IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 21 June 2023, accepted 16 August 2023, date of publication 18 August 2023, date of current version 25 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3306534

SURVEY

Resource Allocation in Networking and Computing Systems: A Security and Dependability Perspective

MD MUHIDUL I. KHAN AND GIANFRANCO NENCIONI
Department of Electrical Engineering and Computer Science, University of Stavanger, 4021 Stavanger, Norway

Corresponding author: Md Muhidul I. Khan (md.m.khan@uis.no)

This work was supported by the Norwegian Research Council through the 5G-MODaNeI Project under Grant 308909.

ABSTRACT In recent years, there has been a trend to integrate networking and computing systems, whose management is getting increasingly complex. Resource allocation is one of the crucial aspects of managing such systems and is affected by this increased complexity. Resource allocation strategies aim to effectively maximize performance, system utilization, and profit by considering virtualization technologies, heterogeneous resources, context awareness, and other features. In such complex scenario, security and dependability are vital concerns that need to be considered in future computing and networking systems in order to provide the future advanced services, such as mission-critical applications. This paper provides a comprehensive survey of existing literature that considers security and dependability for resource allocation in computing and networking systems. The current research works are categorized by considering the allocated type of resources for different technologies, scenarios, issues, attributes, and solutions. The paper presents the research works on resource allocation that includes security and dependability, both singularly and jointly. The future research directions on resource allocation are also discussed. The paper shows how there are only a few works that, even singularly, consider security and dependability in resource allocation in the future computing and networking systems and highlights the importance of jointly considering security and dependability and the need for intelligent, adaptive and robust solutions. This paper aims to help the researchers effectively consider security and dependability in future networking and computing systems.

INDEX TERMS Resource allocation, dependability, security, computing, networking.

I. INTRODUCTION

Computing and networking systems are two important components of technology infrastructure. Computing system composed of a wide range of hardware and software components. These system also consists of resources, e.g., processing units, memory, storage, input/output devices. These resources help to execute any program, run any application and also used for managing data. Network systems enable data exchange and communication between computing devices, allowing users to share resources and access information across a network. Networking technologies and standards provide connectivity for businesses, organizations, and individuals, allowing to collaborate, share information, and access online services and resources [1].

The resource allocation in networking and computing systems is getting more and more challenging. The systems are getting more and mote complex. The virtualization paradigms have increased the flexibility of the systems leading to new potentials in the management and orchestration [2]. The new systems integrate heterogeneous networking and computing resources, which can be jointly allocated to provide new advanced services. Moving computing capabilities to the edge of the network allows increased performance and context awareness. To exploit this potential and cope with the complexity, a pervasive ubiquitous intelligence will be considered in the future networking and computing systems.

The associate editor coordinating the review of this manuscript and approving it for publication was Zesong Fei.

Computing and networking systems have changed widely the way the people interact with technology and each other. These systems help a lot for providing services, e.g., cloud computing and cellular communication. Furthermore, these play a crucial role for the economic growth and social development worldwide.

The integration of networking and computing systems covers all the latest technologies associated with computation, communication, and networking among connected devices. The motivation for considering resource allocation in networking and computing systems is essential for the future connectivity of the billions of devices. The motivation for resource allocation in computing and networking systems is driven by the need for optimal resource utilization, performance optimization, Quality of Service (QoS) assurance, scalability, load balancing, prioritization, service differentiation, and cost optimization. Effective resource allocation enhances system efficiency, responsiveness, reliability, and cost-effectiveness, improving overall system performance and user satisfaction [3]. For example, the joint allocation of networking and computing resources is of utmost importance in the Fifth Generation (5G) of mobile networks, which has as enabling technologies the Multi-Access Edge Computing (MEC) and will also be for the Sixth Generation (6G).

The resource allocation challenges include workload balancing, latency optimization, performance guarantees, dynamic resource provisioning, and ensuring fairness and isolation in complex integrated networking and computing systems. Effective resource allocation strategies and mechanisms are crucial for achieving efficient utilization, meeting diverse application requirements, and delivering reliable, high-performance services in such environments [4]. For example, MEC resource allocation in 5G-and-beyond networks presents several challenges and complexities. Network heterogeneity, scalability, QoS requirements, mobility support, and security considerations are among the key challenges that must be addressed by developing resource allocation algorithms and techniques that tackle these challenges [5].

Economic costs, performance, and resource consumption are the key to considering resource allocation. However, in this revolutionary era of computation and communication, security is quite a concern for resource allocation. Security may arise for the allocation of resources by so many issues, e.g., data breaches, Distributed Denial of Services (DDoS), side-channel attacks, eavesdropping, and faulty/malicious/noisy/compromised nodes. The system should adapt to these attacks and run successfully to allocate resources.

A more complex and intelligent system can help to a decrease of common failures that have minor consequences, but can lead to an increment of critical failures with severe consequences [6]. For this reason, the dependability, which includes more common aspects such as reliability and availability, is another important concern for the networking and computing systems.

The importance of considering security and dependability in resource allocation should be better investigated. For example, a particular task that needs to be allocated can have different security requirements, and the resource providers have different security guarantees. A general good practice is to add a threshold for resource consumption and guarantee some resources for different security functionalities [7]. Otherwise, by compromising the providers, an adversary can use excessive resources and thus affect the performance. In addition, the provider's resources can be compromised by failures caused by faults in the components, therefore dependability should also be considered.

However, computing and networking systems also pose significant challenges in terms of security, privacy, and accessibility. As the complexity and diversity of these systems continue to grow, it becomes increasingly important to design and implement solutions that ensure their reliability, efficiency, and sustainability while safeguarding users' rights and interests.

Resource allocation is a critical component of network design that can significantly impact the security and dependability of a network. In this context, resources can refer to network bandwidth, computational power, memory, storage space, and other similar resources required for a network's proper functioning [8]. In general, there are two primary ways in which resource allocation is related to security and dependability:

- Resource allocation can affect the ability of a network to prevent or mitigate security threats. For example, if a network has limited computational power, it may be unable to perform the necessary encryption and decryption tasks to protect data from eavesdropping or interception [9]. Similarly, suppose a network has insufficient bandwidth. In that case, it may be unable to detect and block distributed denial of service (DDoS) attacks, which can cripple the network and make it unavailable to users. Thus, resource allocation decisions need to be made to ensure that the network has the resources it needs to maintain its security.
- Resource allocation can affect the ability of a network to remain dependable in the face of failures. For example, in a distributed system, resource allocation decisions need to be made to ensure that no single point of failure can bring down the entire system [10]. This means that resources must be allocated in a way that allows the system to continue operating even if some of its components fail. Similarly, resource allocation decisions need to be made to ensure that the network has the resources it needs to detect and recover from failures, such as through redundancy or failover mechanisms.

The main contribution of this survey is to explore how security and dependability can be considered in the resource allocation for various applications/technologies of computing and networking systems. We explore the issues and the attributes of security and dependability that are considered for resource allocation. Furthermore, we also consider the type of allocated resources, e.g., computation, data rate, and radio resources, and the overall scenario of the system model, e.g., distributed, centralized, and clustered, which has an impact on security and dependability. Moreover, we categorize the solutions for security and dependability considerations.

To our best knowledge, there are no surveys that explore security and dependability for resource allocation in general networking and computing systems. This paper will highlight the impact of security, dependability, and joint security and dependability for resource allocation. The final target of the paper is to help the researchers to effectively consider security and dependability in the future networking and computing systems.

The contributions of this survey paper can be summarized as follows:

- Exploration of how security and dependability is considered in current research works on resource allocation for various applications in networking and computing systems.
    - To this purpose, the research works have been classified into the allocated type of resources for different technologies, scenarios (e.g., distributed, centralized), issues, attributes, and solutions.
    - In the perspective of a problem formulation, we also indicate if the issues and the attributes can be expressed as an objective or as a constraint.
- Discussion of the impact of joint security and dependability on resource allocation in future networking and computing systems by highlighting the possible future research directions.

The rest of the paper is organized as follows. Section II introduces the background on security and dependability and the related works. Section III presents the state-of-the-art resource allocation strategies by considering security and dependability, singularly and jointly. Moreover, Section IV discusses the future research directions. Finally, a conclusion highlights the main findings of this survey. Figure 1 depicts the diagrammatic view of the organization of the paper.

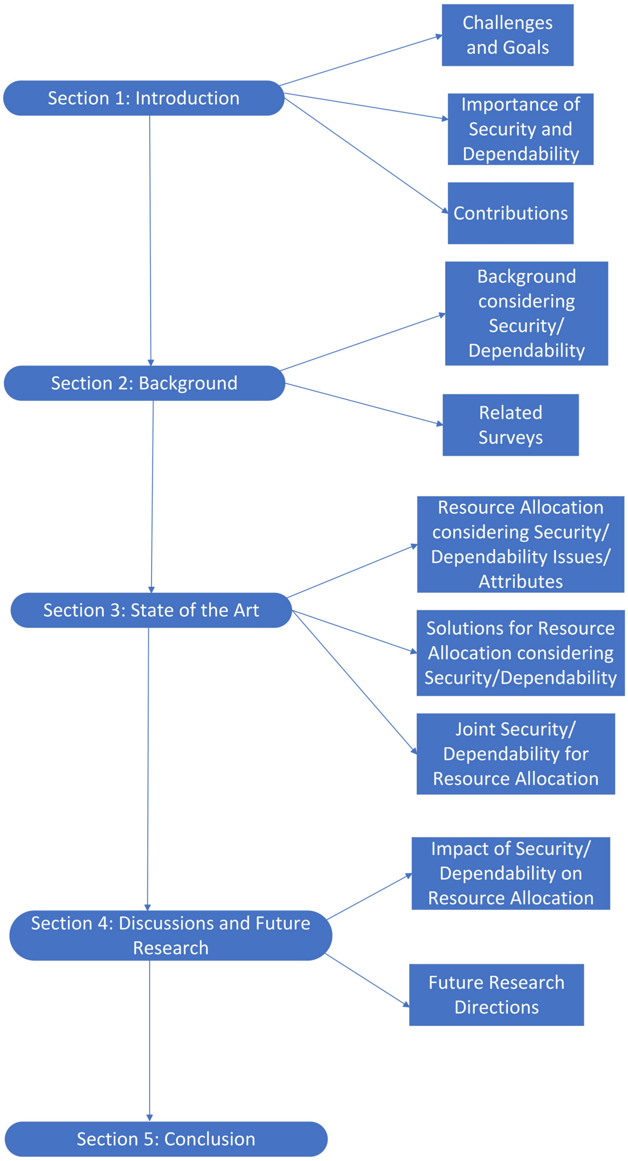
Section 1: Introduction
Challenges and Goals
Importance of Security and Dependability
Contributions
Section 2: Background
Background considering Security/ Dependability
Related Surveys
Section 3: State of the Art
Resource Allocation considering Security/ Dependability Issues/ Attributes
Solutions for Resource Allocation considering Security/Dependability
Joint Security/ Dependability for Resource Allocation
Section 4: Discussions and Future Research
Impact of Security/ Dependability on Resource Allocation
Future Research Directions
Section 5: Conclusion

FIGURE 1. Diagrammatic View of the Organization.

II. BACKGROUND

Security in resource allocation involves protecting resources and data from unauthorized access and ensuring confidentiality, integrity, and availability. Dependability focuses on the unwanted failures caused by the nature of the components that compose a system. These concepts are essential for building a robust and secure resource allocation system in different domains and applications [11].

The first step in resource allocation is understanding the available and required resources. Available resources refer to the capacity of system elements, while required resources are needed to run a service. The resource allocation problem involves deciding how much resources should be dedicated to meeting specific demands. Available resources include all the system's elements' storage and computing power capacity. Sufficient available resources are necessary to store and execute service demands. The capacity available can impact performance, such as computing power capacity affecting task execution delay and storage capacity involving queuing delay. Overall, two types of resources need to be provided in the system: data resources (computing, memory, and storage capacity) and network resources (data rate and spectrum bandwidth) [5].

The metrics for evaluating resource allocation strategies can vary depending on the system or application context [12]. The selection of metrics should align with the goals and requirements of the specific system and consider the desired outcomes, such as performance optimization, efficient resource utilization, or profitability.

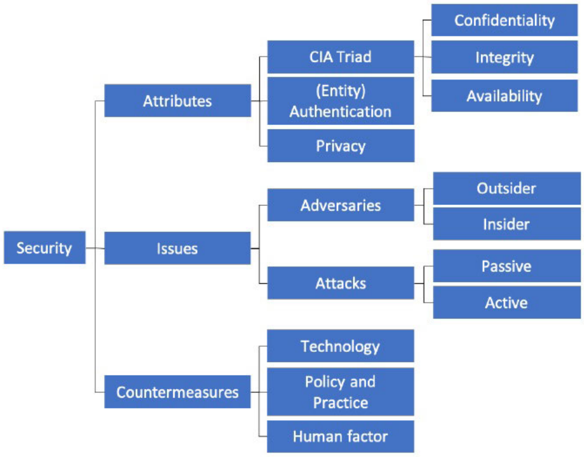

FIGURE 2. Security Taxonomy [13].

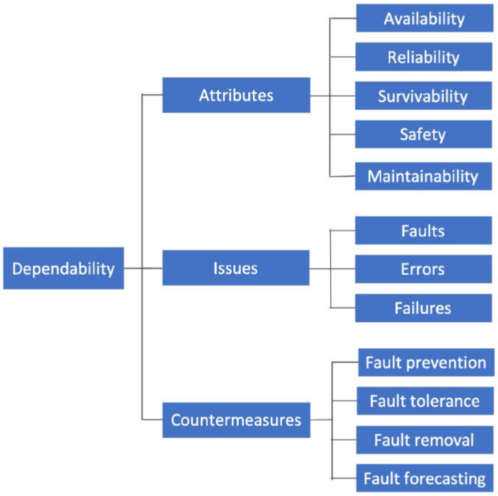

FIGURE 3. Dependability Taxonomy [13].

A. SECURITY

Security is a concern for resource allocation in every networking and computing application for preventing the communication and computation from being compromised by adversaries. A secure system will, for example, allocate resources from an authenticated infrastructure to the clients/devices. Figure 2 shows the taxonomy of security overall. The security attributes cover the CIA (Confidentiality, Integrity, and Availability) triad, authenticity, and privacy. Security issues can arise from adversaries (outsider and insider) and attacks (active and passive). Innovation of technologies, applying the policies and practices, and human factors can be countermeasures to the security issues. The attributes are the ways to evaluate security and dependability. The issues are the causes that may lead to the lack of security and dependability. The countermeasures are a way of enhancing the security and dependability of the system.

B. DEPENDABILITY

Between the "security" and "dependability," dependability is the less known term. Dependability consists mainly of availability and reliability. In addition, safety, survivability, and maintainability are dependability attributes. These attributes can be defined as follows:

- Availability: Readiness for the correct behavior from the system
- Reliability: Continuity of correct service
- Safety: Absence of catastrophic consequences in the system
- Integrity: Absence of system alterations
- Maintainability: Ability to undergo modifications and repairs

Dependability of a system is the ability to avoid service failures that are more frequent and more severe than is acceptable [14]. System A is dependent on system B when system A's performance is affected by system B. This dependence leads to the term trust. When there is trust, the dependence can be accepted. Figure 3 depicts the attributes, issues, and countermeasures for dependability.

C. RELATED WORKS

Existing surveys are focused on resource allocation for various applications considering security and privacy, whereas our work is very much focused on security and dependability perspectives for resource allocation in computing and networking based applications. In [15], the authors do a survey for security vulnerabilities, privacy issues and countermeasures in 5G-Multi Access Edge Computing (MEC) systems. They identify some security vulnerabilities, e.g., intrusion-based, intervention, Denial of Service (DoS), or Distributed DoS (DDoS) attacks, which are capable of ceasing ME Apps launched in the edge from accessing the relevant infrastructure services and also they study different privacy issues happened for this. They explore novel security solutions that are proposed for cyber-physical systems, advanced cryptographic algorithms, Federated Learning (FL) for proving privacy, Blockchain based technologies. In [16], the authors survey the security and privacy issues for device discoveries in next-generation networks. Device-to-Device (D2D) communication is one of the critical enabling technologies for future communication networks. Device discovery is a challenging aspect of D2D communication. Devices send signals for discovering the other devices in neighbors to communicate. However, these signals can be cracked by Denial of Service (DoS) attacks, camouflaging, session stealing, IP hoaxing, eavesdropping, jamming, location hoaxing, man-in-the-middle attack, imposture, bandwidth hoaxing, inference attacks, malware attacks, trust manipulation attacks, free-riding attacks. These types of attacks make the system vulnerable to privacy. They mention different kinds of solutions for security and privacy-aware resource allocation.

Some survey papers focus on different parameters for resource allocation. In [17], the authors perform a comprehensive survey for resource allocation in cloud computing environments. They consider different parameters, e.g., Quality of Service (QoS), resource failure, resource mapping, resource prediction, resource pricing, resource provisioning, resource scheduling, Virtual Machine (VM) migration placement, and workload balancing for classifying existing works for the survey. In [18], the authors survey the dynamic aspect of resource allocation in the cloud, thereby improving its importance. This paper studies the aspects of Dynamic Resource Allocation (DRA) in cloud computing environments. This paper develops two research questions to address the issues of DRA in cloud computing. The research questions are: "How are the current circumstances of the cloud computing environment regarding resource allocation?" and "How does each search deal with the DRA aspect (approaches, dynamic aspect, scheduling, and optimization metrics)?". In [19], the authors survey scalable resource allocation methodologies in cloud computing. The cloud provides software and hardware as resources via the internet to the remote servers. They consider scalability with the factors of energy, cost, and time for their survey. In [20], the authors perform the survey based on Software-Defined Networking (SDN) for resource allocation in cloud computing. The inclusion of SDN is helpful for the cloud for better management and to perform cloud computing. They evaluate and categorize existing works based on the measured parameters and the problems presented. All these works do not consider security and dependability, but other specific parameters, and focus only on cloud computing.

In [21], the authors survey the radio resource allocation in the Vehicle-to-Everything (V2X) communication. They consider reliability and latency requirements. Long-Term Evolution (LTE) is a crucial technology for V2X communication. In D2D communications, the devices share the same resources as cellular devices. Reliability is defined in terms of outage probability. They consider the dependability of the system. However, they do not consider the security issues in their survey. This paper has various novelties with respect to the previous works. It is not focusing on a specific networking or computing system, but consider, a briefly introduce, many networking and computing technologies. This works not only surveys security and dependability in resource allocation singularly, but also jointly, and it discuss the future research direction.

III. STATE OF THE ART

In this section, the state of the art is presented. We first present the works on resource allocation that consider security, then the ones that consider dependability, and at the end the ones that jointly consider both security and dependability. We consider the classification of resource allocation considering security and dependability based on allocated resources, technologies, scenarios, issues/attributes, considerations and solutions. The choice of scenarios (distributed, centralized, or clustered) is crucial for resource allocation because it directly impacts security and dependability. Each model has distinct implications for these factors. Distributed systems offer enhanced dependability through redundancy but require robust security measures to address vulnerabilities. For example, centralized systems provide better control over security but can become a single point of failure. Clustered systems enable load balancing and fault tolerance, improving dependability, but demand secure communication and coordination between nodes. Choosing the suitable scenario ensures efficient resource allocation while addressing security and dependability concerns [22].

A. SECURITY

We explore the resource allocation for communication and computing technologies considering the security issues and attributes. Security issues are caused by adversaries that mount attacks. For the resource allocation, security issues can be taken into account as the objective function to optimize or as a constraint. Furthermore, we explore the resource allocation methods/solutions considering the security issues and attributes.

Here for each security issue and attribute, we provide some state of the art of research and consider different computing and networking applications, e.g., 5G, IoT, D2D communications, etc.

1) RESOURCE ALLOCATION CONSIDERING SECURITY ISSUES

a: DATA BREACH

The data breach is crucial for security in resource allocation as a breach can expose a lot of information during allocation. A data breach may happen if the system model is poor and vulnerable in design [23]. The lack of a security model can also be a reason for data breaching. Proper encryption techniques and dynamic methods with security as constraints will be helpful as a countermeasure for the data breach.

Internet of Things (IoT) deals with massive amounts of data and performs the processing. Devices need to complete the processing either locally or send it to the server for better processing. Mobile Cloud Computing (MCC) is one of the technologies used for faster processing. Low communication latency, security enhancement, and efficient bandwidth utilization shift from MCC to Multi-access Edge Computing (MEC). Data offloading is a challenging aspect considering the security and efficient utilization of the bandwidth. It is also important to decrease energy consumption and minimize the delay. In [24], the authors propose a deep Reinforcement Learning (RL) for resource allocation in a way that the resource is adequately utilized and also security is maintained as an additional layer or constraint for data offloading. For dimensional issues, they apply deep RL to optimize the resources. In deep RL, they use the variant of Q-deep RL. For that, the authors consider states, actions, and rewards in a multi-agent-based distributed system. The states are defined as a computation offloading decision. In addition, actions are considered for shifting from one state to another based on the probability distribution. And the reward is represented as a scalar value. Additionally, they propose Advanced Encryption Standard (AES), a symmetric encryption standard, as a security layer to guarantee data breaches during offloading. After adding the security layer, they also apply deep RL for data offloading. The extra security layer provides communication overhead in the system. They investigate their method with the addition of a cryptographic solution. Their proposed method outperforms other variants of RL in terms of performance gain.

A modern mobile communications network is composed of different cell types and access technologies, known as Heterogeneous Networks (HetNets). In the fifth generation (5G) of mobile network, HetNets are designed to achieve customized service demand for data rates. As HetNets allow different networks and support different protocols, it is important and difficult to manage the heterogeneous network resources simultaneously. Virtualization technologies, e.g., network virtualization and network function virtualization, enable the 5G HetNets, aiming to schedule the physical resources efficiently and flexibly. Security is a concern due to the complexity of virtualization. Information leakage/data breach is one of the key issues for significant vulnerabilities. In [25], the authors propose a novel approach to ensure security-aware resource allocation in 5G HetNets (heterogeneous networks) by leveraging reinforcement learning. The authors highlight the need for effective security measures in 5G networks due to the vast number of connected devices and the diverse range of applications, which poses challenges for traditional security mechanisms. To address this challenge, the paper proposes a framework that uses a reinforcement learning algorithm to allocate virtual resources in 5G HetNets. The proposed algorithm incorporates security awareness as a critical factor in resource allocation decisions. Specifically, the algorithm considers security metrics such as confidentiality, integrity, and availability to guide resource allocation decisions to optimize network performance while minimizing security risks. The paper evaluates the proposed framework through simulations. The results demonstrate that the security-aware resource allocation algorithm outperforms traditional resource allocation algorithms regarding network performance and security. The authors conclude that the proposed framework can provide a practical approach to secure resource allocation in 5G HetNets and contribute to developing more secure and resilient 5G networks.

The arrival of the 5G technology standard for broadband cellular networks and Beyond 5G (B5G) networks raises the speed and robustness ceiling of communicating networks and thereby empowers the rapid popularization of edge computing. Consequently, B5G-Driven edge computing allows a growing volume of data to be collected from and transmitted among pervasive edge devices for big data analytics. The collected big data becomes the driving force of Artificial Intelligence (AI) by training high-quality Machine Learning (ML) models, which is followed by severe individual privacy leakage. In [26], Federated Learning (FL) is proposed to achieve privacy-preserving machine learning by avoiding the exchange of raw data. Centralized processing costs significant communication resources between cloud and edge while data falsification problems persist. In addition, the private data may be reconstructed by malicious participants by exploiting the context of model parameters in FL. To solve the identified problems, the authors propose to integrate blockchain-enabled FL with Wasserstein Generative Adversarial Network (WGAN) enabled Differential Privacy (DP) to protect the model parameters of edge devices in B5G networks. The WGAN is an extension to the generative adversarial network that both improves the stability when training the model and provides a loss function [27]. Blockchain enables decentralized FL to reduce communication costs between cloud and edge while alleviating the data falsification issues, and it also provides an incentive mechanism to alleviate the data island issue in B5G-Driven edge computing. WGAN is used to generate controllable random noise complying with DP requirements, which is then injected to model parameters. WGAN-enabled DP is able to achieve an optimized trade-off between differential privacy protection and improved data utility of model parameters. Time delay analysis is conducted to show the efficiency of the proposed model. Extensive evaluation results from simulations demonstrate superior performance in convergence efficiency, accuracy, and data utility.

b: DDoS ATTACK

Network slicing and resource allocation play an important role in SDN/Network Function Virtualization (NFV)-assisted 5G networks. High data rates and low latency are the pivotal components of the increased traffic rate requirements in various applications in 5G. Distributed Denial-of-Service (DDoS) attackers can exploit the sliced network in network slicing. In [28], the authors propose a novel approach for resource allocation in 5G networks to mitigate the impact of DDoS attacks. The authors highlight the vulnerability of 5G networks to DDoS attacks, which can lead to network congestion, packet drops, and service disruption. To address this challenge, the paper proposes the Traffic-aware Scheduling for Secure Slicing and Resource Allocation (T-S3RA) algorithm, which is designed to allocate network resources in a way that optimizes network performance while minimizing the impact of DDoS attacks. The proposed algorithm is based on the principles of Software Defined Networking (SDN) and Network Function Virtualization (NFV) and uses a two-stage approach to allocate network resources. The first stage involves traffic-aware slicing, where the network is partitioned into multiple virtual networks (slices) based on the traffic patterns. The second stage involves resource allocation, where the resources are allocated to the different slices based on the current network conditions and the security level of each slice. the T-S3RA algorithm provides a promising approach to secure resource allocation in 5G networks, especially in the context of DDoS attacks. It can help to improve network performance and ensure a high level of security and resilience in 5G networks.

In [29], the authors propose a secure workflow scheduling approach for performance optimization in Software-Defined Networking (SDN) based Internet of Things (IoT)-Fog networks. The proposed approach allocates resources efficiently while considering the network's security against DDoS attacks. The approach is designed to address resource allocation challenges in SDN-based IoT-Fog networks, which face high resource utilization and security issues. The proposed approach uses a Secure Fog Scheduler (S-FoS) algorithm, which schedules the workflows based on their criticality and resource requirements. The S-FoS algorithm considers the resource constraints of the Fog nodes and the bandwidth availability of the links while ensuring the network's security. To mitigate the impact of DDoS attacks on the network, the proposed approach uses a DDoS detection and mitigation module, which monitors the network traffic and identifies any abnormal traffic patterns. The module then uses a network function virtualization (NFV) based approach to dynamically redirect the traffic to a DDoS scrubbing center for analysis and filtering. The proposed approach of S-FoS provides an efficient and secure workflow scheduling approach for SDN-based IoT-Fog networks. It considers resource allocation and DDoS attack mitigation to optimize the network's performance while ensuring security.

Services in the cloud can be auto-scaled by employing an auto-scaling utility. This utility is the main target for Economic Denial of Sustainability (EDoS) attackers [30]. These EDoS attackers may send a huge number of requests to the cloud for processing, scaling resources up, and causing considerable losses to cloud customers. In the cloud environment, EDoS may culminate into DDoS. DDoS attacks provide a huge impact on multi-tenant clouds than traditional infrastructure. DDoS attacks sometimes may take the form of EDoS attacks. In EDOS, economic harms occur due to fake resource usage and subsequent buying of resources using on-demand provisioning. To minimize the DDoS attacks in the cloud, the authors in [31] propose an on-demand resource allocation should also look in addition to network or application layer mitigation. Their proposed method provides auto-scaling decisions by differentiating between legitimate requests and attacker traffic. Attacker traffic is detected and dropped based on human behavior analysis-based detection. In this paper, the share of legitimate clients in resource addition/buying makes subsequent accurate auto-scaling decisions.

c: SIDE CHANNEL ATTACK

Network slicing is one of the key technologies for providing customized services in 5G. Resource allocation for Ultra-reliable Low-Latency Communication (URLLC) and Enhanced Mobile Broadband (eMBB) slices in 5G Radio Access Network (RAN) is a challenging task due to meet the dynamic demands. A side-channel attack is a security exploit that aims to gather information from or influence the program execution of a system by measuring or exploiting the indirect effects of the system or its hardware [32]. A Side-channel Attack (SCA) is an attack for slices, which share resources in the same hardware. In [33], the authors propose a novel approach for resource allocation in 5G networks that consider the network's vulnerability to side-channel attacks. The authors highlight that side-channel attacks can extract sensitive information from the system by analyzing physical signals or other non-cryptographic channels, making them a significant threat to the security of 5G networks. To address this challenge, the paper proposes a side channel attack-aware resource allocation algorithm for ultra-reliable and low-latency communication (URLLC) and enhanced mobile broadband (eMBB) slices in 5G Radio Access Networks (RAN). The proposed algorithm is designed to allocate network resources to optimize network performance while minimizing the risk of side-channel attacks. The proposed algorithm is evaluated through simulations, and the results demonstrate that it can effectively mitigate the impact of side-channel attacks and improve network performance. Specifically, the algorithm is shown to reduce the error rate and improve the Quality of Service (QoS) compared to traditional resource allocation algorithms. This side-channel attack-aware resource allocation algorithm provides a promising approach to secure resource allocation in 5G networks, especially in the context of side-channel attacks. It can help improve network performance and ensure high security and resilience in 5G networks.

In [34], the authors propose a novel approach to resource allocation in 5G networks that address the challenge of side-channel attacks. The proposed method uses a model-based adaptive Proximal Policy Optimization (PPO) algorithm to migrate service function chains (SFCs) in response to security threats. The SFC migration approach proposed in this paper is based on the premise that side-channel attacks can compromise the security and performance of 5G networks. The authors propose an adaptive approach to SFC migration that considers the network's current state, the available resources, and the potential security threats. The approach involves continuously monitoring the network's performance and identifying potential security threats based on predefined security metrics. Once a security threat is identified, the proposed approach uses the model-based adaptive PPO algorithm to migrate the SFC to a more secure location in the network. The algorithm considers the network's current state and the available resources to find the best place for the SFC migration. Using an adaptive algorithm, the approach can quickly adapt to changes in the network's state and resource availability, ensuring the network's security and performance. The paper's experimental evaluation demonstrates the effectiveness of the proposed approach in protecting against side-channel attacks. The results show that the approach can identify and mitigate security threats while ensuring the network's overall performance.

d: EAVESDROPPING

D2D communications are key enabling technologies in the 5G era. Information security for resource allocation in D2D communication for cellular and D2D users is challenging. In [35], the authors propose a security-enhanced social aware resource allocation for D2D communication. Most of the existing works consider imperfect Channel State Information (CSI) that includes estimation errors. The authors frame a coalitional game approach, enabling multiple D2D pairs to share the cellular user spectral resource. A heterogeneous cellular network-based practical scenario has been considered with multiple eavesdroppers, intra-cell interference, and inter-cell interference to evaluate the parameters, e.g., sum-rate and secrecy capacity for both CUs and D2D pairs. Moreover, the authors justify the proposed algorithm's stability, computational complexity, and convergence.

In [36], the authors propose a resource allocation approach to address eavesdropping in 5G and beyond wireless communication networks. The approach involves allocating resources in a way that makes it difficult for eavesdroppers to intercept communication signals. The proposed approach considers various factors, such as the number of users, the distance between users, and the signal-to-noise ratio to allocate resources effectively.

2) RESOURCE ALLOCATION CONSIDERING SECURITY ATTRIBUTES

Confidentiality, Integrity, and Availability are the fundamental components of security attributes. Confidentiality provides privacy and guarantees the privacy of the data. Privacy includes other aspects, e.g., privacy of identity and location. Data integrity can be considered data authentication because it guarantees that the data has not been altered in any way. Availability assures that the legitimate parties can access the service whenever required.

Security is an essential issue for allocating parallel jobs on clusters in real-time. However, existing resource allocation approaches do not consider real-time parallel jobs on clusters with security requirements. The authors in [37] propose a security-aware resource allocation for parallel jobs on homogeneous and heterogeneous clusters of computing platforms. They propose two types of resource allocation schemes. One is task allocation for parallel applications with deadlines and security constraints, i.e., a collection of security services required by a task. Here, the security services are security attributes, e.g., confidentiality, integrity, and availability. Another one is heterogeneity-aware resource allocation for parallel jobs by taking into account applications' timing and security requirements, i.e., weights for different services required for the task. The authors build mathematical models to describe the system model, security overhead, and parallel applications with timeline and security constraints. The proposed methods are based on a heuristic that allows allocating the resources to maximize the security and the probability of meeting deadlines for parallel jobs running in different clusters.

Non-Orthogonal Multiple Access (NOMA) is one of the most promising radio access technologies for next-generation wireless networks. In order to improve spectral efficiency, NOMA plays a vital role in the cognitive radio network. Resource allocation with delay and security attribute as a constraint for NOMA-based cognitive radio network is a challenging aspect. In the paper [38], the authors propose a downlink security-aware resource allocation problem with delay constraint via spectrum sensing, where it is modeled as a mixed-integer nonlinear problem for a NOMA-based cognitive radio network. Here, authentication is considered as a security attribute. The proposed resource allocation method considers security with the delay constraints in secondary users and inferences constraints to primary users and total power consumption at the Base Station (BS). The security-aware resource allocation is based on CSI at the physical layer and Queue State Information (QSI) at the link layer. The secrecy transmission rate of each secondary user is considered by the ratio of channel gains by the secondary user and the unauthenticated user. A probability upper bound of exceeding the maximum packet delay based on the queueing model is analyzed for a required minimum secrecy transmission rate. The authors propose that security-aware user scheduling and power allocation problems be solved separately. The secondary user scheduling problem is solved via the greedy algorithm, and successive convex optimization methods propose the power allocation algorithm.

a: SOLUTIONS FOR RESOURCE ALLOCATION CONSIDERING SECURITY

In the existing works of resource allocation considering security, security is considered either an issue or an attribute. Most of the existing works consider the issues or attributes as a constraint of resource allocation. We can observe that the main objective of resource allocation of existing works for various applications is basically for various resources, e.g., computation, radio resources, data rate, virtual resources, network slices, spectral resources, etc., and optimizing energy consumption, delay, performance. The security issues and attributes are considered in this work as constraints.

Figure 4 depicts the methods associated with the resource allocation considering the security. We can find several solutions for resource allocation with security in computing and communication from the existing literature. One of the solutions is the cryptographic solution, e.g., introducing a security layer with a cryptographic algorithm, e.g., AES, to protect the data and information. Before offloading the data, protect by cryptographic algorithms will be helpful to protect it from eavesdropping and data breaches. One crucial aspect of allocating resources with security is applying adaptive methods, e.g., reinforcement learning and deep learning. Adaptive learning methods can be used for learning the potential attacks, selecting the secure nodes/devices,

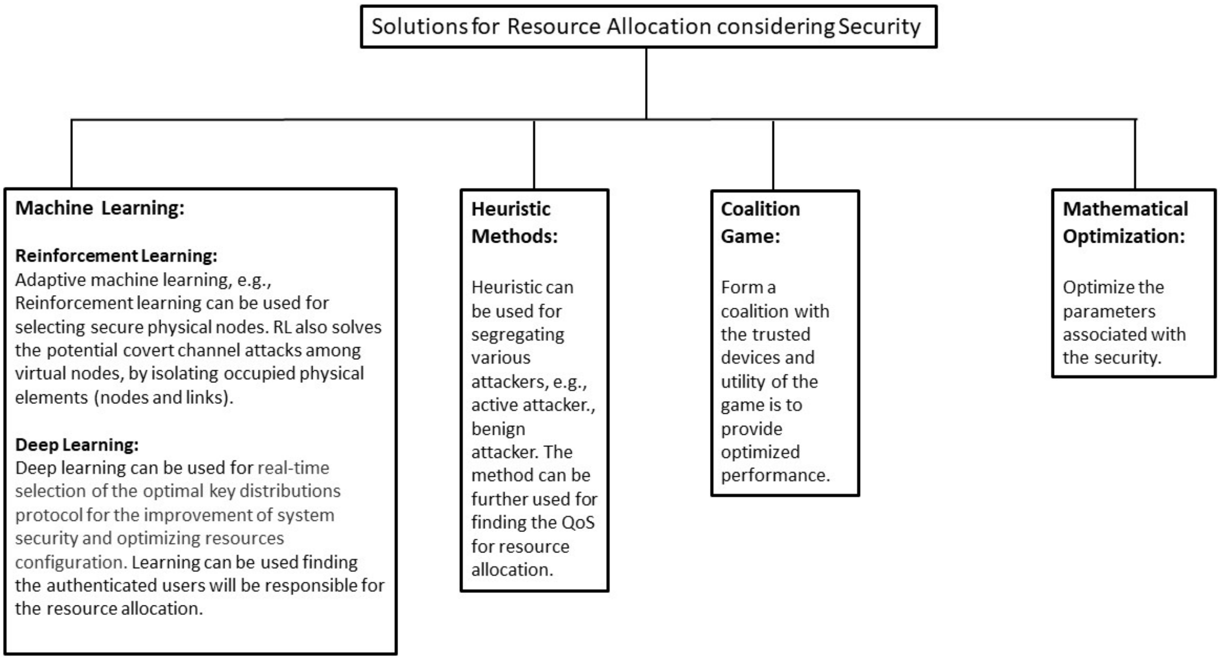
Solutions for Resource Allocation considering Security
Machine Learning:
Reinforcement Learning:
Adaptive machine learning, e.g., Reinforcement learning can be used for selecting secure physical nodes. RL also solves the potential covert channel attacks among virtual nodes, by isolating occupied physical elements (nodes and links).
Deep Learning:
Deep learning can be used for real-time selection of the optimal key distributions protocol for the improvement of system security and optimizing resources configuration. Learning can be used finding the authenticated users will be responsible for the resource allocation.
Heuristic Methods:
Heuristic can be used for segregating various attackers, e.g., active attacker., benign attacker. The method can be further used for finding the QoS for resource allocation.
Coalition Game:
Form a coalition with the trusted devices and utility of the game is to provide optimized performance.
Mathematical Optimization:
Optimize the parameters associated with the security.

FIGURE 4. Solutions for resource allocation considering security.

TABLE 1. Security Considerations for Resource Allocation.

Works	Allocated Resources	Technology	Scenario	Issues/Attributes	Consideration	Security Solution
[24]	Computation, Radio Resources	5G MEC	Distributed	Data breach	Security layer	AES as security layer
[25]	Data rate, Virtual resources	5G HetNets	Distributed	Data breach	Constraint	Reinforcement learning
[26]	Data	5G	Distributed	Data breach	Constraint	Federated learning
[27]	Data	5G	Distributed	Data breach	Constraint	Blockchain
[28]	Network slices	SDN/NFV enabled 5G	Distributed	DDoS attack	Constraint	Deep learning
[29]	Bandwidth	IoT	Distributed	DDoS attack	Constraint	Scheduling algorithm
[31]	Computation	Cloud computing	Distributed	DDoS attack	Constraint	Heuristic
[33]	Network Slices	5G RAN	Centralized	Side channel attack	Constraint	Attack-aware heuristic method
[35]	Spectral resource	D2D communications	Distributed	Eavesdropping	Constraint	Coalition game
[37]	Homogenous and heterogeneous clusters	Cluster computing	Parallel	CIA Triad	Constraint	Mathematical optimization
[38]	Radio resource	Cognitive radio networks	Distributed	Authentication	Constraint	Mathematical optimization

learning the adversaries, etc. Deep learning can be used for learning proper key distribution for authentication. Heuristic methods can be applied for various security solutions. For example, the heuristic can be used for segregating various attackers. Coalition games can be used for finding trusted devices, and the utility of the game is to provide optimized performance. It has also been applied to finding the quality of service of the network. A software-defined solution is applied for taking security measurements. Mathematical optimization can be applied to optimizing the essential parameters based on security.

Figure 4 shows the methods for the resource allocation considering the security issues and attributes.

Table 1 shows the classification of works based on different allocated resources for various technologies, considered scenarios, issues, or attributes of the security, which is considered as either constraint or attribute, and various solutions.

B. DEPENDABILITY

In the following, We explore different resource allocations considering different dependability attributes or issues either as objectives or a constraint. We also explore different resource allocation methodologies considering different aspects of dependability.

1) RESOURCE ALLOCATION CONSIDERING DEPENDABILITY ISSUES

Dependability can be considered as issues for resource allocation. Faults, errors, and failures are the issues for dependability.

Fault tolerance and load balancing are vitally crucial in resource allocation against failures in a distributed network. The weighted value of unavailable probability (W-UP) measures the probability of unsuccessful recovery and the maximum unavailable probability after recovery among physical nodes. In [45], the authors propose a fault-tolerant resource allocation with W-UP. They consider that node failure is based on workload-dependent failure probability. Each failure occurs based on a probability. The authors introduce a recovery strategy to deal with the workload variation determined at the operation start time and can be applied for each failure pattern. Once a failure occurs, the recovery process has been done using the priority setting of the recovery algorithm of the failed nodes. The authors also explore the unsuccessful recovery probability by considering the maximum number of arbitrary recoverable functions by a set of available nodes without the priority setting. The authors formulate the optimization problem as a Mixed-Integer Linear Programming (MILP) problem. A heuristic algorithm has been proposed to solve the larger size problem. They present an initial Workload-Aware Greedy Algorithm (WAGA). The algorithm determines an initial primary and backup resource allocation by considering the workload-dependent failure probability. It avoids uneven failure probabilities among all nodes by evenly utilizing a part of capacity in a node with corresponding different failure probabilities. In addition to considering the ordered failure probability of nodes for allocating the functions, the algorithm considers three aspects for allocation. Firstly, it evenly distributes the primary resource of each function to nodes so that the number of the functions hosted by each node can be almost the same. The uneven number of concurrent function failures caused by the failed nodes among all failure patterns may be avoided. Secondly, the nodes hosting any of the primary or backup resources of a function are not allowed to host another backup resource. Thirdly, the backup resources of the functions whose primary resources are hosted by the same node are distributed to different nodes with the best.

2) RESOURCE ALLOCATION CONSIDERING DEPENDABILITY ATTRIBUTES

a: AVAILABILITY

High-Performance distributed Computing Systems (HPCS), e.g., grids, cloud, and hybrid infrastructures provide access to a large amount of resources. These resources are required to execute parallel jobs, which are submitted by the HPCS users and include computing nodes, links, data storage, software, network channel, etc. Resource allocation for parallel jobs execution in distributed computing is challenging as the complex distributed environment works on operating under conditions of resource availability. Unplanned maintenance works, global and local events, and imprecise estimation of jobs do not allow considering the accurate resource allocation with the proper resource utilization. The resource scheduling algorithm is very important to consider the resource availability for utilizing the resources properly. When scheduling under uncertainties, proactive and reactive approaches are usually classified [46]. Proactive algorithms concentrate on resource utilization based on predictions and heuristic-based advanced resources allocations and reservations. Reactive algorithms analyze the current state of the computing environment and make decisions for jobs migration and rescheduling. Both types of algorithms may be used in a single system to achieve even greater resource usage efficiency. The resource availability predictions for the considered scheduling interval may be obtained based on the historical data processing, linear regression models, or with the help of expert and machine learning methods. In [39], the authors propose an efficient job-flow execution in compliance with QoS constraints for resource allocation. The novelty of their proposed method is to select the nodes based on the availability for the resource allocation. They propose special Knapsack and greedy algorithms in the market-based computing model. They consider a set of heterogeneous computing nodes with different performance and price characteristics. The resources availability and utilization probabilities for the scheduling interval are provided as input data. They model the resources utilization profile as an ordered list of utilization events, such as resource allocation or release events. Jobs execution time uncertainties are modeled as a sequence of allocation, occupation, and release events with the occupation probability. Global resources utilization uncertainties, e.g., maintenance works or network failures, are modeled as continuous occupation events during the whole considered scheduling interval. Scheduling interval is divided in number of windows. When a set of resources is required for a job execution for a time period, the total window availability during the expected job execution interval can be estimated as a product of the availability probabilities of each independent window node. If any window is occupied during the desired job execution interval, the parallel job will be postponed or even aborted. A common issue of resource allocation problem is maximizing the available probability of total resources. They initialize variables

TABLE 2. Dependability Considerations for Resource Allocation.

Works	Allocated Resources	Technology	Scenario	Issues/Attributes	Consideration	Dependability Solution
[39]	Computation	Distributed system	Distributed	Availability	Constraint	Greedy algorithm
[40]	Data	4G-LTE	Centralized	Availability	Constraint	Utility based method
[41]	Data	Cloud computing	Distributed	Reliability	Objective	Heuristic algorithm
[42]	Computation and communication	Distributed system	Distributed	Reliability	Constraint	Mixed integer linear programming
[43]	Virtual	Cloud computing	Distributed	Safety	Constraint	Prediction based
[44]	Homogenous and heterogeneous clusters	Cluster computing	Distributed	Safety	Constraint	Hybrid method
[45]	Computation and links	Distributed system	Distributed	Faults	Constraint	Greedy algorithm

for the best availability criterion value and corresponding best window. The computing nodes available during the interval select different groups by their performance. After executing the greedy algorithm, the window contains the resulting window with the maximum attainable availability probability.

A surge in the importance of sensors and real-time monitoring has brought about the convergence of two major technologies, the cloud, and IoT, which lead to the emergence of the cloud of Things. Processing of large streaming data and providing low latent, power-efficient, high accurate decision making has yet again emerged a new technology called Fog Computing. Real-time decision-making is the key thing for latency-aware, on-demand resource allocation. The dynamic and heterogeneous nature of fog computing has made resource allocation a challenge and has caught the attention of researchers in recent times. To provide a balanced load, a proper node selection has to be based on resource availability and the energy availability of the node. The fog nodes have limited capacity and do not take on heavy tasks. Any compute-intensive tasks are offloaded to the cloud, and hence there is no task migration involved in load balancing, and the tasks are assumed to be non-preemptive for simplicity of the problem. Fog nodes with the cloud infrastructure can ensure real-time decision-making. Fault tolerance is a challenging aspect of resource allocation. In [40], the authors propose a fault-tolerant resource allocation method for fog environments using game theory-based reinforcement learning. Their work is based on game theory and reinforcement learning. The allocation is done based on network status and traffic history. The method finds the fail-over cluster formation to explore the link failures. To provide a balanced load, a proper selection of node has to be based on resource availability along with the energy availability of the node. The work considers the energy of the node as an inclusion of the processing time, response time, and the setup cost, which includes the data center cost and the VM cost. In this work, the problem is formulated considering the fog nodes have limited capacity and do not take heavy tasks. Any compute-intensive tasks are offloaded to the cloud, and hence there is no task migration involved in load balancing, and the tasks are assumed to be non-preemptive for simplicity of the problem. The proposed algorithm ensures the energy and latency-aware load balancing to provide availability and improve the performance of the fog network. The time taken for a task to be executed at a node is given as the sum of the transmission time and the execution time. Thus, for each node, the energy consumption is dependent on the data being transmitted and the transmission power. The cost optimization is considered analogous to the bin packing problem, which in turn is an NP-hard problem. Most of the NP-hard problems are solved with the help of heuristics or approximation techniques. Here, in this work, the problem of optimization is looked upon as a minimization problem. This total cost optimization is considered a game theory problem that analyzes and predicts the behavior of the nodes based on other nodes' strategies. To use game theory, we need to prove that there is an existence of Nash equilibrium for the scheduling problem. The proposed methodology makes use of the bidirectional forwarding detection algorithm, which is used in failure observation between nodes either connected directly or by multiple hops. This algorithm works based on control packet transmission. The node receiving the control packet sends back an echo message which contains the transmit time or interval based on which the failure detection time depends. Based on the least transmission time, the two best alternate paths are generated and stored in the routing table by the controller.

b: RELIABILITY

Cloud provides resources to the users based on requirements using several resource allocation schemes. Reliable resource allocation is one of the key challenges for cloud-based resource allocation. The objective of the paper [41] is to provide a reliable service for the resource allocation in cloud computing, minimizing the cost. The authors propose a novel approach to resource allocation in cloud computing that considers the resources' reliability. The authors highlight that in cloud computing, the reliability of the resources can significantly impact the overall system performance and user satisfaction. To address this challenge, the paper proposes a reliability-based resource allocation approach that considers the reliability of the resources as a key factor in the resource allocation decision. The proposed approach uses a reliability model to estimate the reliability of each resource and incorporates this information into the resource allocation decision process. The proposed approach is evaluated through simulations, and the results demonstrate that it can effectively improve the system's reliability and provide a higher level of service availability compared to traditional resource allocation approaches. Specifically, the approach reduces the system downtime and improves the Quality of Service (QoS) for the users. The reliability-based resource allocation approach provides a promising approach to resource allocation in cloud computing, especially in ensuring high service availability and user satisfaction. It can improve the system's reliability and ensure that the resources are allocated to maximize the overall system performance.

In [47], the authors propose a novel hybrid approach to achieve reliability in cloud computing by considering resource allocation. The proposed approach aims to improve the reliability of cloud computing systems, which are vulnerable to various failures and errors. The approach combines the benefits of both hardware and software redundancy to enhance the reliability of cloud computing systems. It uses a resource allocation algorithm to allocate redundant resources cost-effectively while ensuring high reliability. The algorithm considers various factors, such as the system's workload, the availability of resources, and the cost of redundant resources. The proposed approach also incorporates a fault-tolerant mechanism, which detects and mitigates failures in the system. The mechanism uses proactive and reactive approaches to detect and reduce failures. The proactive approach involves monitoring the system and identifying potential failures, while the reactive approach involves recovering from failures and restoring the system's functionality. The experimental results show that the proposed approach can achieve high reliability in cloud computing systems while minimizing the cost of redundant resources. The approach outperforms other existing approaches regarding reliability, availability, and cost-effectiveness. The proposed hybrid approach provides a novel solution for achieving reliability in cloud computing systems by considering resource allocation. It combines the benefits of hardware and software redundancy and incorporates a fault-tolerant mechanism to detect and mitigate failures in the system. The approach can improve the reliability of cloud computing systems while minimizing the cost of redundant resources.

c: SAFETY

The Intelligent Transportation System (ITS) is an essential component of the smart city, which is applied to safer roads, better traffic control, and on-demand service by information collected from vehicles and roadside infrastructure. In ITS, Vehicular Cloud Computing (VCC) is a novel technology balancing the requirement of complex services and the limited capability of onboard computers. A safety issue is considered here as the disconnection of communication between the vehicle and the Vehicular Cloud (VC) when this vehicle is computing for a service. More importantly, the connection fault will seriously disturb the normal services of VCC and impact the safety works of the transportation. In [43], the authors propose a resource allocation mechanism against connection fault in VCC by using a modified workflow with prediction capability. The authors propose the probability model for the vehicle movement, which satisfies the high dynamics and real-time requirements of VCC. In addition, the authors propose a Prediction-based Reliability Maximization Algorithm (PRMA) to realize the safety resource allocation for VCC. The heuristic algorithm is widely used to solve optimization problems. In addition, this algorithm is used to find the locally optimal solution or suboptimal solution. The proposed safety resource allocation mechanism is also based on the workflow theory.

In 4G, the dual connectivity technique helps utilize the radio resources scheduled by two distinct base stations for the single-user equipment to enhance data throughput. Multi-connectivity is the key enabling technology for the 5G, which extends dual connectivity and improves user performance and overall resource utilization. This also allows dynamic user traffic steering across multiple connections of one or more radio access technologies. However, one of the key challenges is to allocate the resources in multi-connection based on the heterogeneous quality of service requirements. For public safety applications, multi-connectivity is one of the key things to consider as the failure of one connection, others can be as backup connections. In the paper [44], the authors examine a resource allocation problem under multi-connectivity in an evolved LTE network and propose fairness based on utility that supports QoS in terms of requested rates for the public safety scenario. Their objective is to allocate the resource optimally to user-to-user traffic based on the utility function. The utility is defined as the percentage of allocated Physical Resource Block (PRB) to total PRBs in decimal form along UL/DL direction to transport user-to-user traffic of user pair through BS. They consider two different utility functions, one provides proportional fairness, and the other extends proportional fairness by considering QoS. Multi-connectivity can boost the aggregated data rate of user-to-user traffic in under-loaded and uneven-loaded scenarios compared with the single connectivity case. In addition, the User Plane Function (UPF) is able to fulfill the requested rate and increase the satisfaction ratio when there are available radio resources among multiple connections.

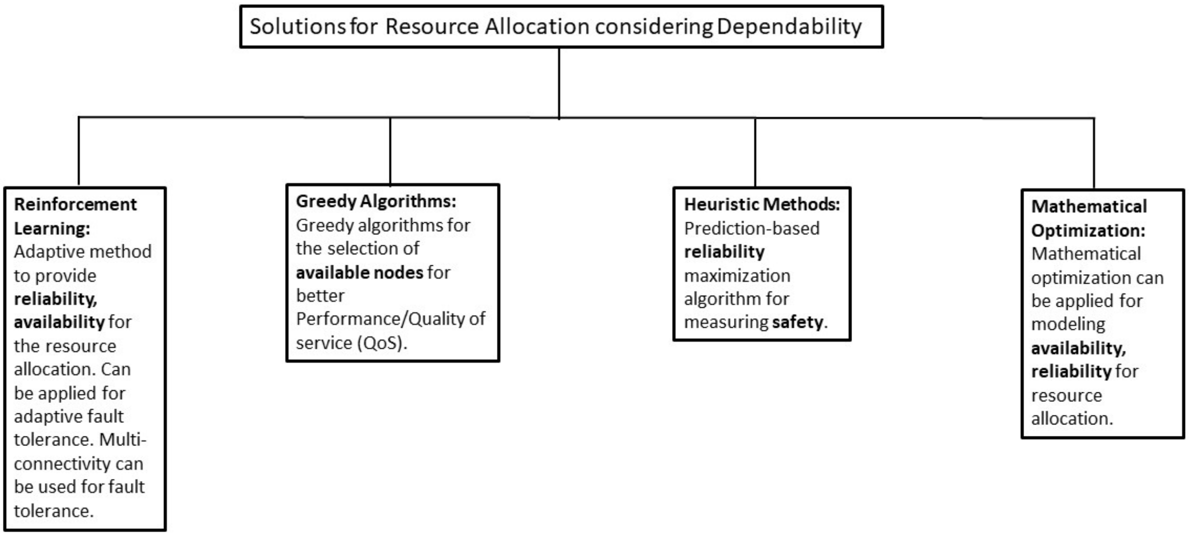
Solutions for Resource Allocation considering Dependability
Reinforcement Learning: Adaptive method to provide **reliability, availability** for the resource allocation. Can be applied for adaptive fault tolerance. Multi-connectivity can be used for fault tolerance.
Greedy Algorithms: Greedy algorithms for the selection of **available nodes** for better Performance/Quality of service (QoS).
Heuristic Methods: Prediction-based **reliability** maximization algorithm for measuring **safety**.
Mathematical Optimization: Mathematical optimization can be applied for modeling **availability, reliability** for resource allocation.

FIGURE 5. Solutions for resource allocation considering dependability.

d: SOLUTIONS FOR RESOURCE ALLOCATION WITH DEPENDABILITY

Solutions for resource allocation with dependability have been considered with the dependability attributes and issues, e.g., reliability, availability, safety, integrity, and faults. In most of the existing works, availability and reliability-based resource allocation can be achieved through the adaptive method. Based on our study, greedy algorithms can be helpful for availability-based resource allocation. Prediction-based heuristic methods are beneficial for safety-based resource allocation. Fault-tolerant resource allocation is possible to achieve through machine learning, e.g., reinforcement learning, a multi-connectivity-based method.

Figure 5 shows the methods used for the resource allocation considering the dependability issues and attributes.

Table 2 shows the allocated resources for various technologies, scenarios for the resource allocation, different issues/attributes for dependability, consideration of dependability as either constraint or as an objective, and various dependability solutions.

C. JOINT SECURITY AND DEPENDABILITY

Considering joint security and dependability for resource allocation is a challenging issue. Adding security and dependability as constraints to optimize the trade-off between resource consumption and performance might be complex for increasing the number of parameters to handle [48].

1) RESOURCE ALLOCATION CONSIDERING ATTACK-DEFENSE SCENARIO

There are some existing works where there are considerations of security attacks for resource allocation and dependability constraints to defend against that attack. So, one classification for considering joint security and dependability is the resource allocation considering the attack-defense scenario. In [49], the authors develop a multi-round network attack-defense scenario with dual-role players who can attack and defend. A mathematical model is established to optimize the resource allocation and predict the network survivability by the Average Degree Of Disconnectivity (ADOD) or failures. In each round, the players allocate their attack resources in the nodes of their network and in another player's network after updating related information of another player. Furthermore, they can reallocate the defense resources and repair compromised nodes. The gradient method and the game theory are adopted to find the optimal resource allocation for both players.

Cyber vulnerabilities are becoming very common nowadays. Especially with the increase of the industrial sector, the vulnerabilities are also increasing. One example is the attack on the Ukrainian power grid. There are works where attacks in the cyber-physical system are designed to defend those by creating a defender. In [50], the authors propose a multi-stage attack-defense game analysis for resource allocation optimization. There are two types of actors in this work. Attackers try to attack the resources in a way that failure occurs, and defenders try to neutralize the effect through allocating resources. Attackers and defenders have their resources, costs, and utility functions. They play a game using graph theory and try to allocate the virtual resources so that the defender neutralizes the hamper caused by the attacker.

Adversarial Risk Analysis (ARA) provides a framework to deal with risks originating from the intentional actions of adversaries. In multi-agent-based systems, ARA is a critical issue to consider. Security resource allocation is one of the critical challenges considering different mob attacks in a particular environment. In [51], the authors propose how to efficiently allocate the security by police authority for the mob attacks in an urban setting. The police and the mobs are the two actors in this work. The police have some resources and want to deploy those for the probable criminal attacks. The mob has also had some resources by which they could destroy the normal environment. Game theory has been applied to recover the adversarial attack in this scenario.

Lin et al. [52] propose a resource allocation strategy to maximize network survivability considering of average degree of disconnectivity. In this paper, the authors consider ADOD as a metric. The ADOD combining the concept of the probability calculated by the contest success function with the ADOD metric would be used to evaluate the damage degree of the network. The larger the ADOD value, the more damage degree of the network would be. An attack-defense scenario as a mathematical model would be used to support network operators in predicting all the likelihood strategies both cyber attackers and network defenders would take. The attacker could use the attack resources to launch an attack on the nodes of the network. On the other hand, the network defender allocates existed resources of the defender to protect the survival nodes of the network. In the process of problem-solving, the "gradient method" and "game theory" would be adopted to find the optimal resource allocation strategies for both cyber attackers and network defenders.

2) FAULT TOLERANT RESOURCE ALLOCATION

Fault-tolerant resource allocation is one classification where security issues can be dependable by providing dependability through availability. In [53], the authors propose a method to efficiently canvass an area of interest using distributed sensing methods, assisted by fault-tolerant resource allocation. By implementing multiple aircraft in an assessment configuration, aerial monitoring and diverse sensing can be accomplished through the use of ad-hoc networking principles; aircraft act as nodes, each being a distributed agent in the network. Combined with the Distributed Apt Resource Transference System (DARTS) method for reallocating redundant or alternately-allocatable resources, such implementations can enjoy longer operational duration, increased coverage, and a higher probability of executing the desired reconnaissance. DARTS employs a hybridization of gossip and flooding-based resource discovery methods to find suitable replacement resources in the case of a node failure. Failures may arise due to natural (environmental) interference or malicious attacks designed to disrupt the mission. Testing of the fault-tolerant resource management techniques demonstrated the system's resiliency, resulting in minimal bandwidth requirements to reallocate (up to a 6-fold reduction in traffic) and a faster speed of resource reallocation even in the face of an inconsistent state of operation. By implementing Intrusion Detection System (IDS) technologies to spawn the reallocation process (a procedure called triggering), DARTS provides a flexible, lightweight, and scalable method to efficiently allow reconnaissance and other distributed sensing applications to occur on a mobile, airborne platform.

Recent technological developments have enabled the execution of more scientific solutions on cloud platforms. Cloud-based scientific workflows are subject to various risks, such as security breaches and unauthorized access to resources. Attackers may destroy servers by attacking side channels or virtual machines, causing interruption and delay or incorrect output. Although cloud-based scientific workflows are often used for vital computational-intensive tasks, their failure can come at a great cost. To increase workflow reliability, in [54] the authors propose the Fault and Intrusion-tolerant Workflow Scheduling algorithm (FITWS). The proposed workflow system uses task executors consisting of many virtual machines to carry out workflow tasks. FITWS duplicates each sub-task three times, uses an intermediate data decision-making mechanism and then employs a deadline partitioning method to determine sub-deadlines for each sub-task. This way, dynamism is achieved in task scheduling using the resource flow. The proposed technique generates or recycles task executors, keeps the workflow clean, and improves efficiency. Experiments were conducted on WorkflowSim to evaluate the effectiveness of FITWS using metrics such as task completion rate, success rate, and completion time.

Effective allocation of resources with fault tolerance is one of the key issues in any computational grid environment to perform the task execution on time. In the paper, [42], a Fault-Folerant Hybrid Resource allocation Model (FTHRM) is proposed to minimize the TurnAround Time (TAT) for the batch of tasks. In addition, their proposed method ensures fault tolerance in a dynamic grid environment. The model uses the prior reservation method to allocate the resources for the guaranteed task execution. Furthermore, resources are reserved in advance for time slots with resource configuration as required by the set of tasks. In the case of failures, alternate resources are provided by the system. Here, the resources with the least previous workload and lowest execution time will prefer over other resources for task accomplishment. The proposed system is designed for the processing of the Batch Of Tasks (BOT). Tasks belong to different users and are independent with no restrictions, such as a sequence of dependencies. The BOT will submit to the grid resource broker for processing. The tasks will go through among several states. Initially, the tasks will be waiting. Once it has been ready for execution, it will move from waiting to the ready state. Afterward, when the task is dispatched for execution, then it will move from ready to running state. However, if the task faces a timeout situation, then it would be shifted again from the running to the ready state. If any interruption occurs in the running state due to resource failure, the task will be in the failed state. Next, a reallocation of resources will occur for the successful task completion due to the resource reservation, and the task will switch from this failed to the ready state. When the task execution gets completed, it exits from the system by a completion stage.

In Wireless Underground Sensor Networks (WUSNs), "holes" pose significant challenges to resource allocation, security, and dependability. Holes refer to regions where sensor nodes cannot communicate directly due to obstacles like rocks, soil density variations, or water bodies. In [55], the author provide an insight that these holes disrupt the connectivity and create gaps in the network coverage, affecting the efficient allocation of resources. In terms of security, holes can make the network susceptible to attacks or unauthorized access, as malicious entities may exploit these gaps for unauthorized entry or disruption of data transmission. Additionally, the lack of direct communication paths due to holes can impact the network's dependability, as it becomes challenging to ensure reliable data transmission and timely response to critical events. Addressing the problem of the hole in WUSNs requires innovative resource allocation strategies that optimize routing paths and consider the limited resources of sensor nodes. Moreover, robust security mechanisms, such as encryption and authentication protocols, must be employed to protect data transmission across the network. By addressing these challenges, the resource allocation in WUSNs can be enhanced, leading to improved security and dependability in underground sensing applications.

Federated learning has emerged as a powerful approach for training machine learning models in distributed environments while ensuring data privacy. When applied to fog-cloud-enabled cellular networks, federated learning enables the integration of Intelligent Reflecting Surfaces (IRS) into the network architecture. Intelligent reflecting surfaces, also known as reconfigurable intelligent surfaces or smart mirrors, consist of passive elements that can dynamically manipulate nearby wireless signals. By controlling the amplitude and phase of the reflected signals, IRS can enhance the overall network performance by optimizing signal coverage, improving channel capacity, and reducing interference. In [56], the authors consider that in the context of fog-cloud-enabled cellular networks, federated learning plays a crucial role in resource allocation for IRS. The distributed nature of federated learning allows individual IRS units to train local models using data collected from their specific environment. These local models are then aggregated and updated collaboratively with the cloud server, resulting in a global model that captures the collective intelligence of the entire network. Resource allocation in federated learning for IRS involves determining the optimal allocation of computational resources, such as bandwidth and power, to facilitate model training and communication between the IRS units and the cloud server. Security and dependability are critical considerations in federated learning for IRS in fog-cloud-enabled cellular networks. As data is collected and shared across multiple IRS units, preserving data privacy and ensuring secure communication becomes paramount. Robust encryption techniques, secure aggregation protocols, and authentication mechanisms are implemented to safeguard the privacy and integrity of the data during the federated learning process. Furthermore, dependability ensures the reliability and availability of the federated learning system. Redundancy mechanisms, fault tolerance techniques, and robust error handling mechanisms are incorporated to mitigate potential failures and ensure uninterrupted operation of the system.

In [57], the authors focuses on addressing resource allocation challenges in cloud computing while considering security and dependability aspects. The authors propose a novel approach that combines machine learning techniques to optimize resource allocation, task scheduling, and enhance the overall security of cloud systems. The main objective of the research is to improve the performance and reliability of cloud computing environments by allocating resources efficiently while ensuring the security of sensitive data and applications. The authors identify the resource allocation problem as a multi-objective optimization challenge that requires balancing the conflicting goals of maximizing resource utilization, minimizing response time, and enhancing security. The proposed approach considers both computational resources and security-related factors in the allocation process. The authors integrate security mechanisms such as encryption, authentication, and access control to safeguard data and applications from unauthorized access or attacks. By incorporating security considerations into the resource allocation process, the system ensures the integrity, confidentiality, and availability of cloud resources. Additionally, the paper addresses task scheduling as a critical component of resource allocation in cloud computing. The hybrid machine learning techniques are applied to optimize task scheduling algorithms, ensuring that tasks are assigned to appropriate resources based on their requirements and security levels.

In [58], the authors focuses on resource allocation in the context of a fog computing environment for smart healthcare systems, while considering both security and dependability aspects. The authors propose an approach called Effective Prediction and Resource Allocation Method (EPRAM) that combines prediction techniques and resource allocation strategies to optimize the allocation of resources in a secure and dependable manner. The main objective of the research is to improve the efficiency and reliability of resource allocation in fog computing environments specifically designed for smart healthcare systems. The authors recognize the challenges posed by the dynamic nature of healthcare data and the critical need for ensuring data security and system dependability.

In [59], the authors provides an overview of Mobile Edge Computing (MEC) infrastructure, focusing on design, resource management, and optimization approaches. The survey explores various aspects of resource allocation in MEC, with considerations for security and dependability. The main objective of the research is to analyze the existing literature and present a comprehensive survey of MEC infrastructure, specifically addressing resource allocation strategies while taking into account security and dependability requirements. The paper discusses the design principles and components of MEC infrastructure, highlighting the key role of edge servers located at the network edge. It examines the challenges associated with resource management in MEC, including efficient utilization of computing, storage, and communication resources while meeting the demands of diverse applications.

In [60], the authors focuses on resource allocation in the context of wireless and edge computing environments, specifically addressing the dynamic selection of network slices. The authors propose a comprehensive approach that considers security and dependability aspects in the resource management process. The main objective of the research is to optimize resource allocation by dynamically selecting appropriate network slices in wireless and edge computing systems. Network slicing allows the creation of virtual networks that cater to specific application requirements, enabling efficient resource allocation. In terms of security, the authors recognize the importance of safeguarding the resources and data in wireless and edge computing environments. They emphasize the need to incorporate security mechanisms such as access control, encryption, and authentication in the resource management process. By considering security measures, the system ensures the confidentiality, integrity, and availability of resources and data.

Based on the above existing literature, we can come up with decisions that several factors should be considered when implementing and deploying resource allocation strategies that incorporate security and dependability. Here are some insights and considerations:

- Security and Dependability Requirements: We need to start by identifying the system's specific security and dependability requirements. This may include confidentiality, integrity, availability, fault tolerance, and resilience. In addition, we need to clearly define the objectives and constraints related to security and dependability [61].
- Risk Assessment: Need to conduct a comprehensive risk assessment to identify the system's potential threats, vulnerabilities, and risks. Furthermore, to evaluate the impact and likelihood of these risks and prioritize them based on their severity. This assessment will help in designing appropriate resource allocation strategies [62].
- Security and Dependability Measures: Implement security and dependability measures to mitigate the identified risks. These may include encryption, access controls, authentication, redundancy, backup and recovery mechanisms, monitoring systems, intrusion detection systems, and disaster recovery plans. Consider both preventive and reactive measures [63].
- Resource Allocation Strategies: Develop resource allocation strategies integrating security and dependability considerations [64]. These strategies should ensure that critical resources are allocated appropriately to support the required security measures and maintain system dependability. This may involve allocating resources based on risk levels, criticality, or prioritization.
- Monitoring and Evaluation: Implement monitoring and evaluation mechanisms to assess the effectiveness of the resource allocation strategies in terms of security and dependability. Continuously monitor the system for potential security breaches, performance issues, and dependability concerns. Regularly evaluate the implemented design and make adjustments based on the observed outcomes [61].
- Technologies and Tools: Several technologies and tools can facilitate the integration of security and dependability into resource allocation strategies. These include virtualization, Intrusion Detection Systems (IDS), Security Information and Event Management (SIEM), Configuration Management Tools, Fault tolerant middleware [65].
- Context awareness techniques: Context awareness techniques play a crucial role in resource allocation strategies by considering dynamic factors and environmental information to make informed decisions [66]. Here are some examples of specific context awareness techniques that have been utilized in resource allocation strategies: network conditions, location awareness, user behavior and preferences, energy efficiency, security requirements, workload characteristics, device capabilities.
- Heterogeneous resources consideration: Heterogeneous resources refer to resources that differ in terms of their capabilities, capacities, performance characteristics, or other attributes. The presence of heterogeneous resources can significantly impact the resource allocation process, as the allocation decisions need to consider the unique characteristics and requirements of each resource. By considering resource compatibility, performance variability, Quality of Service (QoS) requirements, and leveraging adaptive allocation policies and virtualization, efficient and effective allocation of heterogeneous resources can be achieved, leading to improved system performance, scalability, and resource utilization [67].

We need to select the technologies and tools depends on the requirements, system architecture, and budget constraints. It is essential to thoroughly evaluate available options before making decisions.

IV. DISCUSSION AND FUTURE RESEARCH

The impact of security and dependability on resource allocation in future networking and computing systems is potentially huge. New complex systems with integrated network and computation resources require advanced management and orchestration, which rise new security and dependability challenges that require enhanced techniques. Future wireless networking technologies, e.g., the sixth generation (6G) of mobile networks will increase the complexities. The IoT is envisioned as the Internet of Everything (IoE). For secured and dependable resource allocation in this complex environment, intelligent edge and pervasive intelligence will play a vital role in the future. The system should be adaptive enough to deal with the various dynamic behaviors of this complex system. Hence, AI, ML, especially RL will play a vital role in providing security and dependability during resource allocation.

Existing resource allocation solutions often incorporate security and dependability considerations to ensure the protection of critical resources and the reliable operation of the system. Several methodologies and algorithms have been proposed to address these concerns.

A. JOINTLY CONSIDER SECURITY AND DEPENDABILITY

Survivability is one of the key concerns for keeping both security and dependability. There can be several attacks, faults, and errors for resource allocation, and the system should be able to get rid of this. We need to keep the system available and have the survival capability for a more extended period under security attacks. There can be the following issues for finding out the impact on resource allocation with both security and dependability.

- Security model: For performing experiments, a challenging issue is to work on a security model. Security issues can be an attack or any malicious nodes/faulty nodes/fake nodes/noisy nodes, which hamper resource allocation. However, designing this security is a challenging aspect. For example, to design faulty nodes, e.g., to design noisy nodes with noises like Gaussian White Noise (GWN), designing selfish nodes trying to compromise the system's overall objective is challenging. We need to think about how they will pretend to be the original node in the infrastructure. Needs to think about how to provide security impact by these fake nodes. For example, how will it affect the resources? Will it be by broadcasting any fake values or information to the neighbors? Will there be any noises? Will there be nodes to maximize its resources in a collaborative environment?
- Dependability model: The dependability model for resource allocation is challenging. Designing faults, errors, and failures in the running system based on a real-life scenario is challenging. For example, consider some random failure of links in the routing of a multi-hop sensor network or D2D communication. We need to think about the countermeasure of these failures as well, e.g., to make the system fault-tolerant. Combining dependability with security is indeed challenging.
- Attack-defense model: The model for resource allocation can be an attack-defense model to consider both security and dependability. To model attack-defense is a challenge for the complex infrastructure. Attack-defense model can be combined with both security and dependability. An example of an attack-defense model that considers both security and dependability is the "Multi-Layered Security and Resilience Model" for a critical infrastructure system, such as a power grid. This model aims to protect the system from various types of attacks while ensuring its continued operation even in the face of disruptions [68]. As we have already mentioned, dependability addresses outages of systems caused by failures on its components. However, security attacks may also cause outages, the impact of this outages can be reduced by using or adapting some dependability techniques. Most of the existing methods are based on game theory and RL for these attack-defense issues. For applying this method, the system design for resources, costs, and reward functions is critical.

While significant progress has been made in considering security and dependability for resource allocation, gaps in knowledge and areas require further investigation. Some of these gaps include, e.g., dynamic security and dependability-aware resource allocation, quantifying the impact of security and dependability on resource allocation, adaptive resource allocation for emerging technologies, and privacy-preserving resource allocation. Addressing these gaps in knowledge through further research and investigation will contribute to developing more robust and effective resource allocation strategies that integrate security and dependability considerations. This will enhance integrated networking and computing systems' resilience, performance, and trustworthiness.

B. ADAPTIVE METHOD SELECTION WITH SECURITY AND DEPENDABILITY

Choosing an effective adaptive method for resource allocation considering both security and dependability is a challenge for adaptive resource allocation. Static methods for resource allocation are not suitable since in a dynamic environment, dynamic changes of requirements and to meet the requirements from the capacity need an adaptive solution. Machine learning-based methods are widely considered an adaptive solution. The following issues can come up for the adaptive method selection.

- Actor/Agent selection: Appropriate actor selection for the proposed game theory or RL is challenging. It is needed to choose the appropriate attackers and defenders in the system.
- Tuning of the parameters for ML: As an adaptive ML method, RL is very widely used. RL has so many parameters. It is challenging to tune those parameters considering additional parameters for security and dependability.
- Reward function/utility function: Most adaptive methods have reward or utility functions. Designing a proper reward function to justify the utilization of resources with security and dependability is a key concern.
- Evaluation: To compare the different variants of the method is also a challenge. Considering the same

parameters and additional parameters for other variants can create an issue for the adaptive methods.

- Privacy-aware learning: In traditional ML approaches, neural network models are trained at a server or a data center. Thus, the centralized learning approaches typically require the raw data, e.g., photos and location information, collected by mobile devices to be centralized at the server [69]. The centralized learning approaches thus face big issues, including privacy, long propagation delay, and backbone network burden [70]. Recently, FL as a decentralized ML approach has been proposed to address the above issues [71], [72]. In FL, mobile devices, i.e., workers, are required to collaboratively train the neural network model of the model owner. In particular, the model owner first transmits its global model to the workers. The workers then use their data to train the model locally and send the model updates to the model owner. The model owner aggregates the model updates from the workers to a new global model and transmits it back to the workers for training. The model owner and the workers periodically exchange and update the model until a target accuracy is achieved [73]. By updating the models rather than the raw data, FL alleviates many challenging problems, e.g., privacy issues and the backbone network burden issues, of the traditional ML [74].

C. ROBUST RESOURCE ALLOCATION

A resource allocation is defined to be robust concerning specified system performance features against failures/perturbations in specified system parameters if degradation in these features is limited when the failures/perturbations occur. For example, if a resource allocation has been declared to be robust for satisfying a throughput requirement against concerns in the system load, then the system configured under that allocation should continue to operate without a throughput violation when the system load increases. The research questions are: What is the degree of robustness? For the example given above, how much can the system load increase before a throughput violation occur? Measuring the robustness of resource allocation is a challenging issue. Robustness is essential to measure the system's effectiveness and its behavior in terms of any failures, noises, and other adversaries. To achieve robustness, it is important to recover from the failures. Robustness can be built-in with the method that deals with resource allocation, e.g., robust [75], adversarial reinforcement learning [76].

D. BLOCKCHAIN-BASED TECHNOLOGIES

Blockchain is a trusted and shared ledger running on a Peer-to-Peer (P2P) network. The key idea behind the blockchain concept is its decentralization. That is, any single entity does not control data on blockchain [77]. Instead, all blockchain nodes, such as devices, have the equal right to verify and manage the data stored in blockchain-enabled by consensus mechanisms. This decentralized feature makes blockchain resistant to data modifications or attacks. Moreover, the elimination of the central server avoids the risk of single-point failures, thus improving the reliability and stability of blockchain systems. However, blockchain operations incur costs in terms of latency and energy consumption. In fact, the execution of blockchain mining tasks, e.g., block verification and information exchange among miners, requires large energy sources to be consumed. In order to append a new transaction to the blockchain, a blockchain user or a miner needs to run a mining puzzle, e.g., Proof of Work (PoW) [78], which is generally complicated and requires vast computing and storage resources. Smart contracts are the programs on blockchain that run when some preconditions are met [79]. For resource allocation, blockchain can be applied for the provisioning of secure access control. In addition, blockchain helps to transfer access rights from one entity to another in a secure, flexible, and fine-grained manner. Consensus mechanisms and smart contracts can further be able to mitigate faults.

E. MULTI-OBJECTIVE OPTIMIZATION

In recent years, there has been an increasing focus on integrating security and dependability into the design of computer and networking systems. However, integrating security and dependability often comes at the cost of system performance, which can negatively impact the user experience. As a result, there has been a growing interest in multi-objective optimization techniques that can balance the need for security, dependability with the need for system performance. One of the main necessities of multi-objective optimization of security, dependability and system performance is identifying and prioritizing competing objectives. This involves a thorough understanding of the system requirements, potential security threats, dependability issues and the development of appropriate metrics for measuring system performance, security and dependability. For example, system performance may be measured in terms of response time or throughput. In contrast, security may be measured in terms of the level of protection against various attacks. Another necessity is the ability to model and analyze the trade-offs between security/dependability and performance. This involves the development of mathematical models that can capture the complex relationships between various system parameters, such as the number of security, dependability mechanisms and their impact on system performance. Such models can evaluate the performance and security of different system configurations and identify the optimal trade-offs between these competing objectives. The impact of adding the new metric of security to system performance is a key consideration in multi-objective optimization [80], [81]. When security/dependability is added as a new metric, the optimization problem becomes more complex and may require new optimization techniques that can handle multiple conflicting objectives. This may involve using multi-objective evolutionary algorithms [82], which are designed to handle problems with multiple objectives and constraints. It is crucial to note that the specific techniques and algorithms used for resource allocation may vary depending on the context, system requirements, and constraints. The selection of the appropriate strategy depends on the particular trade-offs that need to be balanced in a given scenario. In [13], the authors address the crucial aspects of security, dependability, and performance in the context of 5G Multi-access Edge Computing (MEC). The authors focuses into the trade-offs that arise when striving to optimize these three interconnected factors. This paper provides valuable insights into the challenges, solutions, and trade-offs involved in ensuring secure, dependable, and high-performing edge computing environments in the context of 5G networks.

F. MISSION CRITICAL APPLICATIONS

To consider security and dependability in resource allocation for mission-critical applications brings significant implications and potential benefits. Mission-critical applications are those where system failures, breaches, or disruptions can have severe consequences, such as compromising safety, causing financial losses, or impacting human lives [83]. Furthermore, considering security and dependability in resource allocation for mission-critical applications ensures operational resilience, protects critical data and resources, and enhances overall system performance, thereby mitigating risks and safeguarding the integrity and availability of critical services.

G. SCALABILITY AND ADAPTIBILITY

Scalability and adaptability are crucial considerations in resource allocation strategies for large-scale and dynamic networking and computing systems. Resource allocation strategies in large-scale and dynamic systems focus on scalability and adaptability by employing distributed management, load balancing, elastic provisioning, real-time monitoring, predictive analytics, machine learning, and autonomic computing principles [84]. These techniques enable the systems to handle changing conditions or demands in real time while optimizing resource utilization and maintaining desired performance levels.

H. VIRTUALIZATION TECHNOLOGIES

In the literature, several virtualization technologies are considered for resource allocation in integrated networking and computing systems. These technologies enable the efficient utilization of resources by abstracting and virtualizing physical resources into virtual entities. Here are some primary virtualization technologies commonly discussed in the literature: Containerization, Virtual Machines (VMs), Network Function Virtualization (NFV), Software-Defined Networking (SDN), Edge Computing and Fog Computing. These virtualization technologies offer different levels of isolation, resource management, and flexibility for resource allocation in integrated networking and computing systems [85]. Researchers explore these technologies to design efficient and scalable resource allocation mechanisms that ensure optimal performance, security, and dependability in diverse computing and networking environments.

I. ONGOING PROJECTS

In a Horizon 2020 project, SUPERCLOUD,[1] proposes new security and dependability infrastructure management paradigms that are user-centric, provides self-service clouds-of-clouds where customers define their protection requirements and avoid lock-ins; and self-managed for self-protecting clouds-of-clouds that reduce administration complexity through automation. The objective of SUPERCLOUD is to implement a cloud architecture that gives users the flexibility to define their protection requirements and instantiate policies accordingly. This project proposes trust models and security mechanisms that enable the composition of services and trust statements across different administrative provider domains. In addition, the project focuses on implementing a resource management framework that robustly composes provider-agnostic resources using primitives from diverse cloud providers. The SUPERCLOUD methodology will be validated by testbed integration for real-world use cases in the healthcare domain, ranging from deploying a distributed medical imaging platform to running a full laboratory information system.

There is an ongoing project funded by the Research Council of Norway named 5G-MODaNeI (5G Management and Orchestration for Data and Network Integration),[2] where the main goal is to provide joint security and dependability for resource allocation in 5G MEC. The target is to propose an adaptive method for resource allocation by ensuring security and dependability.

V. CONCLUSION

In this survey paper, we have explored how security and dependability can be considered in the resource allocation in networking and computing systems. We have classified the current research works by considering the allocated type of resources for different technologies, scenarios, issues, attributes, and solutions. We have presented the current research works on resource allocation that include security and dependability, both singularly and jointly. Finally, we have discussed the future research directions.

The paper highlighted that the future works on resource allocation in networking and computing systems will need to consider both security and dependability to meet the advanced requirement of the future applications, such as mission-critical services. There should be consideration of multi-objective optimization for security/dependability and performance. The future solutions will require joint security and dependability models, adaptive methods, robust

[1] https://cordis.europa.eu/project/id/643964

[2] https://5g-modanei.ux.uis.no/

approaches, and might be based on blockchain. The paper can help the researchers to effectively consider security and dependability in the future networking and computing systems.

REFERENCES

[1] R. Stair, F. Moisiadis, R. Genrich, and G. Reynolds, *Principles of Information Systems*. Boston, MA, USA: Cengage Learn. Australia, 2011.

[2] G. Nencioni, R. G. Garroppo, A. J. Gonzalez, B. E. Helvik, and G. Procissi, "Orchestration and control in software-defined 5G networks: Research challenges," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–18, Aug. 2018.

[3] X. Wang, J. Li, Z. Ning, Q. Song, L. Guo, S. Guo, and M. S. Obaidat, "Wireless powered mobile edge computing networks: A survey," *ACM Comput. Surv.*, vol. 55, no. 13s, pp. 1–37, Dec. 2023.

[4] M. Kamatar and P. B. Madhavi, "A comparative study on resource aware allocation and load balancing techniques for cloud computing," *Grenze Int. J. Eng. Technol.*, vol. 9, no. 1, pp. 1–15, 2023.

[5] A. Sarah, G. Nencioni, and M. M. I. Khan, "Resource allocation in multi-access edge computing for 5G-and-beyond networks," *Comput. Netw.*, vol. 227, May 2023, Art. no. 109720.

[6] P. E. Heegaard, B. E. Helvik, G. Nencioni, and J. Wäfler, "Managed dependability in interacting systems," in *Principles of Performance and Reliability Modeling and Evaluation*. Cham, Switzerland: Springer, 2016, pp. 197–226.

[7] R. F. Olimid and G. Nencioni, "5G network slicing: A security overview," *IEEE Access*, vol. 8, pp. 99999–100009, 2020.

[8] P. K. Dutta Pramanik, T. Biswas, and P. Choudhury, "Multicriteria-based resource-aware scheduling in mobile crowd computing: A heuristic approach," *J. Grid Comput.*, vol. 21, no. 1, pp. 1–29, Mar. 2023.

[9] F. A. Shaikh and M. Siponen, "Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity," *Comput. Secur.*, vol. 124, Jan. 2023, Art. no. 102974.

[10] J. Wang, J. Liu, J. Li, and N. Kato, "Artificial intelligence-assisted network slicing: Network assurance and service provisioning in 6G," *IEEE Veh. Technol. Mag.*, vol. 18, no. 1, pp. 49–58, Mar. 2023.

[11] R. U. Rasool, H. F. Ahmad, W. Rafique, A. Qayyum, and J. Qadir, "Security and privacy of Internet of Medical Things: A contemporary review in the age of surveillance, botnets, and adversarial ML," *J. Netw. Comput. Appl.*, vol. 201, May 2022, Art. no. 103332.

[12] L. Torres-Ronda, E. Beanland, S. Whitehead, A. Sweeting, and J. Clubb, "Tracking systems in team sports: A narrative review of applications of the data and sport specific analysis," *Sports Med.-Open*, vol. 8, no. 1, p. 15, Dec. 2022.

[13] G. Nencioni, R. G. Garroppo, and R. F. Olimid, "5G multi-access edge computing: A survey on security, dependability, and performance," 2021, *arXiv:2107.13374*.

[14] J. Kacprzyk, W. Zamojski, T. Walkowiak, J. Sugier, and J. Mazurkiewicz, *Dependable Computer Systems*. Cham, Switzerland: Springer, 2011.

[15] P. Ranaweera, A. Jurcut, and M. Liyanage, "MEC-enabled 5G use cases: A survey on security vulnerabilities and countermeasures," *ACM Comput. Surv.*, vol. 54, no. 9, pp. 1–37, Dec. 2022.

[16] O. Hayat, R. Ngah, Z. Kaleem, S. Z. M. Hashim, and J. J. P. C. Rodrigues, "A survey on security and privacy challenges in device discovery for next-generation systems," *IEEE Access*, vol. 8, pp. 84584–84603, 2020.

[17] S. H. H. Madni, M. S. A. Latiff, Y. Coulibaly, and S. M. Abdulhamid, "Recent advancements in resource allocation techniques for cloud computing environment: A systematic review," *Cluster Comput.*, vol. 20, no. 3, pp. 2489–2533, Sep. 2017.

[18] A. Belgacem, "Dynamic resource allocation in cloud computing: Analysis and taxonomies," *Computing*, vol. 104, no. 3, pp. 681–710, Mar. 2022.

[19] S. Bhagat and P. Gupta, "A survey on scalable resource allocation in cloud computing," in *Recent Innovations in Computing*. Cham, Switzerland: Springer, 2022, pp. 401–414.

[20] A. Mohamed, M. Hamdan, S. Khan, A. Abdelaziz, S. F. Babiker, M. Imran, and M. N. Marsono, "Software-defined networks for resource allocation in cloud computing: A survey," *Comput. Netw.*, vol. 195, Aug. 2021, Art. no. 108151.

[21] A. Masmoudi, K. Mnif, and F. Zarai, "A survey on radio resource allocation for V2X communication," *Wireless Commun. Mobile Comput.*, vol. 2019, pp. 1–12, Oct. 2019.

[22] R. Adler, F. Elberzhager, R. Falcão, J. Siebert, E. C. Groen, J. Heinrich, F. Balduf, and P. Liggesmeyer, "A research roadmap for trust-worthy dynamic systems of systems–motivation, challenges and research directions," Fraunhofer IESE, Germany, Tech. Rep. 1.

[23] B. Srinidhi, J. Yan, and G. K. Tayi, "Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors," *Decis. Support Syst.*, vol. 75, pp. 49–62, Jul. 2015.

[24] A. Shaiba, D. Unal, and M. Khayyat, "Security-aware data offloading and resource allocation for MEC systems: A deep reinforcement learning," techrxiv.org, Tech. Rep. 1.

[25] H. Cao, G. S. Aujla, S. Garg, G. Kaddoum, and L. Yang, "Embedding security awareness for virtual resource allocation in 5G HetNets using reinforcement learning," *IEEE Commun. Standards Mag.*, vol. 5, no. 2, pp. 20–27, Jun. 2021.

[26] S. S. Alshamrani, N. Jha, and D. Prashar, "B5G ultrareliable low latency networks for efficient secure autonomous and smart Internet of Vehicles," *Math. Problems Eng.*, vol. 2021, pp. 1–15, Sep. 2021.

[27] M. Arjovsky, S. Chintala, and L. Bottou, "Wasserstein generative adversarial networks," in *Proc. Int. Conf. Mach. Learn.*, 2017, pp. 214–223.

[28] A. J. Ramadhan, "T-S3RA: Traffic-aware scheduling for secure slicing and resource allocation in SDN/NFV enabled 5G networks," 2021, *arXiv:2107.05056*.

[29] S. Javanmardi, M. Shojafar, R. Mohammadi, V. Persico, and A. Pescapè, "S-FoS: A secure workflow scheduling approach for performance optimization in SDN-based IoT-fog networks," *J. Inf. Secur. Appl.*, vol. 72, Feb. 2023, Art. no. 103404.

[30] M. Naresh Kumar, P. Sujatha, V. Kalva, R. Nagori, A. K. Katukojwala, and M. Kumar, "Mitigating economic denial of sustainability (EDoS) in cloud computing using in-cloud scrubber service," in *Proc. 4th Int. Conf. Comput. Intell. Commun. Netw.*, Nov. 2012, pp. 535–539.

[31] G. Somani, A. Johri, M. Taneja, U. Pyne, M. S. Gaur, and D. Sanghi, "DARAC: DDoS mitigation using DDoS aware resource allocation in cloud," in *Proc. Int. Conf. Inf. Syst. Secur.* Cham, Switzerland: Springer, 2015, pp. 263–282.

[32] H. Maghrebi, "Deep learning based side channel attacks in practice," *Cryptol. ePrint Arch.*, vol. 10, pp. 1–50, May 2019.

[33] Y. Li, Y. Zhao, J. Li, J. Zhang, X. Yu, and J. Zhang, "Side channel attack-aware resource allocation for URLLC and eMBB slices in 5G RAN," *IEEE Access*, vol. 8, pp. 2090–2099, 2020.

[34] T. Zhang, C. Xu, B. Zhang, X. Li, X. Kuang, and L. A. Grieco, "Towards attack-resistant service function chain migration: A model-based adaptive proximal policy optimization approach," *IEEE Trans. Dependable Secure Comput.*, early access, Jan. 17, 2023, doi: 10.1109/TDSC.2023.3237604.

[35] M. Ahmed, Y. Li, Z. Yinxiao, M. Sheraz, D. Xu, and D. Jin, "Secrecy ensured socially aware resource allocation in device-to-device communications underlaying HetNet," *IEEE Trans. Veh. Technol.*, vol. 68, no. 5, pp. 4933–4948, May 2019.

[36] F. Salahdine, T. Han, and N. Zhang, "Security in 5G and beyond recent advances and future challenges," *Secur. PRIVACY*, vol. 6, no. 1, pp. 1–12, Jan. 2023.

[37] T. Xie and X. Qin, "Security-aware resource allocation for real-time parallel jobs on homogeneous and heterogeneous clusters," *IEEE Trans. Parallel Distrib. Syst.*, vol. 19, no. 5, pp. 682–697, May 2008.

[38] L. Xu, A. Nallanathan, X. Pan, J. Yang, and W. Liao, "Security-aware resource allocation with delay constraint for NOMA-based cognitive radio network," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 2, pp. 366–376, Feb. 2018.

[39] V. Toporkov and D. Yemelyanov, "Availability-based resources allocation algorithms in distributed computing," in *Russian Supercomputing Days*. Cham, Switzerland: Springer, 2020, pp. 551–562.

[40] V. Divya and L. R. Sri, "Fault tolerant resource allocation in fog environment using game theory-based reinforcement learning," *Concurrency Comput., Pract. Exper.*, vol. 33, no. 16, pp. 1–15, Aug. 2021.

[41] A. B. M. B. Alam, M. Zulkernine, and A. Haque, "A reliability-based resource allocation approach for cloud computing," in *Proc. IEEE 7th Int. Symp. Cloud Service Comput. (SC2)*, Nov. 2017, pp. 249–252.

[42] S. Sheikh, A. Nagaraju, and M. Shahid, "A fault-tolerant hybrid resource allocation model for dynamic computational grid," *J. Comput. Sci.*, vol. 48, Jan. 2021, Art. no. 101268.

[43] T. Ye, Z. Su, J. Wu, L. Guo, J. Li, and G. Li, "A safety resource allocation mechanism against connection fault for vehicular cloud computing," *Mobile Inf. Syst.*, vol. 2016, pp. 1–13, Jan. 2016.

[44] K. Alexandris, C.-Y. Chang, K. Katsalis, N. Nikaein, and T. Spyropoulos, "Utility-based resource allocation under multi-connectivity in evolved LTE," in *Proc. IEEE 86th Veh. Technol. Conf.*, Sep. 2017, pp. 1–6.

[45] M. Zhu, F. He, and E. Oki, "Resource allocation model against multiple failures with workload-dependent failure probability," *IEEE Trans. Netw. Service Manage.*, vol. 19, no. 2, pp. 1098–1116, Jun. 2022.

[46] T. Chaari, S. Chaabane, N. Aissani, and D. Trentesaux, "Scheduling under uncertainty: Survey and research directions," in *Proc. Int. Conf. Adv. Logistics Transp. (ICALT)*, May 2014, pp. 229–234.

[47] M. A. Shahid, M. M. Alam, and M. M. Su'ud, "Achieving reliability in cloud computing by a novel hybrid approach," *Sensors*, vol. 23, no. 4, p. 1965, Feb. 2023.

[48] N. Bhatt, A. Anand, and D. Aggrawal, "Improving system reliability by optimal allocation of resources for discovering software vulnerabilities," *Int. J. Quality Rel. Manage.*, vol. 37, no. 6/7, pp. 1113–1124, Nov. 2020.

[49] P.-Y. Chen, Y.-J. Chen, and F. Y.-S. Lin, "Resource allocation strategies under attack-defense dual-role and malicious attacks," in *Future Information Technology*. Cham, Switzerland: Springer, 2014, pp. 689–695.

[50] C. Shao and Y. Li, "Multistage attack–defense graph game analysis for protection resources allocation optimization against cyber attacks considering rationality evolution," *Risk Anal.*, vol. 42, no. 5, pp. 1086–1105, May 2022.

[51] C. Gil, D. Rios Insua, and J. Rios, "Adversarial risk analysis for urban security resource allocation," *Risk Anal.*, vol. 36, no. 4, pp. 727–741, Apr. 2016.

[52] F. Y.-S. Lin, P.-Y. Chen, and Q.-T. Chen, "Resource allocation strategies to maximize network survivability considering of average DOD," in *Distributed Computing and Artificial Intelligence*. Cham, Switzerland: Springer, 2012, pp. 751–758.

[53] A. P. Lauf and W. H. Robinson, "Fault-tolerant distributed reconnaissance," in *Proc. Mil. Commun. Conf.*, Oct. 2010, pp. 1812–1817.

[54] M. Farid, R. Latip, M. Hussin, and N. A. W. Abdul Hamid, "A fault-intrusion-tolerant system and deadline-aware algorithm for scheduling scientific workflow in the cloud," *PeerJ Comput. Sci.*, vol. 7, p. e747, Nov. 2021.

[55] P. Sharma, R. P. Singh, M. A. Mohammed, R. Shah, and J. Nedoma, "A survey on holes problem in wireless underground sensor networks," *IEEE Access*, vol. 10, pp. 7852–7880, 2022.

[56] A. Lakhan, M. A. Mohammed, S. Kadry, K. H. Abdulkareem, F. T. Al-Dhief, and C.-H. Hsu, "Federated learning enables intelligent reflecting surface in fog-cloud enabled cellular network," *PeerJ Comput. Sci.*, vol. 7, p. e758, Nov. 2021.

[57] P. K. Bal, S. K. Mohapatra, T. K. Das, K. Srinivasan, and Y.-C. Hu, "A joint resource allocation, security with efficient task scheduling in cloud computing using hybrid machine learning techniques," *Sensors*, vol. 22, no. 3, p. 1242, Feb. 2022.

[58] F. M. Talaat, "Effective prediction and resource allocation method (EPRAM) in fog computing environment for smart healthcare system," *Multimedia Tools Appl.*, vol. 81, no. 6, pp. 8235–8258, Mar. 2022.

[59] L. A. Haibeh, M. C. E. Yagoub, and A. Jarray, "A survey on mobile edge computing infrastructure: Design, resource management, and optimization approaches," *IEEE Access*, vol. 10, pp. 27591–27610, 2022.

[60] S. Jošilo and G. Dán, "Joint wireless and edge computing resource management with dynamic network slice selection," *IEEE/ACM Trans. Netw.*, vol. 30, no. 4, pp. 1865–1878, Aug. 2022.

[61] Z. Amiri, A. Heidari, N. J. Navimipour, and M. Unal, "Resilient and dependability management in distributed environments: A systematic and comprehensive literature review," *Cluster Comput.*, vol. 26, no. 2, pp. 1565–1600, Apr. 2023.

[62] P. A. S. Ralston, J. H. Graham, and J. L. Hieb, "Cyber security risk assessment for SCADA and DCS networks," *ISA Trans.*, vol. 46, no. 4, pp. 583–594, Oct. 2007.

[63] H. Tabrizchi and M. Kuchaki Rafsanjani, "A survey on security challenges in cloud computing: Issues, threats, and solutions," *J. Supercomput.*, vol. 76, no. 12, pp. 9493–9532, Dec. 2020.

[64] T. Islam, D. Manivannan, and S. Zeadally, "A classification and characterization of security threats in cloud computing," *Int. J. Next-Gener. Comput.*, vol. 7, no. 1, pp. 268–285, 2016.

[65] A. Rahman, J. Islam, D. Kundu, R. Karim, Z. Rahman, S. S. Band, M. Sookhak, P. Tiwari, and N. Kumar, "Impacts of blockchain in software-defined Internet of Things ecosystem with network function virtualization for smart applications: Present perspectives and future directions," *Int. J. Commun. Syst.*, vol. 2023, pp. 1–12, Feb. 2023.

[66] M. A. Islam, M. A. Islam, M. A. H. Jacky, M. Al-Amin, M. S. U. Miah, M. M. I. Khan, and M. I. Hossain, "Distributed ledger technology based integrated healthcare solution for Bangladesh," *IEEE Access*, vol. 11, pp. 51527–51556, 2023.

[67] D. G. Sirmon and M. A. Hitt, "Managing resources: Linking unique resources, management, and wealth creation in family firms," *Entrepreneurship Theory Pract.*, vol. 27, no. 4, pp. 339–358, Oct. 2003.

[68] Z. Mahmood and V. Jusas, "Blockchain-enabled: Multi-layered security federated learning platform for preserving data privacy," *Electronics*, vol. 11, no. 10, p. 1624, May 2022.

[69] Y. Jing, B. Guo, Z. Wang, V. O. K. Li, J. C. K. Lam, and Z. Yu, "CrowdTracker: Optimized urban moving object tracking using mobile crowd sensing," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3452–3463, Oct. 2018.

[70] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2322–2358, 4th Quart., 2017.

[71] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Y. Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Proc. 20th Int. Conf. Artif. Intell. Statist.*, 2017, pp. 1273–1282.

[72] T. T. Anh, N. C. Luong, D. Niyato, D. I. Kim, and L.-C. Wang, "Efficient training management for mobile crowd-machine learning: A deep reinforcement learning approach," *IEEE Wireless Commun. Lett.*, vol. 8, no. 5, pp. 1345–1348, Oct. 2019.

[73] B. McMahan and D. Ramage, "Federated learning: Collaborative machine learning without centralized training data," Google Res. Blog, USA, Tech. Rep. 3, 2017.

[74] W. Y. B. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, Y.-C. Liang, Q. Yang, D. Niyato, and C. Miao, "Federated learning in mobile edge networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 2031–2063, 3rd Quart., 2020.

[75] J. Morimoto and K. Doya, "Robust reinforcement learning," *Neural Comput.*, vol. 17, no. 2, pp. 335–359, Feb. 2005.

[76] W. Uther and M. Veloso, "Adversarial reinforcement learning," Dept. Comput. Sci., Carnegie Mellon Univ., Tech. Rep. CMU-CS-03-107, 1997.

[77] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for 5G and beyond networks: A state of the art survey," *J. Netw. Comput. Appl.*, vol. 166, Sep. 2020, Art. no. 102693.

[78] D. Fullmer and A. S. Morse, "Analysis of difficulty control in Bitcoin and proof-of-work blockchains," in *Proc. IEEE Conf. Decis. Control (CDC)*, Dec. 2018, pp. 5988–5992.

[79] B. K. Mohanta, S. S. Panda, and D. Jena, "An overview of smart contract and use cases in blockchain technology," in *Proc. 9th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2018, pp. 1–4.

[80] M. M. Hussain, A. T. Azar, R. Ahmed, S. U. Amin, B. Qureshi, V. D. Reddy, I. Alam, and Z. I. Khan, "SONG: A multi-objective evolutionary algorithm for delay and energy aware facility location in vehicular fog networks," *Sensors*, vol. 23, no. 2, p. 667, Jan. 2023.

[81] A. Ali, G. Abbas, M. U. Keerio, M. A. Koondhar, K. Chandni, and S. Mirsaeidi, "Solution of constrained mixed-integer multi-objective optimal power flow problem considering the hybrid multi-objective evolutionary algorithm," *IET Gener., Transmiss. Distrib.*, vol. 17, no. 1, pp. 66–90, Jan. 2023.

[82] Y. An, X. Chen, K. Gao, L. Zhang, Y. Li, and Z. Zhao, "A hybrid multi-objective evolutionary algorithm for solving an adaptive flexible job-shop rescheduling problem with real-time order acceptance and condition-based preventive maintenance," *Expert Syst. Appl.*, vol. 212, Feb. 2023, Art. no. 118711.

[83] R. Sedar, C. Kalalas, F. Vázquez-Gallego, L. Alonso, and J. Alonso-Zarate, "A comprehensive survey of V2X cybersecurity mechanisms and future research paths," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 325–391, 2023.

[84] J. Zou, R. Liu, C. Wang, Y. Cui, Z. Zou, S. Sun, and K. Adachi, "Aiming in harsh environments: A new framework for flexible and adaptive resource management," *IEEE Netw.*, vol. 36, no. 4, pp. 70–77, Jul. 2022.

[85] A. Domeke, B. Cimoli, and I. T. Monroy, "Integration of network slicing and machine learning into edge networks for low-latency services in 5G and beyond systems," *Appl. Sci.*, vol. 12, no. 13, p. 6617, Jun. 2022.

MD MUHIDUL I. KHAN received the master's degree from the Bangladesh University of Engineering and Technology (BUET), in 2009, and the joint Ph.D. degree in interactive and cognitive environment from Klagenfurt University, Austria, and the University of Genova, Italy, in September 2014, under the Erasmus Mundus Grant from European Commission. He is a Research Fellow with the University of Stavanger, Norway, from 2021. He joined as an Assistant Professor with BRAC University, Bangladesh, and served there for one year. After that, he completed his one-year postdoctoral from the Hebei University of Technology, Tianjin, China. He was a Research Scientist with the Electronics Department, Tallinn University of Technology, Tallinn, Estonia. He was a Senior Lecturer with the School of Information Technologies, Tallinn University of Technology. He has participated in the "eLINK"-Project at the Corvinus University of Budapest, Hungary, from September 2009 to July 2010 (funded by the European Union). His specialization lies in the fields of wireless sensor networks, networked embedded systems, and pervasive computing.

GIANFRANCO NENCIONI received the M.Sc. degree in telecommunication engineering and the Ph.D. degree in information engineering from the University of Pisa, Italy, in 2008 and 2012, respectively. In 2011, he was a visiting Ph.D. student with the Computer Laboratory, University of Cambridge, U.K. He was a Postdoctoral Fellow with the University of Pisa, from 2012 to 2015, and the Norwegian University of Science and Technology, Norway, from 2015 to 2018. He is currently the Head of the Computer Networks (ComNet) Research Group and the Leader of the Project 5G-MODaNeI funded by the Norwegian Research Council. He is Associate Professor with the University of Stavanger, Norway, from 2018. His research activity regards modeling and optimization in emerging networking technologies (e.g., SDN, NFV, 5G, network slicing, and multi-access edge computing). His past research activity has been focused on energy-aware routing and design in both wired and wireless networks and on dependability of SDN and NFV.