of this paper is structured as follows: Section II describes the study method followed by search execution in Section III. In Section IV, we present the findings especially on definition, key characteristics, benefits, challenges and criticisms of SASE. Finally, Section V presents conclusions and future research directions.

II. RESEARCH METHODOLOGY

In this section, we provide an overview of the research methodology and the process followed in this study.

A. Multivocal Literature Review

A MVLR was the method considered applicable for the aim of this study. Given the novelty of the topic, this tool was deemed the most accurate by the authors. This decision is grounded on the amount of material published as gray literature; authors understood that the nature of MVLR completely justifies the need to conduct the study using this mean.

A MVLR is another form of Systematic Literature Review (SLR) with the inclusion of gray literature like blogs, posts and white papers in addition to journal and conference papers [13]. MVLR is effective and necessary because of its characteristics and capability to provide accessibility on emerging topics to researchers and practitioners [13], [14]. Also, the work by [15] was used in order to complement MVLR guidelines.

B. Research Questions

To achieve the objective of this paper, four research questions have been formulated:

RQ1: What is the definition of SASE?

RQ2: What are the main characteristics of SASE?

RQ3: What are the reported challenges and benefits of adopting SASE?

RQ4: What are the reported criticisms of SASE?

C. Data Sources

In this work in the form of a MVLR, we use Google Scholar to locate available academic literature. Google Scholar also include most of the top databases in the field (e.g., SpringerLink, IEEE Xplore or ScienceDirect) and can be seen as a metadatabase. Also, we use Google searches to locate gray literature (e.g., articles, white papers, blogs, etc.)

D. Search Terms

The search string is constructed in order to retrieve the most relevant literature on SASE. In all databases, the search string used is the same and is as follows:

("Secure Access Service Edge") AND ("definition" OR "characteristics" OR "benefits" OR "challenges" OR "criticism")

E. Search Process

Four steps were taken to process the findings. First of all, the search string was applied in selected search engines in order to gather documents from the above-mentioned databases. To remove the duplicates, studies identification process was conducted in this phase. Firstly, to verify the relevance to the topical subject, all titles, abstracts and keywords of all documents were reviewed in order to find relevant papers. Finally, all the documents were read completely to check their relevance.

F. Search Criteria

The search criteria were designed to classify studies that offered direct scientific data regarding our research questions. Inclusion and exclusion criteria are developed to narrow down the initial search results.

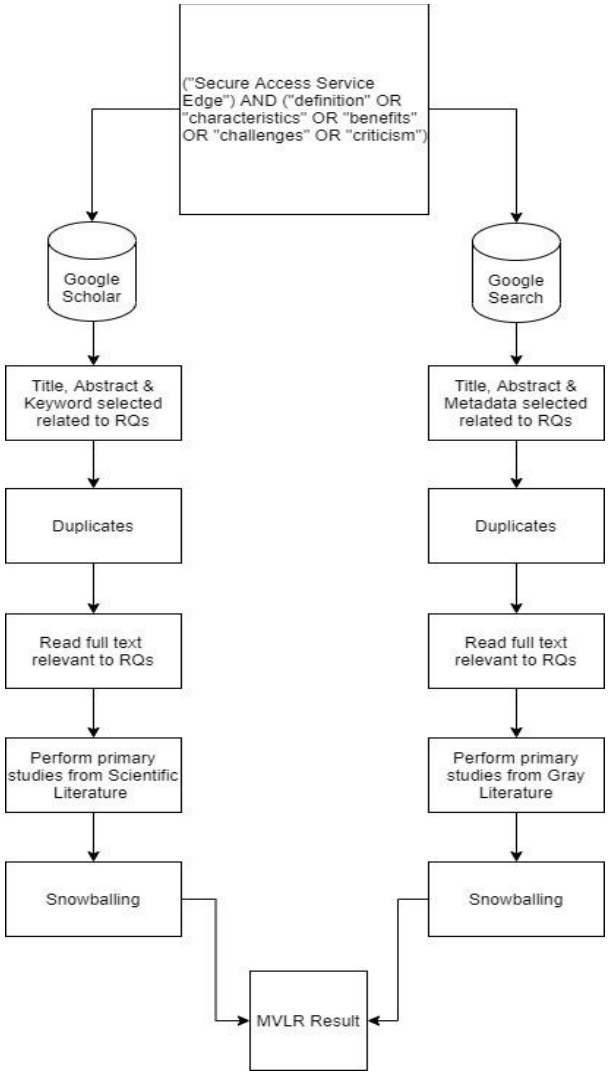

FIGURE I. OVERVIEW OF THE SEARCH PROCESS

G. Study Inclusion and Exclusion Criteria

Once initial search results have been found, the following inclusion and exclusion criteria are applied to the process to remove irrelevant documents:

Inclusion Criteria:

- Studies that explicitly discuss the concept of SASE.
- Studies that discuss characteristics of SASE.
- Studies that discuss the present challenges to SASE.
- Studies that discuss the benefits of SASE.
- Studies that discuss the criticism of SASE.

Exclusion Criteria:

- Studies that are not relevant to SASE.
- Studies that are not accessible.
- Results in Google Search deems too similar to other results.
- Studies that are not written in the English language.

III. SEARCH EXECUTION

This section presents the results of the above-mentioned search process. However, the use of the relevant ranking method (e.g., PageRank algorithm for Google) was narrowed to search space during Google Search. In this case, the above-mentioned search string was used for Google Search and authors documented 310000 results. As we found that the first few pages were important for our examination, however, after observation. This is to say $(n+1)^{th}$ page was checked just in the case the result was considered to be significant. The same search string was used in Google Scholar and 10 results were returned. In this case, researchers examined all papers obtained from Google Scholar. The following Table-I shows the process's key outcomes.

TABLE I. SEARCH RESULTS OBTAINED

Source	Initial result	Title, abstract & keywords	Duplicates	Reading Full text	Snow-bowling	Selected studies
Google Scholar	10	4	1	1	-	1
Google Search	310000	154	6	20	4	24

In summary, first applying the search string in Google Scholar and Google search, 310010 results include in the first phase (Google Search returned 310000 results and Google Scholar returned 10). In the first phase, 309852 results were excluded after reviewing the title, keywords and abstract resulted 158 articles. In second phase, all the duplicate papers were removed, which left 151 papers. Table-II shows the papers selected from full reading (21) and snowballing (4) approaches.

TABLE II. PAPER SELECTED FROM FULL READING AND SNOW BOWLING

	Google Search		Google Scholar		Total
Full Reading	20	[7,8,10,11,15-21, 23,24,27-33]	1	[6]	21
Snow bowling	4	[5,12,22 25]	-	-	4

All 25 papers were sorted in a reference manager tool, in this case Zotero. To guarantee the inclusion of all relevant papers, forward and backward snowballing approach was used as recommended by MVLR guidelines, on the set of sources already in the pool.

All the selected sources were used to answer the four research questions listed in Section II. Table III presents the search results according to the research questions and the search engines. First column presents RQs, second and third, presents the number of papers collected from Google Scholar and Google Search to answer the specific research question. Therefore, the selected sources reported more benefits than challenges in the SASE scope.

TABLE III. SOURCES AND THEIR RELEVANCE TO RESEARCH QUESTIONS

RQs	Google Scholar		Google Search	
RQ1	1	[6]	2	[5, 15]
RQ2	1	[6]	14	[5,8,10,11,16-25]
RQ3	1	[6]	10	[5,8,22,26-29,31-33]
RQ4	-	-	4	[7,11,12,25]

IV. FINDINGS

RQ1: What is the definition of SASE?

As SASE is a new emerging concept coined by Gartner, there is no generally accepted definition apart from their own definition. To answer this RQ, authors select one scientific paper, and the remaining two were considered gray literature to find the best definition. While reviewing scientific and gray literature, the authors observed a standard opinion/view on SASE based on Gartner's report. The term SASE was invented by Gartner in its report 'The Future of Network Security is in the Cloud' [5] defined SASE as follows,

"The secure access service edge is an emerging offering combining comprehensive WAN capabilities with comprehensive network security functions (such as SWG, CASB, FWaaS, and ZTNA) to support the dynamic, secure access needs of digital enterprises."

Similarly, according to Fortinet [16], SASE can be seen as a *"cloud-delivered service that combines network and security functions with WAN capabilities to support the dynamic, secure access needs of today's hybrid organizations."*

So, in a nutshell, SASE is the convergence into one infrastructure of cloud-based networks and security technologies in a single framework [6]. This convergence continues to take place with the maturity and development of technologies. Network devices and smartphones are notable examples. Usually, these integrations provide consumers with greater functionality, interoperability and stability, as will be the case with SASE in a set of independent services [6].

RQ2: What are the main characteristics of SASE?

Fourteen papers were selected to answer this question where thirteen of them are gray, and one is scientific literature. There are several characteristics associated with SASE that makes the technology efficient and noteworthy, but the following are the principal components,

Identity-driven: Because of its inability to meet complex safety access criteria, conventional enterprise architecture must evolve in response to the growing popularity of the cloud-centric business model [8], [17]. In legacy architectures, access techniques rely on network details such as IP addresses and networking edge devices with strict connection methods [18]. In this scenario, IT teams find it more challenging to handle and upgrade various security services and access policies. Implementing identity-based zero trust access policies on the edge network enables businesses to expand their network to all end-users, regardless of location or device type [5]. This level of protection guarantees both external and internal data leaks and other threats, which is a significant improvement over the highly permissive and potentially insecure VPN [19].

Cloud-based architecture: As organizations shift towards more Software-as-a-service and other cloud-native applications, backhauling Software-as-a-service traffic to the data center increased the latency and networking cost [6], [20]. To overcome this issue, security should be placed between the users and the cloud [10]. SASE is a cloud-based architecture that puts the cloud at the center of the network. Additionally, without any specific hardware specifications, SASE cloud architecture made it possible to use cloud resources [18], [21]. That helps IT professionals monitoring and implementing enterprise policies using a single console, thus, make straightforward operations [22].

Supports all edges: Modern digital businesses are rapidly adopting job models that are more outside of the workplace than inside. Furthermore, as mobile and other edge computing devices proliferate, services must communicate with more than just sites [23]. SASE enables the creation of a network for the entire enterprise, including data centers, branches, cloud services, smartphones, and remote customers, SD-WAN devices, for example, utilizing physical edges, while continuing mobile customers and clientless browsers meet on-going users [11], [24].

Globally distributed: SASE technology provides a global SD-WAN infrastructure that operates over a private backbone to provide optimum network performance for any application, regardless of its location [25]. Rather than relying on the global internet, routing all traffic via the SASE backbone private network will minimize latency and ensure optimum network and security efficiency for any application. [22], [26].

RQ3: What are the benefits and challenges of adopting SASE?

SASE is a relatively new idea, but it has reported several potential advantages with many challenges. To answer this question, ten papers were selected, one from scientific literature and nine from gray literature.

Benefits:

Total visibility in hybrid environments: Legacy organization's architecture had problems with blind spots and the traffic inspection of remote users. The combination of network services such as FWaaS, SWG, DLP, and CASB technologies and functions in SASE provides enterprise security complete visibility of hybrid network operation [8]. SASE capabilities provide organizations more control to inspect, manipulate, and secure the entire business network, including data centers, offices, branches, public and private clouds and mobile users [5].

Control of users, data and apps: As users are increasingly gripping various SaaS applications from multiple devices and locations, many of these applications can operate on nonstandard ports. Users can force applications to run over these ports through protocols, regardless of violating the company policies [8]. By default, SASE can distinguish traffic by operation on all ports. It does not impose an administrative burden by making which applications use which ports to configure relevant policies and regulations [8]. SASE offers a complete insight into device use and the ability to comprehend and monitor its use.

Cost and complexity reduction: With a reduction in the total number of providers, SASE would help to minimize IT personnel expenses by consolidating safe access facilities from a single supplier [5]. Besides, reducing the number of physical and virtual apparatus in a division and reducing the number of agents required on the end-user system [5], [27]. SASE allows enterprises to cost-effectively expand the networking and security infrastructure to all of their locations by using a converged, cloud-delivered system that entirely incorporates networking and security technologies and functions [8].

Improved performance and latency: Leading SASE vendors are offering a global footprint in latency-optimized routing [8]. This is particularly critical for applications that need low latency, such as coordination, recording, VoIP and online conferencing. This reduces the congestion and latency involved with backhauling Internet traffic through MPLS links or routing traffic through a link experiencing high usage or performance problems [5], [28].

Enhances the user experience: Easy control is one of the key advantages of SASE. Since SASE is a key cloud-based management framework, the whole operation from one point is controlled [5], [29]. For example, the management by several offices within an enterprise network of SWG and SD-WAN, NGFW, and VPN devices demands more IT work as additional sites are installed. However, the sophistication of SASE management does not evolve with the network since it is a single cloud-based manager [30]. It manages the whole service and it does not take long for the IT department to perform heavy repair duties such as removal of patches and hardware [24], [29].

Improved security: Each access session can be reviewed and the same set of policies applied to the SASE providers that support the control of content by identifying confidential data, malware and so on [5].

Increased effectiveness of the network and network security staff: Network security experts should concentrate on identifying, regulating, and application access specifications and the mapping of them to SASE capacities instead of the repetitive activities of setting up infrastructure [5].

Challenges:

Culture and politics between siloed teams: Buyers of network security services and SWG, CASB are often different groups. These various teams are engaged in traditional rivalry and spend more time and energy blocking each other to defend their turf [5], [31], [32]. To drive SASE adaptation, solid and significant leadership assistance is needed to support its adoption.

Complexity: Those companies who want to make their SASE out of a wide range of suppliers and cloud offers, combining this can lead to incoherent management and compliance, low efficiency, and costly implementations [33]. A similar issue arises if the supplier from many acquisitions and/or alliances integrates SASE in its offer [5].

Legacy vendors do not have a cloud-native mindset: Hardware-centered network and network security suppliers would find it difficult to adapt to the provision of cloud-native and cloud-based services [5], [33]. Both distribution and reward channels will modify business models. Vendors who previously offered dedicated hardware on-premises would most likely take the easiest route and deliver initial SASE products focused on single-tenant architectures [33].

Investment needed for POPs and Peering Relations: The policy and implementation capability of SASE must be located in any part of the endpoint identity. This means worldwide access for bigger companies that embrace a mobile population and a connected digital economy [5]. Smaller SASE suppliers would not be able to support the investments needed for competitive results. SASE offers which only use Infrastructure as a Service (IaaS) Internet backbone capability but do not have local POPs/edge capabilities, face latency, performance problems, and consequent end-user discontent [5], [23].

The inclusion of agent for leading SASE packages: To interface with forward-thinking proxy architectures and handle some conventional framework protocols, a local agent is needed [23] Furthermore, SASE providers hire additional agents to obtain additional system context.

However, if many agents are used to helping connectivity, agents increase the difficulty of SASE deployments. [5], [34].

Too much payment and the chaos of the SASE: The entire SASE industry is under pressure as the industry consolidates and continues to encourage economies of scale for larger providers. It also moves away from bandwidth-oriented models for WAN edge/SD-WAN and toward entity-driven subscription models based on the price categories of inspection introduced [5].

RQ4: What are the criticisms of SASE?

A variety of stakeholders, including IDC and IHS Markit [11], [12], [26] have been criticizing SASE. Where both analyst firms are uncertain of Gartner's argument that SASE is a panacea idea and also a new concept, or commodity, rather than an integration into one single management source of current technology [12], [26].

In an email, Clifford Grossner, Executive Director of Science and Technology at the IHS Markit Fellow, told SDxCentr, "*SASE seems not like a new industry, let alone a new technology or product"*. He also conveyed that integrated management is advanced computation, networking, and stability. On the other hand, it is still very rare that any companies would not purchase from a single seller all this [12], [26].

Additionally, Grossner also criticized the absence of analytics, artificial intelligence and edge automation Machine Learning, which he said seemed to be lacking from the SASE concept by Gartner [7], [12].

V. CONCLUSIONS

The migration of data and software to the cloud brings apparent advantages such as reduced costs, higher efficiency, and increased agility, but it also introduces new challenges [35]. It also brings some challenges SASE is a model that offers many enterprises the best direction to modernizing their organizations in an integrated and secure way.

SASE provides all of the benefits of cloud-based as-a-service delivery, including plug-and-play deployment, accelerated optimization, scalability, the lower overall cost of ownership, and hands-free updates and maintenance. Security is a prerequisite at any endpoint where SASE can provide an efficient way to solve current challenges.

However, some problems remain, such as transitioning to this new technology and some organizations' refusal to focus on vendors/agents because they want greater leverage of their security processes and infrastructure. Businesses that are established in the cloud age would find it easier to embrace SASE, but the fact is that most are not starting from scratch. And some industries will still need on-premises IT infrastructure where hardware is required on-site. Also, it is unclear whether or not SASE can achieve the widespread popularity identified by vendors for cloud storage and applications.

As a potential future work, authors aim to investigate the concept from a security perspective, performing research on the impact of its adoption in the detection of security incidents. As a second research direction, the authors want to investigate the integration of SASE in SecDevOps environment.

ACKNOWLEDGEMENT

This paper is partially funded by the Research Council of Norway (RCN) in the INTPART program under the project "Reinforcing Competence in Cybersecurity of Critical Infrastructures: A Norway-US Partnership (RECYCIN)" with the project number #309911.

REFERENCES

[1] Y. Siriwardhana, C. D. Alwis, G. Gür, M. Ylianttila, and M. Liyanage, "The Fight Against the COVID-19 Pandemic With 5G Technologies," *IEEE Eng. Manag. Rev.*, vol. 48, no. 3, pp. 72–84, thirdquarter 2020, doi: 10.1109/EMR.2020.3017451.

[2] Y. Abdulsalam and M. S. Hossain, "COVID-19 Networking Demand: An Auction-based Mechanism for Automated Selection of Edge Computing Services," *IEEE Trans. Netw. Sci. Eng.*, pp. 1–1, 2020, doi: 10.1109/TNSE.2020.3026637.

[3] T. Weil and S. Murugesan, "IT Risk and Resilience—Cybersecurity Response to COVID-19," *IT Prof.*, vol. 22, no. 3, pp. 4–10, May 2020, doi: 10.1109/MITP.2020.2988330.

[4] B. Ellison, "IT Management Challenges During COVID-19," *BDO Digital*. https://www.bdo.com/digital/insights/managed-services/it-management-challenges-during-covid-19 (accessed Feb. 17, 2021).

[5] N. MacDonald, L. Orans, and J. Skorupa, "The Future of Network Security Is in the Cloud." https://www.gartner.com/doc/reprints?id=1-1ZFQJAP6&ct=200709&st=sb (accessed Feb. 17, 2021).

[6] M. Wood, "How SASE is defining the future of network security," *Netw. Secur.*, vol. 2020, no. 12, pp. 6–8, Dec. 2020, doi: 10.1016/S1353-4858(20)30139-2.

[7] A. Pandya, "The Impact of COVID-19 on SD-WAN." https://www.thefastmode.com/expert-opinion/18447-the-impact-of-covid-19-on-sd-wan (accessed Feb. 17, 2021).

[8] L. Miller, "Secure Access Service Edge (SASE) for Dummies," p. 65, 2020.

[9] "Secure Access Service Edge (SASE)," *trustgrid.io*. https://trustgrid.io/sase/ (accessed Mar. 24, 2021).

[10] "What is SASE (Secure Access Service Edge)? - Citrix Norway," *Citrix.com*. https://www.citrix.com/no-no/glossary/what-is-sase-secure-access-service-edge.html (accessed Mar. 24, 2021).

[11] "Secure Access Service Edge," *Wikipedia*. Feb. 28, 2021. Accessed: Mar. 10, 2021. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Secure_Access_Service_Edge&oldid=1009415786

[12] T. Mann, ,"Analysts Debate SASE's Merits as Vendors Board Hype Train," *SDxCentral*, Nov. 09, 2019. https://www.sdxcentral.com/articles/news/analysts-debate-sases-merits-as-vendors-board-the-hype-train/2019/11/ (accessed Feb. 17, 2021).

[13] V. Garousi, "Guidelines for including grey literature and conducting multivocal literature reviews in software engineering," *Inf. Softw. Technol.*, p. 21, 2019.

[14] R. T. Ogawa and B. Malen, "Towards Rigor in Reviews of Multivocal Literatures: Applying the Exploratory Case Study Method," *Rev. Educ. Res.*, vol. 61, no. 3, pp. 265–286, Sep. 1991, doi: 10.3102/00346543061003265.

[15] S. Misra, "A Step by Step Guide for Choosing Project Topics and Writing Research Papers in ICT Related Disciplines," in *Information and Communication Technology and Applications: Third International Conference, ICTA 2020, Minna, Nigeria, November 24–27, 2020, Revised Selected Papers 3*, 2021, pp. 727–744.

[16] "What is SASE (Secure Access Service Edge)?," *Fortinet*. /resources/cyberglossary/sase (accessed Apr. 23, 2021).
[17] "SASE identity policies enhance security and access control," *SearchCloudSecurity*. https://searchcloudsecurity.techtarget.com/tip/SASE-identity-policies-enhance-security-and-access-control (accessed Apr. 26, 2021).
[18] "What is SASE? | Secure Access Service Edge," *Cloudflare*. https://www.cloudflare.com/learning/access-management/what-is-sase/ (accessed Apr. 23, 2021).
[19] "Secure Access Service Edge (SASE) to Secure and Streamline Network Infrastructure - Pupuweb." https://pupuweb.com/sase-secure-streamline-network-infrastructure/ (accessed Apr. 24, 2021).
[20] "C. Craven, "What Is SASE (Secure Access Service Edge)?," *SDxCentral*. https://www.sdxcentral.com/security/sase/definitions/what-is-sase-secure-access-service-edge/ (accessed Apr. 23, 2021).
[21] "Secure Access Service Edge (SASE)." https://www.netsurion.com/secure-edge-networking/secure-access-service-edge-sase (accessed Mar. 18, 2021).
[22] D. Greenfield, "The Secure Access Service Edge (SASE) Architecture: Here's Where Your Digital Business Network Starts - Cato Networks." https://www.catonetworks.com/sase/sase-architecture/ (accessed Mar. 18, 2021).
[23] M. Conran, "Secure Access Service Edge (SASE): A reflection of our times," *Network World*, Oct. 03, 2019. https://www.networkworld.com/article/3442941/secure-access-service-edge-sase-a-reflection-of-our-times.html (accessed Apr. 25, 2021).
[24] "The Benefits of SASE - Cato Networks." /blog/the-benefits-of-sase/ (accessed Mar. 10, 2021).
[25] "Secure Access Service Edge (SASE) Definition & Examples," *Awake Security*. https://awakesecurity.com/glossary/secure-access-service-edge-sase/ (accessed Apr. 23, 2021).
[26] "SASE -The Ultimate Guide to Secure Access Service Edge |," *SD-WAN Experts*. https://www.sd-wan-experts.com/sase/ (accessed Mar. 21, 2021).
[27] "What are the benefits of SASE? — Masergy." https://www.masergy.com/blog/what-are-the-benefits-of-sase (accessed Mar. 10, 2021).
[28] "What is SASE? Architecture Overview," *Securus Communications Ltd*, Nov. 22, 2020. https://www.securuscomms.co.uk/what-is-sase-architecture-overview/ (accessed Mar. 10, 2021).
[29] A. Radford, "10 Benefits of SASE Explained," *Securus Communications Ltd*, Nov. 30, 2020. https://www.securuscomms.co.uk/10-benefits-of-sase/ (accessed Mar. 10, 2021).
[30] A. Ruppin, "Council Post: Four Reasons Why SASE Is The Future Of Network Security," *Forbes*. https://www.forbes.com/sites/forbestechcouncil/2020/12/16/four-reasons-why-sase-is-the-future-of-network-security/ (accessed Mar. 21, 2021).
[31] J. Cavanaugh, "SASE challenges include network security roles, product choice." https://searchnetworking.techtarget.com/tip/SASE-challenges-include-network-security-roles-product-choice (accessed Mar. 09, 2021).
[32] J. Cavanaugh, "How SASE convergence affects network and security roles." https://searchnetworking.techtarget.com/tip/How-SASE-convergence-affects-network-and-security-roles (accessed Mar. 09, 2021).
[33] CSHub.com Editorial Staff"A How To Guide To Secure Access Service Edge (SASE)," *Cyber Security Hub*, Nov. 10, 2020. https://www.cshub.com/executive-decisions/articles/a-how-to-guide-to-secure-access-service-edge-sase (accessed Mar. 20, 2021).
[34] M. Korolov, "What is SASE? A cloud service that marries SD-WAN with security," *Network World*, Sep. 07, 2020. https://www.networkworld.com/article/3574014/what-is-sase-a-cloud-service-that-marries-sd-wan-with-security.html (accessed Apr. 23, 2021).
[35] N. Jambhekar, S. Misra, and C. Dhawale, "Cloud computing security with collaborating encryption," *Indian J Sci Technol*, vol. 9, no. 21, pp. 1–7, 2016.