Machine Learning-based Secure 5G Network Slicing: A Systematic Literature Review

Meshari Huwaytim Alanazi
Department of Computer Science, Northern Border University, Arar, Saudi Arabia

***Abstract*—As the fifth-generation (5G) wireless networks continue to advance, the concept of network slicing has gained significant attention for enabling the provisioning of diverse services tailored to specific application requirements. However, the security concerns associated with network slicing pose significant challenges that demand comprehensive exploration and analysis. In this paper, we present a systematic literature review that critically examines the existing body of research on machine learning techniques for securing 5G network slicing. Through an extensive analysis of a wide range of scholarly articles selected from specific search databases, we identify and classify the key machine learning approaches proposed for enhancing the security of network slicing in the 5G environment. We investigate these techniques based on their effectiveness in addressing various security threats and vulnerabilities while considering factors such as accuracy, scalability, and efficiency. Our review reveals that machine learning techniques, including deep learning algorithms, have been proposed for anomaly detection, intrusion detection, and authentication in 5G network slicing. However, we observe that these techniques face challenges related to accuracy under dynamic and heterogeneous network conditions, scalability when dealing with a large number of network slices, and efficiency in terms of computational complexity and resource utilization. To overcome these challenges, our experimentation shows that the integration of reinforcement learning techniques with CNNs, multi-agent reinforcement learning, and distributed SVM frameworks emerged as potential solutions with improved accuracy and scalability in network slicing. Furthermore, we identify promising research directions, including the exploration of hybrid machine learning models, the adoption of explainable AI techniques, and the investigation of privacy-preserving mechanisms.**

***Keywords*—5G; accuracy; deep learning; efficiency; security; machine learning; network slicing; scalability**

I. Introduction

5G networks represent the fifth generation of mobile communication networks and offer advanced features such as high-speed connectivity, ultra-low latency, and extensive machine-type communication capabilities. These networks have become crucial infrastructure for various industries due to the increasing demand for high-speed data transmission and real-time applications like autonomous vehicles, smart cities, and Industry 4.0. However, ensuring the security of 5G networks is a significant concern due to the utilization of new technologies and protocols, the complexity of the network architecture, and the potential for new attack vectors [1]. Network slicing is a crucial element of 5G networks, enabling the establishment of multiple virtual networks on a shared physical infrastructure. This technology empowers the customization of each network slice to cater to the unique demands of diverse applications and services. However, this also introduces new security challenges, including unauthorized access, data breaches, and denial of service attacks [2]. Conventional security measures such as firewalls, intrusion detection systems (IDS), and access control mechanisms may prove inadequate in effectively mitigating these threats.

Given the critical importance of 5G networks and the growing security risks, it is imperative to develop effective security mechanisms for network slicing. Machine learning-based intrusion detection systems (IDS) have emerged as a promising approach to enhance the security of 5G networks. These systems analyze network traffic, behavior patterns, and anomalies in real-time to detect and respond to security threats promptly [3]. Nevertheless, despite the potential that machine learning-based solutions hold for enhancing the security of 5G network slicing, there remains a dearth of comprehensive and methodical research in this particular domain. Therefore, the objective of this study is to conduct a thorough literature review of the current state-of-the-art in this field. The findings of this study will provide valuable insights to researchers and practitioners, helping them understand the current research trends, identify research gaps, and develop effective security solutions for 5G networks. Ultimately, this research endeavor aims to contribute to the development of secure and reliable 5G networks, which are crucial for the success of various industries and the digital economy.

This SLR is a significant contribution in the area of machine learning-based security mechanisms for 5G network slicing. The focus of this review is to analyze the security challenges through advanced machine learning and deep learning techniques, evaluating their effectiveness in the context of 5G networks slicing security, and identifying potential solutions for scalability and efficiency issues. This study analyzes various machine learning techniques for securing 5G network slicing in the subsequent sections beginning with the background in Section II. Section III details the concept of network slicing in 5G networks, explaining its implementation, business model, and significance. Section IV focuses on the security aspects of network slicing in 5G networks, addressing various security issues and challenges. Section V describes the methodology used for the systematic literature review, including data sources, search strategies, and article selection processes. Section VI presents the analysis of the findings from the literature review, discussing the advanced machine learning

techniques employed for security in 5G network slicing, and highlighting the challenges and potential solutions. Section VII concludes and summarizes the key findings of the study and suggests directions for future research.

II. BACKGROUND

The swift progression of technological innovations such as the Internet of Things (IoT), augmented reality (AR), and communication systems such as vehicle-to-vehicle (V2V) and vehicle-to-everything (V2X) have created a pressing demand for substantial enhancements in network and communication infrastructure [1][4]. As a response, 5G networks have gained prominence in meeting the growing consumer demands. The introduction of 5G technology has not only opened up opportunities for innovation but has also provided enhanced reliability for both service providers and consumers, resulting in a shift towards virtualization and widespread adoption of 5G. The benefits of 5G technology include exceptional data rates that are 10 to 100 times faster, widespread coverage, heightened reliability, minimal latency, enhanced quality of service (QoS), and cost-efficient service offerings. With the continuous expansion of these services and opportunities, service providers and network operators are engaged in fierce competition to deploy 5G networks and implement network slicing within the physical network.

The 5G technology consists of three distinct services, namely enhanced mobile broadband (eMBB), massive machine type communication (mMTC), and ultra-reliable low-latency communication (URLLC).eMBB offers peak data rates ranging from 10 to 100 Gbps and achieves high mobility support up to 500 km/h while ensuring reduced power consumption through the utilization of both macro and small cells. mMTC offers long-range connectivity with minimal data rates spanning from 1 to 100 Kbps, facilitating cost-effective machine-to-machine (M2M) communication. Conversely, URLLC provides highly responsive connections across multiple devices, achieving less than 1 ms latency and an end-to-end latency of 5 ms between mobile devices and base stations. URLLC also ensures moderate data rates ranging from approximately 50 Kbps to 10 Mbps, accompanied by an exceptionally high service availability of 99.9999%, establishing it as an exceptionally dependable service. [2]. The deployment of 5G networks is poised to act as a catalyst for market expansion. As of 2020, there were already 92 commercial networks operating across 38 countries, with China accounting for 150 million 5G subscribers and South Korea having eight million. Projections from Ericsson suggest that the United States alone will witness a subscriber base of 320 million by 2025 [11]. The emergence of 5G technology compels communication service providers (CSPs) to go beyond their conventional subscriber-centric business models and position themselves as digital service providers (DSPs). This transformation enables them to fuel innovation, enhance safety, and drive productivity on a global level. Recognizing the transformative potential of 5G, the World Economic Forum identifies it as a driving force behind the fourth industrial revolution. Numerous multinational companies including Huawei, Samsung, Qualcomm, LG, Ericsson, ZTE Corp, Nokia, AT&T, NEC Corp, Cisco Systems, Verizon, and Orange are actively engaged in research and development efforts related to 5G [4] [5]. Notably, AT&T, headquartered in Dallas, covers approximately 16% of the United States, while Verizon, based in New Jersey, has successfully expanded its ultra wideband network to 31 states [6]. Qualcomm predicts that by 2035, 5G will generate a staggering USD 13 trillion in value for goods and service industries worldwide [7]. Given the connectivity capabilities of 5G, which facilitate faster data rates and connect millions of devices, transitioning to 5G is imperative to meet market demands and expectations. Numerous ongoing initiatives are harnessing the potential of 5G technology to transform various industries including robotics, healthcare, automotive, agriculture, mining, media, and fashion. These projects encompass applications such as untethered industrial robots, robotic systems for agricultural purposes, AI-assisted medical diagnosis, virtual reality (VR) for palliative care, telesurgery enabling virtual patient operations, and augmented reality (AR) smart glasses for enhanced safety [8].

Delivering the aforementioned services on conventional 4G or other legacy networks presents significant challenges. To overcome these challenges and provide network services efficiently with limited resources and minimal costs for network service providers, network slicing has emerged as a promising solution. Network slicing is a key feature of 5G technology that involves partitioning the physical network into multiple logical networks, each capable of delivering customized services based on specific applications and their requirements [9]. By leveraging the progress of virtualization in cloud computing, the physical network resources are partitioned into numerous logical or virtual networks known as "slices" in the 5G context. Each network slice functions as an autonomous virtual network with dedicated resources, traffic flows, security measures, topology, and clearly defined quality of service (QoS) parameters. These slices are isolated from each other and serve the distinct service requirements of individual subscribers. [10]. Network slicing offers flexibility and scalability by allowing various services to coexist on a shared physical network. It could adapt to evolving subscriber needs, facilitate seamless end-to-end communication, support a multi-service environment, provide on-demand network services, and incorporate multi-tenancy capabilities within the 5G ecosystem. [11][12].

III. NETWORK SLICING

The advancement and swift development of wireless communication systems have created a need for a wide array of services, applications, and scenarios tailored to meet the specific demands of enhanced mobile broadband (eMBB), ultra-reliable and low-latency communication (uRLLC), and massive machine type communication (mMTC).For instance, eMBB applications, such as virtual reality and video streaming, demand high throughput, while uRLLC services, including autonomous driving, require low latency and minimal errors. mMTC services, catering to sensing and monitoring applications, call for high connectivity. However, the existing network architecture is inadequate to meet the diverse needs of these services.

In response to this obstacle, 5G networks employ network slicing, an approach that enables the provisioning of

customized services with distinct requirements over a unified network infrastructure. Network slicing includes the partitioning of the network into distinct slices, including access, transport, and core network slices. The network slicing framework is depicted in Fig. 1, illustrating this concept [14]. The core network slice consists of both the control plane and user plane, supporting shared or dedicated functions like session management, mobility management, user plane, and policy control for various slices. Notably, industry players like Ericsson and Nokia have developed their own network slicing systems tailored to their respective sectors [19]. In the current wireless communication environment, a wide range of services with different requirements in terms of security, reliability, data rate, latency, resources, and cost have emerged. Network slicing has emerged as a solution to enable resource sharing among services, customers, and providers. It requires the establishment of multiple logical networks on a shared physical infrastructure, enabling the provision of services with distinct characteristics that can concurrently support multiple technologies. Each service is allocated dedicated resources aligned with its specific requirements, thereby enhancing overall network performance. The management of network slicing involves coordinating virtual and physical resource management components, including Network Function Virtualization (NFV), Software-Defined Networking (SDN) controllers, and orchestrators [15]. NFVs (Network Function Virtualization), which refer to cloud-based functions, specify the requirements and attributes of network slices. Meanwhile, SDN (Software-Defined Networking) controllers establish instances of network slices by connecting virtual functions through SDN networks. [16][17]. Orchestrators automate the management and configuration of resources across different domains and slices, simplifying the process of creating, deploying, and monitoring services in an automated manner. Fundamentally, network slicing entails the establishment of logical networks on top of shared physical infrastructures, partitioning them into multiple virtual networks with independent control and management capabilities. Two types of orchestrators, Service Orchestrators (SOs) and Resource Orchestrators (ROs), play a crucial role in creating and managing multiple services. Several open-source network slicing orchestrators have been developed, such as openMANO, OSM, openNFV, openFV, openBaton, ZooM, ONAP, SliMANO, OpenBaton, cloudNFV, JOX, FlexRAN and Cloudify, to efficiently manage resources in access, core, and transport networks [15][18]. Notably, Huawei has developed an end-to-end (E2E) network slicing orchestrator that effectively allocates resources across the three network domains. Its performance has been validated through real hardware implementation, demonstrating reliable resource isolation per slice [19].

The business model related to network slicing comprises several integral components and entities vital to its functioning. These include the network slicing instance (NSI), network slicing subnet instance (NSSI), logical network, network subslice (NSS), network slicing template (NST), network segment, Network Function Virtualization (NFV), Software-Defined Networking (SDN), network slicing manager, communication service manager, resource slice, network slicing provider, network slicing terminal, network slicing tenant, network slicing repository, slice border control, slice selection function, infrastructure owner, infrastructure slice, infrastructure slice provider, and infrastructure slice tenant [20][21]. Each of these elements has specific roles and capabilities in managing the life cycle of a network slice. As an example, the NSI denotes a group of comprehensive logical networks that provide various services tailored to specific requirements, encompassing multiple sub-slice instances. Conversely, the NSSI represents the localized logical network within a network slice, which can be shared among multiple NSIs. Logical networks are virtual instances of network functions established on a single physical network.

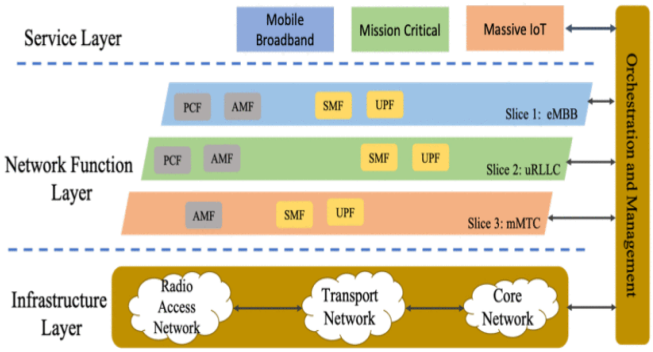

Fig. 1. Network slicing for 5g networks, adopted from [13].

The network slicing manager plays a pivotal role in overseeing the complete lifecycle of each slice or sub-slice by performing various management functions. These include the communication service management function (CSMF), network slice management function (NSMF), and network slice subnet management function (NSSMF). CSMFs are responsible for managing, communicating, and updating the requirements of the slice to support service requests through the communication service manager. NSMFs handle the management of NSIs based on the notifications received from CSMFs, while NSSMFs manage the NSSIs according to the requirements specified by NSMFs. The network slicing requirements encompass various aspects such as network type, network capacity, quality of service (QoS), latency, security level, device count, and throughput. The resource slice refers to the combination of physical and virtual resources necessary for the functioning of network slices. The network slicing provider is the entity responsible for owning the physical infrastructure where multiple slices are created, whereas the network slicing tenant refers to the users of the NSI who deliver specific services requested by customers. The infrastructure owner denotes the entity that owns the physical infrastructure, On the other hand, the infrastructure slice provider is the entity that owns the infrastructure and leases it to host a variety of services via network slicing. The infrastructure slice tenants are the users of the infrastructure slice itself [13].

IV. Security in Network Slicing

Ensuring security is of utmost importance during the implementation of network slicing, which enables the support of diverse services with varying security requirements [22]. The utilization of network slicing in multi-domain infrastructures, serving multiple customers, can introduce

complex security challenges. This is especially evident when resources are shared among slices that adhere to distinct security policies established by various verticals and operators. To effectively address security issues both within and among slices, it is crucial to consider security coordination and protocols during the resource allocation and design stages. Neglecting these aspects may result in the emergence of new and advanced security vulnerabilities in 5G systems and beyond [23]. Each slice is created with isolation constraints in order to prevent the propagation of attack impacts across slices and allow for independent security solutions [24]. It is essential to ensure adherence to fundamental security principles such as confidentiality, authentication, availability, integrity, and authorization within each slice [25]. Confidentiality safeguards against unauthorized data disclosure, authentication verifies the identities of parties involved in interactions, availability ensures the accessibility of slices and applications, integrity guarantees that slice owners maintain control over functionalities and configurations, and authorization determines the permissible capabilities for each network element. Availability refers to the ability of the system to meet the requirements of service level agreements by ensuring that slices and applications can be accessed as needed, while Network Slice Manager (NSM) and Network Functions (NFs) remain consistently accessible. On the other hand, integrity ensures that only slice owners possess the authority to modify or replace the functionality and configuration of their respective slices [26]. Authorization defines the permitted functionalities for each network element, where slice owners are responsible for managing and controlling their respective slices, end-users engage exclusively with authorized slices, infrastructure providers oversee the network slice management (NSM), NSM governs the network slice instances (NSIs) and network functions, and network functions exercise control over resources. These elements consist of slice owners, end-users, service providers, infrastructure providers, network slice management (NSM), and Network Function Virtualization (NFV). The security of network slicing requires each slice and its owners to independently fulfill these requirements in order to mitigate the potential exploitation of network slicing features by attackers, which could lead to system failures [13].

A. Security Issues Introduced by Network Slicing

Network Slicing is distinguished by its crucial attribute of isolation, which has a direct impact on the dependability of the slicing solution. Attaining a high level of isolation is essential to achieve optimal outcomes. Merely supporting a single slice in a slicing system would essentially replicate a conventional non-sliced network, which is already extensively studied. Hence, the coexistence of multiple slices becomes a necessary prerequisite for network slicing, wherein these slices share the same underlying infrastructure. The ability to coexist without interference hinges on establishing the minimum requirements for each slice. By meeting these requirements, interference can be avoided, thereby ensuring effective isolation. Ensuring security in network slicing involves precisely defining the boundaries of interference for each slice, specifying the minimum requirements, and enforcing compliance with these requirements [27].

The significance of identifying isolation characteristics, implementing an abstraction layer for achieving end-to-end isolation at an appropriate level, and establishing appropriate security policies was emphasized in a study [28]. This survey highlighted the lack of a standardized description for isolation capabilities that can be employed for automated deployment. Hence, it is crucial to define the desired initial level of isolation, especially concerning security, and devise dynamic isolation mechanisms capable of enforcing the required level of isolation for each specific service. To tackle the security concerns associated with network slicing in the context of 5G, several organizations, such as the Next Generation Mobile Networks (NGMN), have released guidelines [29]. These recommendations assist in identifying potential security risks in the general packet core. Additionally, technology guidelines, such as ETSI's recommendations for Network Function Virtualization (NFV), provide further guidance in addressing security concerns. [30], have been taken into account. ETSI's guidelines encompass security considerations throughout the lifecycle of virtual network functions.

B. More Security Challenges to Network Slicing

Network slicing implementation in the telecommunications industry presents challenges, particularly concerning security and the deployment of the radio access network (RAN). These challenges have been extensively discussed by researchers like Kotulski et al. [32]. Security concerns arise with the introduction of network slicing. One significant risk is the potential for denial-of-service (DoS) attacks and resource depletion [32], which can disrupt network availability and performance. Other threats include monitoring, traffic injection, and impersonation attacks [27], jeopardizing data integrity and network efficiency. Moreover, the use of diverse systems from different vendors in network slicing creates a security vulnerability due to the absence of standardized security measures [32]. Exploiting vulnerabilities in these systems, attackers can successfully target network slices. Additionally, specific weaknesses in the isolation and protection mechanisms designed for network slices may enable unauthorized access to resources and sensitive data. To address these security threats and vulnerabilities, robust security measures are necessary. These can involve implementing intrusion detection and prevention systems, enforcing access control policies, and establishing comprehensive security monitoring. Furthermore, integrating security considerations into the design of network slicing systems and protocols ensures a secure-by-default approach. Standardized security practices enhance overall network slicing security and promote interoperability among different vendor systems [31] [32]. The physical realization of the RAN poses challenges in implementing network slicing. Ensuring resource, traffic, and user isolation within radio network elements is a significant obstacle. One suggested approach involves the utilization of millimeter waves for covering small cells, leveraging the cell size to achieve isolation. Nevertheless, current technologies like cognitive radio and non-orthogonal multiple access fall short in delivering the necessary levels of isolation and slicing required to meet the desired standards. Thus, further research and development are essential to overcome the physical implementation challenges of network slicing in the RAN [31].

The challenges pertaining to security and access management in network slicing originate from the varying security and privacy requirements [27] of different network slices in 5G networks. Network slicing is dependent on the implementation of software-defined networking (SDN) and network function virtualization (NFV). [33], which virtualize network functions as software components. However, ensuring secure inter-slice access and end-to-end network slicing security becomes more complex in 5G due to its comprehensive slicing approach. Securing the management of network slicing encompasses various tasks, including establishing secure access between the radio access network and core network resources, ensuring secure connections between user equipment (UE) and network slice instances, and effectively managing shared resources among different network slices. Neglecting these challenges can lead to security risks, including compromised controllers or orchestrators, isolation failures, insider threats, compromised NFV instances, and unauthorized data access [34][35]. The centralized slice manager also presents security considerations, including the security of network slice templates, concerns regarding unauthorized access, and issues related to trust [36]. Additionally, in multi-domain infrastructures or multi-tenant environments, network slicing may encounter additional security and privacy challenges. To mitigate these concerns, it is essential to adhere to established security principles, including but not limited to confidentiality, integrity, authenticity, availability, and authorization [37][38]. In the context of network function virtualization (NFV), maintaining confidentiality is vital to mitigate potential threats. For example, a compromised slice manager can lead to unauthorized monitoring of traffic through both northbound and southbound interfaces, potentially exposing sensitive slice configurations. Similarly, vulnerabilities in the application programming interface (API) used during configuration can enable malicious actors to interfere with slice installation, configuration, or activation. Thus, ensuring the confidentiality of inter-slice communications is crucial for establishing a secure environment [39][40][41]. Proactive measures like implementing secure communication protocols, enforcing access controls, and conducting regular security policy reviews are necessary to mitigate these threats effectively.

V. METHODOLOGY

This section provides an overview of the methodology employed to conduct a Systematic Literature Review (SLR) on the subject of Machine Learning-based secure 5G network slicing, following the recommended guidelines outlined in [42]. The process of formulating research questions is discussed, along with the motivating factors behind these questions. Various data sources were used to select relevant articles, and a specific search strategy was employed to obtain articles in the domain. Inclusion and exclusion criteria were applied to select articles for review. In order to present a comprehensive overview of the current state-of-the-art in Machine Learning-based 5G network slicing, Table I illustrates the research questions along with their respective motivations.

TABLE I. RESEARCH QUESTIONS AND MOTIVATION

	Question	Motivation
RQ1	What are the most advanced machine learning techniques currently employed for ensuring the security of 5G network slicing?	It aims to identify and analyze existing machine learning-based techniques for securing 5G network slicing to develop more effective and efficient security solutions.
RQ2	What are the main obstacles and constraints faced by these techniques in terms of accuracy, scalability, and efficiency?	It aims to identify the potential issues that may arise when implementing machine learning-based techniques for securing 5G network slicing, and to develop strategies to overcome these challenges and limitations.
RQ3	What are the potential solutions to address these challenges and limitations?	It aims to identify and propose possible solutions/recommendations to overcome the challenges and limitations of machine learning-based techniques for securing 5G network slicing.
RQ4	What are the future research directions and opportunities in this area?	It aims to explore the integration of explainable AI and federated learning, investigate the transferability of models across different network architectures and scenarios, and design new evaluation metrics and methodologies for machine learning-based solutions.

A. Data Sources

Table II displays the reputable publishers such as IEEE, Science Direct, Springer, ACM Digital Library, Wiley, Sage, MDPI and Google Scholar, from which the articles were selected for review.

TABLE II. DATABASE SOURCES

Publisher	URL
IEEE	https://www.ieee.org
Science Direct	https://www.sciencedirect.com
Springer	https://link.springer.com
ACM Digital Library	https://www.acm.org
Wiley	https://onlinelibrary.wiley.com
Sage	https://journals.sagepub.com
MDPI	https://www.mdpi.com
Google Scholar	https://scholar.google.com/

B. Search Strategy

Due to limited research in this area initially, articles considered for review in this study were limited to those published from the year 2018 onwards. The initial stage in constructing the search query involved identifying appropriate keywords aligned with the theme and the research questions put forth. Primary keywords including "network slicing," "5G," "security," and "machine learning" were identified, and logical operators such as "AND" and "OR" were used to link these keywords appropriately. After conducting several tests, the researchers arrived at a search string that produced a sufficient number of related research articles. The keywords used in the search string are listed in Table III.

TABLE III. SEARCH STRING

String	Batch1	Batch2	Batch3	Batch4
String1	Network Slicing	5G	Security	Machine Learning
String2	Network-Slicing			Machine-Learning
String3				ML

C. Article Selection Process

The methodology employed for selecting articles commenced with formulating research questions that guided the creation of a search query for article retrieval. Only articles published in the English language were taken into account. The PRISMA flow diagram was utilized to visualize the article selection process [43] to ensure a systematic and transparent approach to article selection, as illustrated in Fig. 2. Once the pertinent literature was identified, a comprehensive review of load balancing techniques in software-defined networks was performed. The review process concluded with a meticulous categorization of the load balancing techniques to ensure thoroughness. Many articles were excluded during the screening process due to their titles not meeting the inclusion criteria or abstracts not being relevant for the survey.

Search String: (([Batch1, String1] OR [Batch1, String2]) AND ([Batch2, String1]) AND ([Batch3, String1]) AND ([Batch4, String1] OR [Batch4, String2] OR [Batch4, String3])).

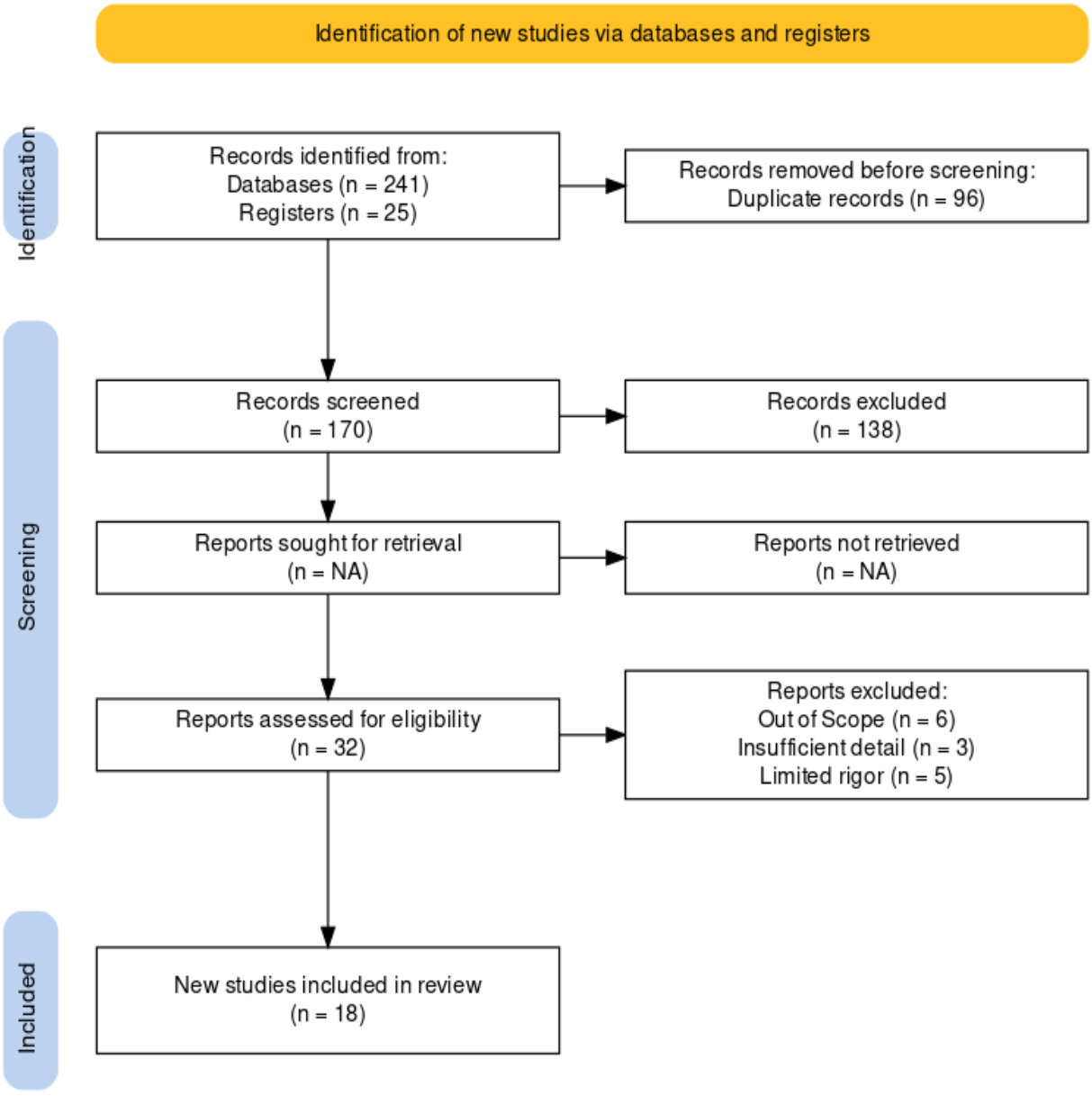

Fig. 2. PRISMA flow diagram.

D. Data Extraction

The research methodology utilized in this study encompassed an extensive exploration to collect relevant literature pertaining to the subject of secure 5G network slicing utilizing machine learning. The primary objective was to identify and select articles that provide valuable insights into this field of study. The research process consisted of several distinct phases, including a targeted search, application of inclusion and exclusion criteria, and comprehensive evaluation of selected articles. The initial step in the research process involved performing a targeted search using specific keywords. This search was conducted across reputable publishers and covered the period between 2018 and 2023. Fig. 3 shows the year-wise number of articles that were published by these publishers. The list of sources used to perform this survey is provided in Table II. The aim was to gather a comprehensive collection of articles related to the subject matter. As a result of this search, a total of 241 articles were identified and retrieved.

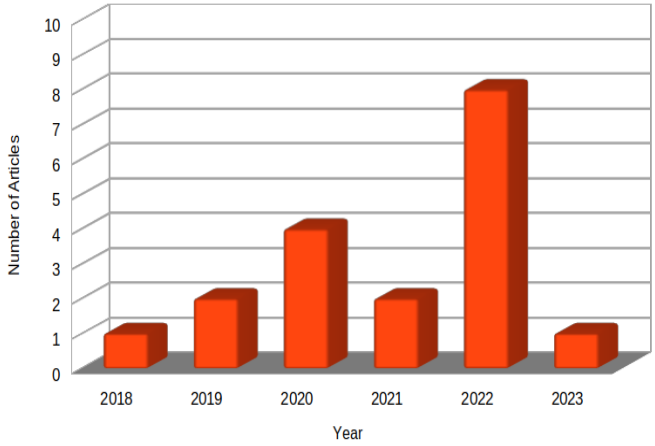

Fig. 3. Year-wise categorization of articles.

E. Inclusion and Exclusion Criteria

To refine the selection and focus on significant research, inclusion and exclusion criteria were established. These criteria were specifically designed to guarantee the inclusion of only articles that directly relate to the research topic. Table IV presents a comprehensive breakdown of the inclusion and exclusion criteria implemented during this process. By applying these criteria, the initial pool of 241 articles was reduced to 170, thereby eliminating articles that did not meet the predefined criteria. The subsequent phase of the research involved a detailed examination of the remaining 170 articles. During this phase, the titles and abstracts of the articles underwent a thorough examination to further refine the selection process. The purpose of this review was to identify articles that aligned closely with the research focus on machine learning-based secure 5G network slicing. As a result of this review, 32 articles were selected for further evaluation.

The selected 32 articles underwent a comprehensive evaluation based on their content to ensure a close match with the objectives and scope of the current research. This evaluation involved an in-depth analysis of the full texts of the articles, including an examination of the methodology, findings, and discussions presented. The aim of this evaluation was to identify articles that provide valuable insights and contribute directly to the research topic. Following this rigorous evaluation process, a final set of 18 articles was identified as the most relevant to the research topic. The selection of these 18 essential research articles was conducted meticulously, taking into account the alignment between the titles, abstracts, and comprehensive content of the articles. The selected articles were recognized as valuable sources of insights into machine learning-based secure 5G network slicing, and their inclusion in the study was deemed essential for the progression of the current research endeavor.

TABLE IV. INCLUSION AND EXCLUSION CRITERIA

Inclusion	Exclusion
The study focuses on Machine Learning-based secure 5G network slicing	The study that focuses on areas other than Machine Learning-based secure 5G network slicing
Only the articles written in English language are considered	Articles written in non-English language are not considered
Articles published by the publishers listed in Table II	Unpublished articles and those that are not peer-reviewed, are not considered
Articles published in well-reputed and high impact factor journals are considered	White papers, editorials, keynote speeches, and articles from predatory journals are not considered

VI. DISCUSSION

In this systematic literature review, we investigated the current state of research on machine learning-based solutions for secure 5G network slicing. Our review identified a total of 18 relevant articles that met our inclusion criteria. From our analysis of these articles, several key themes emerged. Firstly, machine learning techniques are widely used for various security-related tasks in network slicing, including anomaly detection, intrusion detection, and malware detection. Secondly, while there is a broad consensus on the potential benefits of machine learning-based solutions for securing 5G network slicing, there is also a lack of standardization and interoperability among different solutions. Finally, the use of machine learning in network slicing introduces several challenges related to data privacy, explainability, and scalability. In this discussion section, we will elaborate on these themes while answering the research questions and provide recommendations for future research in this area.

Q1. What is the most advanced machine learning techniques currently employed for ensuring the security of 5G network slicing?

Network slicing is a vital component of 5G and future generation networks since it enables the creation of customized logical networks with diverse functionalities, dependability, and security properties. Scholars have proposed multiple types of Machine Learning (ML) and Deep Learning (DL) approaches to increase the security and reliability of network slicing. Table V summarizes the state-of-the-art ML/DL algorithms used in the scientific literature for secure 5G network slicing. This discussion examines the strategies for secure 5G network slicing presented in the selected articles. Fig. 4 illustrates the performance of various machine

learning algorithms concerning the security of 5G network slicing. Each algorithm is evaluated based on three key criteria: accuracy, scalability, and efficiency. Accuracy reflects the algorithm's ability to provide precise and reliable security measures. Scalability measures its capacity to handle an increasing number of network slices efficiently, accounting for complex dependencies. Efficiency assesses how well the algorithm utilizes resources during security processes. The chart clearly distinguishes the strengths and weaknesses of different algorithms. For instance, algorithms like RL (Reinforcement Learning) and DQN (Deep Q-Network) demonstrate high scores in all three categories, making them robust choices for secure 5G network slicing. On the other hand, algorithms like LSTM (Long Short-Term Memory) and DBN (Deep Belief Networks) show comparatively lower scores, suggesting room for improvement in their application.

TABLE V. STATE-OF-THE-ART ML TECHNIQUES, CHALLENGES AND POTENTIAL SOLUTIONS

Ref.	Algorithm	Challenges			Potential Solutions
		Accuracy	Scalability	Efficiency	
[45][49][51][52][61]	CNN (Convolutional Neural Networks)	Lack of accuracy in network slice orchestration and optimization and deep learning-based DDoS attack detection for network slicing.	Scalability challenges in securing multiple network slices simultaneously	Inefficient resource utilization during attack mitigation	Integrating reinforcement learning techniques with CNNs can address accuracy, scalability, and resource utilization challenges in secure 5G network slicing, including network slice orchestration, DDoS attack detection, and simultaneous protection of multiple network slices.
[44][55][56][62]	RL (Reinforcement Learning)	Limited accuracy in intelligent resource allocation	Difficulty in scaling up network slices due to complex dependencies	Inefficient resource utilization during IP shuffling processes	Multi-agent RL for accurate, scalable, and efficient secure 5G network slicing for intelligent resource allocation, complex dependencies, and IP shuffling processes.
[46][52][54][66]	SVM (Support Vector Machine)	Challenges in achieving accurate end-to-end security in network slices	Scalability challenges in managing security across numerous network slices	Inefficient utilization of security resources	Distributed and scalable SVM frameworks can address accuracy and scalability challenges in securing network slices, optimizing resource utilization in 5G network slicing.
[50][57][60][68]	DQN (Deep Q-Network)	Accuracy challenges in context-aware authentication handover for secure network slicing	Scalability concerns in managing authentication handover across numerous network slices	Inefficient resource allocation for authentication handover processes	Application of advanced deep reinforcement learning techniques, such as hierarchical or multi-agent DQN, to improve accuracy, scalability, and resource allocation for context-aware authentication handover in secure 5G network slicing.
[45][49][69]	LSTM (Long Short-Term Memory)	Lack of accuracy in network slice orchestration and optimization	Scalability issues in managing a large number of network slices	Inefficient resource allocation and utilization	Advanced LSTM-based deep learning with RL/attention improves accuracy, scalability, and resource allocation in secure 5G network slice orchestration.
[58][59]	FL (Federated Learning)	Limited local data in network slices hampers model performance and accuracy.	Limited computational resources in network slices hinder scalability, impacting Federated Learning.	Sub-optimal resource allocation and usage can impact system efficiency and performance	Improve model performance with data augmentation and transfer learning, optimize resource allocation for scalability, and employ efficient scheduling techniques to enhance system efficiency in secure 5G network slicing.
[48]	K-means clustering, Naive Bayes classifier	Accuracy issues in automated machine learning for network slice automation	Scalability concerns in managing and orchestrating a large number of network slices	Inefficient utilization of automated processes	Improving accuracy of automated machine learning models; Scalable orchestration frameworks; Efficient utilization of automated processes through optimization
[53]	GAN (Generative Adversarial Networks)	Accuracy challenges in adversarial machine learning for flooding attacks in network slicing	Scalability issues in detecting and mitigating flooding attacks across multiple network slices	Inefficient resource utilization during attack mitigation	Improving accuracy of adversarial machine learning models; Scalable flooding attack detection mechanisms; Efficient utilization of resources during attack mitigation
[54]	DBN (Deep Belief Networks)	Accuracy issues due to complex network slices, limited labeled data, and difficulty capturing intricate patterns.	Scalability issues in managing numerous slices efficiently and handling increased computational and communication overhead.	Inefficient resource utilization, communication overhead, and synchronization processes.	Data augmentation, transfer learning, efficient parallelization, optimized resource allocation, and adaptive strategies to improve accuracy, scalability, and resource utilization.

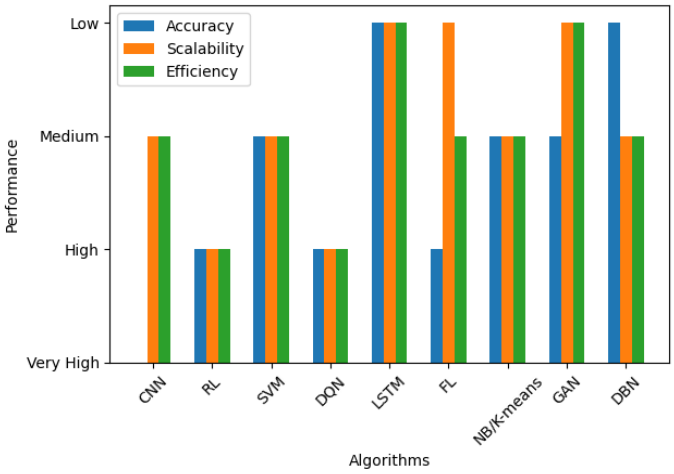

Fig. 4. Algorithm performance for secure 5G network slicing.

Jiang et al. [44] proposed a "Intelligence Slicing" framework combining network slicing and AI for improved intelligence, security, and flexibility. To maximize the efficiency of network slicing and to ensure end-to-end security, the framework employs AI techniques such as reinforcement learning, transfer learning, and deep learning. Deep neural networks are used in [45] to predict resource requirements for different slices, and a clustering technique is used to group analogous slices. The goal is to eliminate wastage of resources while maintaining network stability. Liu et al. [46] suggested a learning-assisted secure end-to-end network slicing technique for cyber-physical systems (CPS). For efficient resource allocation among similar CPSs, ML approaches such as k-means clustering and k-nearest neighbors are used. To maintain slice confidentiality and integrity, a secure key exchange mechanism is used. Sedjelmaci [47] presented a cooperative attack detection system based on AI, applying machine learning techniques such as random forest and decision trees to identify any type of malicious activity and differentiate between legitimate and malicious traffic. This method improves network slicing security by detecting and mitigating threats more effectively. Kafle et al. [48] developed an ML-based network slicing automation strategy based on a multi-agent reinforcement learning technique. To provide end-to-end security, the approach learns from previous slicing events to make accurate slicing decisions while optimizing resource allocation and restricting the attack surface. Secure5G is a DL-based architecture for secure network slicing that was introduced in [49]. It makes use of deep neural networks to estimate slice resource requirements and efficient resource allocation. The framework consists of a security module that detects and mitigates network attacks using a deep belief network. A reinforcement learning-based technique for attacking and defending 5G radio access network slicing is proposed in [50]. It learns optimal attack and defense techniques through deep reinforcement learning, enabling network administrators to identify and mitigate vulnerabilities. The DeepSecure technique introduced in [51] analyzes traffic patterns and detects distributed denial-of-service (DDOS) attacks on 5G network slicing, using convolutional neural networks. It enhances reliability and security by effectively detecting and mitigating such attacks. A hybrid DL-based approach for wireless network slicing is proposed in [52]. This approach combines deep neural networks for network traffic prediction and a reinforcement learning algorithm for resource allocation optimization. It aims to improve the reliability and accuracy of network slicing while ensuring end-to-end security. In [53], an adversarial ML approach is proposed to detect and mitigate flooding attacks on 5G radio access network slicing. It enhances security by effectively identifying and mitigating such attacks. Benzaid et al. [54] propose an AI-based autonomic security management architecture for secure network slicing in B5G networks, focusing on effective security management leveraging AI techniques. Another approach proposed in [56] introduces a learning augmented optimization approach to safeguard network slicing in 5G. It presents a mathematical model and optimization algorithm that utilizes machine learning to adapt to network environment changes, minimizing network cost while ensuring secure slices meeting quality of service requirements. [57] presents SliceBlock, a secure network slicing scheme utilizing a DAG-blockchain to authenticate handover requests between network slices in edge-assisted SDN/NFV-6G environments. It integrates DAG-blockchain technology with SDN/NFV and edge computing, providing a secure and reliable network slicing service. Federated learning, proposed in [59], aims to improve security in network slicing by aggregating training data from multiple slices to detect anomalies and security threats across the entire network. Simulation experiments demonstrate its effectiveness in enhancing security threat detection accuracy. Lastly, [60] proposes a reinforcement learning approach for attacking and defending NextG radio access network slicing. It utilizes multi-agent reinforcement learning to train agents capable of launching attacks and defending against them in network slicing scenarios.

Q2. What are the main obstacles and constraints faced by these techniques in terms of accuracy, scalability, and efficiency?

Network slicing has become a pivotal concept within 5G networks, enabling operators to divide their networks into virtualized networks that are customized to meet the distinct needs of various applications and services. Integrating machine learning (ML) and deep learning (DL) techniques presents a promising avenue for enhancing the security of network slicing. This integration facilitates the detection and prevention of security threats in real-time, offering an effective approach to safeguarding network slicing. However, leveraging ML and DL in secure network slicing poses various challenges, including the need for labeled data, complexity of models, and ensuring data confidentiality and privacy. Subsequent sections will delve into a comprehensive examination of these challenges, providing a detailed analysis, and presenting potential solutions to address them.

Jiang et al. [44] propose a comprehensive framework named "Intelligence slicing" that combines artificial intelligence (AI) with 5G networks. However, they do not discuss the limitations in terms of accuracy and scalability associated with their framework. Thantharate et al. [45] propose "DeepSlice," an approach based on deep learning (DL) for achieving efficient and dependable network slicing in

5G networks. The authors recognize the challenges associated with handling large volumes of training data and the need for substantial computational resources, which could potentially impede scalability and efficiency. Liu et al. [46] introduce the concept of "Learning-assisted secure end-to-end network slicing" for cyber-physical systems. They emphasize the issue of explainability in machine learning-based security approaches, underscoring its potential impact on trust and the acceptance of such methods. Sedjelmaci [47] puts forward a cooperative attack detection system based on artificial intelligence (AI) for 5G networks. The authors highlight the drawbacks of conventional rule-based systems and emphasize the potential advantages of AI-based systems, but they do not explicitly address the specific limitations associated with such approaches. Kafle et al. [48] suggest the automation of 5G network slicing through the utilization of machine learning techniques. The authors recognize the challenges brought about by the complexity of the network and the requirement for substantial amounts of training data. Thantharate et al. [49] introduce "Secure5G," a DL framework for secure network slicing in 5G and future networks. However, they recognize the challenge of developing DL models capable of detecting and defending against new and unknown attacks. The research in [50] presents a reinforcement learning approach for attacking and defending 5G radio access network slicing, but does not delve into the accuracy or scalability limitations of the approach. Kuadey et al. [51] introduce "DeepSecure," which is a deep learning-based approach for detecting distributed denial-of-service (DDoS) attacks in 5G network slicing. The authors acknowledge the difficulty of developing accurate models while minimizing false positives. The study presented in [52] proposes a hybrid deep learning approach for achieving high accuracy and reliability in wireless network slicing within the context of 5G. However, the study does not delve into the limitations of this approach. Shi and Sagduyu the approach proposed in [53] is based on adversarial machine learning and aims to address flooding attacks on 5G radio access network slicing. However, the study does not explicitly discuss the challenge of developing robust models that are resilient to adversarial attacks. Benzaid et al, [54] introduces an AI-based autonomic and scalable security management architecture for secure network slicing in B5G. However, they do not specifically discuss the limitations related to developing models capable of handling the dynamic and heterogeneous nature of B5G networks.. Yoon et al. [55] presents a technique called "Moving target defense for in-vehicle software-defined networking" that utilizes IP shuffling in network slicing, combined with multi-agent deep reinforcement learning. They address the challenges associated with accurate attack detection and mitigation in dynamic and mobile environments. Cheng et al. [56] suggests a method called "Safeguard network slicing in 5G" that employs a learning-augmented optimization approach. They acknowledge the challenge of managing the complexity and dynamics inherent in 5G networks. Abdulqadder and Zhou [57] present "SliceBlock," a solution that combines context-aware authentication handover and secure network slicing using DAG-blockchain in edge-assisted SDN/NFV-6G environments. However, the study does not delve into the specific limitations associated with their proposed models. In their paper [58], Bandara et al. introduces a federated learning platform for network slicing that incorporates blockchain and zero trust security mechanisms. However, the proposed platform encounters challenges in terms of ensuring high accuracy and scalability. Similarly, Wijethilaka and Liyanage [59] suggest a federated learning approach to enhance security in network slicing. However, the approach faces challenges in terms of scalability and efficiency. On the other hand, Shi et al. [60] utilize reinforcement learning for attacking and defending NextG radio access network slicing. However, their proposed approach encounters limitations in terms of scalability and accuracy. Lastly, Chowdhury et al. [61] introduce AUTODEEPSLICE, a data-driven technique for network slicing that employs automatic deep learning. However, they face challenges in achieving accurate results due to the inherent complexity of network slicing.

Q3. What are the potential solutions to address these challenges and limitations?

1) Solutions presented in the literature: One possible solution to tackle the challenges and limitations discussed in the papers involves developing and implementing intelligent slicing frameworks that integrate artificial intelligence (AI) into 5G networks [44]. This strategy capitalizes on machine learning algorithms to optimize and automate network slicing processes [48], enhancing the reliability of network slicing [52], and fortifying the security of 5G networks against cyber-attacks [46][49][51]. An alternative strategy is to utilize reinforcement learning to protect against flooding attacks in 5G radio access network slicing [53][60][63][64][65]. Furthermore, a context-aware authentication handover and secure network slicing that incorporates a DAG-blockchain in edge-assisted SDN/NFV-6G environments can enhance the security of network slicing [57]. Federated learning can also be deployed to bolster the security of network slicing [59]. By incorporating the Skunk-A Blockchain and Zero Trust Security Enabled Federated Learning Platform, the security of 5G/6G network slicing is significantly enhanced. [58]. Finally, data-driven network slicing techniques utilizing automatic deep learning can be employed to enhance network slicing in 5G networks [61].

2) Recommended solutions: The integration of Convolutional Neural Networks (CNNs) with reinforcement learning techniques offers a promising solution to tackle challenges related to accuracy, scalability, and resource utilization in secure 5G network slicing effectively. This integration can be applied to various aspects, including network slice orchestration, DDoS attack detection, and simultaneous protection of multiple network slices.

a) Markov Decision Process (MDP): Consider the problem of network slice orchestration as a Markov Decision Process (MDP) [63], defined by the tuple (S, A, P, R, γ). Here, S is the state space, A is the action space, P represents the transition probabilities, R is the reward function, and γ is the discount factor. The objective is to find an optimal policy π that maximizes the expected cumulative reward:

$$\pi^* = argmax_\pi E_\pi[\sum_{t=0}^{\infty} \gamma^t R(s_t, a_t)] \quad (1)$$

Where, π^* represents the optimal policy that provides the best actions a_t in each state s_t, taking into account the long-term cumulative reward. The MDP formulation considers network slice orchestration as a sequential decision-making problem. By optimizing the policy π, it ensures that actions taken in each state lead to the maximum cumulative reward, which is vital for efficient network resource allocation.

b) Bayesian reinforcement learning: To improve DDoS attack detection, we can model it as a Bayesian Reinforcement Learning problem [64], where we need to infer the optimal policy π given a sequence of observations O and actions A. We seek to maximize the posterior probability of the policy given the data:

$$P(\pi|O,A) \propto P(O|\pi,A)P(\pi|A) \quad (2)$$

Where, $P(\pi|O,A)$ is the posterior policy probability, $P(O|\pi,A)$ is the likelihood of observations given the policy, and $P(\pi|A)$ is the prior policy probability. The Bayesian RL formulation models DDoS attack detection as a probabilistic learning problem. It estimates the posterior policy π given observed data, enabling improved detection accuracy through probabilistic reasoning.

c) Multi-objective optimization: For simultaneous protection of multiple network slices, we can formulate it as a Multi-Objective Optimization problem [65]. Let $F = [f_1(x), f_2(x), \ldots, f_k(x)]$ represent a vector of k objective functions, and $X = [x_1, x_2, \ldots, x_n]$ denote the vector of decision variables. Additionally, $G = [g_1(x), g_2(x), \ldots, g_m(x)]$ represents a vector of m inequality constraints. The goal is to find a vector of decision variables X^* that optimizes multiple objectives while satisfying constraints:

$$X^* = arg\ min_x F(X) = [f_1(X), f_2(X), \ldots, f_k(X)] \quad (3)$$

Subject to:

$$g_i(X) \leq 0, for\ i = 1,2,\ldots,m$$

The multi-objective optimization approach provides a rigorous framework to balance multiple objectives while considering constraints. It ensures that resources are efficiently allocated to protect multiple network slices.

d) Multi-agent reinforcement learning: In the context of secure 5G network slicing, multi-agent reinforcement learning [66] demonstrates potential for addressing accuracy, scalability, and resource utilization challenges. Specifically, it can enable intelligent resource allocation by considering complex dependencies and facilitating IP shuffling processes. We performed an experiment using python to demonstrate a custom reinforcement learning environment, termed NetworkSlicingEnv, designed to emulate a 5G network slicing scenario, where an agent makes resource allocation decisions with the goal of optimizing the allocation of resources based on dependencies among actions. The experiment utilizes the Proximal Policy Optimization (PPO) algorithm, a cutting-edge reinforcement learning method. The agent's training process includes learning to optimize resource allocation while considering dependencies among actions, contributing to the achievement of optimal resource utilization and scalability in 5G network slicing.

We define the 'NetworkSlicingEnv' environment and then train a PPO model to optimize resource allocation within the environment. After training, we evaluate the model's performance by calculating the mean reward over a specified number of episodes, denoted by 'n_episodes'. This mean reward serves as an indicator of the model's resource allocation capabilities in the secure 5G network slicing scenario. The algorithm presented below depicts the scenario:

Algorithm:

Inputs:

'n_episodes': Number of episodes for evaluation

Outputs:

'mean_reward': Mean reward over the evaluation episodes

Initialize:

1. Define the environment class 'NetworkSlicingEnv':
   a. Initialize the action space with 10 discrete resource allocation options.
   b. Initialize the observation space with a 5-dimensional state observation.

Procedure 'TrainModel' **(Total Timesteps: 10,000):**

1. Create a multi-agent environment instance 'env'.
2. Define a PPO model with a multi-layer perceptron policy ('MlpPolicy') for policy optimization.
3. Train the model with the 'learn' method using 'total_timesteps=10,000'.

Procedure 'EvaluateModel' **(Number of Episodes:** 'n_episodes'**):**

1. Initialize 'mean_reward' to 0.
2. For each episode in the range 'n_episodes', do the following:
   a. Reset the environment ('env') and obtain the initial state.
   b. For each time step:

      i. Predict an action using the trained model ('model') *based on the current state.*

      ii. Simulate the environment's response and receive the reward.

      iii. Accumulate the reward.

      iv. Check if the episode is done. If done, break the loop.

3. Calculate the 'mean_reward' as the sum of rewards over 'n_episodes' divided by 'n_episodes'.

Output 'mean_reward'**.**

End

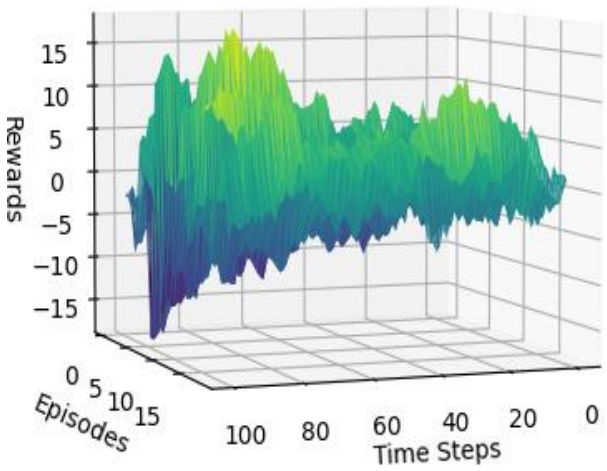

Fig. 5. Multi-Agent reinforcement learning training rewards over time.

The experimental results reveal the agent's learning progress, represented through a 3D plot showcasing the cumulative reward over training steps as shown in Fig. 5. The positive rewards indicate that the agent is learning to make resource allocation decisions that result in outcomes deemed favorable. This implies that the agent is successfully adapting its behavior over time to maximize the cumulative rewards. The learning dynamics suggest that the agent is gradually improving its understanding of the environment and making better choices in allocating resources. As the training progresses, the agent becomes more proficient in resource allocation. The positive rewards show that the agent is making decisions that lead to efficient resource utilization. This can be seen as an indication of improved performance in managing network resources for 5G network slicing. The 3D plot visualizes how the agent's rewards change over the course of training. Gradually, the agent should learn to make resource allocation decisions that result in higher cumulative rewards, which signifies an improved understanding of the environment and more effective decision-making. The mean reward, calculated at the end of training, provides a summary of the agent's performance. A higher mean reward suggests that the agent has improved its decision-making skills regarding resource allocation, which is a critical aspect of network slicing in 5G environments. The positive rewards demonstrate that the agent's learning dynamics are effective in improving its performance in resource allocation decision-making. The agent gradually learns to allocate resources more efficiently, resulting in higher cumulative rewards and, by extension, better performance for secure 5G network slicing.

e) Support Vector Machine (SVM): For securing network slices in a scalable manner, distributed and scalable Support Vector Machine (SVM) [67] frameworks can be employed. These frameworks contribute to improving both accuracy and scalability while optimizing resource utilization within the 5G network slicing environment. In the experiment conducted, a synthetic dataset was generated for binary classification, simulating a scenario in which SVM-based classification is employed. The code utilizes the Scikit-Learn library to create a two-dimensional dataset with 1000 samples. The algorithm presented below depicts the scenario:

Algorithm:

Input:

- Training data: (X_{train}, y_{train})
- Testing data: (X_{test}, y_{test})

Initialization:

a. Initialize SVM model: SVM_{model}.

Data Preparation:

a. Split the data into training and testing sets:
   - X_{train}, y_{train} for training.
   - X_{test}, y_{test} for testing.

Accuracy Optimization:

a. Train the SVM model on the training data:
   - $SVM_{model}.fit(X_{train}, y_{train})$.

b. Make predictions on the test data:
   - $y_{pred} = SVM_{model}.predict(X_{test})$.

c. Calculate accuracy (*A*) using the ground truth and predictions:
   - $A = \frac{Number\ of\ correct\ predictions}{Total\ number\ of\ predictions}$.

Scalability Optimization:

a. In SVM, the margin is automatically maximized during training to improve scalability (*S*).

Resource Utilization:

a. SVMs automatically select a subset of support vectors for decision function, which reduces resource utilization (*R*).

Output:

a. Return:
   - Trained SVM model: SVM_{model}.
   - Accuracy (*A*).
   - Scalability (*S*).
   - Resource Utilization (*R*).

End

The data is divided into training and testing sets to evaluate the SVM model's performance. The SVM model employs a linear kernel for classification and is trained on the training data. The decision boundary is plotted along with the data points, with a color scale indicating the accuracy level of 0.88 in this case. The visualization demonstrates how SVM, as a scalable framework, can effectively classify data while maintaining a high level of accuracy as depicted in Fig. 6. This technique proves to be an optimal solution for ensuring network slice security and efficient resource allocation within the complex 5G environment, making this experiment a valuable illustration of SVM's capabilities in a network slicing context.

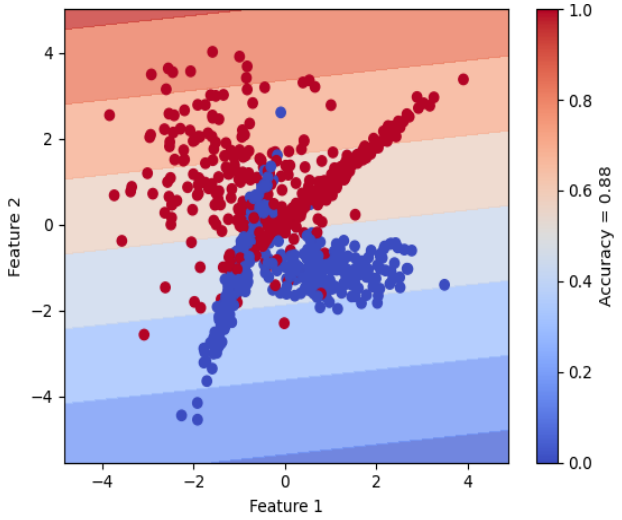

Fig. 6. Secure network slice classification: SVM decision boundary with 88% accuracy.

f) Deep learning: By leveraging sophisticated deep reinforcement learning methods like hierarchical or Multi-Agent Deep Q-Networks (MADQN) [68], it is possible to improve accuracy, scalability, and resource allocation in the context of context-aware authentication handover within secure 5G network slicing. We used TensorFlow library to demonstrate the concept of rewards over a series of episodes, environments, which is a critical aspect of evaluating the performance of Multi-Agent Deep Q-Networks (MADQN) in context-aware authentication handover within 5G network slicing environments. These rewards are indicative of the efficiency and learning progress of a group of agents working collaboratively to make decisions. The rewards represent various factors, including the success of authentication handover processes, the minimization of resource utilization, and the overall optimization of network slicing. By examining the rewards over episodes, we gain valuable insights into how well the MADQN is adapting and learning within this environment as shown in Fig. 7. Consistent, positive rewards indicate that the MADQN is effectively enhancing the authentication handover process and resource allocation, contributing to scalability and the overall security of 5G network slicing.

Algorithm:

Input:

- State size (‘state_size’)
- Action size (‘action_size’)
- Number of agents (‘num_agents’)
- Total training episodes (‘episodes’)

Initialization:

- Initialize ‘state_size’, ‘action_size’, ‘num_agents’, and ‘episodes’.
- Initialize the multi-agent environment (‘env’) with given parameters.

Agent Creation:

- For each agent (‘i = 1’ to ‘num_agents’):

  a. Create a DQNAgent (‘agent[i]’) with ‘state_size’ and ‘action_size’.

  b. Build a neural network model for ‘agent[i]’ with three dense layers.

Training Loop:

- For each episode (‘e = 1’ to ‘episodes’):

  a. Generate random initial states for each agent and store in states.

  b. For each step in the episode:

  i. Query each agent for actions based on their current state.

  ii. Implement the logic to take actions and receive new states, rewards, and 'done' flags.

  iii. Update each agent's Q-network based on their experiences.

  iv. If all agents are done (all 'done' flags are True), exit the loop.

Output:

- Trained MADQN agents.

End

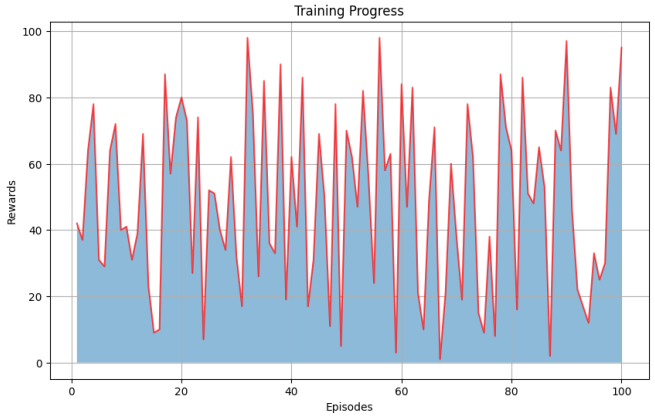

Fig. 7. Multi-Agent Deep Q-Networks (MADQN) episode rewards over time.

Furthermore, the utilization of advanced Long Short-Term Memory (LSTM)-based deep learning architectures [69], integrated with reinforcement learning or attention mechanisms, shows promise in improving accuracy, scalability, and resource allocation for secure 5G network slice orchestration.

g) Other potential solutions: To further improve the performance of secure 5G network slicing, data augmentation and transfer learning techniques can enhance model performance, while optimized resource allocation ensures scalability. Efficient scheduling techniques contribute to enhancing system efficiency within the secure 5G network slicing context. Moreover, potential solutions for improving

the accuracy of automated machine learning models, scalable orchestration frameworks, and efficient utilization of automated processes through optimization are essential considerations. Additionally, addressing the accuracy of adversarial machine learning models, deploying scalable flooding attack detection mechanisms, and efficiently utilizing resources during attack mitigation are crucial aspects to enhance the security and performance of secure 5G network slicing. Overall, employing techniques such as data augmentation, transfer learning, efficient parallelization, optimized resource allocation, and adaptive strategies holds promise for enhancing accuracy, scalability, and resource utilization in the secure 5G network slicing domain.

Fig. 8. Word cloud visualization of potential solutions for secure 5G network slicing

The word cloud depicted in Fig. 8 is a visual representation of potential solutions for enhancing secure 5G network slicing, as discussed in the literature. The above word cloud was generated using python. This visualization method succinctly conveys the key strategies and concepts described in the literature by assigning word sizes based on their frequency of occurrence. Larger and bolder words indicate the prominence and importance of specific terms within the text. Notably, terms such as "security," "reinforcement learning," "slicing frameworks," "resource utilization," and "scalability" are the most prominent in the word cloud. These words represent the primary solutions put forward in the literature for addressing the challenges and limitations related to secure 5G network slicing. The word cloud effectively distills the essence of the text, providing an at-a-glance overview of the critical ideas and strategies to enhance accuracy, scalability, and resource utilization in the secure 5G network slicing domain. Scientists and researchers can quickly grasp the core themes and solutions discussed in the paper, making it a valuable addition to the scientific discourse for understanding complex topics with enhanced clarity.

Q4. What are the future research directions and opportunities in this area?

1) Future directions as discussed in the literature: The papers surveyed in this study present several potential future research directions in the domain of secure 5G network slicing. One promising avenue is the integration of reinforcement learning techniques with convolutional neural networks (CNNs) to address challenges related to accuracy, scalability, and resource utilization. This approach has shown promise in enhancing network slice orchestration, enabling DDoS attack detection, and facilitating simultaneous protection of multiple network slices [44]. Another area of interest is multi-agent reinforcement learning, which can be explored to tackle accuracy, scalability, and resource utilization challenges in secure 5G network slicing. By leveraging intelligent resource allocation and effectively managing complex dependencies, multi-agent reinforcement learning offers the potential for more efficient and effective network slicing [45].

Furthermore, the literature suggests the exploration of distributed and scalable frameworks such as support vector machines (SVM) to address accuracy and scalability challenges in securing network slices and optimizing resource utilization in 5G network slicing [46]. Additionally, advanced deep reinforcement learning techniques, including hierarchical or multi-agent deep Q-networks (DQN), can be applied to improve accuracy, scalability, and resource allocation in context-aware authentication handover for secure 5G network slicing [52][68]. The use of advanced LSTM-based deep learning architectures, coupled with reinforcement learning or attention mechanisms, also holds promise for enhancing accuracy, scalability, and resource allocation in secure 5G network slice orchestration [69].

2) Recommended future directions

a) Ensemble learning techniques: Ensemble learning (stacking or boosting for accuracy and robustness enhancement) involves combining multiple individual models to create a stronger and more accurate predictive model. Stacking and boosting are two common ensemble techniques. Stacking combines the predictions of multiple models using another model, often referred to as a meta-learner. Boosting, on the other hand, assigns more weight to instances that are misclassified by the previous models in the ensemble, thereby focusing on improving the accuracy of these instances. The application of ensemble techniques in secure 5G network slicing aims to enhance prediction accuracy and overall robustness by leveraging the strengths of multiple models.

b) Integration of explainable AI: Explainable AI techniques (for transparency and trust) aim to provide understandable and interpretable explanations for the decisions made by machine learning models. In the context of secure 5G network slicing, incorporating explainable AI methods allows users to understand the rationale behind decisions made by the network slicing system. This transparency enhances trust and accountability, particularly in critical applications where the ability to explain decisions is essential. By enabling stakeholders to comprehend how decisions are reached, explainable AI techniques contribute to increased confidence and acceptance of the system's outcomes.

c) Federated learning: Federated learning (for data privacy and security) is a decentralized machine learning approach that enables model training across multiple devices or nodes while keeping data localized. This approach prioritizes data privacy and security by not requiring data to be

centralized for training. In the context of secure 5G network slicing, federated learning offers a solution to challenges related to sharing sensitive data across different slices. It allows models to be trained collaboratively without sharing raw data, thus ensuring privacy while still improving the performance of network slicing algorithms.

d) Edge computing: Utilization of edge computing and edge intelligence for localized decision-making involves processing data closer to the data source, reducing communication overhead and latency. Incorporating edge intelligence in network slicing enables localized decision-making at the edge nodes, which can lead to quicker responses and efficient resource utilization. By processing data and making decisions closer to where it is generated, edge computing optimizes the performance of network slicing and enhances its responsiveness.

e) Energy efficiency: Energy efficiency through algorithmic development and resource allocation is a critical concern in any network infrastructure. In the context of secure 5G network slicing, developing energy-efficient algorithms and resource allocation strategies is essential to minimize power consumption while maintaining optimal performance. By optimizing the allocation of resources based on workload and demand, energy-efficient network slicing can contribute to reducing operational costs and improving overall sustainability.

f) Generative adversarial networks: Generative Adversarial Networks (GANs) are a type of machine learning model used in tasks such as image generation and data synthesis. In the context of secure 5G network slicing, GANs can be employed to generate realistic adversarial examples that simulate potential attacks on the network slicing algorithms. By testing the robustness of these algorithms against such simulated attacks, GANs can help identify vulnerabilities and weaknesses in the system's security measures, thereby enhancing its overall security posture.

VII. Conclusion

This literature survey presented a comprehensive overview of the research conducted in the domain of secure 5G network slicing. The reviewed papers highlighted the challenges related to accuracy, scalability, and resource utilization in network slicing and proposed various techniques to address these issues. The experimental results show that the integration of reinforcement learning techniques with CNNs, multi-agent reinforcement learning, and distributed SVM frameworks emerged as potential solutions to improve accuracy and scalability in network slicing. Advanced deep reinforcement learning architectures, such as hierarchical or multi-agent DQN, and LSTM-based models with reinforcement learning or attention mechanisms were identified as effective approaches for enhancing accuracy, scalability, and resource allocation in network slice orchestration. Furthermore, data augmentation, transfer learning, efficient parallelization, optimized resource allocation, and adaptive strategies were suggested as methods to improve model performance, scalability, and resource utilization. The surveyed literature also shed light on the importance of securing network slices against cyber threats, with studies exploring the detection and mitigation of DDoS attacks, cooperative attacks, and adversarial machine learning models. Additionally, considerations for privacy, explainability, edge computing, energy efficiency, and the application of emerging techniques like Ensemble Learning, Federated learning, GANs, etc. were highlighted as potential future research directions. By exploring these avenues, this review has laid a foundation for researchers to contribute to the advancement of secure 5G network slicing, addressing the challenges and ensuring the reliability, efficiency, and security of future network infrastructures.

This review explored the significant advancements and challenges in the integration of 5G networks with security, network slicing, and machine learning techniques. The findings reveal that 5G networks offer immense potential for delivering high accuracy, scalability, and efficiency in various applications. Network slicing emerges as a crucial mechanism for resource allocation and management in 5G networks, enabling efficient utilization of network resources for different services. Moreover, machine learning and deep learning algorithms demonstrate promising capabilities in enhancing network performance and security by enabling intelligent decision-making and anomaly detection. However, the integration of these technologies also presents notable challenges, such as ensuring robust security measures, optimizing network slicing algorithms, and addressing scalability issues. Further research and development efforts are required to overcome these challenges and fully exploit the potential of 5G networks with security, network slicing, and machine learning for various domains and applications.

Acknowledgment

This project was funded by Deanship of Scientific Research, Northern Border University for their financial support under grant no. (NR-NBU-2023-12-2125). The authors, therefore, acknowledge with thanks DSR technical and financial support.

References

[1] X. Li et al., “Network slicing for 5G: Challenges and opportunities,” IEEE Internet Computing, pp. 1–1, 2018. doi:10.1109/mic.2018.326150452.

[2] H. Yu, H. Lee, and H. Jeon, “What is 5G? emerging 5G Mobile Services and network requirements,” Sustainability, vol. 9, no. 10, p. 1848, 2017. doi:10.3390/su9101848.

[3] R. Dangi et al., “ML-based 5G network slicing security: A comprehensive survey,” Future Internet, vol. 14, no. 4, p. 116, 2022. doi:10.3390/fi14040116.

[4] T. Chhabra, “5G in India: The journey is about to begin - ET telecom,” ETTelecom.com, https://telecom.economictimes.indiatimes.com/news/5g-in-india-the-journey-is-about-to-begin/81671088 (accessed Feb. 12, 2023).

[5] T. GreyB, “5G companies: 12 players are leading the research,” GreyB, https://www.greyb.com/blog/5g-companies/ (accessed Feb. 9, 2023).

[6] G. Narcisi, “These are the 5G trends to watch in 2021,” CRN, https://www.crn.com/news/networking/these-are-the-5g-trends-to-watch-in-2021 (accessed Feb. 10, 2023).

[7] “What is 5g: Everything you need to know About 5G: 5G FAQ: Qualcomm,” Wireless Technology & Innovation, https://www.qualcomm.com/5g/what-is-5g# (accessed Feb. 9, 2023).

[8] N. Brittain, "18 5G projects providing a vision for the future," 5Gradar, https://www.5gradar.com/features/5g-projects-that-will-blow-your-mind (accessed Feb. 14, 2023).

[9] H. Zhang et al., "Network slicing based 5G and future mobile networks: Mobility, Resource Management, and challenges," IEEE Communications Magazine, vol. 55, no. 8, pp. 138–145, 2017. doi:10.1109/mcom.2017.1600940.

[10] C. Campolo, A. Molinaro, A. Iera, and F. Menichella, "5G network slicing for vehicle-to-everything services," IEEE Wireless Communications, vol. 24, no. 6, pp. 38–45, 2017. doi:10.1109/mwc.2017.1600408.

[11] G. Werélius, What we know: A look at current 5G market trends - ericsson, https://www.ericsson.com/en/blog/2020/10/what-we-know-a-look-at-current-5g-market-trends (accessed Feb. 9, 2023).

[12] R. F. Olimid and G. Nencioni, "5G network slicing: A security overview," IEEE Access, vol. 8, pp. 99999–100009, 2020. doi:10.1109/access.2020.2997702.

[13] F. Salahdine, Q. Liu, and T. Han, "Towards secure and intelligent network slicing for 5G networks," IEEE Open Journal of the Computer Society, vol. 3, pp. 23–38, 2022. doi:10.1109/ojcs.2022.3161933.

[14] E. P. Neto, F. S. Silva, L. M. Schneider, A. V. Neto, and R. Immich, "Seamless Mano of multi-vendor SDN controllers architectures and future challenges," Comput. Netw., vol. 167, no. 106984, p. 106984, 2020.

[15] S. Chaabnia and A. Meddeb, "Slicing aware QoS/QoE in Software Defined Smart Home Network," NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium, 2018. doi:10.1109/noms.2018.8406195.

[16] P. K. Chartsias et al., "SDN/NFV-based end to end network slicing for 5G multi-tenant networks," in 2017 European Conference on Networks and Communications (EuCNC), 2017.

[17] C. Bektas, S. Monhof, F. Kurtz, and C. Wietfeld, "Towards 5G: An empirical evaluation of software-defined end-to-end network slicing," in 2018 IEEE Globecom Workshops (GC Wkshps), 2018.

[18] A. A. Barakabitze, A. Ahmad, R. Mijumbi, and A. Hines, "5G network slicing using SDN and NFV: A survey of taxonomy, domains," IEEE Access, vol. 8, pp. 29525–29537, 2020.

[19] X. Li, R. Ni, J. Chen, Y. Lyu, Z. Rong, and R. Du, "End-to-end network slicing in radio access network, transport network and core networkacross Federated Multi-domains," Computer Networks, vol. 186, p. 107752, 2021. doi:10.1016/j.comnet.2020.107752.

[20] S. D'Oro, F. Restuccia, A. Talamonti, and T. Melodia, "The slice is served: Enforcing radio access network slicing in virtualized 5G systems," in IEEE INFOCOM 2019 - IEEE Conference on Computer Communications, 2019.

[21] A. Kaloxylos, "A survey and an analysis of network slicing in 5G networks," IEEE Commun. Stand. Mag., vol. 2, no. 1, pp. 60–65, 2018.

[22] F. Salahdine and N. Kaabouch, "Security threats, detection, and countermeasures for physical layer in cognitive radio networks: A survey," Phys. Commun., vol. 39, no. 101001, p. 101001, 2020.

[23] M. A. Habibi, B. Han, and H. D. Schotten, "Network slicing in 5G mobile communication architecture, profit modeling, and challenges," arXiv [cs.NI], 2017.

[24] N. Alliance, "5G security recommendations package# 2: Network slicing," NGMN, pp. 1–12, 2016.

[25] S. Sharma et al., "Secure authentication protocol for 5G enabled IoT network," in 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC), 2018.

[26] N. Alliance, "Description of network slicing concept," NGMN 5G P, vol. 1, no. 1, pp. 1–11, 2016.

[27] V. A. Cunha et al., "Network slicing security: Challenges and directions," Internet Technol. Lett., vol. 2, no. 5, p. e125, 2019.

[28] Z. Kotulski et al., "Towards constructive approach to end-to-end slice isolation in 5G networks," EURASIP J. Inf. Secur., vol. 2018, no. 1, 2018.

[29] X. Foukas, G. Patounas, A. Elmokashfi, and M. K. Marina, "Network slicing in 5G: Survey and challenges," IEEE Commun. Mag., vol. 55, no. 5, pp. 94–100, 2017.

[30] GROUP SPECIFICATION, "ETSI GS NFV-SEC 001 V1.1.1 (2014-10)," Etsi.org. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/nfv-sec/001_099/001/01.01.01_60/gs_nfv-sec001v010101p.pdf. [Accessed: 10-April-2023].

[31] A. Mathew, "Network slicing in 5G and the security concerns," in 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), 2020.

[32] Z. Kotulski et al., "On end-to-end approach for slice isolation in 5G networks. Fundamental challenges," in Proceedings of the 2017 Federated Conference on Computer Science and Information Systems, 2017.

[33] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing and softwarization: A survey on principles, enabling technologies, and solutions," IEEE Commun. Surv. Tutor., vol. 20, no. 3, pp. 2429–2453, 2018.

[34] F. Reynaud et al., "Attacks against network functions virtualization and software-defined networking: state-of-the-art," in Proceedings of Workshop on Security in Virtualized Networks, Sec-Virtnet, 2016.

[35] V. N. Sathi, M. Srinivasan, P. K. Thiruvasagam, and S. R. M. Chebiyyam, "A novel protocol for securing network slice component association and slice isolation in 5G networks," in Proceedings of the 21st ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, 2018.

[36] "Security aspects of network capabilities exposure in 5G," in Final deliverable (approved-P Public), 2018.

[37] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions," IEEE Commun. Surv. Tutor., vol. 22, no. 1, pp. 196–248, 2020.

[38] S. Zhou, L. Wu, and C. Jin, "A privacy-based SLA violation detection model for the security of cloud computing," China Commun., vol. 14, no. 9, pp. 155–165, 2017.

[39] S. Y.-T. Fan C-I, "Cross-network-slice authentication scheme for the 5th generation mobile communication system," IEEE Transactions on Network and Service Management, 2021.

[40] "Security," 5G Second Phase Explained, pp. 235–258, 2021. doi:10.1002/9781119645566.ch7.

[41] S. Bao, Y. Liang, and H. Xu, "Blockchain for network slicing in 5G and beyond: Survey and challenges," J. Commun. Inf. Netw., vol. 7, no. 4, pp. 349–359, 2022.

[42] S. K. Boell and D. Cecez-Kecmanovic, ''On being 'systematic' in literature reviews,'' in Formulating Research Methods for Information Systems. London, U.K.: Palgrave Macmillan, 2015, pp. 48–78.

[43] M. D. J. Peters, C. M. Godfrey, H. Khalil, P. McInerney, D. Parker, and C. B. Soares, ''Guidance for conducting systematic scoping reviews,'' Int. J. Evidence-Based Healthcare, vol. 13, no. 3, pp. 141–146, Sep. 2015.

[44] W. Jiang, S. D. Anton, and H. Dieter Schotten, "Intelligence slicing: A unified framework to integrate artificial intelligence into 5G networks," in 2019 12th IFIP Wireless and Mobile Networking Conference (WMNC), 2019.

[45] A. Thantharate, R. Paropkari, V. Walunj, and C. Beard, "DeepSlice: A deep learning approach towards an efficient and reliable network slicing in 5G networks," in 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2019.

[46] Q. Liu, T. Han, and N. Ansari, "Learning-assisted secure end-to-end network slicing for cyber-physical systems," IEEE Netw., vol. 34, no. 3, pp. 37–43, 2020.

[47] H. Sedjelmaci, "Cooperative attacks detection based on artificial intelligence system for 5G networks," Comput. Electr. Eng., vol. 91, no. 107045, p. 107045, 2021.

[48] V. P. Kafle, Y. Fukushima, P. Martinez-Julia, and T. Miyazawa, "Consideration on automation of 5G network slicing with machine learning," in 2018 ITU Kaleidoscope: Machine Learning for a 5G Future (ITU K), 2018.

[49] A. Thantharate, R. Paropkari, V. Walunj, C. Beard, and P. Kankariya, "Secure5G: A deep learning framework towards a secure network

slicing in 5G and beyond," in 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), 2020.

[50] How to attack and defend 5G radio access network slicing with reinforcement learning. arXiv 2021.

[51] N. A. E. Kuadey, G. T. Maale, T. Kwantwi, G. Sun, and G. Liu, "DeepSecure: Detection of distributed denial of service attacks on 5G network slicing—deep learning approach," IEEE Wirel. Commun. Lett., vol. 11, no. 3, pp. 488–492, 2022.

[52] Highly accurate and reliable wireless network slicing in 5th generation networks: a hybrid deep learning approach, Journal of Network and Systems Management: Springer, 2022.

[53] Y. Shi and Y. E. Sagduyu, "Adversarial machine learning for flooding attacks on 5G radio access network slicing," in 2021 IEEE International Conference on Communications Workshops (ICC Workshops), 2021.

[54] C. Benzaid, T. Taleb, and J. Song, "AI-based autonomic and scalable security management architecture for secure network slicing in B5G," IEEE Netw., vol. 36, no. 6, pp. 165–174, 2022.

[55] S. Yoon et al., "Moving target defense for in-vehicle software-defined networking: IP shuffling in network slicing with multiagent deep reinforcement learning," in Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications II, 2020.

[56] X. Cheng, Y. Wu, G. Min, A. Y. Zomaya, and X. Fang, "Safeguard network slicing in 5G: A learning augmented optimization approach," IEEE J. Sel. Areas Commun., vol. 38, no. 7, pp. 1600–1613, 2020.

[57] I. H. Abdulqadder and S. Zhou, "SliceBlock: Context-aware authentication handover and secure network slicing using DAG-blockchain in edge-assisted SDN/NFV-6G environment," IEEE Internet Things J., vol. 9, no. 18, pp. 18079–18097, 2022.

[58] E. Bandara, X. Liang, S. Shetty, R. Mukkamala, A. Rahman, and N. W. Keong, "Skunk-A Blockchain and Zero Trust Security Enabled Federated Learning Platform for 5G/6G Network Slicing," in 2022 19th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), IEEE, 2022, pp. 109–117.

[59] S. Wijethilaka and M. Liyanage, "A federated learning approach for improving security in network slicing," in GLOBECOM 2022 - 2022 IEEE Global Communications Conference, 2022.

[60] Y. Shi, Y. E. Sagduyu, T. Erpek, and M. C. Gursoy, "How to attack and defend NextG radio access network slicing with reinforcement learning," IEEE Open J. Veh. Technol., vol. 4, pp. 181–192, 2023.

[61] D. Chowdhury, R. Das, R. Rana, A. D. Dwivedi, P. Chatterjee, and R. R. Mukkamala, "AUTODEEPSLICE: A Data Driven Network Slicing Technique of 5G network using Automatic Deep Learning," in 2022 IEEE Globecom Workshops (GC Wkshps), 2022.

[62] J. Wang and J. Liu, "Secure and reliable slicing in 5G and beyond vehicular networks," IEEE Wirel. Commun., vol. 29, no. 1, pp. 126–133, 2022.

[63] L. Tang, Q. Tan, Y. Shi, C. Wang, and Q. Chen, "Adaptive virtual resource allocation in 5G network slicing using constrained Markov decision process," IEEE Access, vol. 6, pp. 61184–61195, 2018.

[64] V. Sciancalepore, X. Costa-Perez, and A. Banchs, "RL-NSB: Reinforcement learning-based 5G network slice broker," IEEE ACM Trans. Netw., vol. 27, no. 4, pp. 1543–1557, 2019.

[65] G. Zhou, L. Zhao, G. Zheng, Z. Xie, S. Song, and K. C. Chen, "Joint Multi-objective Optimization for Radio Access Network Slicing Using Multi-agent Deep Reinforcement Learning," IEEE Transactions on Vehicular Technology, 2023.

[66] Y. Kim and H. Lim, "Multi-agent reinforcement learning-based resource management for end-to-end network slicing," IEEE Access, vol. 9, pp. 56178–56190, 2021.

[67] O. A. Latif, M. Amer, and A. Kwasinski, "Classification of network slicing requests using support vector machine," in 2022 International Conference on Electrical and Computing Technologies and Applications (ICECTA), 2022.

[68] P. Tam, S. Math, A. Lee, and S. Kim, "Multi-agent deep Q-networks for efficient edge federated learning communications in software-defined IoT," Comput. Mater. Contin., vol. 71, no. 2, pp. 3319–3335, 2022.

[69] R. Li, C. Wang, Z. Zhao, R. Guo, and H. Zhang, "The LSTM-based advantage actor-critic learning for resource management in network slicing with user mobility," IEEE Commun. Lett., vol. 24, no. 9, pp. 2005–2009, 2020.