

Original Research

Received 07 June 2026

Revised 18 July 2026

Accepted 01 August 2026

Natural Resources for Human
Health 2026, Vol. 6 (14s): 1474–1491

KEYWORDS:

6G Networks, Intelligent Security,
Reinforcement Learning, Deep
Reinforcement Learning, Privacy
Preservation, Federated Learning,
Edge Intelligence, Cross-Layer
Optimization, H2H
Communication, H2M
Communication, M2M
Communication.

An Integrated Survey of Intelligent Security Frameworks for 6G Communication Networks: Reinforcement Learning, Privacy Preservation, Edge Intelligence, and Cross-Layer Optimization

Unnati Ukanal^{1,*}, Shubhangi D C²

¹Research Scholar, Department of Computer science and engineering, Visvesvaraya Technological University Centre for PG Studies Kalaburagi, Karnataka, India.

²Professor, Department of Computer science and engineering, Visvesvaraya Technological University, Centre for PG studies Kalaburagi, Karnataka, India.

*Corresponding Email: unnathi.g.09@gmail.com

ABSTRACT: With 6th-generation (6G) wireless communication networks on the horizon, a new era of ultra-low latency, massive device connectivity, intelligent automation, and human-to-human (H2H), human-to-machine (H2M) and machine-to-machine (M2M) communication convergence is approaching. 6G promises new horizons of next-generation applications, ranging from autonomous vehicles, smart healthcare, digital twins, and industry automation, to virtual realities and smart environments. However, these transformative features pose considerable security and privacy challenges. Because the traditional security solutions for previous generations of wireless systems are often insufficient for 6G networks, which are dynamic, heterogeneous, and massive in nature, adaptive and intelligent security solutions are essential to contend with increasingly complex threats and adapt to dynamic conditions. In this survey paper, we provide a detailed review of recently developed intelligent security frameworks for 6G wireless communication networks. Specifically, we examine reinforcement learning (RL)-based security, privacy-preserving mechanisms, edge intelligence, and cross-layer optimization techniques.

Reinforcement learning (RL) and deep reinforcement learning (DRL) techniques are explored as suitable approaches for providing adaptive intrusion detection and prevention systems, intrusion detection/avoidance systems (ID/ASs), and intelligent resource management under dynamic network conditions. We discuss the state-of-the-art privacy-preserving techniques, such as federated learning, differential privacy, and secure aggregation, that can effectively protect sensitive user and device data during collective learning processes. The benefits and applications of edge intelligence for the purpose of providing intelligent security decision-making in real time and reducing the communication overhead are discussed. Furthermore, cross-layer optimization solutions for security, latency, energy efficiency, and performance trade-offs are presented. Lastly, the key limitations and open research challenges of current intelligent security mechanisms, such as scalability, complexity, and the balance between security and privacy, are highlighted. Our analysis can serve as a guidance and source of inspiration for future research in 6G intelligent security.

1. INTRODUCTION

The swift advancement of wireless communication technologies have revolutionised communication amongst humans, machines, and smart devices. Moving from first generation (1G) mobile communications to ubiquitous fifth-generation (5G) networks, each technology generation has drastically enhance capacity, throughput, coverage, and quality of service (QoS)[2]. To support a rise in always-on connection, ubiquitous intelligence, smart control and high-bandwidth applications, professionals and academics have already started working on sixth-generation (6G) communication technologies, which promises to have revolutionary services, and unprecedented network capabilities, such as high speed, low latency, the integration of AI within network systems[1].

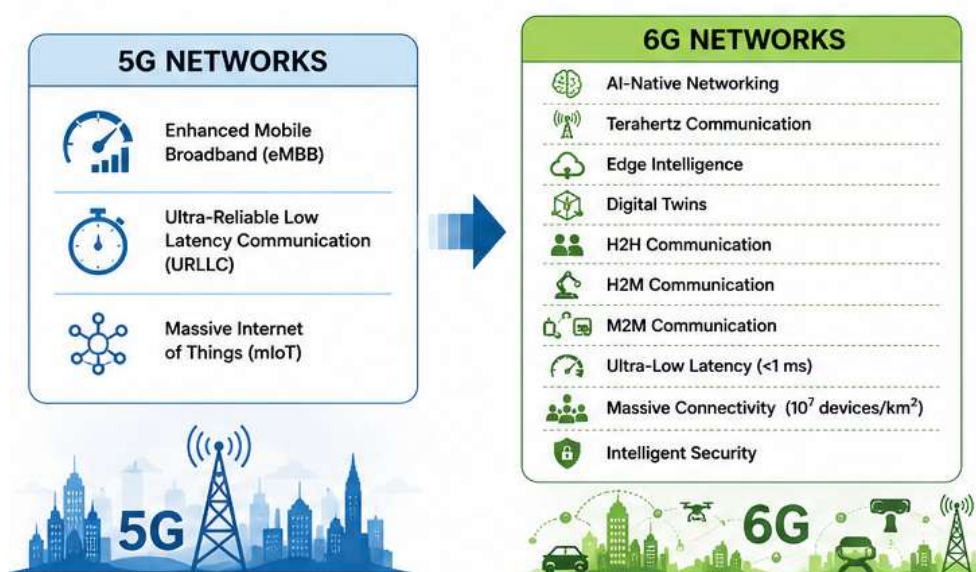


Figure 1. Evolution from 5G to 6G Networks

Figure 1. Technological Evolution from 5G to 6G Networks 5G systems laid the groundwork for connectivity in terms of massive mobile broadband (MBB), ultra-reliable low-latency communications (URLLC) and ultra-massive device connectivity (mMTC). Future 6G networks are going beyond these services and are aiming to provide AI native networking, ultra-low latency communications, edge intelligence, and secure-at-all-cost connectivity features. The future network generation will consist of Human to Human (H2H), Human to Machine (H2M) and Machine to Machine (M2M) interactions. Novel technologies such as the internet of skills (IoS) [9], autonomous vehicles, ubiquitous computing, massive industrial automation [9], digital twins, extended Reality (xR) [9] and intelligently managed services in smart city or intelligent healthcare have been enabled due to the secure and reliable 6G connectivity infrastructure [9]. On the other hand, as the scale and heterogeneity increase the threat surface increases considerably, leading to new security and privacy issues in 6G networks [2]. Because static rule-based protection approaches do not perform as well in the dynamic, highly interconnected and distributed 6G communication environments, researchers have started considering intelligent security mechanisms to defend against a wide variety of security and privacy concerns. The high penetration of edge devices, cloud-connected devices, IoT services and AI intelligence elements within a large scale, and geographically widely dispersed networks, has opened doors for new attack vectors such as Unauthorized Access (UA), Distributed Denial of Service (DDoS), Data Integrity Attack (DIA), Source spoofing, Eavesdropping (E), Adversarial attacks against Machine Learning, Privacy attack [10], etc. Therefore, adaptive security approaches that can dynamically protect networks are required to react with a varying threat level in a timely and efficient manner. For addressing such problems researchers are extensively using AI-based and ML-based methods for developing intelligent security solutions, especially for dynamic threats identification, intrusion detection, resource management and automation of network functionalities [1]. Particularly, reinforcement learning (RL) and deep reinforcement learning (DRL) have shown promise in many of the described areas, including but not limited to autonomous decision making, security anomaly detection, intrusion prevention, resource allocations [1]. Since RL algorithms learn security policy by learning from dynamic

and adaptive interaction from the network environment they fit well within the dynamically fluctuating characteristics of next generation wireless networks. To safeguard sensitive information, while allowing collaborative intelligence through distributed devices, Privacy Preserving Mechanisms (PPM) such as Federated Learning (FL), Differential Privacy (DP), Secure Aggregation, and Homomorphic Encryption (HE) have recently gained substantial attention [7]. The new concept of Edge intelligence where, AI intelligence and computational capabilities are brought much closer to end devices, can reduce the end to end latency, perform real time analysis of traffic for threat identification, and enable autonomous response by performing localized security decision [6]. Cross layer design provides an approach by optimizing various communication aspects including security in coordination among different communication layers in the network to attain efficient use of resources [3]. Cross layer Optimization (CO) techniques will optimize a wide set of network parameters at multiple layers and make decisions for the global optimization [8]. The research is spread across different domains like reinforcement learning, privacy-preserving methods, edge computing/intelligence and cross layer optimization and no systematic work covers the overall security in 6G networks, therefore we try to bridge this gap in our survey [15]. This survey offers an extensive review of intelligent security frameworks for 6G networks by surveying the following research areas in the domain: Reinforcement Learning-based Security mechanisms, Privacy Preserving approaches, Edge Intelligence in 6G Security and Cross Layer Optimization techniques [5]. The survey briefly discusses the state of art, comparison of existing techniques, identifies research gaps and proposes future directions for the development of secure and intelligent 6G communication networks [5]. Rest of the paper is organized as follows: Section 2 presents the 6G communications landscape and its major security challenges. In Section 3, we review the various reinforcement learning-based intelligent security mechanisms for 6G networks. Section 4 addresses privacy-preserving and edge intelligence in security. Section 5 covers cross-layer optimization techniques for secured 6G communications. Section 6 highlights current research gaps and future directions, and Section 7 concludes the survey.

2. SECURITY CHALLENGES AND THREATS IN 6G NETWORKS

6G can lead to a digital ecosystem which is thoroughly connected, such that ubiquitous intelligent 6G network is able to feature unprecedented speed, huge connectivities for machineries, smart network control and in-network AI capabilities[18]. 6G has many more potential uses, but on the other side, it introduces many difficult security issues and privacy issues[20]. Since the network in 6G is heterogeneous and will be loaded with more and more IoT devices, mobile robots, edge servers, digital twins and AI-powered applications, various types of attacks are launched and many more can be invented[2]. It is imperative to ensure security and privacy in the deployment of 6G.

2.1 H2H Communication Security

Human-to-Human(H2H) communications continue to be an essential part of wireless networks and include voice communications, video conferencing, social networking, immersive extended reality services [21]. In 6G networks, H2H communications are going to accommodate large amount of personal and sensitive data which have higher potential to be accessed, intercepted or misused and prone to identity theft, identity misrepresentation, eavesdropping and data interception attacks [10]. Some of the more sophisticated types of cyber threats such as phishing, session hijacking and man-in-the middle attacks threaten user confidentiality and data integrity. Addition concerns with regards to privacy may arise due to the combination of AI driven services and use of biometric technologies [2].

2.2 H2M Communication Security

H2M communication allows a human to interact with the “intelligent” device such as autonomous cars, smart medical, factory robotics, smart home [10]. Since the failure to maintain the integrity or secrecy of H2M will directly endanger people’s safety or the operational procedures, so its reliability and security become crucial. An attacker exploits security flaws in communication channel, software interface, device firmware in order to take unauthorized control of the machine[20]. For example, an attacker can insert fake commands, manipulate device remotely, insert malicious software or launched Denial of Service (DoS) attack into the H2M system. In application domain such as medical, transportation, a failure to protect it will result in a great loss of money or even loss of life. We need secure access control system, surveillance system and intelligent intrusion detection systems to ensure the security of H2M communication[13].

2.3 M2M Communication Security

Future 6G will be dominated by machine-to-machine (M2M) communication because of the dramatic increases in the number of Internet of things (IoT) devices and autonomous systems[14]. M2M communication allows information exchange between machines such as sensors, actuators, intelligent appliances and industrial machines without the participation of human[1].

M2M communication brings significant benefits in efficiency and productivity, however, it introduces more security concerns because most devices in M2M systems have small computational and power resources[3]. Therefore it is impossible to implement advanced security solutions. Due to these limitations, intruders may exploit the limited number of authentication measures, unreliable wireless communication links, obsolete firmware versions etc to conduct cyber-attacks.

The major security threats to M2M systems include botnet attacks targeting many machines, theft of sensitive information, machine spoofing and network intrusion[20]. With the tremendous number of devices connecting to the network in the future, scalable and lightweight security solutions will be essential for keeping network available and intact[3].

2.4 Major Security Threats in 6G Networks

2.4.1 Authentication and Access Control Attacks

Authentication mechanisms that limit access to the network resources only to legitimate users and devices should be used, because attackers try to overcome it using the user and service credential theft, session hijackers, credential replaying and other techniques for spoofing an entity identity. Insufficient secure network authentication leads to granting the network resources for unauthorized attackers and attackers compromise the confidential data in the network.[20].

2.4.2 Distributed Denial-of-Service (DDoS) Attacks

The DDoS attack is designed to inundate network capacity with floods of network traffic, from an army of distributed attacking devices[20]. Within a typical 6G network, we anticipate with a massive increase in the count of connected IoT devices, the exposure of large-scale DDoS attacks can be expected[20]. In such attacks, QoS can be deteriorated, latency will surge up and the communication for ordinary services will be broken.

2.4.3 Eavesdropping and Data Interception

Wireless channel communication is more susceptible to wiretap attack that one eavesdrops on communication information with illicit measures. The transmitted communication data that exists between the users or terminals and the system server are likely to disclose sensitive private information when insufficient protection provided or the implementation of protection is faulty[2].

2.4.4 Spoofing and Impersonation Attacks

Spoofing attacks occur when malicious actors masquerade as genuine users, devices or any other components of a network. Forging identities or communication signatures allows attackers to attain unauthorized access, modify network operations and propagate inaccurate information. A key vulnerability for the spoofing attacks is with device spoofing in large-scale M2M environments[3].

2.4.5 Data Manipulation and Integrity Attacks

Attackers might also modify the data packets that have been sent or insert bad data into the lines of communication. In these kinds of attack the contents are attacked and the resulting changes might have harmful consequences in automatic decision making, which may happen on autonomous driving systems, industrial automation, or smart transportation systems [10].

2.4.6 Adversarial Attacks on AI Models

As AI will also be widely utilized in the future 6G systems, AI models have become the target of adversarial attacks. Attackers try to craft some samples (attacked data) which cause machine learning models to make wrong prediction or security decision when feeding attacked data to them[17]. These adversarial attacks cause a great performance reduction in AI-based IDS and risk mitigation techniques[13].

2.4.7 Model Poisoning Attacks

In such collaborative training environment (e.g., federated learning), a malicious user can poison his or her training data and send the contaminated training data and corrupted model update to participants[7]. Such attacks against the model, e.g., model poisoning, may degrade the accuracy of the intelligent systems[7].

2.4.8 Privacy Leakage Attacks

These massive amounts of personal, behavioral and positional data generated will continuously flow into these networks, and security at any of these points may give access to the data for private information and stolen identities of users[6]. Security needs to be built into any future communication networks.

Table 1. Security Threats in 6G Networks

Threat Type	Description	Affected Communication	Impact
DDoS Attack	Flooding network resources	H2H, H2M, M2M	Service disruption
Spoofing	Fake identity impersonation	H2M, M2M	Unauthorized access
Eavesdropping	Interception of transmitted data	H2H	Privacy leakage
Data Manipulation	Alteration of communication data	H2M, M2M	Integrity loss
Adversarial AI Attack	Manipulation of AI models	All	Incorrect decisions
Model Poisoning	Corrupted training updates	M2M	Reduced model accuracy
Privacy Leakage	Exposure of sensitive data	All	Confidentiality breach

Table 1 depicts the main security threats of 6G networks and their consequences on the three environments H2H, H2M and M2M. It shows the increased sophistication of threats in the future.

2.5 Summary of Security Challenges

Security of 6G Networks Compared to past generations of wireless networks, security of 6G is much more intricate, owing to incorporation of edge computing, IoT, artificial intelligence, massive machine communication etc [20]. Security issues related to H2H, H2M, M2M environments that are to be taken care are: authentication attacks, DDOS attacks, spoofing, snooping, manipulation, adversarial machine learning attacks and leaking out private data. The future generations are expected to secure and manage those high dynamic and scaled up 6G environments with such intelligent, adaptive, privacy enhancing methods. In the subsequent segment, we would study about different approaches of RL based network security solutions for 6G Networks.

3. Intelligent Security Approaches For 6G

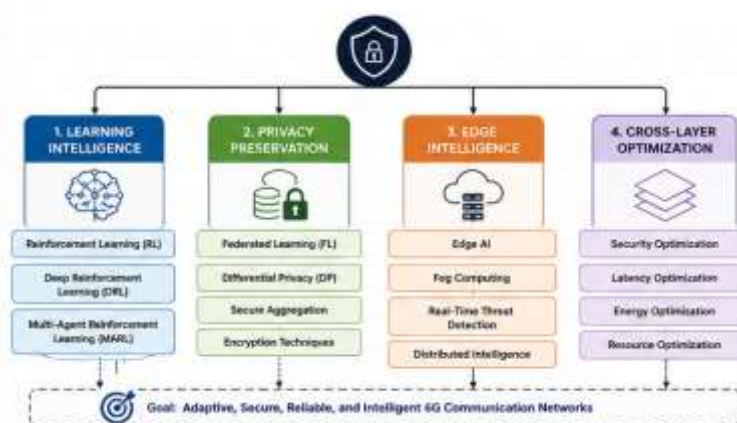


Figure 2. Taxonomy of Intelligent Security Frameworks in 6G

Taxonomy of intelligent security frameworks in 6G networks is depicted in Fig. 2. These security solutions are classified into reinforcement learning based frameworks, privacy preserving frameworks, edge intelligent based frameworks and cross layer optimization frameworks. With complexity of the 6G networks and the security threats are evolving, the security mechanisms need to be adaptive in nature to counter these new threats and varying network conditions. Conventional network security mechanisms rely mainly on predefined rules and signature, which are incompetent in facing unseen and unknown attacks. This led the researchers to explore the concepts of artificial intelligent (AI) and machine learning (ML) for network intelligent security. In the AI domain, techniques of Reinforcement learning (RL), Deep Reinforcement learning (DRL), and Multi-agent Reinforcement learning (MARL) have gained research community's focus since these techniques learn optimum policies through an online process and interactive mechanism.

Autonomous threat detection, allocation of dynamically adjustable resources, blocking intrusions, making intelligent real-time decisions is achievable through smart security paradigms. It becomes indispensable in the context of 6G where number of intelligent services and billions of devices and intelligent edges generate and exchange data [12].

3.1 Reinforcement Learning-Based Security

Reinforcement Learning (RL) is a type of machine learning where a system called an agent interacts with an environment. Actions the agent takes lead to either rewarding or punishing signals, and the agent tries to figure out how to best behave in each state to achieve a cumulative reward[1]. In 6G security, RL-based methods could keep tracking the current state of the network and take automatic measures to cope with new types of attacks. It avoids the problem of need to get the pre-labeled data, that makes it appropriate to the highly dynamic and unpredictable nature of the network environment in which the RL needs to adapt automatically to these changes.

Several security applications of RL in 6G networks include:

- Dynamic Intrusion Detection
- Adaptive Authentication Systems
- Spectrum Access Control
- Optimal secure routing
- Resource Allocation in presence of security constraints

Cyber Attack Control RL based security system learn the behavior of the system or the network and can respond to a threat intelligently and dynamically without human intervention and ensure the higher availability and lesser risk for the system/network.

3.2 Deep Reinforcement Learning Techniques

While traditional RL algorithms can be applied to the relatively simple environment, they are unable to deal with the high-dimensional state spaces of 6G networks. By combining deep neural networks (DNNs) with RL algorithms [9], DRL algorithms can be designed to perform deep feature extraction from massive data, automatically obtain high-level abstract representations and perform intelligent decision-making in real-time. DRL agents have the ability to adapt to various dynamic topologies, a large number of heterogeneous devices and the changing environments.

The main DRL algorithms that have been used in network security attacks detection and defense include

- (i) Deep Q-Network (DQN) [10];
- (ii) Double Deep Q-Network (DDQN) [11];
- (iii) Deep Deterministic Policy Gradient (DDPG) [12];
- (iv) Proximal Policy Optimization (PPO) [13];
- (iv) Actor-Critic Algorithms (ACA) [14].

In 6G networks, DRL has already demonstrated the potential application in: intelligent threat detection; adaptive network defense; secure spectrum sharing; autonomous resource management; and energy-efficient communication security [15]. Owing to the mechanism that allows continuously self-improvement, DRL algorithms is a highly attractive and promising technology for the next generation of intelligent communication systems.

3.3 Multi-Agent Learning Approaches

Future 6G networks would feature a vast number of connected devices, edge servers, base stations, and intelligent agents working together concurrently. In these distributed scenarios, there would not be one learning agent capable of handling the network security requirements. Multi-Agent Reinforcement Learning (MARL) addresses this limitation as it allows multiple agents to cooperate in learning [13]. In MARL environments, each agent observes and adapts to its local view, learning from and sharing its insights with others to jointly pursue the common network security objectives. Such distributed learning enables increased network adaptability, scalability, and threat awareness.

Applications of MARL in 6G security include:

- Cooperative intrusion detection
- Distributed attack prevention
- Secure edge computing
- Multi-domain resource allocation

Multi-agent cooperative threat Intelligence MARL decrease decision time by delegating tasks for training and learning on different agent that would enhance efficiency for security and large-scale networks.

3.4 Advantages and Limitations of Intelligent Security Approaches

The Benefits of Intelligent Security There are several benefits that intelligent security solutions have over other more traditional security systems: They are inherently adaptive and able to provide appropriate responses to unidentified threats and dynamic network environments. Intelligent security systems are designed to automate and streamline the administration of security and decrease the need for human involvement. Security systems that are intelligent can also constantly enhance and improve their security performance.

Advantages

- Adaptive threat Detection and response
- Capability to perform decisions on the fly
- Network's defense in an autonomous manner
- High scalability required for a very large network
- Optimized use of resources
- Minimize the use of rule defined manually

But still some limitations still need to be handled.

Limitations

- High computational complexity
- Large training data requirements
- Slow convergence in dynamic environments
- Partial observability of network states
- Vulnerability to adversarial attacks
- Privacy concerns during collaborative learning

In addition, reinforcement learning algorithms can suffer from a performance hit if feedback received is slow or partial, and intensive deep learning computations can preclude implementation on constrained devices such as at the edge.

3.5 Comparative Analysis of Intelligent Security Techniques

The diverse intelligent security methods have varied advantages and disadvantages. The traditional reinforcement learning approaches offer intuitive and understandable learning process, but may fail in the large complex networks. The decision-making precision of deep reinforcement learning approach is further improved by the use of deep neural network at the cost of higher computation overhead. The distributed agents in multi-agent reinforcement learning system lead to better scalability, enhanced co-operative and robustness with high communication overhead and co-ordination requirements. Thus, more recently the interest is shift to hybrid approach based on DRL, federated learning, edge intelligence, and privacy-aware techniques to overcome these limitations. Such intelligent integrated framework will play important role for 6G network security.

Table 2. Reinforcement Learning-Based Security Solutions

Technique	Advantages	Limitations	Applications
RL	Adaptive learning	Slow convergence	Intrusion detection
DRL	Handles large state spaces	High complexity	Threat mitigation
DQN	Improved decision-making	Training overhead	Resource allocation
PPO	Stable learning	Computational cost	Secure routing
MARL	Distributed intelligence	Coordination complexity	Multi-agent security

6G intelligent security solutions for protection with reinforcement learning In Table 2, several ML strategies for intelligent security in the 6G network are contrasted with their corresponding pros, cons, and primary domains. Overall, Intelligent Security strategies, especially using reinforcement learning (RL), deep reinforcement learning (DRL), and multi-agent reinforcement learning (MARL), have great potential in making intelligent security of next-generation communications (6G) much robust to any kinds of cyberattacks due to intelligent learning capabilities, and their autonomy, adaptivity and responsiveness make it necessary for future intelligent security infrastructure. Yet, issues on the privacy protection, computational efficiency, and scalability of the RL/DRL/MARL solutions are remaining as the critical research issues for a trustworthy and efficient intelligent security management system. In the next section, some solutions concerning privacy-preserving techniques and edge intelligence methods to make it more trustworthy and efficient will be presented.

4. PRIVACY PRESERVATION AND EDGE INTELLIGENCE

The 6G communication networks are moving toward highly intelligent and interconnected ecosystem, with vast amounts of personal, industrial and operational data continuously being produced and shared among users, devices and network infrastructure. Services, such as smart healthcare, autonomous vehicles, industrial automation and digital twin, are constantly sharing large amounts of data in order to make intelligent decisions and deliver efficient services. The vast amount of collecting and processing of personal data will definitely result in a series of privacy issues. It is harmful to trust and security if private data leak or are abused. Hence, privacy-preservation is an inevitable concern for 6G communications. Edge intelligence that allows processing data and executing machine intelligence functions on edge devices is gaining popularity with ever-increasing demand for real-time and ultra-low-latency communication. Moreover, edge intelligence brings several benefits, such as, reduced latency, improved security due to localized attacks and less dependence on network server for sensitive computation. Consequently, combining privacy-preserving techniques and edge intelligence can create a unified and effective mechanism of intelligent security for the 6G communication systems.

4.1 Federated Learning

Federated Learning (FL) A training method for ML, whereby several devices or network components, that cannot share their raw, privacy-sensitive, data to each other, collaboratively train a central model[15]. The mobile entities train the model locally on their local data, without transmitting any sensitive user information to the centralized system. Instead, they only update the

parameters of the trained model to send to the global model at the server. As user data resides locally at the mobile devices, the risk associated with privacy is greatly decreased. In 6G, federated learning is a perfect solution for applications where privacy is an issue, such as healthcare applications, autonomous vehicles, smart cities and industrial IoT systems[16]. Top reasons to use federated learning: Increased data privacy Decreased communication load Data privacy regulation adherence distributed intelligence for distributed AI Systems with a large number of devices However, FL is susceptible to a range of attacks, including model poisoning attacks, data inference attacks and malicious parameter modification, making additional privacy techniques required.

4.2 Differential Privacy

Differential Privacy (DP) Differential privacy (DP) is a method of preserving privacy in datasets or updates to learning models by adding a carefully calculated amount of random noise. Its main goal is to make it impossible for malicious parties to deduce specific information from any particular individual, but still retain overall utility. Differential privacy is often used in the context of federated learning to protect local model updates before they are transmitted to an aggregate server, thus making it harder for attackers who intercept the transmitted parameters to reconstruct the initial data. Advantages of Differential Privacy are: Information Leakage Prevention Inference Attack Protection Improved Individual User Privacy Compatibility with Distributed Learning Systems There's a potential downside however: adding too much noise to the model may decrease its learning accuracy.

4.3 Secure Aggregation

Secure aggregation A cryptographic method for multiple participants to submit their model updates, without making their individual contributions visible. In this approach, model updates from the participants are encrypted and transmitted to the server for aggregation, ensuring only aggregated results can be viewed by the latter. Secure aggregation helps in further enhancing the privacy guarantee for federated learning. The server and any third parties will not be able to know the individual parameters of a specific participant's model. This is a key technique for collaborative model training for intelligent security model development in a large scale 6G systems by several participants. Advantages: local model updates are confidential risk of information leakage is minimized trust among participants can be enhanced confidentiality in collective learning improves Disadvantages: the communication and computation burden in a large scale environment.

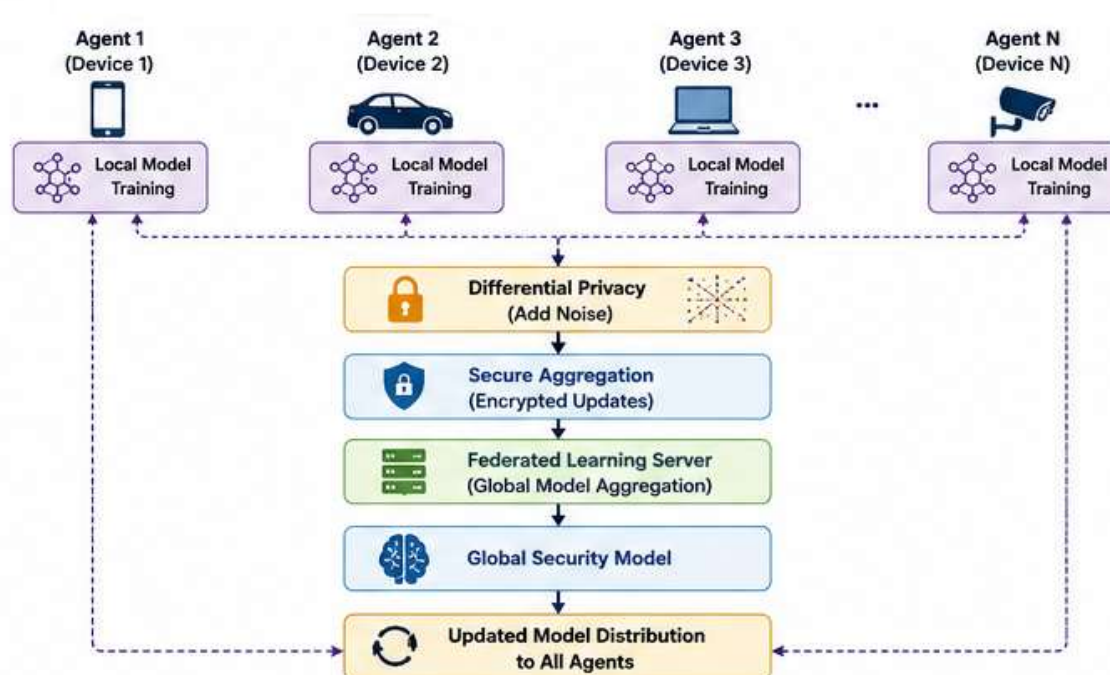


Figure 3. Privacy-Preserving Multi-Agent Learning Architecture

The system architecture illustrated in Fig.3 describes an illustration of how different agents can collaborate together with sharing and exchanging the knowledge in the system to update and retrain their models, preserving data privacy using different approaches such as differential private federated learning, and secure aggregation technique, to ensure that no confidential data leaks out.

4.4 Edge Intelligence for Secure Communication

Edge Intelligence (EI) It entails extending intelligent computation capabilities to edge environments that are in close proximity to users and edge devices. EI offers several advantages, including reducing the communication overhead and the latency associated with communication by processing data closer to the data's source rather than transmitting everything to the cloud server[11]. Edge intelligence enables rapid response and real-time operation in 6G, for instance, by securing edge computing for a fast, real-time attack detection and response, thus avoiding frequent updates of remote servers[19]. ApplicationsEI in 6G Security. • Real time intrusion detection• Intelligent anomaly detection• Secure Resource Allocation• Adaptive Access control• Autonomous Threat detection and mitigationsAdditionally, edge intelligence will reduce the transmission of sensitive information on the network and thus, enhance the security and the protection of the transmitted information.

4.5 Challenges in Privacy Preservation and Edge Intelligence

While privacy-preserving and edge intelligence solutions can yield a great number of benefits, there exist many unanswered challenges in these areas.

Challenges in Privacy

- The possibility of model inversion attacks.
- Vulnerability to poisoning attacks.
- The dilemma of a privacy-utility trade-off.
- Heterogeneity in the capabilities of devices.
- Low degree of trustworthiness between stakeholders.

Challenges in Edge Intelligence

- The constraints on edge devices resources.
- Limited processing power and speed at edge devices.
- Concern over energy consumption.
- The complexity of the distributed management of edge devices.
- Security at the edge nodes of network.
- The consistency of security policy over a number of distributed edge devices at a large 6G environment.

4.6 Comparative Analysis of Privacy-Preserving Techniques

There are a variety of privacy-preserving solutions available, which are varying in security, computational overhead, and implementation difficulty. Federated learning[5] can achieve intelligence in a decentralized manner and avoid the direct transmission of massive data; Differential privacy[6] can guarantee privacy by adding noise; secure aggregation[6] can protect model updates via cryptology when transmitted; edge intelligence[7] can facilitate the local process in the device and avoid the massive data transmission.

Table 3. Privacy-Preserving Techniques Comparison

Technique	Privacy Level	Computational Cost	Advantages
Federated Learning	High	Medium	Data remains local
Differential Privacy	Very High	Low	Prevents data inference
Secure Aggregation	High	Medium	Protects model updates
Homomorphic Encryption	Very High	High	Computation on encrypted data
Blockchain	High	High	Tamper-resistant records

Table 3 lists the privacy-preserving technologies used in Distributed Learning, which considers the privacy protections offered (privacy protection), the computational cost and its usefulness.

In conclusion, these new technologies for privacy preservation and edge intelligence play a very crucial role in shaping the future 6G security architectures. These new mechanisms like federated learning, differential privacy and secure aggregation can provide us the statistical techniques to protect and assume the access to information efficiently during the process of distributed learning, whereas edge intelligence offers us the primary means of security, with execution at real time and localized mechanism. Combining all these facets in a proper manner can lead to a much more secure and more energy/latency efficient next generation communication. Nonetheless, challenges regarding scalability, computational overhead, security management are still active research areas. In the subsequent section, the cross-layer optimization techniques to enhance the security performance with reduced latency and energy cost will be discussed.

5. CROSS-LAYER OPTIMIZATION FOR SECURE 6G NETWORKS

Security in 6G networks isn't the only key component: efficient usage of resources in the network is also essential. To that extent, 6G is foreseen to enable ultra reliable low latency communication, massive machine-type communication, intelligent services, and energy efficient functionality. However, to implement stringent security, some overhead on computational complexity, delay, and energy has to be accounted for. Hence, a thorough balance between security, performance, and resource efficiency became an important challenge [3]. Conventional networks mostly view each layer in protocol separately from the others with no cross-interaction amongst them. This layered architecture simplifies the network management but often fails to efficiently utilize the available resources and make ideal choices for security guarantees. Cross-layer optimization attempts to solve such problems by exchanging information between different layers and coordinated decision-making among various layers in communication stack.

5.1 Concept of Cross-Layer Security

Cross-layer security involves the integrated application of security mechanisms across various layers of a communication network such as physical, data link, network, transport, and application layer. Instead of the isolated application of security mechanisms, cross-layer security allows exchanging information between layers to offer an intelligent and dynamic form of security. For example, physical layer data including signal quality and jamming levels can be correlated with network-level data patterns, including traffic and application-level behaviour. This comprehensive perspective can lead to a higher detection rate of malicious attacks, including those which would not be detectable in any single layer in isolation. The primary goals of cross-layer security are : Enhanced threat detection Better resource efficiency Lower security overhead Increased robustness, flexibility and adaptability.

5.2 Security-Latency Trade-off

Among the core characteristics of 6G network will be the extremely low communication latency that supports time-critical applications like autonomous driving, remote surgery, and industrial automation, and extended reality (ER). The utilization of cutting edge security protocols including encryption, authentication, and privacy-preserving mechanism can have an adverse effect on the communication delay. Generally speaking, stricter and more comprehensive security algorithms provide better security at the expense of higher complexity and thus, communication delay and transmission time. Cross-layer optimization techniques offer potential to solve this trade-off between security and latency, where the network entity dynamically adapt the

security requirements according to various network context and application types. Critical applications could afford higher latency while still have the most secure protocol, whereas the time-unaware application can still maintain low communication delay by adopting simpler security mechanism. An ideal solution needs to satisfy these requirements: Minimum communication delay; Quickly identify threats; Efficient authentication procedures; Real-time security decisions; Ultimately, the trade-off between security and latency would still be a challenging issue for 6G communications.

5.3 Security-Energy Trade-off

Device security for IoT requires low power consumption because the device runs on a finite battery. Encrypting, authenticating and performing ML to detect malware uses lots of energy[8]. 6G security models with ML-trained networks may result in higher power consumption since this is calculation-intensive. With more connected devices, this will pose serious energy constraints on 6G devices. Smart cross-layer design approaches can lower power consumption by: dynamically allocating network resources; adapting to dynamic threat situation level by altering security parameters; controlling schedules for transmissions; utilizing edge computation instead of on-device execution; reduce non-critical security measures.

5.4 Resource Allocation Optimization

Optimal Resource Allocation The security and reliability of communication in 6G networks require optimal allocation of network resources. This includes careful utilization of limited resources like available bandwidth, spectrum, computation capabilities and transmission power to cater for a variety of services and applications. Various algorithms can be used to facilitate Intelligent Resource Allocation by ensuring timely prioritization of security-relevant tasks and a robust network performance. Reinforcement learning and other optimization schemes, are increasingly utilized for flexible and adaptable resource assignment as a function of real time network parameters and the present level of threat. Typical optimisation criteria used for allocation include: - Maximisation of network throughput - Minimisation of packet loss - Minimisation of energy consumption - Optimisation of security related performance metrics - Maximisation of quality of service (QoS) Cross-layer optimisation makes it possible to better manage all the parameters concurrently so that overall network resource efficiency may be achieved.

5.5 Existing Cross-Layer Optimization Approaches

Several cross-layer optimization methods have been suggested by researchers to enhance secure and efficient communications in future communication networks. They can mainly be split into: (a) artificial intelligence techniques (e.g., fuzzy logic, neural network etc.), (b) edge computing capabilities and (c) dynamic resource allocation approaches.

Some commonly adopted strategies include:

AI-Based Cross-Layer Optimization

Artificial intelligence methods are used to assess network states and automatically adapt security policies, transmission factors and decisions on the allocation of resources.

Reinforcement Learning-Based Optimization

The reinforcement learning agents proactively learn effective methods of security and resource management through interactions with the network environment.

Edge-Assisted Optimization

Edge computing platforms offer local processing and decision making of computing services so that delays have been reduced in the communication process and resources are best utilized.

Multi-Objective Optimization

Multi-objective optimization approaches incorporate energy, security, throughput, payload, and reliability into the same optimization process. More specifically, operational conditions with efficient trade-offs among said parameters can be obtained. It is thought that these methods lead to the evolution of performance driven, intelligent and flexible secure architectures which can satisfy the onerous requirements of 6G networks [6].

5.6 Comparative Analysis of Cross-Layer Optimization Techniques

In practice, various optimization techniques provide different capabilities in terms of efficiency, performance, and computational cost. The performance gains of AI techniques vary due to intelligence and flexibility but at the cost of significantly greater computational requirements. Learning algorithms such as reinforcement learning support unsupervised optimization but usually necessitate a very lengthy training phase. By leveraging an edge environment to perform computations closer to devices, edge-assisted optimization techniques offer lower latency and higher responsiveness while a multi-objective optimization can provide the optimal trade-off among a list of criteria [1].

Table 4. Cross-Layer Optimization Approaches

Approach	Objective	Benefits	Challenges
AI-Based Optimization	Dynamic resource management	Intelligent adaptation	High complexity
RL-Based Optimization	Security-aware decision making	Autonomous learning	Training time
Edge-Assisted Optimization	Reduce latency	Fast response	Limited resources
Multi-Objective Optimization	Balance security and performance	Improved efficiency	Complex implementation

Table 4 enumerates a variety of Cross-Layer Optimization techniques that intend to address the issue of security, latency, energy and general network performance improvements in the 6G network.

5.7 Summary

Cross-layer optimization has been regarded as an efficient paradigm to tackle diverse security and performance issues of 6G wireless communications. The technique of cross-layer facilitates the joint decisions across several protocol layers to enhance the effectiveness of threat detection, resource allocation, energy efficiency and communication performance. Balancing the trade-off among security, delay and energy is critical for some future 6G applications including autonomous driving, smart city, industrial internet of things and enhanced virtual or augmented reality. As a consequence of various potential trade-offs and security/performance trade-offs, cross-layer technologies still has a range of challenges, such as computational complexity, scalability and real-time adaptation to dynamic network environments. In particular, there are great needs for development of integrated intelligent security system for secure, efficient and scalability.

6. RESEARCH GAPS AND FUTURE DIRECTIONS

The surveyed literature confirms that reinforcement learning based security, privacy preserving learning, edge intelligence and cross-layer optimisation techniques have made rapid progress in the 6G communication networks. Nevertheless, majority of the currently available literature studies each field separately and has failed to overcome the challenges in providing holistic security frameworks and adaptability of security mechanism for 6G Networks. The future research direction and remaining gaps are identified from analysis made in the previous section.

Table 5. Research Gaps and Corresponding Future Directions

Gap ID	Research Gap	Observations from Existing Studies	Future Research Need
G1	Lack of Unified Security Frameworks	Most studies focus on individual technologies	Integrated intelligent security architecture
G2	Limited Adaptability	Existing models struggle in dynamic environments	Adaptive DRL and online learning

G3	Privacy-Security Trade-Off	Strong privacy may reduce model performance	Balanced privacy-preserving learning
G4	AI Model Vulnerability	Susceptible to adversarial and poisoning attacks	Trustworthy and robust AI security
G5	Scalability Issues	Evaluated in small-scale environments	Massive IoT-ready architectures
G6	Computational Overhead	High resource and energy consumption	Lightweight security mechanisms
G7	Limited Cross-Layer Integration	Independent optimization approaches	Unified cross-layer security design

Table 5 identifies the research gaps found from the literature and suggests future research directions. It guides us to designing a generic integrated intelligent security architecture framework of 6G Networks. The GAPs identified in table 5 is the motivations for us to study the integrated intelligent security frameworks for 6G Communication Networks. Namely, G1, G2 are motivate us to develop adaptive Reinforcement learning approaches, G3, G4 are motivate us to develop trustworthy and Privacy-preserving AI approaches, and G5-G7 are motivated us to use scalable edge intelligence and Cross-layer optimization approaches.

6.2 Future Directions

With reference to the identified research gaps, future research directions on the design of 6G security framework have good prospect.

6.2.1 Privacy-Preserving Reinforcement Learning

Additional studies should focus on combining reinforcement learning with privacy technologies, such as federated learning, differential privacy, and secure aggregation, to build smart and sensitive decision making frameworks.

6.2.2 Explainable Artificial Intelligence for Security

Majority of AI in security systems use a black-box model, making it nearly impossible to know how the system reaches a conclusion. Explainable Artificial Intelligence (XAI) offers greater trust, transparency, and accountability in the security decision and prediction of security threats through clear explanations.

6.2.3 Edge-Enabled Intelligent Security

Using intelligent security mechanisms at network edges can potentially reduce communication overheads and speed up response time. More research should be done on designing light AI models that perform effectively on resource-constrained edge devices without compromising security quality.

6.2.4 Secure Multi-Agent Learning Systems

Given that intelligence becomes more distributed in future 6G networks, multi-agent learning will find more application in cooperative security management. Further research will need to be undertaken to develop robust coordination mechanisms, trust establishment protocols and secure information exchange for multiple learners.

6.2.5 Quantum-Resistant Security Mechanisms

Existing cryptography techniques, such as asymmetric crypto algorithms that make digital signatures possible, are currently vulnerable to advances in quantum computers. Next-generation 6G will need to include quantum-resistant cryptography methods for ensuring secure data transfer and mitigating new forms of attack enabled by future technology.

6.2.6 Energy-Efficient Security Frameworks

Energy will continue to be one of the challenges for future communication system designs. Lightweight security solution with limited computational complexity but high security performance should be proposed by researchers. Combining edge intelligence and resource-aware optimization may achieve it.

6.2.7 Integrated Cross-Layer Security Optimization

Future security architecture should mutually enhance security, delay, energy consumption, reliability and utilization within different layers of networks. The cross-layer interaction designs of such integrated security architectures can provide more powerful and adaptive defenses for complex security threats.

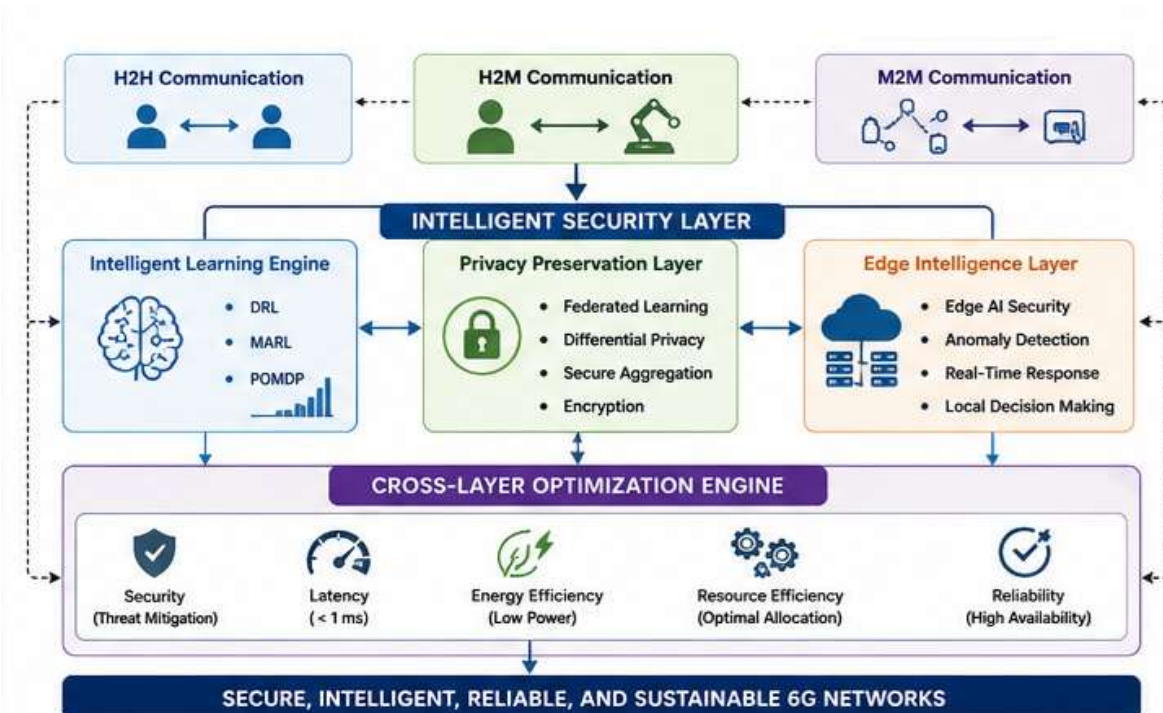


Figure 4. Future Integrated Security Framework for 6G

The architecture of future integrated security solution is described in figure 4, which can offer scalable, secure and dynamic protection capabilities for the 6G communication networks by combining machine learning, privacy preserving technologies, edge intelligence, cross-layer optimization techniques.

6.3 Research Roadmap for Intelligent Security in 6G Networks

The identified research gaps and current technological trends help to formulate a multi-stage research road-map to facilitate intelligent security framework of 6G communication systems, as illustrated in Fig. 1. Specifically, the 6G intelligence security development can be divided into three levels: baseline security modeling, privacy-preserving intelligent security, and edge-enabled cross-layer optimization.

Stage 1: Baseline Security Modeling

- Extensive analysis and discovery of security threats and vulnerabilities.
- Implementation of AI based intelligent threat identification and prevention methods.
- Experimental performance evaluation in multiple communication contexts.

Stage 2: Privacy Preserving Intelligent Security

- Incorporate with technologies such as Federated Learning (FL), Differential Privacy (DP) and Reinforcement Learning (RL).
- Facilitate secure cross-device learning for distributed network devices.
- Intelligent learning models to improve the adaptability of security and threat detection.

Stage 3: Edge Enabled Cross Layer Optimization

- Employ edge intelligent devices for prompt and real-time decision making.
- Design of low cost and lightweight security schemes.
- Simultaneous optimization of security, delay, energy consumption and resource utilization. The outlined roadmap provides a progression toward the development of a comprehensive and intelligent, scalable and privacy-conscious security system which are crucial to satisfy the stringent security and performance requirements in future 6G communications.

6.4 Summary

Despite great breakthroughs have been made in intelligent security research for 6G communication networks, there are still many challenges such as scale, privacy, computation efficiency, AI reliability and cross-layer collaboration. While existing research has attempted to deal with these challenges independently, it is essential to develop an end-to-end integrated architecture to address the challenges together. For future work, it is necessary to further combine Reinforcement learning, privacy-preserving techniques, edge intelligence, cross-layer optimization, and design a holistic security system to support smart, secure and efficient services in 6G networks.

7. CONCLUSION

The next-generation 6G communication systems are envisioned to usher in the future of wireless communications with unprecedented data rates, extremely low latency, enormous connection, and intelligent network orchestration. The aforementioned capabilities promise a plethora of advanced applications including autonomous vehicle, smart cities, industrial automation, digital twins, extended reality (XR), intelligent healthcare services, and many more. Nevertheless, the complexity, heterogeneity and massive scale of the 6G ecosystems, coupled with unprecedented security and privacy challenges that conventional security techniques fail to handle efficiently. This survey discusses the paramount security challenges, the threat landscape associated with the human-to-human (H2H), human-to-machine (H2M), and machine-to-machine (M2M) communications within the 6G ecosystems. Various cyber attacks including authentication attacks, spoofing, eavesdropping, distributed denial of service (DDoS), data manipulation, adversarial ML based attacks, and privacy leakages were discussed, revealing an evolution of the security requirements in future-generation networks. It further analyses various intelligent security approaches in terms of Reinforcement Learning (RL), Deep Reinforcement Learning (DRL) and Multi-Agent Reinforcement Learning (MARL) that could aid in detection of the unknown and novel threats, autonomous decision making, resource management and intrusion prevention in dynamic environment of communication networks. The potential benefits of privacy-preserving technologies such as Federated Learning (FL), Differential Privacy (DP) and Secure Aggregation for information protection while conducting decentralized learning processes were also discussed. Edge intelligence is one of the critical research topics to realize in-situ security and minimize communication delays, therefore its Role in security operation was analyzed. Similarly cross-layer optimization approaches considering security along with latency, energy consumption and resource utilization, are fundamental for an optimized communication process. Despite the significant progress made, some research gaps and remaining challenges were identified, including lack of scalability, high computational complexity, a privacy-security trade-off issue, vulnerable ML based security mechanisms, and fragmentation among current security techniques. Consequently, based on these identified research gaps, the future research directions should focus on the development of unified intelligent security frameworks that integrate all intelligent technologies such as RL, privacy-preserving methods, edge intelligence and cross-layer optimization to provide robust, adaptive, scalable, energy-efficient and privacy-aware security solutions that address the needs of future 6G systems. We believe that the insights of this survey would guide researchers and practitioners on their journey toward developing next-generation secure and intelligent wireless communications system.

ACKNOWLEDGEMENT:

FUNDING INFORMATION:

This research was no support from any funding agencies.

CONFLICT OF INTEREST:

Authors here by declared that, there is no conflict of interest.

REFERENCE:

- [1] Lu, X., Xiao, L., Li, P., Ji, X., Xu, C., Yu, S., & Zhuang, W. (2022). Reinforcement learning-based physical cross-layer security and privacy in 6G. *IEEE Communications Surveys & Tutorials*, 25(1), 425-466.
- [2] Mao, B., Liu, J., Wu, Y., & Kato, N. (2023). Security and privacy on 6G network edge: A survey. *IEEE communications surveys & tutorials*, 25(2), 1095-1127.
- [3] Mustafa, R., Sarkar, N. I., Mohaghegh, M., & Pervez, S. (2024). A cross-layer secure and energy-efficient framework for the internet of things: A comprehensive survey. *Sensors*, 24(22), 7209.
- [4] Liu, Y. J., Du, H., Xu, X., Zhang, R., Feng, G., Cao, B., ... & Tafazolli, R. (2025). A survey of integrating generative artificial intelligence and 6G mobile services: Architectures, solutions, technologies and outlooks. *IEEE Transactions on Cognitive Communications and Networking*, 11(3), 1334-1356.
- [5] Balaji, C. G., Menaka, S., Rajeswari, G., & Ponnusamy, S. (2025). A unified AI-driven framework for quantum-secured 6G THz networks with intelligent reflecting surfaces and federated edge learning: *Scientific Reports*, 15(1), 42510.
- [6] Blika, A., Palmos, S., Doukas, G., Lamprou, V., Pelekis, S., Kontoulis, M., ... & Askounis, D. (2024). Federated learning for enhanced cybersecurity and trustworthiness in 5G and 6G networks: A comprehensive survey. *IEEE Open Journal of the Communications Society*, 6, 3094-3130.
- [7] Allaw, Z., Zein, O., & Ahmad, A. M. (2025). Cross-layer security for 5g/6g network slices: An sdn, nfv, and ai-based hybrid framework. *Sensors*, 25(11), 3335.
- [8] Jiao, L., Shao, Y., Sun, L., Liu, F., Yang, S., Ma, W., ... & Guo, Y. (2024). Advanced deep learning models for 6G: Overview, opportunities, and challenges. *IEEE Access*, 12, 133245-133314.
- [9] Abdullahi, A. D., Bahrami, E., Dargahi, T., Al-Khalidi, M., & Hammoudeh, M. (2025). Interplay Between Security, Privacy and Trust in 6G-Enabled Intelligent Transportation Systems. *IEEE Open Journal of Intelligent Transportation Systems*, 6, 1625-1654.
- [10] He, C., Wang, W., Jiang, W., He, Z., Wang, J., & Xie, X. (2025). Security for the Internet of Vehicles with Integration of Sensing, Communication, Computing, and Intelligence: A Comprehensive Survey. *Sensors*, 25(16), 5119.
- [11] Senthilkumar, P., Sheela, V., Praveenkumar, G. D., Bostani, A., Tukhtaeva, N., Nalini, M., & Karpagam, M. (2025). Artificial Intelligence-Empowered Digital Twins For Simulation-Driven Security, Privacy, And Resiliency Optimization In 6g Networks. *Archives for Technical Sciences/Arhiv za Tehnicke Nauke*, (34), 1006.
- [12] Kalodanis, K., Papapavlou, C., & Feretzakis, G. (2025). Enhancing Security in 5G and Future 6G Networks: Machine Learning Approaches for Adaptive Intrusion Detection and Prevention. *Future Internet*, 17(7), 312.
- [13] Kuldip, D., Dhurendra, P., Prashant, K., & Sachin, R. (2025). AI-Driven Spectrum Intelligence and Energy Optimization Techniques for 6G Networks: A Comprehensive Review. *Radius: Journal of Science and Technology*, 2(2), 252002.
- [14] Wymeersch, H., Saleh, S., Nimr, A., Halili, R., Berkvens, R., Moghaddam, M. H., ... & Fettweis, G. P. (2024, March). Joint communication and sensing for 6G-A cross-layer perspective. In *2024 IEEE 4th International Symposium on Joint Communications & Sensing (JC&S)* (pp. 01-06). IEEE.
- [15] Duan, Q., Huang, J., Hu, S., Deng, R., Lu, Z., & Yu, S. (2023). Combining federated learning and edge computing toward ubiquitous intelligence in 6G network: Challenges, recent advances, and future directions. *IEEE Communications Surveys & Tutorials*, 25(4), 2892-2950.
- [16] Zhao, C., Du, H., Niyato, D., Kang, J., Xiong, Z., Kim, D. I., ... & Letaief, K. B. (2024). Generative AI for secure physical layer communications: A survey. *IEEE Transactions on Cognitive Communications and Networking*, 11(1), 3-26.
- [17] Ogenyi, F. C., Ugwu, C. N., & Ugwu, O. P. C. (2025). A comprehensive review of AI-native 6G: integrating semantic communications, reconfigurable intelligent surfaces, and edge intelligence for next-generation connectivity. *Frontiers in Communications and Networks*, 6, 1655410.

- [18] Saeed, M. M., Saeed, R. A., Hasan, M. K., Ali, E. S., Mazha, T., Shahzad, T., ... & Hamam, H. (2025). A comprehensive survey on 6G-security: Physical connection and service layers. *Discover Internet of Things*, 5(1), 28.
- [19] Sandeepa, C., Zeydan, E., Samarasinghe, T., & Liyanage, M. (2024). Federated learning for 6G networks: Navigating privacy benefits and challenges. *IEEE Open Journal of the Communications Society*, 6, 90-129.
- [20] Mao, C., Mu, Z., Liang, Q., Schizas, I., & Pan, C. (2023). Deep learning in physical layer communications: Evolution and prospects in 5G and 6G networks. *IET Communications*, 17(16), 1863-1876.
- [21] Osorio, D. P. M., Ahmad, I., Sánchez, J. D. V., Gurtov, A., Scholliers, J., Kutila, M., & Porambage, P. (2022). Towards 6G-enabled internet of vehicles: Security and privacy. *IEEE Open Journal of the Communications Society*, 3, 82-105.