Ministère de l'enseignement Supérieur et de la recherche Scientifique
وزارة التعليم العالي والبحث العلمي

Université Badji Mokhtar – Annaba
Faculté de Technologie

Département Informatique

جامعة باجي مختار– عنابـــة
كـليـة التكنـولـوجيـا
قســم الاعلام الالـي

Thèse

Présentée pour obtenir le diplôme de

Doctorat Troisième Cycle

Filière : Informatique

Spécialité : Réseaux et Sécurité

Par :
SAKRAOUI Sabrina

Thème :

Une architecture basée Blockchain pour la sécurité des réseaux 6G

Thèse soutenue le 12/02/2026 devant le jury composé de :

N°	Nom et prénom	Grade	Etablissement	Qualité
01	Ghoualmi-Zine Nacira	Professeur	Université Badji Mokhtar - Annaba	Président
02	Derdour Makhlouf	Professeur	Université d'Oum el Bouaghi	Encadreur
03	Ahmim Ahmed	Professeur	Université de Souk Ahras	Co-encadreur
04	Hakim Bendjenna	Professeur	Université de Tébessa	Examinateur
05	Kerrache Chaker Abdelaziz	Professeur	Université Amar Telidji - Laghouat	Examinateur
06	Hafidi Mohamed	Professeur	Université Badji Mokhtar - Annaba	Examinateur

الملخص

تناقش هذه الأطروحة القضايا الأمنية المصاحبة لهندسة شبكة الجيل السادس الناشئة، والتي ستؤدي إلى تحقيق مكاسب غير مسبوقة في الاتصال والسرعة والذكاء. ومع استعداد شبكات الجيل السادس لتقديم عوالم شديدة الاتصال مع تريليونات الأجهزة، وزمن انتقال منخفض للغاية، وسعة بيانات هائلة، فإن تدابيرالأمن المركزية التقليدية لن تكون كافية لحماية الشبكات والمعطيات على حد سواء. لمعالجة هذا الأمر، تقدم هذه الدراسة أطرًا أمنية جديدة في شكل تقنيات البلوك تشين والذكاء الاصطناعي التي تعد دفاعات لامركزية وقابلة للتكيف والحفاظ على الخصوصية.

وتبدأ الدراسة بتحديد السمات المستقبلية لبنية شبكة الجيل السادس، والإشارة إلى نقاط الضعف الرئيسية مثل هجمات الشبكات فائقة الكثافة، والهجمات الإلكترونية المدعومة بالذكاء الاصطناعي، وهجمات التهديدات الكمية. يُقترح نظامان جديدان لكشف التسلل للدفاع ضد التهديدات. الأول، 6G-SecureIDS، يدمج نظام 6G-SecureIDS، التعلم الموحد والنقل الآمن للمعرفة عبر الأمن القائم على سلسلة الكتل لتمكين الكشف عن التهديدات الموزعة على حساب عدم وجود خصوصية للبيانات. أما الثاني، FBMP-IDS، فيقوم بتطوير الحل بشكل أكثر تعقيدًا بمساعدة الحوسبة متعددة الأطراف لتحقيق الحد الأدنى من تكاليف الحوسبة وزمن انتقال الاتصالات دون المساس بأداء الكشف العالي. بالإضافة إلى ذلك، تقدم الأطروحة TL2AB، وهو إطار عمل موثوق به وخفيف الوزن للمصادقة يدمج تقييم المخاطر القائم على الذكاء الاصطناعي مع التحقق من سلسلة الكتل لضمان إدارة آمنة وقابلة للتطوير للهوية في بيئات الجيل السادس الضخمة.

تُظهر التقييمات التجريبية أن كلا النظامين المقترحين يتفوقان على أطر عمل أنظمة تحديد الهوية التقليدية من حيث قابلية التوسع والمرونة والكفاءة، مما يؤكد إمكانات الحلول الأمنية اللامركزية لشبكات الجيل السادس. لا يوفر هذا العمل أساسًا قويًا لتأمين الاتصالات اللاسلكية من الجيل التالي فحسب، بل يمهد الطريق أيضًا للتطورات المستقبلية في تشفير ما بعد الكمية، وبروتوكولات الإجماع الموفرة للطاقة، وتقنيات تعزيز الخصوصية. في نهاية المطاف، تساهم هذه الأطروحة في نهج شامل وتطلعي لضمان تحقيق القدرات التحويلية لشبكات الجيل السادس بطريقة آمنة وجديرة بالثقة ومستدامة.

الكلمات مفتاحية : أمان الجيل السادس، والبلوك تشين، والخصوصية، وكشف التطفل، والتشفير، والخصوصية، والتشفير

Abstract

This thesis tackles the security issues that accompany the emerging 6G network architecture that will usher in unprecedented connectivity, speed, and intelligence gains. With 6G networks on a path to provide hyper-connected worlds with trillions of devices, ultra-low latency, and massive data capacity, traditional centralized security measures are proving ever more inadequate. To address this, the present study introduces new security frameworks in the form of blockchain and artificial intelligence technologies that are decentralized, adaptive, and privacy-preserving defenses.

The study begins with delineating the future attributes of 6G network architecture and referencing major vulnerabilities such as ultra-dense network attacks, AI-powered cyber-attacks, and quantum threat attacks. Two new intrusion detection systems are suggested to defend against the threats. The first, 6G-SecureIDS, integrates federated learning and secure knowledge transfer via blockchain-based security to enable distributed threat detection at the expense of no data privacy. The second, FBMP-IDS, more complexly elaborates on its solution with the assistance of multi-party computation to achieve minimal computation costs and communication latency without compromising high detection performance. Additionally, the thesis presents TL2AB, a trusted lightweight authentication framework that fuses AI-based risk evaluation with blockchain verification to ensure secure and scalable identity management in massive 6G environments.

Experimental evaluations validate that the two systems proposed in this research outperform conventional IDS frameworks in scalability, resilience, and effectiveness, proving the feasibility of distributed security solutions for 6G networks. This study not only sets a strong cornerstone to achieve future-proof wireless communication but also opens up avenues for further studies on post-quantum cryptography, green consensus protocols, and privacy-preserving technologies. In essence, this thesis provides a comprehensive and forward-looking solution to making the revolutionary promise of 6G networks a reality in a secure, dependable, and sustainable manner.

Keywords : 6G security, Blockchain, privacy, Intrusion Detection, Cryptography

---

Résumé

Cette thèse aborde les questions de sécurité qui accompagnent l'architecture émergente du réseau 6G, qui inaugurera une connectivité, une vitesse et des gains d'intelligence sans précédent. Alors que les réseaux 6G sont en passe de fournir des mondes hyperconnectés avec des trillions d'appareils, une latence ultra-faible et une capacité de données massive, les mesures de sécurité centralisées traditionnelles s'avèrent de plus en plus inadaptées. Pour y remédier, la présente étude introduit de nouveaux cadres de sécurité sous la forme de technologies de blockchain et d'intelligence artificielle qui sont des défenses décentralisées, adaptatives et préservant la vie privée.

L'étude commence par définir les futurs attributs de l'architecture du réseau 6G et fait référence aux principales vulnérabilités telles que les attaques de réseaux ultra-denses, les cyberattaques basées sur l'IA et les attaques de menaces quantiques. Deux nouveaux systèmes de détection d'intrusion sont proposés pour se défendre contre ces menaces. Le premier, 6G-SecureIDS, intègre l'apprentissage fédéré et le transfert sécurisé des connaissances via la sécurité basée sur la blockchain pour permettre la détection distribuée des menaces au détriment de la confidentialité des données. Le second, FBMP-IDS, élabore sa solution de manière plus complexe avec l'aide d'un calcul multipartite pour minimiser les coûts de calcul et la latence de communication sans compromettre les performances de détection élevées. En outre, la thèse présente TL2AB, un cadre d'authentification léger et fiable qui fusionne l'évaluation des risques basée sur l'IA avec la vérification blockchain pour garantir une gestion de l'identité sécurisée et évolutive dans les environnements 6G massifs.

Les évaluations expérimentales démontrent que les deux systèmes proposés surpassent les cadres IDS traditionnels en termes d'évolutivité, de résilience et d'efficacité, confirmant le potentiel des solutions de sécurité décentralisées pour les réseaux 6G. Ce travail fournit non seulement une base solide pour sécuriser les communications sans fil de la prochaine génération, mais ouvre également la voie à de futures avancées dans le domaine de la cryptographie post-quantique, des protocoles de consensus à faible consommation d'énergie et des technologies de renforcement de la protection de la vie privée. En fin de compte, cette thèse contribue à une approche globale et prospective visant à garantir que les capacités de transformation des réseaux 6G sont réalisées de manière sûre, fiable et durable.

Mots clés : Sécurité 6G, blockchain, vie privée, détection d'intrusion, cryptographie.

Table of Contents

List of Figures

List of Tables

General Introduction

As we stand at the dawning of the sixth generation wireless technology (6G), there seems to be a paradigm shift in the telecommunication space. Even as commercial 5G networks are recently starting to roll out worldwide, researchers and industry leaders are envisioning the transformative potential of 6G — expected anytime in the next decade — that can bring extremely high speed data rates, ultralow latency communications, and essentially complete connectivity for a new breed of use cases [11]. But as technology advances, so do security threats, and in increasingly complicated ways that require equally innovative answers. The 6G networks are anticipated to provide functionalities that will change the face of our connected world as we know it [12]. From a theoretical peak of 1 terabit per second to enable real-time holographic type communications and an immersive three-dimensional augmented reality experience [13]. Also, by aiming for end-to-end latencies of 1 ms or shorter, 6G could enable nearer-immediate remote manipulation of crucial systems and genuinely fluid human-machine connections [14]. In addition, 6G seeks to universally achieve global coverage – from space and underwater, through the densest urban areas and all remote parts of our planet fused into a single network that connects every man-made device, sensor or system on Earth [11, 12, 15]. Furthermore, 6G networks will be home to many (if not all) of the endeavours for Artificial Intelligence, such as autonomous network optimization, predictive maintenance and intelligent service provisioning along with several others [16]. 6G networks will combine advanced materials with smart architectures to enable zero-energy devices as well as sustainable communication infrastructures [17, 18]. Also, 6G will provide advanced perception capabilities that allow these networks to serve as distributed radar systems with centimeter level positioning [19, 20].

These capabilities will spark the imagination of industry sectors, ranging from autonomous transportation and smart cities to health products and robotics personnel. Yes, but for all the increased connectivity and intelligence, we see an increasing threat landscape.

Problem statement

The security world surrounding the emergence of 6G technology is multi-faceted and far more sophisticated than what we face now in existing networks [21]. Now 6G will be the bedrock of mission-critical systems, power billions of IoT devices and transfer immense amounts of crucial data, all making it an even more tempting target for state-sponsored hackers and cybercriminals alike. Traditional security mechanisms, located in the centralized architectures of past generations, are unlikely to be effective enough to

respond to these new specificities associated with 6G [8]. The security hurdles to be taken in the 6G era includes, but not limited to:

- *Ultra-Dense Network Threats:* 6G networks have a much higher node density than 5G by an order of magnitude, millions nodes per square kilometer where new problems for attack tracking and vulnerability detection need to be addressed [4]. In a sense, each and every node — from nano-sensors to macro base stations — becomes an open door for attackers.
- *Multi-mixed Technology Integration:* Multi-perspective heterogeneous integration of various communication systems and aerial facilities [11], creates new challenges that existing or previous security approaches [22], are just not prepared to handle given the different networks have various protocols, bandwidths, and latencies.
- *AI Emulating Cyberattacks:* The more AI plays a role in 6G, the more it lends itself to adversarial exploitation [23]. Since AI-powered attacks could dynamically change, thereby might escape from protection of conventional defense solutions and effectively contaminate whole network sets. One of these main concerns is Quantum Computing Threats, if we can get to practical quantum computers, 6G will have to cope with quantum resistant security measures as current cryptographic protocols could be made obsolete [24].
- *Privacy in an Ultra-Connected World:* As we predict 6G capable of pervasive sensing and data collection [11], keeping individual privacy becomes ever more difficult. New data protection and anonymization paradigms are needed.
- *Autonomous systems trust:* When 6G networks evolve to be more autonomous, establishing trust in their decision-making processes will become critical for application areas such as tele-surgery and vehicle control [25].
- *Edge security:* The transfer to the edge in 6G will also bring new security concerns, particularly in edge computing security [26], where network edges with limited computational resources.
- *Scalability of Security Solutions:* Traditional centralized security solutions may not scale to the massively distributed 6G networks [27], and therefore calls for a redefined decentralized security paradigm.

In this regard, there is an urgent requirement of comprehensive, efficient, and resilient security frameworks, which can preserve the integrity, confidentiality, and availability of future 6G networks.

Research Objectives and Contributions

This thesis tries to address the primary security challenges of 6G networks by proposing new decentralized security models based on blockchain, federated learning, and secure multiparty computation. The ultimate goal is to provide solutions that are capable of

thwarting the new threats of 6G while upholding the privacy and performance requirements of this new paradigm.

The thesis begins with a thorough analysis of the security threats and vulnerabilities of the 6G ecosystem, taking into consideration ultra-dense deployments, AI-driven attacks, and quantum computing's threats. Based on this point, the thesis discusses how blockchain and distributed ledger technologies can facilitate decentralized trust mechanisms, tamper-proof data handling, and privacy-preserving cooperation among heterogeneous nodes within the networks.

To implement these concepts, the thesis proposes *6G-SecureIDS*, a blockchain-based, federated learning-powered intrusion detection system that ensures distributed, privacy-conscious threat analysis at network nodes. The thesis also introduces *FBMP-IDS*, an effective and secure IDS that leverages multiparty computation and blockchain to minimize communication overhead and enhance detection accuracy. Finally, the thesis presents *TL2AB*, a secure lightweight authentication framework combining AI-driven risk assessment with blockchain-based verification to offer scalable secure identity management for billions of internet-of-things devices in 6G ecosystems.

Extensive experimental evaluations confirm the performance, scalability, and efficiency of the proposed architectures compared to traditional security mechanisms. With these primary research objectives laid out, the thesis complements a futuristic security roadmap for 6G networks so they can be secured, reliable, and sustainably deployed.

Thesis Structure

This thesis is structured as follows:

- *Chapter 1:* This chapter introduces 6G networks and emphasizes their anticipated breakthroughs over past generations, for example, ultra-low latency, high data rate, and extreme connectivity. The chapter explores 6G's architectural concepts, such as merged space-air-ground-underwater networks and AI-based optimization. It also identifies significant security issues, such as ultra-dense network attacks, AI-mimicking cyberattacks, and quantum computing risks. Last but not least, blockchain is presented as a potential security solution, providing decentralized trust, tamper-proof data management, and secure authentication.

- *Chapter 2:* This chapter explores AI and blockchain (DLT) convergence towards 6G network security. It discusses AI's deployment in optimizing network operations, detecting cyber attacks, and managing resources at low costs. The strengths of blockchain towards decentralization, integrity, and secure data exchange are examined. The combination of AI and DLT is discussed with an emphasis on applications such as blockchain-protected federated learning and AI-driven smart contracts. Computational overhead challenges, privacy challenges related to data, and scalability are also dealt with.

- *Chapter 3:* This chapter presents 6G-SecureIDS, a proposed blockchain-based 6G network intrusion detection system. The system uses federated learning to enable

privacy-preserving security analysis in the distributed nodes. Decentralized trust mechanisms, anomaly detection powered by AI, and secure knowledge transfer using blockchain are the key features. The chapter provides an overview of the system architecture, advantages over the traditional IDS models, and functionalities against future threats. Experimental testing is performed to confirm its effectiveness in detecting network abnormalities without compromising data privacy and security.

- *Chapter 4:* This chapter proposes FBMP-IDS, a blockchain and multi-party computation secured federated learning-based intrusion detection system. FBMP-IDS addresses 6G security and privacy challenges by using efficient gradient compression, on-the-fly MPC protocol execution, and decentralized threat detection. This chapter provides a comparative analysis of FBMP-IDS with traditional federated learning-based IDS models in detail. It also provides computational complexity analysis, experimental results, and performance comparisons on real-world data sets to confirm its advantages for communication overhead reduction and detection accuracy improvement.

- *Chapter 5:* This chapter introduces TL2AB (Trusted Lightweight Authentication using AI and Blockchain) for 6G networks. TL2AB aims to provide secure, scalable, and privacy-preserving authentication mechanisms suitable for the high device density of 6G environments. It integrates AI-driven risk evaluation with blockchain-based verification, offering a resilient authentication framework. The chapter details the system design, experimental evaluations, formal security analysis, and comparative assessments with existing authentication schemes.

Chapter 1

6G Networks Vision and Security Challenges

1.1 Introduction

This chapter introduces 6G networks, a future generation of wireless communication systems that will drastically change our connected world. We define 6G and its reaching vision, which includes unprecedented levels of performance such as ultra-low latency, massive connectivity, and much higher data rates. A comparative study with the previous generations, notably 5G, is carried out by highlighting the most important advances and technological leaps to be expected in 6G.

We then focus on the architectural foundation for 6G networks, discussing key enablers that enable these transformative capabilities. This covers an in-depth discussion of the arising communication infrastructures, including integrated terrestrial and aerial networks, and how AI drive strategic roles in this.

After this, the focus is shifted to the benefits that 6G networks have in store for different sections. We will discuss how 6G will bring revolution to industries such as healthcare, transportation, and manufacturing by making possible new applications that could transform life.

However, for the development and operation of this 6G vision, a suitable security framework is essential. We will therefore dedicate a large part of this chapter to discussing the unique security challenges that 6G networks will necessarily face. We will review the ever-changing threat landscape, including the discovery of new types of vulnerabilities and the impact of quantum computing on current security paradigms.

Finally, we will introduce Blockchain technology as a promising solution to solve various security challenges of 6G. We will discuss the inherent advantages of Blockchain, immutability, transparency, and decentralization, and further explore how these properties can be leveraged to enhance security, privacy, and trust in 6G networks.

1.2 Introduction to 6G

1.2.1 Definition and vision of 6G

6G is the sixth generation of wireless communication systems, imposing a paradigm change in cellular network technology [15]. It envisions a hyper-connected world characterized by intelligence, seamless integration between the physical and digital worlds, and unprecedented levels of performance. Unlike its predecessors, 6G is intended to go beyond traditional mobile communication with:

- *Ultra-high data rates:* as high as 1 Tbps can be achieved [28], enabling real-time transmission of big datasets and bandwidth-intensive applications like holographic communication and immersive virtual reality [13, 12].
- *Ultra-low latency:* reduction of latency below a millisecond that enables real-time control and automation for mission-critical applications such as remote surgery, autonomous cars, and industrial automation [11].
- *Massive connectivity:* Supporting an extremely high density of connected devices, enabling the realization of the Internet of Things (IoT) and massive machine-type communication (mMTC) on an unprecedented scale [29].
- *Improved security:* by embedding advanced security mechanisms [4], that are able to handle changing threats such as: quantum-resistant cryptography, intrusion detection systems powered by AI, and blockchain-based security solutions [8].
- *AI/ML Integration:* Use AI with machine learning to make the network performance at all resource utilization levels effective by intelligently managing the network [14].

The vision for 6G is much larger than just speed and capacity; the thought is all about a holistic approach toward wireless communication, based on aspects that include:

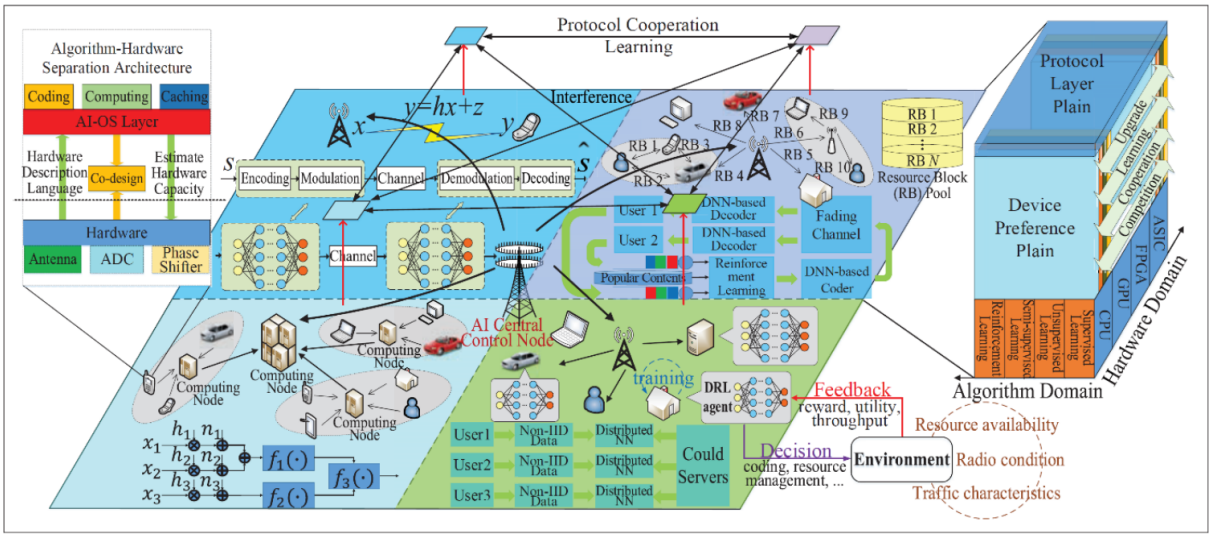


Figure 1.1: 6G Architecture [1]

- *Energy Efficiency:* Minimize energy consumption with minimal environmental effects [17], enabling network sustainability.
- *Spectrum efficiency:* It means the best utilization of available spectrum resources for the ever-growing demand for wireless connectivity [20].
- *User experience:* To provide a seamless and personalized user experience [18], tailored to individual needs and preferences.

In other words, 6G is the vision of a world where everything around us is smart and connected, and wireless communication will be woven into the fabric of life to enable people, transform industries and advance society, as forecasted by [1] and illustrated in Fig 1.1.

1.3 Architectural Principles and Logical Components

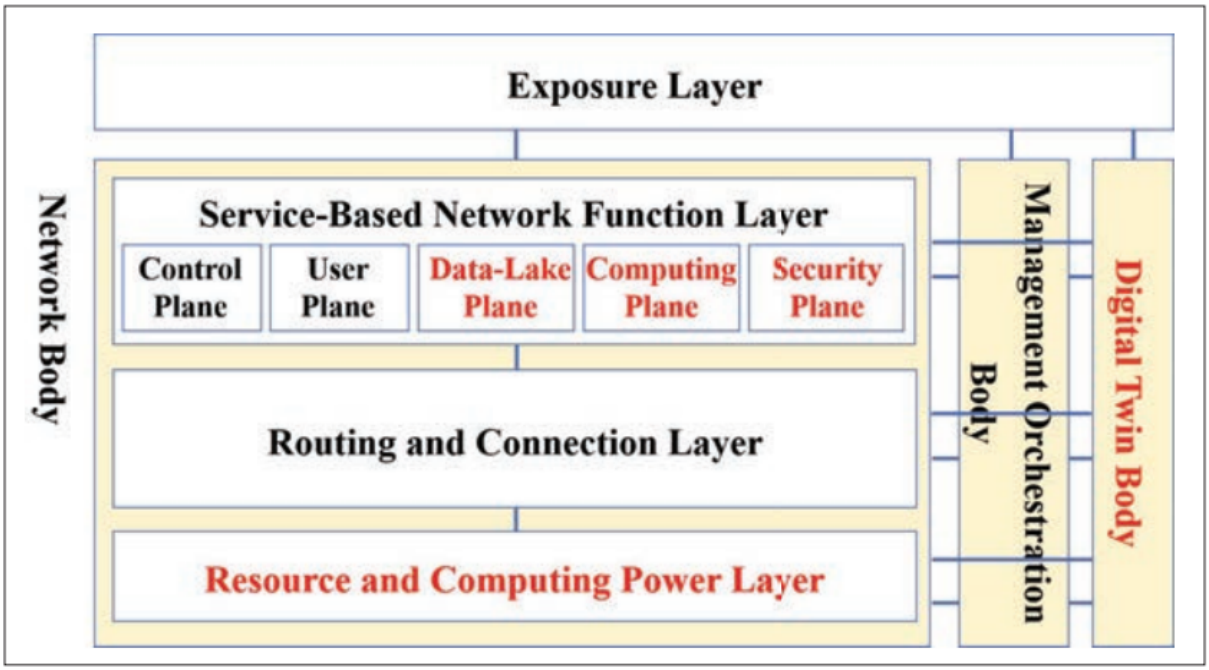


Figure 1.2: 6G Logical Architecture [2]

1.3.1 Analysis of key components in a 6G network architecture

The sixth generation of wireless networking is envisioned to include a paradigm shift in the networking architecture design, where the traditional concepts are being reformed. Some works forecast introducing a multi-faceted framework encompassing three distinct operational bodies (Network Body, Management Orchestration Body, and Digital Twin Body), four functional layers (Resource and Computing Power Layer, Routing and Connection Layer, Service-Based Network Function Layer, and Exposure Layer), and five specialized planes (Control Plane, User Plane, Data-Lake Plane, Computing Plane, and Security

Table 1.1: Comprehensive Analysis of 6G Network Architecture Components

Component	Elements	Technical Specifications and Capabilities
Bodies	Network Body	• Integration of radio access, core, and transport networks [30] • Native computing power infrastructure [31] • Pool-based capability for connection, computing, and storage resources [32]
	Management Orchestration Body	• Intent-driven resource optimization [33] • AI/ML-based network orchestration [34] • Automated operation and maintenance capabilities [3] • Cross-domain implementation efficiency [11]
	Digital Twin Body	• Virtual network modeling and simulation [35, 36] • Runtime environment reconstruction [35] • Closed-loop control optimization [33] • Real-time parameter synchronization [37]
Layers	Resource and Computing Power	• End-to-end system resource integration [37] • Computing power as core resource [31] • Deep integration of connection, computing, and storage [11]
	Routing and Connection	• Intelligent Static and dynamic connection modes [38] • Unified connection infrastructure [12] • Deterministic forwarding capabilities [39] • Flexible service invocation [29]
	Service-Based Network Function	• Small cloud units (SCUs) support [40] • Distributed deployment architecture [12] • Independent operation modes [41]
	Exposure	• API/SDK capability exposure [42] • Cross-layer capability integration [42] • Third-party service enablement [42]
Planes	Control Plane	• Unified control of fixed, mobile, and satellite resources [43] • Atomic service-based control [44] • AI-enabled precise control mechanisms [44]
	User Plane	• Programmable forwarding capabilities [45] • Service-based architecture [45] • Cross-domain deterministic transmission [45]
	Data-Lake Plane	• Refined data collection mechanisms [45] • Flexible storage architecture [46] • Distributed data collaboration [45]
	Computing Plane	• Distributed task processing [47] • Resource scheduling optimization [48] • Native intelligence support [49]
	Security Plane	• Native security capabilities [8] • Security awareness mechanisms [50] • Active protection systems [28] • Flexible security service collaboration [28]

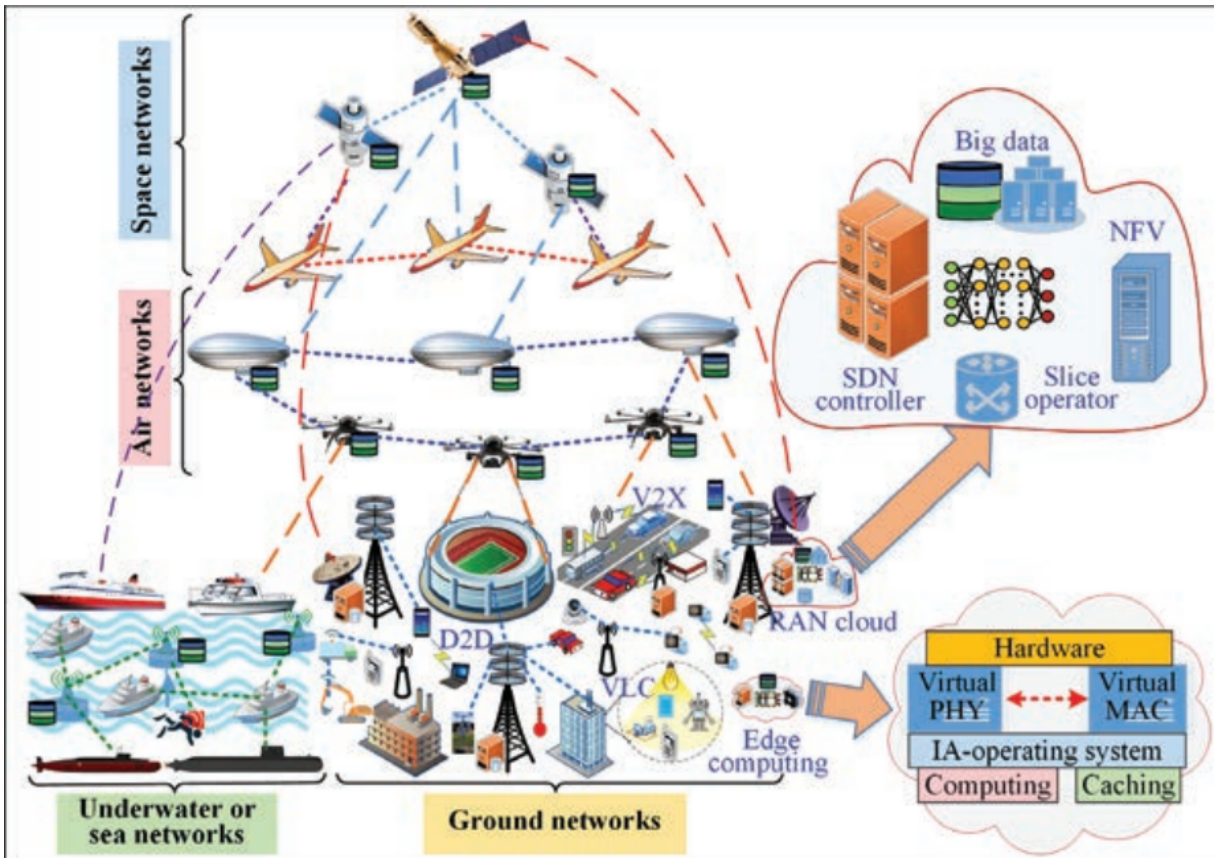


Figure 1.3: Integrated space-air-ground-underwater network (ISAGUN) architechture for 6G Networks [3]

Plane), as comprehensibly discussed by [2], and provided in Tab. 1.1. This innovative architecture represents a fundamental evolution from conventional telecommunications infrastructure, particularly through its integration of computing capabilities as a core network resource rather than an auxiliary component. The Network Body, serving as the physical infrastructure foundation, incorporates radio access networks, core networks, and transport networks with embedded computing power enablement for native intelligence capabilities. The Management Orchestration Body introduces intent-driven operations for dynamic resource optimization [51], while the Digital Twin Body enables predictive optimization through virtual network modeling and simulation. This comprehensive framework addresses the emerging challenges of ultra-high network density (reaching 0.1-100 Million devices/km^3) and unprecedented traffic density (up to 0.1–10Gbps/m^2) [2], while facilitating the integration of advanced technologies such as Time Sensitive Communication (TSC) and AI across all architectural layers.

The inspiration for this radical architecture is that the integration of computing capabilities as a core underpinning network resource, rather than as an auxiliary component [2], drives a very different approach in designing the conventional telecommunications infrastructure. It includes computing power as one of the native network elements to facilitate intelligence natively, autonomously operating itself and performing dynamic resource allocations across the network ecosystem [52].

Within this more advanced architectural framework, the Management Orchestration

organization offers unparalleled levels of control for the network through intent-driven operations. At a high level, it describes the operational goals that can be automatically translated by sophisticated AI/ML algorithms into granular network configurations [53]. This orchestration mechanism represents a significant improvement from traditional policy-based management systems in that it will enable dynamic optimization of several network parameters related to energy efficiency, latency characteristics, and resource utilization patterns [2]. Moreover, a Digital Twin body allows predictive optimization based on virtual network modeling [54]; however, considerable challenges remain regarding how to perform an accurate large-scale network representation and to maintain temporal synchronization across distributed network elements [2].

It also executes a sophisticated approach to integrating resource management with connectivity control, service provisioning, and interface exposure on an advanced principle of layering within the architectural framework. This is supported by an innovative plane configuration where, in addition to traditional control and user planes, there will be added specialized planes for data analytics [55], computational operations, and security functions [8]. Perhaps most important, this includes the implementation of a data analytics plane as a basic architectural innovation to enable the systematic collection, processing, and use of network operational data across multi-domains and hierarchical levels [2].

To enable near-instant and seamless super-connectivity, 6G networks will be empowered by an Integrated Space-Air-Ground-Underwater Network architecture, as shown in Fig. 1.3. This multi-tiered architecture consists of space, air, ground, and underwater networks, each employing diverse technologies and platforms to provide comprehensive and resilient connectivity across diverse environments and user needs.

1.3.2 Exploration of new design

The evolution towards next-generation wireless has catalyzed innovative architectural approaches in the domains of service-oriented frameworks [41] and distributed autonomous operations [40]. The Holistic Service-Based Architecture [56] represents the extension of conventional service-based concepts to all network elements, introducing fine-grained service decomposition and dynamic composition mechanisms on top of advanced protocols such as HTTP/3 for efficient service delivery. This comprehensive service-oriented approach enables multi-vendor interoperability and standardized service discovery while supporting efficient resource utilization through lightweight service deployment mechanisms [2]. The most important innovation in 6G architectural design is the introduction of Distributed Autonomous Networks (DAN) [40], which will introduce modular deployment units with advanced self-configuration and optimization capabilities. These autonomous units are typified by independent resource management and dynamic topology adaptation, hence representing a fundamental shift in network deployment strategies. The DAN architecture addresses critical challenges in scalability and operational efficiency through the implementation of AI-driven optimization mechanisms and scenario-specific function deployment, while maintaining sufficient flexibility to accommodate emerging applications and services [2].

The architectural innovations in 6G networks extend beyond traditional telecommu-

nications boundaries, incorporating advanced capabilities for immersive communication systems and holographic interactions [13]. It does so by providing advanced cross-domain integration mechanisms, as well as standardized service exposure interfaces that can help the different elements of the network and service components in a seamless manner. The architecture also addresses several challenges in terms of energy efficiency through its intelligent resource allocation mechanisms [2], simplifying complex problems through modular design principles while not forgetting robust security implementations across the distributed network elements.

1.3.3 Comparison with previous generations

6G is an enabler of a paradigm shift in wireless communication and overcomes the limitations set by its predecessors, 4G and 5G. While 4G focused on high-speed mobile broadband, 5G opened up completely new dimensions in data rates, latency, and network capacity; 6G will be truly transformative of wireless by:

- *Overcoming 5G Limitations:* 5G, despite its advancements [57], may face challenges in accommodating the exponential growth of IoT devices [58], supporting the demanding requirements of emerging applications like holographic communication and extended reality (XR), and integrating seamlessly with the increasing reliance on AI/ML [59]. 6G aims to overcome these limitations by providing significantly higher data rates, ultra-low latency, and massive connectivity [60].

- *Higher Frequency Leverage:* Higher frequency bands, such as THz frequencies, will most likely be utilized with 6G [11], which promises much higher bandwidth and capacity compared to the lower frequencies used in both the 4G and 5G systems. This shift upward in frequency will enable the transmission of considerably more data within a given timeframe [61], thus supporting the demands of bandwidth-intensive applications.

- *Employing Advanced Technologies*: 6G will benifit from a suite of cutting-edge technologies to enhance network performance and coverage. For instance, Integrated Terrestrial and Aerial Networks (ITAN) [62], which combine terrestrial and aerial infrastructure, such as drones and high-altitude platforms (HAPs), to provide seamless and ubiquitous coverage, especially in remote or challenging environments. Also, Holographic Beamforming [13], which enables highly precise beamforming techniques to direct radio signals with greater accuracy, improving spectral efficiency and reducing interference. In addition, Intelligent Reflecting Surfaces (IRS) [63], by deploying large arrays of reconfigurable surfaces to intelligently reflect and steer radio waves, optimizing signal propagation and enhancing coverage. Furthermore, Smart Network Slicing [49],by enabling the creation of customized and isolated network segments, tailored to the specific requirements of different applications and services, ensuring quality of service and security.

- *Native Integration of AI/ML:* 6G will be deeply integrated with AI/ML [49, 14], enabling intelligent network management, dynamic resource allocation, and proactive threat mitigation. AI/ML algorithms will be employed for tasks such as predictive

maintenance [64], by identifying and preventing network failures before they occur. Also, dynamic spectrum management [65], by optimizing spectrum utilization by dynamically adjusting transmission parameters based on real-time network conditions. In addition, user behavior analysis [66], personalize network services and improving user experience based on individual preferences and usage patterns.

In essence, 6G aims to build upon the foundations laid by 4G and 5G, addressing their limitations and leveraging advanced technologies to create a truly transformative wireless communication system that will underpin the digital revolution and drive innovation across various sectors.

1.3.4 Possible applications in various sectors: healthcare, transport, industry

The foreseen performance gains of 6G are much larger than incremental compared to its predecessors [67]. 6G has the possibility to offer a truly disruptive wireless experience, featuring performance levels never seen or even imagined before.

First and foremost, 6G will strive for ultra-low latency down to the sub-millisecond or even microsecond range. This will really open up a whole new world for real-time applications and services. While this is the case, it will also enable real-time industrial process controls with high precision, such as robotics and automation processes critical to Industry 4.0, at an unprecedented scale [13]. Moreover, it is about to be indispensable for fully autonomous driving by enabling real-time communication among vehicles, infrastructures, and pedestrians with assurance of safety and efficiency [40]. Ultra-low latency will enable, in the case of healthcare, surgical procedures to be performed remotely with least delay and will improve access to and expand the availability of specialized medical care [44]. Further, ultra-responsiveness and seamless user experience will be assured in immersive applications such as AR and VR [36]; hence, latency-induced motion sickness will be reduced, which in turn increases user comfort.

Again, 6G will offer much higher data rates, even up to terabits per second. This exponential growth in data throughput will affect many industries significantly. This will enable very bandwidth-intensive applications like holographic communication [13], 8K video streaming, and high-definition video conferencing that will offer an immersive and realistic user experience [68]. This will further speed up the development of AI/ML-driven applications in verticals such as healthcare, finance, and scientific research by enabling the swift transfer and processing of voluminous data [69]. Finally, it will efficiently support the transfer of large-sized files and data-intensive applications such as software updates, medical imaging, and scientific simulations [70].

Thirdly, 6G will enable the connection of a number of devices never before realized by any generation [69]. This huge connectivity will potentially enable the realization of the vision of IoT where billions of devices, from sensors and actuators up to autonomous vehicles and smart appliances, will seamlessly interconnect with each other [11]. It will therefore have a much farther-reaching consequence, enabling further smart cities, smart grids, and intelligent transport systems, which will eventually enhance efficiency, sustain-

ability, and resilience [7]. This will be further enabling new business models and services built on top of gigantic connectivity and generated data from interoperable devices.

These performance enhancements will not only make the performance of existing applications much better but will indeed open a tidal wave of applications and services previously unimaginable. Thus, 6G will provide the foundation needed for a well-connected and genuinely intelligent society whereby different aspects of daily life contribute positively to economic progress [71].

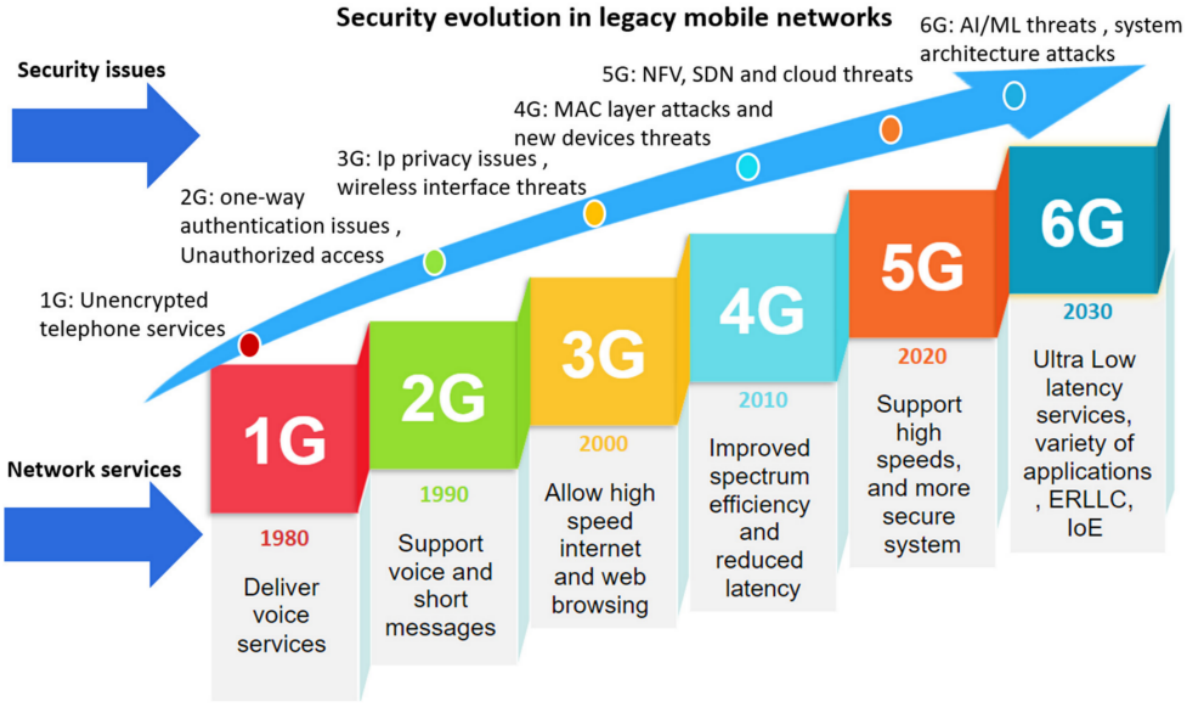


Figure 1.4: The security evolution of mobile communications from 1G to the predicted future 6G [4]

1.4 Security Challenges

1.4.1 Nature of specific threats to 6G networks

The evolution to 6G networks presents a very complex landscape of security threats that go beyond the conventional vulnerabilities of mobile networks, as summarized in Fig. 1.4 [4]. Advanced technologies such as Terahertz communications, VLC, and molecular communications introduce new attack surfaces that can be exploited by malicious actors [72, 73].

The 6G ecosystem will introduce an unprecedented level of interconnectedness and, correspondingly, an unprecedented increase in the attack surface [11]. Billions of interconnected devices operating from omnipresent sensors and actuators in smart cities to autonomous vehicles and drones will form a huge, complex mesh of interconnected systems [40]. This pervasive connectivity, while providing unprecedented levels of automation and efficiency, also exposes new vulnerabilities. The consequences of such a

compromise would, therefore, be much more serious, ranging from disruptions to critical infrastructures and user privacy issues to human lives. For example, a cyberattack on the power grid or transportation network may have devastating results due to impacts on essential services and wide disruption.

Communications relying on Terahertz, that fall in a frequency window from 0.1-10 THz exhibit security apprehension due to physical properties of transmission media. Despite better theoretical safeguards from the nature of the THz communication system [74], various works showed the feasibility of capture by unauthorized users simply by correctly scattering radiation by appropriately placed objects in the transmission path [75]. This is especially alarming in the case of ultra-high-capacity data transmission, where the compromise of the THz channel may lead to massive data breaches.

In the Visible Light Communication domain, new dimensions of threats or attacks are developed based on the basic needs: CIAA-Confidentiality, Integrity, Authenticity, and Availability of wireless network security [76]. VLC systems are especially susceptible to signal overlap attacks, where different transmitter signals may interfere with one another, potentially compromising the authenticity and integrity of transmitted data. Moreover, VLC systems are more vulnerable to sniffing and eavesdropping attacks in high reflection areas [77], which demands complex countermeasures against these attacks, such as linear precoding in VLC MIMO systems [78].

Molecular communication, while promising for specialized applications, introduces unprecedented security challenges across multiple protocol layers. At the transport layer, desynchronization and flooding attacks mirror traditional network threats but require novel mitigation strategies due to the unique nature of molecular transmission. The link layer faces collision and unfairness attacks, while the network layer must contend with molecular packet loss handling attacks [42, 79]. These challenges increase with the incapability of traditional security solutions, such as frequency hopping methods, which are inefficient in the context of molecular communication.

While new technologies bring many advantages, they also open up new avenues of exploitation. Broad use of AI/ML in 6G, while opening up a plethora of intelligent Radio Resource Allocation and enhanced security capabilities, does come with inherent vulnerabilities . Adversarial attacks against an AI/ML model can include poisoning attacks-which corrupt training data-or evasion attacks-which manipulate model inputs to induce incorrect outputs [80, 27, 4]. In particular, adversarial examples, that is, inputs crafted with the only purpose of misleading an AI/ML model, can be used to bypass intrusion detection systems, manipulate network traffic, or even compromise critical control systems.

What is more critical, the rise of quantum computing is a serious menace to the security of all current cryptographic algorithms, including those that secure 5G and the earlier generations [67]. If powerful enough, quantum computers can break many of the public-key cryptography algorithms in use today efficiently, such as RSA and ECC [81]. This means developing and using the so-called postquantum cryptography, including but not limited to such aspects as lattice-based cryptography and code-based cryptography, which are assumed to be resistant against quantum computers' attacks [82]. In the same vein, shifting to PQC requires a lot of research and development effort to be done, not to mention new standards and protocols.

The increasing reliance on SDN and NFV also introduces new attack vectors. While virtualization technologies provide flexibility and agility, they also introduce vulnerabilities such as VM escape, where an attacker can exploit vulnerabilities in the hypervisor or guest operating systems to gain unauthorized access to the host system or other virtual machines [83]. This can enable attackers to move laterally within the network, access sensitive data, and disrupt critical services.

Security and data privacy are definitely in question in the upcoming 6G era [75]. Such huge volumes of data produced and processed by the networks, including sensitive user data, location information, and important infrastructure data of any given device, will form a highly coveted target for various types of attack vectors [84]. Increased data-driven applications-like personalized services, precision medicine, and autonomous cars-require comprehensive data protection that considers security risks so as to guard user privacy from data breaches.

1.4.2 Analysis of emerging vulnerabilities

The 6G ecosystem brings in a host of new attack surfaces that need deep understanding of the various emerging vulnerabilities. These can be broadly categorized as outlined in Table 1.2. While the integration of AI/ML into 6G networks offers enhanced capabilities, it also introduces significant vulnerabilities across multiple architectural layers [22]. The intelligent sensing layer, which is responsible for collecting data from the physical world, is threatened on all levels-from device-level physical attacks to sophisticated attempts of information theft [4].

6G will heavily rely on new frequency bands, for instance, Terahertz, introducing further challenges [74]. Moreover, physical-layer attacks, like interference and beam hijacking, will cause disruption or disclosure of services and data [88], whereas virtualization technologies, despite increased flexibility, add new vectors related to the tampering of NFV infrastructure and utilization of hypervisor vulnerabilities [88]. In addition, 6G will heavily depends on AI/ML in many aspects, like resource management, traffic handling, and security. All these are vulnerable to several forms of attack [89], including: adversarial attacks manipulate the AI model for wrong predictions; data poisoning can compromise training data in the event of bias or inaccuracy; and inference attacks elicit sensitive information from trained models. Also, Quantum computers can be regarded as the most terrifying challenge against 6G security. Most of the popular cryptographic algorithms are vulnerable to Shor's algorithm [81]. Thus, existing security mechanisms become null. Moreover, quantum channel attacks may use unique properties of quantum states in their action, hence breaking the communication or violating data integrity.

6G's edge computing paradigm, while enhancing performance and latency, introduces new vulnerabilities. Resource depletion attacks can overwhelm edge devices, hindering service delivery. Node compromise attacks can grant attackers control over critical edge infrastructure. Furthermore, the deployment of AI/ML models at the edge increases the risk of model theft and inference manipulation [89]. Even with many evolutions in the security of 6G protocols [92], they are all still vulnerable to many traditional attacks. Furthermore, zero-day exploits may also take advantage of unknown vulnerabilities against

Table 1.2: Emerging 6G Network Vulnerabilities Classification

Category	Attack Vectors	Impact	Risk Level
Network Infrastructure	**Physical:** THz interference, beam hijacking, RF fingerprinting [85, 86, 21] **Virtual:** NFV tampering, hypervisor exploits [87]	Service disruption, data interception, isolation breach, resource theft [88]	Critical
AI/ML Systems	**Model:** Adversarial attacks, poisoning, backdoors [89]. **Data:** Training manipulation, inference attacks [89]	False predictions, system manipulation, privacy leakage, model bias [80]	Critical
Quantum	**Crypto:** Shor's algorithm, post-quantum transition [81] **Channel:** State measurement, entanglement breaks [90]	Key compromise, authentication failure, protocol breakdown	Severe [81]
Edge Computing	**Resources:** Depletion, hijacking, node compromise [91] **Intelligence:** Model theft, inference manipulation [80]	Service unavailability, data theft, algorithm exposure [22, 25]	High
Protocol Security	**Auth:** Zero-day exploits, protocol downgrade [22] **Routing:** Route poisoning, BGP hijacking [25]	Unauthorized access, traffic redirection, network isolation [25]	High

new protocols. Protocol downgrade attack [93] forces devices down to the older, not so secure, protocols. Many routing protocols are attacked by route poison and BGP hijacking [27] to enable routing traffic to preferred directions, disrupting network operations.

1.5 Blockchain as a Solution

6G wireless networks introduce a paradigm shift into connectivity and intelligent services on an unprecedented scale. The development of the networks toward the requirements of future applications will be very much enabled by blockchain technology to solve some of the fundamental challenges and bring in new capabilities [47]. Several factors are driving the integration of blockchain in 6G networks. First, the expected explosion in mobile traffic to multiple exabytes per month by 2030 calls for robust decentralized manage-

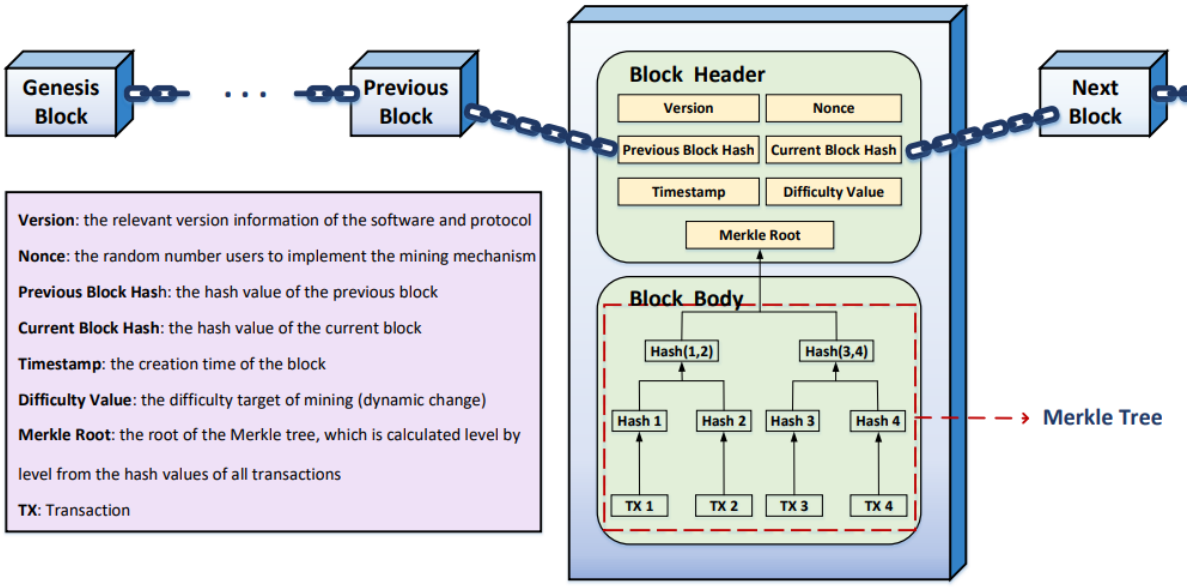


Figure 1.5: The structure of Blockchain's blocks [5]

ment systems [94]. Second, mission-critical applications such as autonomous vehicles, remote surgery, and industrial automation will require a level of security and reliability unparalleled by traditional centralized architectures.

Blockchain technology provides a distributed security model that can greatly enhance the security of 6G networks [94], as we can see in Fig. 1.5, the blocks are linked together cryptographically. The decentralized architecture avoids single points of failure, while cryptographic mechanisms ensure data integrity and confidentiality. Smart contracts provide automated security policy enforcement, which is especially useful in managing dynamic network slices and heterogeneous access control scenarios [95]. The technology therefore allows for quite sophisticated resource management through transparent and automatized mechanisms. Smart contracts dynamically allocate spectrum, ensuring maximum efficiency in frequency bands ranging from sub-6 GHz to terahertz range [94]. The ledger keeps an irrevocable record of allocations, thus no conflict can be created, and resources may be distributed fairly among network participants. Regarding mMTC, the blockchain provides an expandable framework of trust under which devices are securely authenticated and verified without central intervention [94], a core requirement when, later in this decade, billions of devices would be connected into use cases created for Industrial IoT and smart city deployments.

1.5.1 Advantages of Blockchain in securing 6G networks

Some of the features provided by the blockchain is illustrated in Fig. 1.6 [6]. The blockchain technologies have a lot of cryptographic embeddings [96], such as elliptic curve cryptography and zero-knowledge proofs, which provides a good framework for 6G enhancements in security postures. Due to the decentralized nature, all replicas of distributed ledgers will be across many nodes in a network, thus removing single failure points, which increases resistance to focused attacks, reducing this particular risk

from impacting service availability. Immutability, brought about through cryptographic hashing and consensus, ensures the authenticity and provenance of critical network information, including device identities, traffic patterns, and configuration parameters, hence mitigating data tampering, unauthorized modifications, and fraudulent activities.

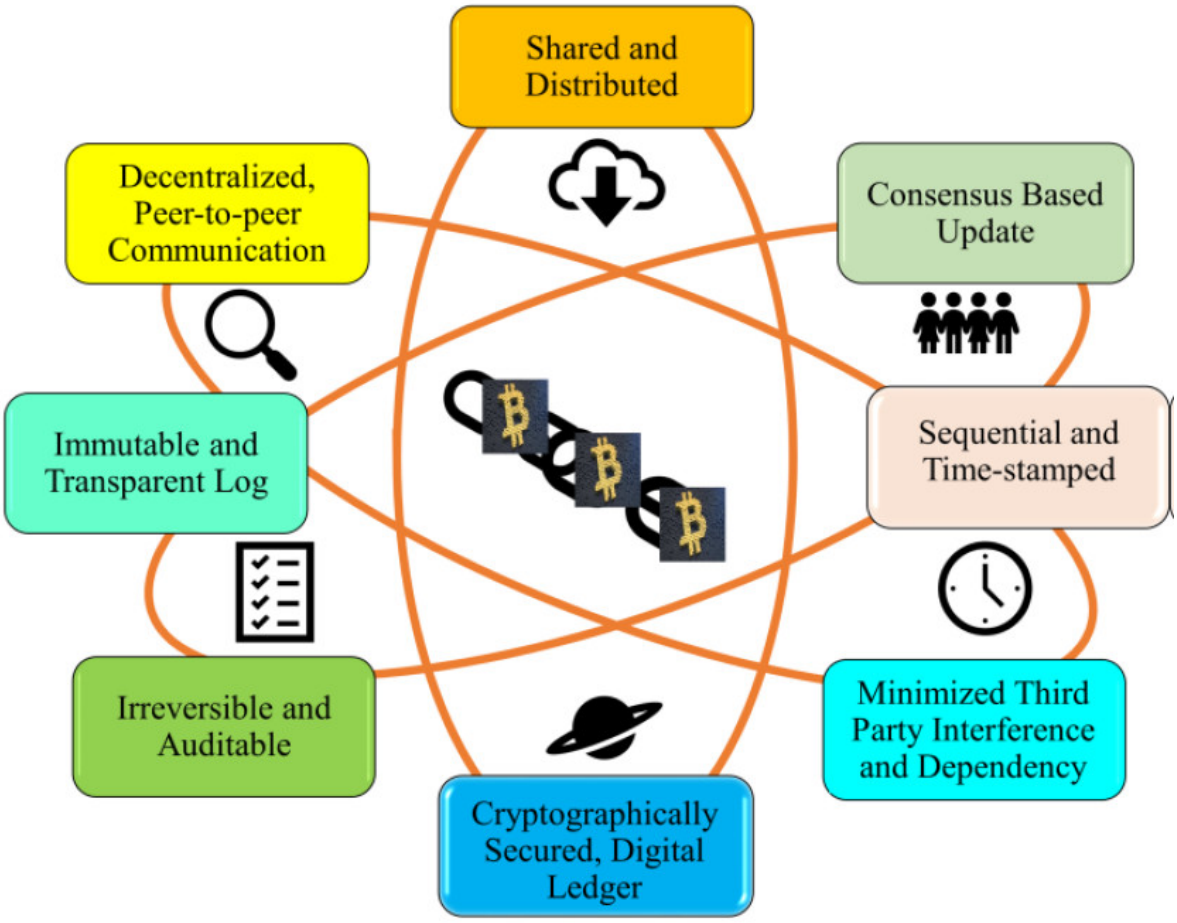


Figure 1.6: Blockchain features [6]

Since all transactions happening over a blockchain are, by design, transparent and their history auditable [96], tracing ill activities and detecting misbehavior in act will be allowed not only by rapid reactions against emerging threats but also by increased network situational awareness [95]. More transparency in a network builds trust, and with that, dependence on centralized authorities that ensure collusion cannot happen diminishes, reducing insider threat probabilities. Finally, blockchain can provide a concrete backbone for employing secure and privacy-preserving data sharing mechanisms [97], while allowing collaborative applications by adhering to strict data-privacy regulations based on techniques including homomorphic encryption and differential privacy.

1.5.2 Use cases of Blockchain in 6G scenarios

Blockchain technology is applied to solve a wide variety of critical use cases in the 6G ecosystem through an extension of traditional security paradigms in various innovative ways, as illustrated in Fig. 1.7, and classified in Tab. 1.3. The use cases span across

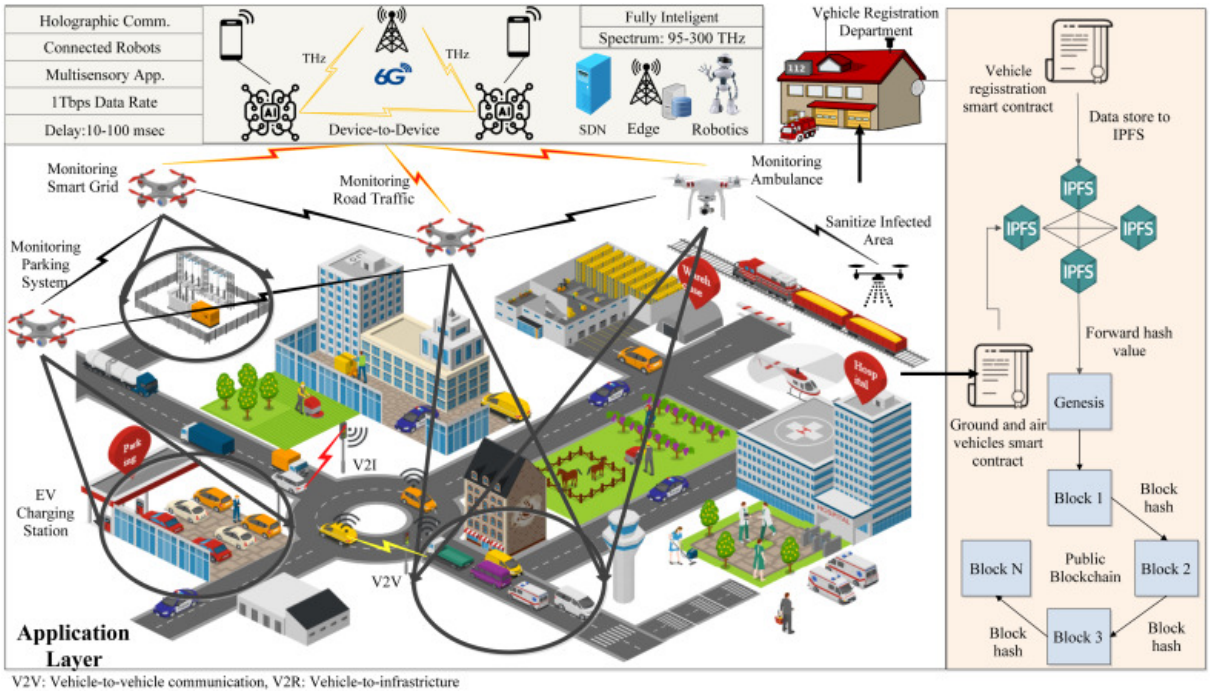


Figure 1.7: Blockchain for future cities and networks [7]

the spectrum of creating secure and tamper-proof registries for all devices by applying cryptographic techniques on device authentication through digital signatures down to zero-knowledge proof on device access control policy enforcement [47]. It creates an immutable record of data transactions, ensuring that the integrity and provenance of all data in transit across the network are maintained. Furthermore, it allows for secure data sharing with different stakeholders in a privacy-preserving manner while enabling collaborative applications on strict data privacy regulations [7].

Blockchain technology could also contribute to the 6G network by optimizing resource management, thereby allowing secure and transparent allocation of scarce resources such as spectrum, energy, and computation using decentralized autonomous organizations and smart contracts [70]. Resulting in a secure and efficient management of AI/ML models, including their development, deployment, and update in the ever-changing environment of 6G, machine learning models will maintain integrity and provenance while minimizing the risk of model poisoning attacks and data breaches simultaneously. Finally, blockchain technology can be used to increase the security and resilience of IoT devices operating within the 6G ecosystem by allowing secure device provisioning, over-the-air updates with verifiable integrity, and anomaly detection based on sensor data recorded on blockchain, which prevents complex attacks like device hijacking, data exfiltration, and denial-of-service from taking place.

Thus, with the integration of blockchain in 6G industrial networks, manufacturing process management, supply chains, and quality control will be securely managed effectively [94]. Smart contracts, on other side, will automate all the complex workflow procedures with all guarantees of maximum transparency and accountability [95]. Also, Blockchain has a very specific role in assuring privacy for patient data in healthcare while sharing medical information with different caregivers safely. The technology offers

real-time health monitoring systems coupled with secured telemedicine services critical to remote health delivery [98]. It has also ensured that autonomous cars and drone networks keep the exchange of data for V2V and V2I interactions in a safe place [99]. Blockchain ensures data integrity for critical data exchanges, enabled by secure over-the-air updates and secure traffic management.

1.5.3 Challenges and Considerations

Although Blockchain brings immense potential in terms of improving the security aspects of 6G networks, there are also many challenges and issues related to its implementation.

First, The existing blockchain technology is not well suitable to support the gigantic scale and dynamic nature of 6G networks [107]. The massive amount of transactions emanating from various devices and requiring real-time processing of events occurring over the network can bring most existing blockchain platforms to a grinding halt. Such scalability challenges can only be overcome through sharding, layer-2 scaling solutions, and development of more efficient consensus mechanisms [107]. In addition, transaction processing in a blockchain, with most of those involving complex cryptography, is particularly computation-intensive and thus may introduce latencies that inhibit real-time performance requirements for many 6G applications [11]. The optimization of transaction processing time and latency using techniques such as parallel processing and hardware acceleration is paramount to ensure the viability of blockchain-based solutions in the 6G environment [48].

Although blockchain allows secure data sharing in a privacy-preserving manner, much forethought should be given over to privacy concerns [108]. In this respect, differential privacy, homomorphic encryption, and zero-knowledge proof are some techniques which may lighten the risk pertaining to privacy and help ensure sensitive user information is disclosed in confidence [108]. Furthermore, in the wide adoption of blockchain-based solutions in the 6G ecosystem, interoperability will be a must-have between different blockchain platforms and protocols [109]. Standardized interfaces and protocols should be developed that could easily integrate and allow interoperability among various implementations of blockchains [109]. Regulatory mechanisms are in evolution for this advanced blockchain technology. From a legal point of view, blockchain solutions must be designed so that when implementing them in 6G, regulatory concerns about data privacy, cybersecurity, and consumer interest would be given full weight [30]. And regulations should support this by focusing on enabling innovation but allowing the proper development and deployment of this blockchain technology.

While blockchain technology itself is quite secure, it is not beyond the realm of vulnerabilities. Specific kinds of attacks, such as 51% attack, Sybil attack, and vulnerabilities in smart contracts, significantly reduce security and integrity for blockchain systems [110]. The robustness in security will have to be done with a variety of advanced cryptographic techniques, rigorous security audits, and continuous monitoring and threat intelligence for mitigating risks. Also, most blockchain technologies, especially proof-of-work consensus mechanisms, can be power-consuming [111]. The environmental impact of blockchain operations has to be carefully considered; furthermore, every effort should be made to de-

Table 1.3: Classification of Blockchain Applications in 6G Networks

Domain	**Applications**	**Key Benefits**	**Technical Requirements**
Security	• Access Control [94] • Authentication [100] • DDoS Prevention [94]	• Decentralized Trust • Immutable Records • Automated Policy Enforcement	• Low Latency • High Throughput • Scalable Architecture
Resource Management	• Spectrum Sharing [101] • Network Slicing [102] • Edge Computing [103]	• Efficient Allocation • Fair Distribution • Transparent Management	• Real-time Processing • Dynamic Adaptation • Energy Efficiency
Industrial IoT	• Supply Chain [104] • Quality Control [105] • Asset Tracking [105]	• Process Automation • Traceability • Compliance Management	• High Reliability • Massive Connectivity • Low Latency
Healthcare	• Patient Records [106] • Remote Monitoring [98] • Drug Traceability [106]	• Data Privacy • Secure Sharing • Audit Trail	• Data Security • Interoperability • Quick Access
Autonomous Systems	• V2V Communication [7] • Traffic Management [7] • Safety [7]	• Secure Communication • Reliable Updates • Coordinated Control	• Ultra-low Latency • High Bandwidth • Robust Security

velop more energy-efficient consensus mechanisms, such as proof-of-stake, and to optimize blockchain operations to minimize energy consumption.

The idea in this thesis highlights the way, and considerations towards making such challenges act during successful and safe implementation of blockchain into the 6G security ecosystem. For blockchain to fully let all those advantages come into operation in enhancing security, reliability, and efficiency in prospective 6G, more and continued research on scalability, performance, privacy, interoperability, and energy efficiency will take place.

1.6 Conclusion

The chapter discussed the visions, architectural basis of the 6G network, and probable benefits of the 6G network. 6G is a big leap forward in the technology roadmap of wireless communication, promising to provide unparalleled performance, including ultra-low latency, ultra-high data rates, and massive connectivity, hence opening ways for a new era in applications and services to change the face of healthcare, transportation, industry, and so on. Further, the chapter has discussed advanced technologies such as AI/ML, edge computing, and network slicing as the key enablers for realizing the 6G vision. With these technologies, 6G is targeting a very flexible, intelligent, and service-centric network architecture that will be able to meet diverse demands from future applications and services.

However, terahertz communications, advanced antenna technologies, and novel network architectures are some of the fields that require heavy research and development effort to realize all the potentialities of 6G. Special security challenges like new emerging vulnerabilities due to 6G and possible quantum computing-based attacks have to be identified and resolved to guarantee secure and dependable operation of the future 6G networks.

Chapter 2

Convergence of Artificial Intelligence and Distributed Ledger Technologies in 6G Security Architectures

2.1 Introduction

Where 6G networks are concerned, a new frontier of connectivity empowers applications previously unknown, such as holographic communications, autonomous swarm robotics, and immersive extended reality. But this quantum leap forward is only half of a paradox: the same technologies empowering 6G's transformative potential-namely, AI-driven intelligence, hyper-dense edge computing, and ubiquitous IoT integration-amplify its vulnerability to sophisticated cyber threats. The security paradigms that used to work with static and centralized architectures can barely meet the requirements of such dynamic, decentralized, hyper-scalable 6G. Convergence of AI with DLT unsurprisingly emerges as a game-changing paradigm in this turbulent landscape, offering genuinely a mix of adaptability, trust, and resilience.

The aim of this chapter is to present a deeper exploration of such a convergence and outline how AI and DLT together can reshape the security paradigm for 6G. We begin by teasing apart the roles that each technology can play: AI-a technology capable of learning, predicting, and autonomously acting in real time; DLT with its decentralized, tamper-proof infrastructure ensuring trust in an environment inherently untrusted. Beyond their independent value, however, lies their synergy-AI clears the bottlenecks of consensus mechanisms in DLT and solves scalability issues, while DLT makes the training data, models, and decision-making processes of AI manipulation-resistant.

Further on, the chapter proceeds with a detailed description of the technical frontier in such fusion cataloging state-of-the-art techniques, including blockchain-secured federated learning, AI-driven smart contracts for dynamic policy enforcement, and decentralized threat intelligence networks. The critical lens also examines real-world case studies and simulations that have proven the capability of hybrid AI-DLT frameworks to evade quantum-era attacks, secure large-scale device authentication, and enable privacy-preserving data sharing across the heterogeneous infrastructure in 6G.

We also face the challenges and research gaps that temper today's optimism. This duo (AI and DLT) faces several open questions: Is it possible for these technologies to scale up to terahertz speeds demanded by 6G? How do we balance decentralization against regulatory compliance? And what are the safeguards that will prevent AI itself from being turned into a weapon in adversarial hands? While mapping the state of the art, this chapter provides a crystal-clear view not only of what lies ahead but also lays the baseline for new frameworks and solutions throughout the remainder of this thesis-a sort of roadmap toward securing the future of 6G.

2.2 Overview of AI in 6G Security

Unprecedented in complexity and dynamic nature, the security solutions for 6G networks need to shift from rule-based systems to adaptability and intelligence [112, 90]. AI is the key in this paradigm, which will give the network autonomy to learn, reason out, and respond on its own in real time [113]. Unlike security frameworks sitting statically, AI-driven systems thrive in 6G's hyper-connected environment [38]. In this environment, terabits-per-second flows of data, massive-device ecosystems, and sub-millisecond latency requirements, [11] create a threat landscape of such breadth and dynamism that no human oversight can completely master [37]. This places AI as shield and sentinel alike for 6G-optimizing network slicing configurations, preempting zero-day exploits [8].

Central to this revolution are some advanced AI techniques that are now reshaping cybersecurity. Machine Learning, the backbone of modern threat detection, empowers systems to classify anomalies-rogue base stations, data-injection attacks-via supervised models trained on historical attack signatures [114]. Unsupervised learning, in turn, clusters unknown threats in real time, a way to identify novel attack vectors like AI-generated network traffic [115]. DL takes it to the next level: CNNs parse multidimensional network telemetry for intrusion detection [116], while RNNs predict attack probabilities by modeling temporal dependencies in network behavior [117]. Finally, FL addresses the distributed nature of 6G, allowing the collaborative training of models by edge devices without exposure to raw data-a game-changer for privacy-critical verticals like healthcare and defense [118].

While AI may present perhaps one of the most prized promises for 6G security, there also comes many challenges [8]. The very data that fuels AI-network logs, user metadata, and streams raise many privacy concerns under regulations such as GDPR. An adversarial attack exploits this dependency: subtly perturbed inputs can deceive ML models into misclassifying malicious traffic as benign [89], a vulnerability amplified by 6G's reliance on AI for mission-critical decisions [8]. Scalability is another issue. While federated learning does decentralize training, billions of devices coordinating updates strain bandwidth and computational resources [119]. Worse, the "black-box" nature of deep learning obscures decision logic in ways that complicate compliance audits and erode trust in AI-driven security actions [120]. These issues further underscore a basic truth: AI alone cannot secure 6G, it has to be symbiotically integrated with technologies like DLT in a way that their weaknesses get mitigated in order to unlock full potentials [5], as illustrated in Fig. 2.1 [8].

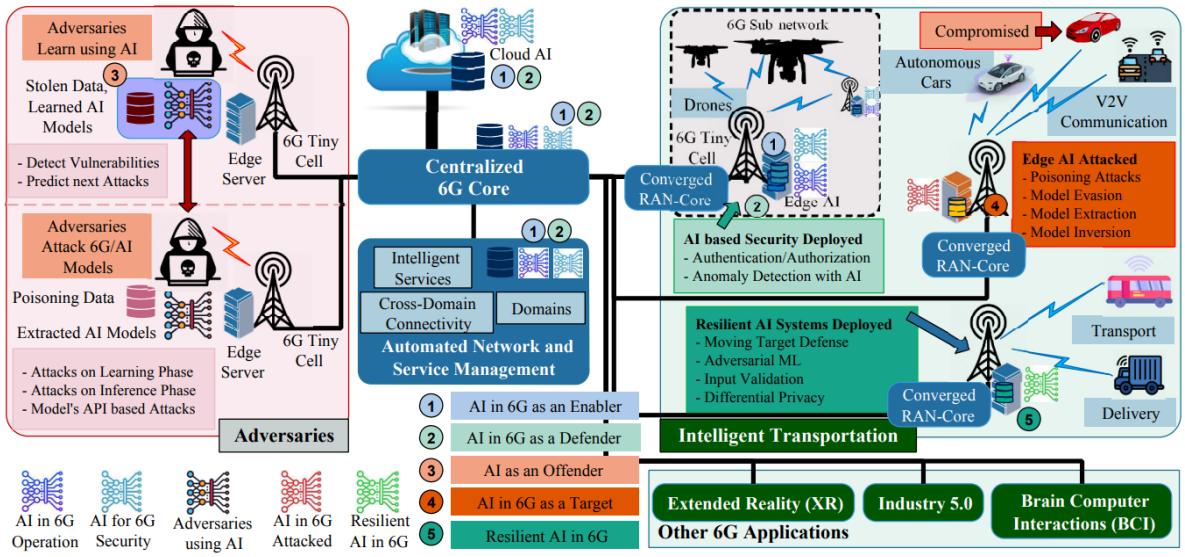


Figure 2.1: AI in 6G: Enabler, Defender, Offender, and Target. [8]

2.2.1 Role of AI in 6G Networks

AI integration is not an enhancement but a foundational necessity for 6G networks. With the coming of 6G into a hyper-connected ecosystem, it will have massive-device densities, terahertz-frequency communications, and immersive applications like holographic telepresence; AI will hold the key for security, efficiency, and adaptability. Each of the domains-network optimization, threat detection, and resource allocation-addresses some unique challenges due to scale and complexity of 6G.

For instance, 6G's architecture, comprising ultra-dense HetNets, non-terrestrial nodes such as satellites and drones, and dynamic network slicing, requires real-time optimization that is well beyond human or conventional algorithmic capabilities. AI-driven optimization ensures seamless connectivity and QoS in this fluid environment. For example, AI models using DRL independently detect and reroute traffic around failed nodes or congested links [121]. This can be for faster re-configuration by the help of aerial base stations and satellite backhaul for disaster recovery over damaged terrestrial infrastructure. Also, AI minimizes power consumption in energy-constrained edge devices. Techniques such as TinyML make lightweight neural networks optimize IoT sensors' transmission power [116] and sleep cycles for extending battery life by 40–60% in smart agriculture or industrial IoT deployments.

As for threat detection, the attack surface for 6G is huge-from quantum computing, AI-generated attacks to vulnerabilities in natively AI protocols [122]. AI completely changes how threats are detected, from reactive to proactive. The unsupervised learning algorithms of autoencoders and GANs identify the deviation from normal network behavior [123] by flagging such new threats that include adversarial attacks on beamforming configurations or AI-poisoned training data. In addition, AI has secured the communications of 6G over the terahertz band, against eavesdroppers who attacked the directional-beam vulnerability. RNN detects anomalies in channel state information representing beam alignment deviations [124], whereas encryption keys are dynamic, with

tuning performed by reinforcement learning agents. Furthermore, AI correlates threats across network layers. For example, a DDoS attack on the 5G core network would, in 6G, be manifested as abnormal physical-layer signal interference [79]-a linkage that only AI can make through multi-modal data fusion.

AI ensures the guarantee of spectrum, computation, and energy usages under tight resources but highly stringent latency in 6G: Cognitive Radio Systems [30]- employ AI models, including CNN, performing real-time sensing of spectrum usage and detecting unused frequency bands for dynamic assignment to services that have a high priority, for instance. Federated learning frameworks split AI jobs across the edge nodes [125], reducing latency for such applications as autonomous driving. AI predicts spikes in compute demand (e.g., for a live holographic event) and pre-allocates GPU resources at the edge.

2.2.2 AI Techniques for Security

The security of the 6G network needs to shift from rule-based systems to adaptive and intelligent frameworks that can cope with dynamic and evolving threats [8]. Machine Learning, Deep Learning, and Federated Learning are three AI techniques at the center of this transformation, offering different kinds of abilities for securing 6G's hyperconnected heterogeneous architecture. We present in Tab 2.1 a summary of a selected techniques.

Machine Learning acts as the base layer for real-time threat detection and mitigation. In particular, application of the supervised learning algorithms, such as support vector machines [132] and gradient-boosted decision trees, will use labeled datasets to classify the known attack signatures. These include rogue base station emulation, data injection, and spoofed network slices. Such models are fit for applications requiring very fast decision-making, for example, in identifying malicious traffic in URLLC channels intended for autonomous road vehicles or industrial automation [124]. Autoencoders and DBSCAN are examples of unsupervised learning methods, which tackle the zero-day attack challenge by ingesting raw, unlabeled network telemetry and looking for deviations from normal behavior [133]. For example, subtle anomalies in latency in haptic feedback may be detected by unsupervised ML in 6G's tactile internet applications. Semi-supervised learning bridges the gap by combining a small amount of labeled data with large unlabeled datasets to train models on emerging threats, such as AI-generated network traffic, which may mimic legitimate user behavior in order to bypass traditional defenses [115].

Deep Learning extends ML's capabilities by leveraging hierarchical neural architectures to process 6G's massive, multimodal datasets. CNNs analyze spatial and temporal patterns in network traffic, thus enabling intrusion detection at unprecedented scales. For instance, CNNs parse 2D heatmaps of terahertz-band channel state information to identify adversarial beamforming attacks [79], where malicious actors leverage directional signal vulnerabilities to eavesdrop or jam communications. The RNNs, in particular, the LSTM networks [117], model sequential dependencies in time-series data such as API call logs or spectrum utilization trends, to predict multi-stage attacks targeting 6G's AI-native core. Transformers, which are renowned for their success in NLP, will provide semantic security in 6G by detecting malicious intent within an incoming text or voice command that controls critical infrastructure, such as smart grids or emergency response systems

Table 2.1: Summary of Some AI Techniques for 6G Security

Technique	Key Components	Applications in 6G Security	Limitations & Mitigations
Machine Learning (ML)	• Supervised Learning (e.g., SVMs, Decision Trees) • Unsupervised Learning (e.g., DBSCAN, Autoencoders) • Semi-supervised Learning	• Anomaly detection in URLLC channels [126] • Clustering unknown threats in IoT ecosystems [127] • Detecting adversarial latency injection [128]	• **Limitations**: Dependency on labeled data, adversarial attack vulnerability • **Mitigations**: Active learning, adversarial training, hybrid AI-DLT frameworks
Deep Learning (DL)	• CNNs (spatial-temporal analysis) • LSTMs/RNNs (sequential threat prediction) • Transformers (semantic intent detection)	• Detecting adversarial beamforming in terahertz bands [79] • Forecasting multi-stage attacks on 6G core [117] • Securing semantic communications (NLP) [129]	• **Limitations**: High computational cost, black-box opacity • **Mitigations**: Model pruning/quantization, explainable AI (XAI), TinyML
Federated Learning (FL)	• Federated Averaging (FedAvg) • Differential Privacy (DP) • Blockchain-integrated FL (e.g., PoC consensus)	• Privacy-preserving threat intelligence aggregation [130] • Scalable detection of swarm-based DDoS attacks [131] • Secure model training in healthcare/defense [44]	• **Limitations**: Model poisoning, Byzantine failures • **Mitigations**: Blockchain validation, gradient compression, Proof of Contribution (PoC)

[134]. However, DL's computational intensity requires hardware-aware optimizations-such as pruning and quantization-to deploy models on energy-constrained edge devices without compromising inference speed.

Federated Learning (FL) addresses the dual challenges of privacy and scalability inherent to 6G's decentralized architecture [125]. By enabling collaborative model training across distributed edge devices without centralized data aggregation, FL preserves user privacy—a critical requirement for healthcare, defense, and other sensitive sectors. Differential privacy (DP) mechanisms further anonymize model updates, adding calibrated noise to prevent adversaries from reconstructing raw data from gradient transmissions [22]. In 6G's huge IoT ecosystems, the global models are aggregated using FL frameworks like Federated Averaging, developing threat intelligence from billions of sensors that can detect novel attack patterns, such as swarm-based DDoS attacks orchestrated by compromised drones. On the other hand, FL also introduces unique risks, including model poisoning and Byzantine failures, where malicious participants submit adversarial updates to degrade global model performance. Hybrid FL-DLT architectures dispel these risks by incorporating blockchain-based consensus mechanisms to validate the contribution to ensure that only trusted updates have an influence on the federated model [135, 136]. For example, Proof of Contribution algorithms favor updates contributed by devices that have established their reliability [137], while smart contracts trigger automated exclusion of outliers showing abnormal behavior.

2.2.3 Challenges of AI in 6G Security

The integration of AI into the security architecture of 6G brings both capabilities and challenges that threaten to undermine its efficacy. These challenges arise from the singular interplay of 6G's hyper-scalable architecture, its reliance on heterogeneous and distributed data sources, and the adversarial landscape amplified by AI-native threats. Overcoming these obstacles requires a deep understanding of the technical underpinnings and the development of effective countermeasures balancing performance, privacy, and resilience.

Data Privacy and Regulatory Compliance

6G will be rolled out in an environment of acute sensitivity towards data, wherein the integration of AI with terahertz-frequency communications, pervasive IoT deployments, and immersive applications will create unparalleled volumes of personal and operational data [11]. The dependency of AI on large-scale datasets for training and inference, from user location traces to network slicing configurations, inherently creates systemic privacy risks [8]. For example, while FL is designed to be privacy-preserving by decentralizing model training, it inadvertently reveals metadata patterns-such as gradient updates-that can be leveraged by adversaries to induce sensitive attributes through model inversion attacks [89]. DP mechanisms introduce calibrated noise into the training data or gradients and provide partial mitigation [138], but often degrade model accuracy for mission-critical applications such as autonomous vehicle coordination or remote surgery, where precision cannot be compromised. Furthermore, 6G's global reach intersects with conflicting reg-

ulatory regimes: the European Union's General Data Protection Regulation (GDPR)[1] imposes strict data localization requirements, while AI-driven threat detection systems in cross-border networks must dynamically reconcile these constraints with real-time security operations [8]. The emergence of quantum computing exacerbates these risks, as future quantum algorithms could retrospectively decrypt anonymized datasets, rendering today's privacy-preserving techniques obsolete [81].

Adversarial Attacks and Model Robustness

The AI models that form the backbone of 6G security are inherently susceptible to adversarial attacks-sophisticated exploits that manipulate either input data or model parameters to deceive learning systems [89]. Such attacks manifest themselves along multiple dimensions:

- *Evasion Attacks:* Along this line, the adversary introduces variability in network traffic patterns, such as packet arrival time or signal characteristic variations, which can easily bypass AI-driven IDS [139]. For example, slight changes in terahertz channel state information may easily make CNNs misclassify jamming attacks as benign interference.
- *Poisoning Attacks:* Attackers inject poisoned data into the training datasets to make the AI models geared towards some kind of exploitable behavior [140]. Compromised RAN Intelligent Controllers may lead to poisoning federated learning processes within 6G's O-RAN ecosystems, making global models misallocate resources or even ignore legitimate threats.
- *Model Extraction/Inversion:* Attackers leverage API access to query AI models and reverse-engineer proprietary algorithms or training data [141]. This is particularly critical in 6G's AI-as-a-Service paradigms, where third-party vendors supply threat detection models to network operators.

Such threats need adversarial training techniques that basically harden models against perturbed inputs during training, while integrating XAI frameworks for auditing of decision logics [14]. However, adversarial robustness often comes at the expense of model accuracy and computational efficiency [89], which would be a delicate balance for latency-sensitive 6G applications like industrial automation or augmented reality.

2.3 Overview of Distributed Ledger Technologies in 6G Security

The integration of DLT into 6G security architectures is a conceptual change toward a system that is decentralized, transparent, and tamper-evident [48]. As 6G networks develop to support ecosystems of billions of devices, terahertz-frequency communications, and AI-native services, the traditional security paradigm based on centralization is incapable of

[1] https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf

addressing scalability, complexity, and trust needs for next-generation connectivity. DLT, with its inherent features of decentralization, immutability, and cryptographic trust, provides a strong basis for securing the hyperconnected and heterogeneous infrastructure of 6G [94] (an example is illustrated in Fig 2.2 [9]). This section provides an overview of the role that DLT can play in 6G networks, the technical frameworks that allow its application, and the challenges to be overcome for the full realization of its potential.

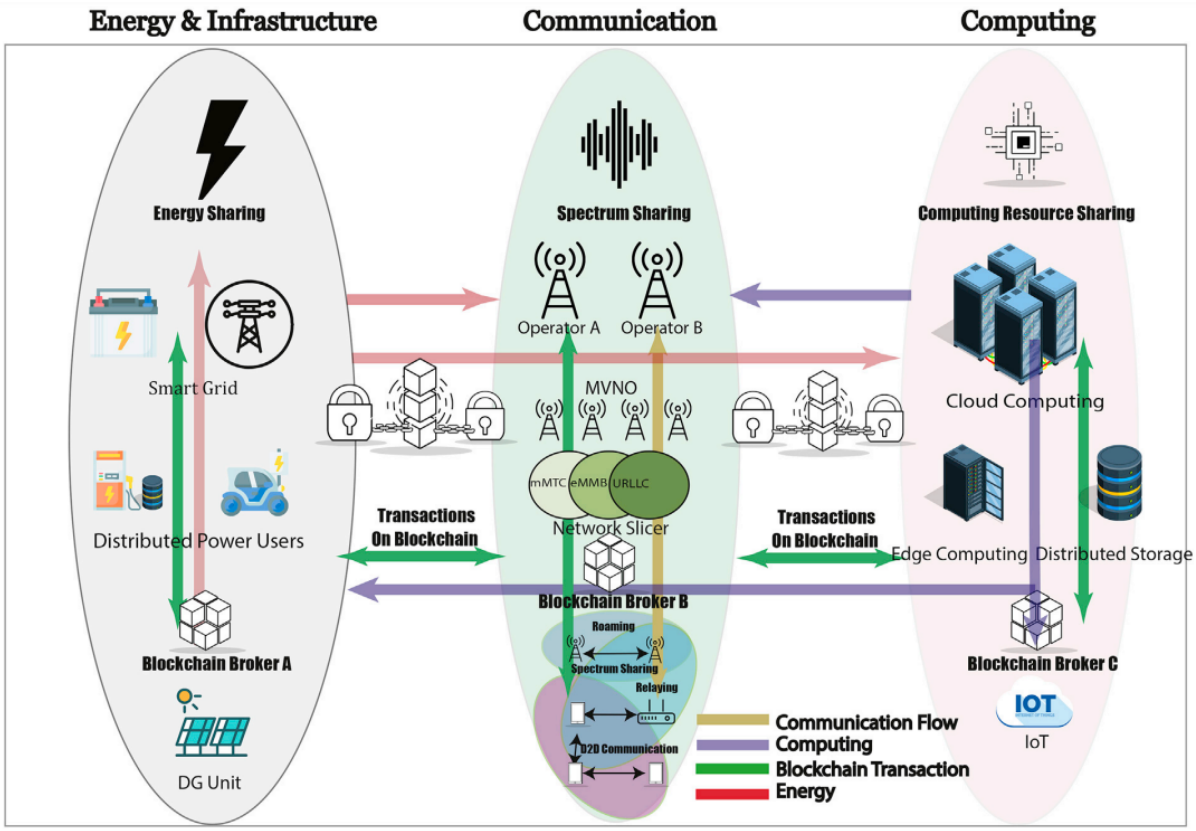


Figure 2.2: Blockchain-enabled resource management framework. [9]

2.3.1 Role of DLT in 6G Networks

DLT is perfectly suited for the 6G vision of a truly distributed, self-organizing network architecture [142]. In contrast to a traditional system's single point of failure, DLT distributes trust among nodes in a network to provide resilience against both targeted attacks and systemic failures [143]. This will be of particular criticality in the ultra-dense deployments of 6G, with edge devices, drones, and satellites forming a dynamic mesh of interconnected nodes [130]. Another cornerstone for DLT comes in the form of immutability: any data recorded on the ledger cannot be changed or deleted without consensus from the network [144]. This property makes it very desirable to handle audit trails for security-critical applications, which can range from tracking device identities in gigantic IoT ecosystems all the way to logging network slicing configurations within O-RAN architectures [144]. Basic verifiability grounds the cryptographic trust mechanisms for secure transactions and communication in the case of risks, such as spoofing, man-in-the-middle attacks, and unauthorized access, by public-private key pairs and consensus algorithms

[136]. These features collectively set DLT as the transformative enabler of 6G security by fostering trust in an inherently untrusted environment [145].

2.3.2 DLT Techniques for Security

Most of the technical variants of DLTs are best suited for different security requirements and operational constraints. The best-known form of DLT is blockchain, a tamper-proof ledger that enables secure data sharing and identity management [142]. Blockchain may be applied in 6G wireless for the authentication of devices in massive-node IoT ecosystems [100], ensuring that only authorized entities participate in network operations. A blockchain-based identity management system, for example, might block rogue drones from infiltrating a swarm or unauthorized sensors from accessing critical infrastructure [142]. Smart contracts are self-executing programs deployed on blockchain platforms that automate the enforcement of security policies dependent on centralized authorities [48]. While intelligent contracts can autonomously compute resource allocation for service-level agreements (SLAs) enforcement [146] and access revocation of a compromised slice, grounded on an unalterable history of transactions in the 6G dynamic network slicing context. Directed Acyclic Graphs (DAGs) [147], a scalable alternative to traditional blockchain architectures, address the performance limitations of linear blockchains by enabling parallel transaction processing. This makes DAGs especially suitable for IoT-driven 6G networks, where millions of devices generate high-frequency, low-latency transactions.

2.3.3 Challenges of DLT in 6G Security

In spite of the bright transformative potential of DLT into 6G security, critical challenges exist as a consequence of scalability, consumption of energy, and integrability. Scalability remains an area of vital interest, because DLT architectures most commonly cited as viable cannot enable transaction throughput or latency necessary within 6G's massive-device ecosystems [6]. For example, blockchain's consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), introduce delays that are incompatible with 6G's sub-millisecond latency requirements. Energy consumption is another important issue, especially for PoW-based blockchains, since their transaction validation requires enormous computational resources [148]. In the energy-constrained environments foreseen for 6G, like battery-powered IoT devices or solar-powered drones, this inefficiency is untenable. This can be done by transitioning into energy-efficient consensus mechanisms, like PoA or PoC; however, such a shift comes at the potential cost of compromised network neutrality or trust [149]. Challenges also arise with respect to integrations with both legacy systems and emerging 6G technologies. For example, DLT frameworks will need to be interoperable with AI-native protocols, quantum-resistant cryptographic algorithms, and heterogeneous network architectures in compliance with dynamic regulatory standards. These are holistic challenges that require advances in DLT design to go in parallel with energy-efficient hardware and cross-industry collaboration, allowing for full potential to be unlocked regarding decentralized security in 6G networks.

2.4 Convergence of AI and DLT in 6G Security

The integration of AI and DLT in 6G is about a paradigm shift from merely adaptive intelligence toward decentralized trust at scales, dynamics, and complexity never witnessed in connectivity. The following section goes beyond the coexistence of the two and covers this synergistic framework where AI and DLT reinforce each other's powers and reduce their respective limitations. Further sections detail the synergy, technical methodology, and emerging frontiers of research marking this transformational integration.

2.4.1 Synergies Between AI and DLT

AI reinforces DLT in terms of improving performance and scalability, which is very crucial for 6G's massive-device ecosystems [148]. ML algorithms, such as reinforcement learning, dynamically adjust the consensus mechanisms within the blockchain network to reduce latency and energy use [150]. As a concrete example, an RL agent may use immediate network congestion to continuously calibrate the hardness of PoW puzzles so that transaction validation times are not delayed, while the security features are protected [151]. On the other hand, DLT strengthens AI with immutable, auditable frameworks for data and model governance [148]. Tamper-proof ledgers from blockchain ensure that AI training datasets are safe from adversarial tampering, allowing for verifiable provenance of federated learning updates or sensor data in mission-critical applications such as navigation in autonomous vehicles [150]. Smart contracts further automate trust in AI workflows [146], as they enforce fairness in the aggregation of federated models, penalize malicious participants in decentralized AI marketplaces, and trigger automated responses to AI-detected threats-such as isolating compromised network slices. Together, these synergies create a self-reinforcing security loop—AI-driven efficiency sustains DLT's scalability, while DLT's transparency anchors AI's adaptability in trustless environments [150]. An illustration of such synergy can be found at Fig. 2.3 [10].

2.4.2 Technical Methods and Approaches

Bringing AI and DLT integration into sixth-generation security is operationalized through three core methodologies, each of which solves distinct challenges while amplifying the strengths of both disciplines. AI-enabled blockchain optimization uses machine learning to improve the performance and adaptability of DLT frameworks [152]. Reinforcement learning algorithms [151], trained on real-time network telemetry, dynamically refine consensus mechanisms such as Proof of Stake or Delegated Byzantine Fault Tolerance [153]. In particular, an RL agent can perform optimal validator selection in a sharded blockchain and cut down the consensus latency from minutes to milliseconds at Byzantine fault tolerance for 6G ultra-dense edge networks. That would be very critical in applications such as real-time spectrum auctions or vehicular network handovers, where delays might compromise safety and efficiency [151]. Blockchain-secured AI models make use of DLT for assurance of integrity and traceability of the AI workflow [150]. Anchoring the training data, model parameters, and inference results in an immutable ledger, blockchain removes all risks such as data poisoning or model tampering [137]. In the case of federated learning

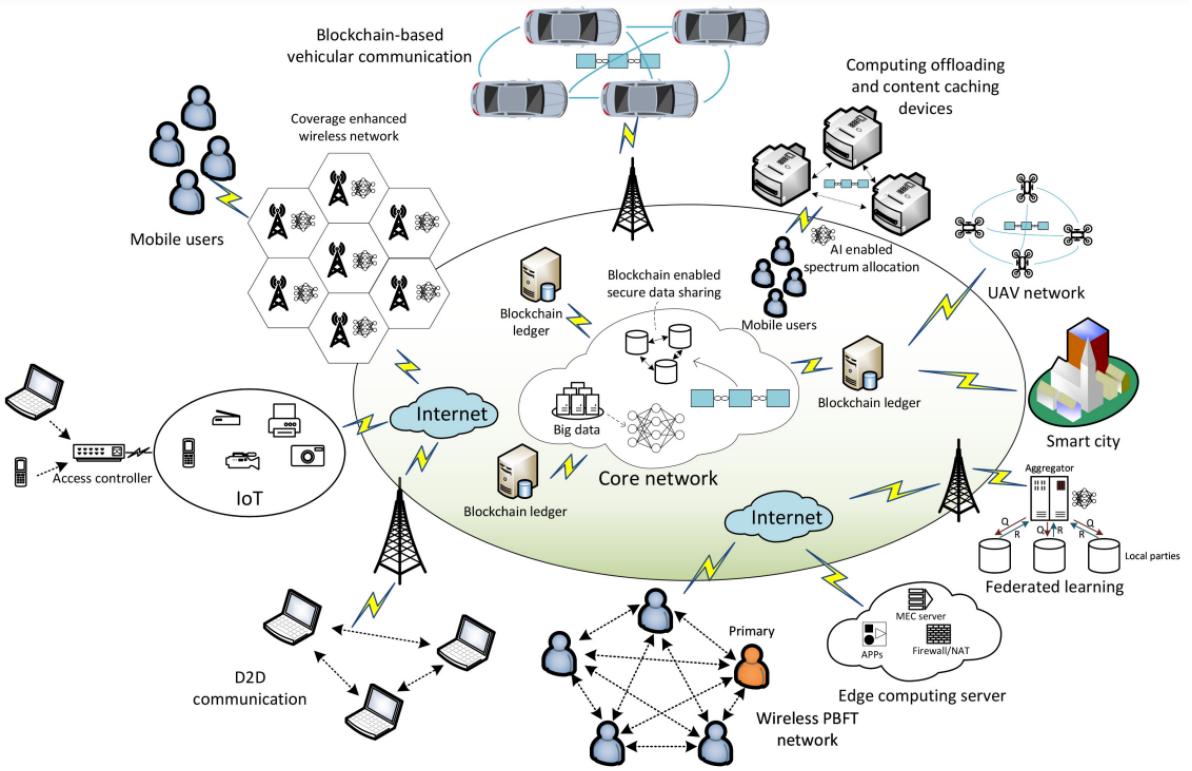


Figure 2.3: AI-DLT technologies synergy for 6G [10]

in 6G healthcare IoT, for example, smart contracts will enforce strict access controls and log all contributions, allowing auditors to track down adversarial inputs to the source-compromised edge devices. These get merged into cohesive architectures in the case of joint AI-DLT frameworks, such as federated learning with blockchain-based aggregation [137]. Here, edge devices collaboratively train intrusion detection models without essentially sharing raw data [154]. A blockchain ledger records updates of models and also verifies the contribution through Proof of Contribution consensus. This hybrid approach will not only preserve privacy but ultimately thwart Sybil attacks wherein malicious nodes attempt to corrupt the training process based on fake identities. Such schemes are necessary to secure 6G's massively scaled IoT ecosystems, wherein centralized trust authorities are impractical [155].

2.4.3 Emerging Research Trends

This convergence of AI and DLT in 6G security has been forwarded, in turn, by a set of state-of-the-art research directions. Quantum-resistant DLT addresses the looming threat of quantum computing against classical cryptographic primitives [156]. Among others, lattice-based blockchain protocols [157]. AI-driven smart contracts embed machine learning directly into the DLT workflows [158], thus granting adaptive, context-aware security policies. Transformer- or GNN-powered neural smart contracts independently modify access controls or resource allocations based on real-time threat intelligence [159]. For instance, such smart contracts can allow for dynamic traffic rerouting through uncompromised slices during DDoS attacks predicted by the AI or isolating slices where a breach was

Table 2.2: Classification of Related Works in 6G Security

Category	Focus	Examples	Key Strengths	Limitations
AI-centric	Intrusion detection, anomaly detection, threat classification using ML/DL	CNNs on THz bands [163], Transformers for semantic analysis [8]	Real-time detection, adaptation to evolving threats	Privacy risks, vulnerability to data/model poisoning [89]
DLT-centric	Decentralized identity, secure handovers, access control	Blockchain for vehicular handovers [94], smart contract enforcement [105]	Immutability, transparent trust, no SPoF	Latency, scalability issues in dense IoT environments [156]
AI-DLT Hybrid	Federated learning with blockchain, consensus tuning with RL, auditable AI	FL + Blockchain [137], RL-enhanced validator selection [151], Explainable AI anchored to DLT [108]	Privacy-preserving, traceable, robust to Sybil attacks [155]	Complexity, integration overhead [135]

detected, immutably recording all the associated actions on-chain. Blockchain thus democratizes AI resources in the decentralized marketplaces of 6G. By tokenized incentivization, it allows edge nodes to trade their computational powers, datasets, and pre-trained models, with quality contributions audited by AI themselves. Obstacle detection models can, for instance, be crowdsource-trained by swarms of autonomous drones with fair compensation and provenance guaranteed by blockchain [160]. Other emerging trends involve self-healing AI-DLT networks, where GNNs predict node failures in decentralized ledgers and trigger automated recovery protocols [161], while ethical AI governance frameworks are proposed where, thanks to blockchain, fairness and accountability in AI decisions affecting multi-stakeholder 6G infrastructures are visibly enforced [162]. Put together, these advancements are redefining the boundaries of secure, cognitive, and decentralized networking.

2.5 Comparative Analysis of Existing Solutions

The future landscape for 6G security solutions requires an essential investigation into AI-centric, DLT-centric, and hybrid AI-DLT approaches. In this regard, this section classifies the methodologies adopted, benchmarked the performance metrics, and pinpoints unresolved challenges, therefore acting as a stepping stone toward advancing integrated frameworks to fit the unique requirements of 6G.

2.5.1 Classification of Research

The variety of existing research in the domain of 6G security could be divided into three paradigms (Table 2.2). *AI-focused solutions* prioritize machine and deep learning in solving dynamic threats [8]. For instance, terahertz-band channel state information is analyzed in convolutional neural networks to detect physical-layer spoofing [163], while transformers model semantic communication for identifying adversarial intent in text or voice commands. These approaches are excellent at real-time anomaly detection but usually overlook the aspects of trust and decentralization, hence becoming vulnerable to data poisoning and model inversion attacks [89]. *DLT-based solutions* create decentralized trust by building on blockchain, DAGs, and smart contracts. This includes blockchain-secured handover protocols in vehicular networks that make use of immutable ledgers to authenticate vehicles during handing over from 5G or 6G base stations and smart contracts for automation of zero-trust access policies in network slicing [94]. While robust against single points of failure, these frameworks are at struggles concerning scalability and latency in ultra-dense IoT environments [105]. *Integrated AI-DLT solutions* bridge the gaps by amalgamating the adaptability of AI with DLT's transparency [135]. Hybrid authentication frameworks, including federated learning with blockchain-based model aggregation, can enable device authentication in privacy-preserving manners across 6G's massive-node ecosystems [94]. Other examples of current interest include AI-optimized consensus algorithms, reinforcement learning for sharded blockchains, and blockchain-anchored explainable AI for auditing autonomous security decisions [47, 108, 164].

2.5.2 Comparison of Related Works on 6G Security Architectures

Such model effectiveness varies across critical sixth-generation metrics. Solutions centered on AI achieve sub-millisecond response times for threat detection using lightweight models such as TinyML [116], ideal for URLLC applications such as remote surgery or industrial automation. Yet their reliance on centralized data aggregation poses privacy risks and limits scalability beyond 10^7 devices per square kilometer [165]. DLT-focused solutions provide unequaled trust and immutability. For example, Blockchain-based secure handover protocols prevent man-in-the-middle attacks [166]. However, their energy consumption is still forbidding: PoW-based blockchains consume much more power than AI-driven alternatives [111], making them unfit for battery-constrained edge devices. Integrated AI-DLT frameworks balance these trade-offs. AI-optimized proof-of-stake mechanisms achieve faster consensus times in federated learning [167], while still offering GDPR-compliant audit trails [168]. However, within this complexity is also a plethora of issues-including interoperability bottlenecks between AI and DLT protocols [169]. Tab 2.3 provide a summary of a comparison between selected related works.

2.5.3 Discussion and Thesis Contributions

Literature review analysis reveals that while considerable advancement has been achieved in leveraging AI, DLT, and their combination for 6G security, certain significant challenges

Table 2.3: Comparison of Related Works on 6G

Ref.	Approach	Security Focus	Technique	Benefits	Limitations
[94]	DLT-centric	Authentication, secure handovers	Blockchain-based identity validation	Decentralized access control, high auditability	Latency under mobility, resource-intensive consensus
[105]	DLT-centric	Access control, zero-trust enforcement	Smart contracts for network slicing	Zero-trust automation, transparent access logs	Smart contract bugs, interoperability gaps
[151]	AI-DLT Hybrid	Validator optimization	RL-based consensus in sharded blockchains	Reduced latency, dynamic trust model	Requires frequent retraining, complex policy tuning
[137]	AI-DLT Hybrid	Intrusion detection, FL privacy	Blockchain-secured federated learning	Privacy-preserving IDS, Sybil-resilient FL	MPC introduces computational cost
[163]	AI-centric	Spoofing detection in PHY layer	CNN on THz channel info	High detection accuracy, no centralized training needed	Doesn't ensure traceability, not decentralized
[108]	AI-DLT Hybrid	AI model auditing	Explainable AI anchored to Blockchain	Traceable inference, auditable learning pipeline	High on-chain data footprint, opaque to users

remain outstanding.

- **AI-centric solutions:** offer strong adaptability and are efficient in identifying zero-day attacks through methods like CNNs on terahertz-band data [163] and transformers for semantic threat analysis [8]. They are prone to data poisoning, adversarial inputs [89], and model lack of transparency [47].
- **DLT-based designs** emphasize decentralized trust and safe resource management using blockchain and smart contracts [94]. Although these structures prevent point failures, they are bound by limitations in performance and scalability in highly dense networks [105, 156].
- **Hybrid AI-DLT paradigms** offer valuable synergies such as AI-facilitated validator choice [151], blockchain-surfaced federated learning [137], and understandable AI augmented with invariant ledgers [108]. Still, the majority of these designs face complexity during deployment, unacceptable latency, and lack of end-to-end standardised integration protocols [135].

In order to do the above, this thesis proposes a joint architecture for blockchain-based federated learning to facilitate privacy-preserving, decentralized intrusion detection in 6G networks. It outlines an IDS model by embracing multi-party computation to ensure confidentiality and reduce latency, and an AI-blockchain architecture that is light for secure and scalable identity verification. Such advancements are designed to address the architectural, operational, and regulatory needs of 6G environments and overcome current shortcomings in terms of adaptability, trust, and performance. Each of these proposed solutions will be presented and elaborately discussed in the following chapters.

2.6 Conclusion

This chapter reviews the transforming potentials of both AI and DLT in the security of 6G networks, discusses their individual strengths and synergistic convergence, and identifies the challenges to be addressed in realizing their full potentials. The adaptability and real-time threat detection capabilities of AI merged with the decentralization of trust and immutability provided by DLT result in a strong base for addressing unprecedented scale and complexity in 6G. However, stat of the art research has some limitations that remains, e.g in energy efficiency, and lightweight model deployment. The next chapter presents our contributions.

Chapter 3

6G-SecureIDS: Blockchain-Enhanced Secure Knowledge Transfer for Distributed Intrusion Detection Systems in Advanced Networks

3.1 Introduction

Exponential growth in wireless communications has set the stage for the next-generation 6G networks. As the natural follow-up to 5G, 6G is expected to offer unparalleled connectivity, extremely high data rates, and a large range of supported applications. With the continuously increasing number of devices connected and more advanced network infrastructures, robust security and privacy are critical in this advanced ecosystem [1].

One of the key challenges is to design effective and efficient distributed Intrusion Detection Systems (IDS) that are able to efficiently identify and counter potential security threats. Traditional IDS solutions typically use centralized models, wherein all the network traffic is funneled into a single server for analysis. Centralized models, however, have serious shortcomings such as weak scalability, excessive bandwidth consumption, and vulnerability to single points of failure.

The inclusion of artificial intelligence in 6G networks has vast potential to drive innovation and enable real-time intelligent decision-making. In the meanwhile, Federated Learning (FL) is a promising approach that can allow distributed parties to learn models jointly with data privacy. Through federated learning techniques, distributed IDS can learn from local datasets collectively without centralizing data aggregation [125].

Though FL has privacy advantages, its adoption in distributed environments comes with new security challenges [80, 170]. While FL permits a number of edge devices to collectively train models without sharing confidential information with a central server, it is not secure against such threats as poisoning attacks and unauthorized exposure of private information by attacking servers [171]. These vulnerabilities emphasize the need for new solutions that ensure the integrity and security of the FL process in 6G networks. To fill these gaps, we present a new framework, *6G-SECUREIDS*, which integrates fed-

erated learning, model distillation, and blockchain technology to train distributed IDS in 6G networks.

3.1.1 Motivation

Our inspiration comes from the realization that 6G networks will become imperative to serve an immense universe of advanced applications—from augmented reality and IoT implementations to autonomous automobiles and so on [172]. Privacy protection and guardship of these applications are far more than technical necessities; rather, they're a necessity in order to enable the mass penetration and success of 6G technology.

Since conventional security mechanisms are unable to manage 6G's new architecture, enormous amounts of data, and varied communication paradigms, stringent security measures must be specifically designed to neutralize such emerging threats. Our aim is to implement preventive techniques that will be capable of detecting and restraining potential attacks before they have even entered the middle layers of the network so that intrusions can be properly halted before they cause any loss. This future-oriented direction aligns with the greater objective of securing and safeguarding 6G wireless networks, thereby achieving maximum total trust and reliability in next-generation communications.

Inspired by the necessity of robust security for this new environment, our proposed framework takes advantage of the robustness of the synergy between blockchain technology and Federated Learning to proactively detect and nullify security attacks. Through addressing the specific complexities of 6G networks, 6G-SECUREIDS is set to bridge existing gaps in security and protect wireless communications integrity.

Table 3.1: Related Works

Work	**Year**	**Main Contribution**	**Network Model**	**Limitations**
[173]	2019	Fl-based IDS for MCPS	MCPS	Model security was not discussed
[174]	2020	FL-Based IDS for IoT	IoT	Model security was not discussed
[175]	2022	Fl-based semi-supervised IDS	IoT	Generalization
[176]	2022	Securing FL from poisoning attacks	IoT	Energy Consumption not considered
[177]	2023	FL-based Cyber Threat Intelligence Sharing Scheme	General-purpose network	- System scalability was not included -Model security was not discussed

3.2 Related Works

There have been numerous studies on employing Federated Learning (FL) to enhance intrusion detection systems that have made invaluable contributions towards this field. For example, Sarhan et al. presented a cyber threat intelligence sharing model that leverages FL to overcome restrictions when imposing machine learning on diverse collections of data samples for detecting network attacks [177]. Their method, validated using the NF-UNSW-NB15-v2 and NF-BoT-IoT-v2 NetFlow datasets, was compared with centralized and localized training methods. The results demonstrated that their approach could differentiate between malicious and benign traffic from various organizations without compromising sensitive information. However, the study also identified that additional research is needed to address scalability, privacy preservation, and practical deployment concerns.

Similarly, Rahman et al. [174] proposed an FL-based solution for IoT intrusion detection to solve scalability and privacy issues. In their solution, local training and prediction are performed on IoT devices and model updates are communicated to a remote server, which aggregates them to produce a better model for all the participants. Although this approach is extremely accurate and better than models trained purely on single devices, it is still vulnerable to being attacked during aggregation, where adversarial attacks or hacked devices can add bad updates.

Aouedi et al. [175] dealt with the problem somewhat differently in that they developed FLUIDS, an IDS that embeds FL with a semi-supervised learning strategy. Combining both supervised and unsupervised learning methods, FLUIDS builds a cooperative environment that can learn under varying data conditions. Nevertheless, its performance can differ in terms of datasets or network configurations utilized, and generalizability across various intrusion detection scenarios requires further testing. Schneble et al. [173] addressed security concerns in Medical Cyber-Physical Systems (MCPS) in another work through the development of a distributed intrusion detection system with the use of machine learning and FL. Their approach had high detection accuracy with low false positives and reduced the overhead of network communication, even though it remains problematic in being robust against adversarial attacks and needing better privacy preservation.

Zhang et al. [176] presented SecFedNIDS, an effective and secure IDS for IoT networks that uses FL to protect against poisoning attacks by malicious clients. Their defense entails defensive methods at both data and model levels; model-level defenses target the selection of key model parameters and the rejection of poisoned models, and data-level defenses involve dropping malicious traffic on the basis of class path similarity. Experimental results showed significant accuracy gains—48% and 36% on the UNSW-NB15 and CICIDS2018 datasets, respectively—when poisoned. Aside from these promising results, there remains doubt regarding the generality of the defense methods to other datasets or actual deployments, along with concerns regarding the increased energy cost on resource-constrained IoT devices in terms of extra computation and communication overhead.

Tab. 3.1 provides an overview of these contributions, the major achievements, network models, and limitations of the respective studies.

In this chapter, we present a novel framework to enhance the security of 6G net-

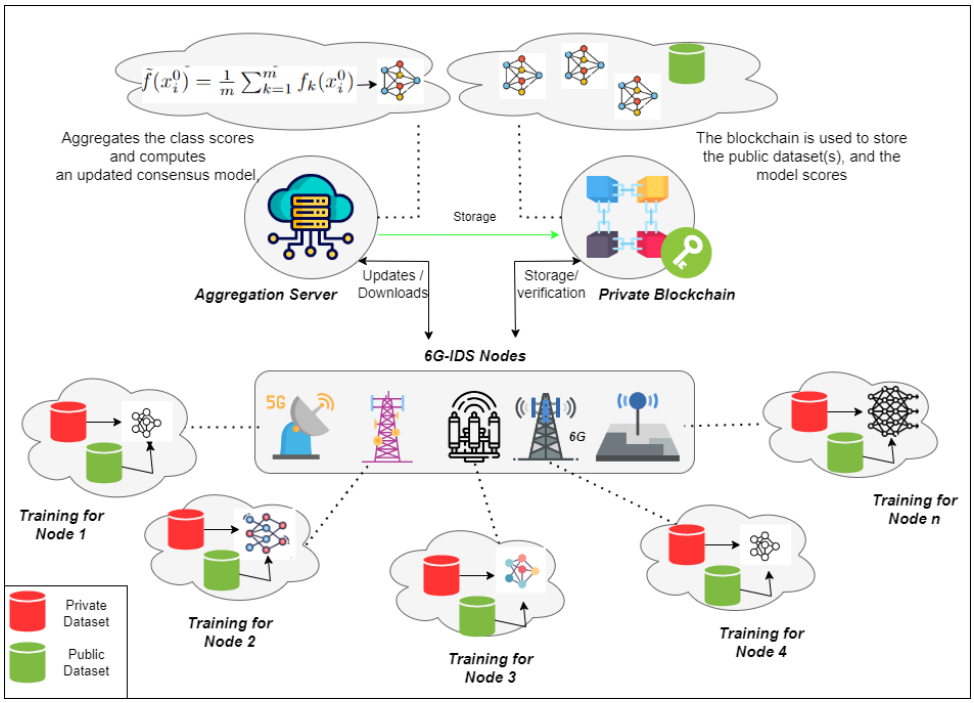


Figure 3.1: 6G-SECUREIDS architecture

work intrusion detection systems via synergistic use of Federated Learning (FL), Model Distillation (MD), and blockchain. The proposed solution counteracts significant FL vulnerabilities—namely, poisoning attacks and potential manipulation by hostile aggregation servers—by injecting advanced MD techniques for enhancing and safeguarding the learning process. Besides, we employ a private blockchain to maintain the teacher model in storage, thereby ensuring model update integrity and verifiability. This coupled model not only resolves the existing security issue but also lays a solid foundation for secure, scalable, and dependable intrusion detection in the future 6G communications environment.

3.3 Proposed Framework: 6G-SECUREIDS

In this section, we present the detailed framework of 6G-SECUREIDS to enhance the security of 6G network intrusion detection systems by synergistic integration of Model Distillation (MD), Federated Learning (FL), and blockchain. The methodology presents solutions to FL's grave vulnerabilities of poisoning attacks and potential intrusion by malicious aggregation servers by applying innovative MD techniques for distilling and securing the learning process. Furthermore, we employ a private blockchain to securely store the teacher model and ensure the integrity and verifiability of revised models. Not only does the integrated framework mitigate common security attacks, but it provides a solid foundation for secure, scalable, and trustworthy intrusion detection in 6G communication's dynamic landscape as well.

3.3.1 Building Blocks

Collaborative Learning for Distributed IDS

At the core of 6G-SECUREIDS is the tactical use of federated learning to facilitate collaborative model training across distributed entities without sacrificing the privacy of local data. Every participating entity, possessing its own dataset, is engaged in an orchestrated communication, aggregation, distribution, and training process. Secure communication channels are utilized to allow them to compute class scores—quantitative outputs derived from their respective IDS models—a public dataset. The class scores are then transmitted to a central server, where they are aggregated to enhance the overall efficacy of the intrusion detection system.

Knowledge Transfer through Model Distillation

In 6G-SECUREIDS architecture, model distillation [178] is a main mechanism to transfer knowledge from a central consensus model to individual local models. After aggregating class scores from the distributed agents, the central server computes a new consensus model by averaging the class scores, as discussed in [179]. The consensus model represents the aggregated knowledge and prediction ability of all participating agents. Each agent then downloads this updated model and employs it to train its local IDS, thus aligning its predictions with the consensus. This training process, involving approximating the consensus model's behavior on a shared public dataset, is in fact a process of knowledge distillation. By this distillation process, local models can take advantage of the distilled knowledge and thus enhance their performance and security threat detection precision. This is done through an extension of [179] to ensure that the distributed IDS is collectively enhanced by a single strong model without invading local datasets' privacy.

Blockchain Integration for Immutable Trust

Blockchain is employed in the 6G-SECUREIDS to establish trust and integrity for the public dataset. A private blockchain layer is used to store a record of the cryptographic hash of the public dataset so that there is an immutable record, which can serve as a trust anchor. It enables every participant independently to authenticate the legitimacy of the dataset using their own credentials. By offering greater transparency and immutability, the blockchain layer protects against the threat of tampering or unlawful modifications [180]. Therefore, the application of blockchain technology greatly enhances the confidence and trustworthiness of the distributed IDS training process.

In addition, to maximize the security of the master node, a very strong set of security controls has been implemented. These include the adoption of very secure encryption methods, the conduct of regular security scans, and continuous monitoring with the aim of detecting any unusual activity. Additional protection is afforded by having the master node operate within a secure, isolated environment to limit exposure to external threats.

Algorithm 1 6G-SECUREIDS: Enhanced Federated Learning Algorithm with Blockchain-based Public Dataset Hash Verification

Require: Public dataset D_0, private datasets D_k, independently designed model f_k, $k = 1, \ldots, m$

Output: Trained model f_k

procedure 6G-SECUREIDS(D_0, D_k, f_k)

Blockchain Initialization: Initialize an empty blockchain B

Compute the hash $H(D_0)$ of the public dataset D_0

Add $H(D_0)$ as the genesis block in the blockchain B

Each node verifies the genesis block using their credentials

Transfer Learning: Each party trains f_k to convergence on the public dataset D_0 and then on its private dataset D_k

for $j = 1, 2, \ldots, P$ **do**

Communicate: Each party computes the class scores $f_k(x_i^0)$ on the public dataset and transmits the result to a central server

Aggregate: The server computes an updated consensus, which is the average: $\tilde{f}(x_i^0) = \frac{1}{m} \sum_{k=1}^{m} f_k(x_i^0)$

Blockchain Update:

a. The server computes the hash $H(\tilde{f}(x_i^0))$ of the updated consensus

b. The server adds $H(\tilde{f}(x_i^0))$ as a new block in the blockchain B

Each node verifies the new block using their credentials

Distribute: Each party downloads the updated consensus $\tilde{f}(x_i^0)$ from the server

Each party verifies the integrity of the downloaded consensus using the blockchain B

Digest: Each party trains its model f_k to approach the consensus $\tilde{f}$ on the public dataset D_0

Revisit: Each party trains its model f_k on its own private data for a few epochs

end for

end procedure

Figure 3.2: 6G-SECUREIDS Algorithm

3.3.2 Framework Implementation

In this subsection, we present the implementation details of the 6G-SECUREIDS framework, describing the steps involved in the collaborative learning process, knowledge transfer through model distillation, and blockchain integration.

Collaborative Learning Process

The algorithm for the collaborative learning process is outlined in Algorithm 1. Here, we provide a step-by-step description of the process:

- **Blockchain Initialization:** The framework starts by initializing an empty blockchain, denoted as B. The public dataset, denoted as D_0, is hashed to obtain its cryptographic hash, $H(D_0)$. This hash value is added as the genesis block in the blockchain B.
- **Transfer Learning:** Each participating entity trains their independently designed model, f_k, on the public dataset D_0 and their respective private datasets D_k to convergence. This transfer learning step allows each entity to acquire initial knowledge from the public dataset and adapt it to their local data.
- **Communication and Aggregation:** In each iteration, the entities compute the class scores, $f_k(x_i^0)$, representing the predictions of their individual models on the public dataset. These class scores are then transmitted to a central server. The server aggregates the class scores and computes an updated consensus model, denoted as $\tilde{f}(x_i^0)$, by taking the average of the individual models' class scores.
- **Blockchain Update:** Each participating entity computes the hash, $H(\tilde{f}(x_i^0))$, of the updated consensus model and adds this hash value as a new block in the blockchain B. This ensures that the updated consensus model is recorded and linked to the previous blocks in the blockchain. The primary objective of storing data hash codes in the blockchain is to provide a tamper-evident and non-repudiable record of the training data. This mechanism enhances the reliability of the intrusion detection process. Also, we recognize that storing the entire machine learning models in the blockchain could potentially pose confidentiality concerns, especially when dealing with sensitive or proprietary data. Storing models in their entirety might risk exposing the underlying patterns and knowledge contained within the data, which could be exploited if the blockchain's security were ever compromised.
- **Distribute and Verify:** Each entity downloads the updated consensus model, $\tilde{f}(x_i^0)$, from the central server. They also verify the integrity of the consensus model by checking the corresponding block in the blockchain B. This step ensures that the model obtained from the server matches the recorded consensus in the blockchain.
- **Digestion and Training:** Each entity trains its local model, f_k, to approach the consensus model $\tilde{f}$ on the public dataset D_0. This step allows the individual models to distill the knowledge from the consensus model and adapt their parameters accordingly.

- **Revisiting Private Data:** After training on the public dataset, each entity revisits its private dataset, D_k, and performs a few additional training epochs to further fine-tune their models based on their local data.

The collaborative learning process iterates for a predetermined number of iterations, denoted as P, allowing the models to continuously improve and converge towards an optimal solution.

3.3.3 Advantages of 6G-SECUREIDS

The 6G-SECUREIDS framework provides substantial advantages compared to conventional federated learning mechanisms. First, it enables efficient utilization of resources by incorporating model distillation techniques that reduce communication overhead and computation complexity, thereby enabling distributed parties to collaboratively learn without the burden of extensive data exchange on a large scale. Second, it enhances privacy preservation with a federated learning approach that maintains sensitive local data within each entity, and the integration of blockchain technology additionally safeguards the integrity of the shared data by maintaining an incorruptible record of the public dataset. Finally, the framework is fault-tolerant in the sense that it distributes the learning process across a set of nodes, thereby minimizing the threats of single points of failure and ensuring continuous, reliable intrusion detection in spite of node compromise or network partitions.

Efficient Resource Utilization

One of the biggest advantages of 6G-SECUREIDS is its maximum resource utilization. Through the exploitation of a collaborative learning paradigm, the system enables distributed IDS nodes to collectively establish an effective model without depending on tremendous raw data exchange. Instead, individual models report class scores only to a server for summation. It minimizes communication overhead significantly and conserves both computational and networking resources, making this approach particularly well-suited for situations where resources are limited, i.e., edge devices or low-bandwidth networks. Consequently, efficient resource management not only maximizes scalability but also allows many entities to be added without subjecting the network infrastructure to excessive stress.

Enhanced Privacy Preservation

Privacy protection is an essential requirement in federated learning, and the 6G-SECUREIDS platform is designed with this as a fundamental principle. Here, class scores and the consensus model are the only items shared between entities during collaborative learning, with sensitive and confidential data remaining securely within each entity. Therefore, individual data sets are never transmitted across the network, so their confidentiality remains safeguarded when training. Additionally, use of blockchain technology is used to promote privacy protection with the public dataset and model modifications being

tamper-proof and unchangeable. This double-edged approach—having the data minimization within federated learning and the decentralized, secure ledger of blockchain—is what gives 6G-SECUREIDS a robust and reliable solution to privacy-sensitive use cases.

Heterogeneous Client Models:

The 6G-SECUREIDS framework accommodates the heterogeneous nature of client models [179]. Each participating entity is allowed to have independently designed models, denoted as f_k. This heterogeneity enables diverse perspectives and modeling approaches, which can enhance the overall effectiveness of the IDS. By aggregating predictions from these varied models, the framework can capture a broader spectrum of intrusion patterns and adapt to different network conditions. This heterogeneity not only enhances the robustness of the IDS but also leverages the complementary strengths of diverse detection strategies, ultimately leading to improved accuracy and resilience against evolving threats.

Fault Tolerance

Fault tolerance is a significant advantage of the 6G-SECUREIDS system. Decentralized design, based on blockchain deployment, inherently provides resilience against single node failure and adversarial attacks. In traditional federated learning environments, loss of a single cooperative client will interrupt the collaborative learning process. In contrast, the 6G-SECUREIDS framework is architected to allow for the learning process to continue even if a single or more than one node fails, thereby ensuring the integrity of the model consensus. The blockchain serves as a distributed ledger that securely maintains past model updates and enables recovery and continuity in case of node failures. This robust fault tolerance mechanism significantly enhances the overall robustness and reliability of the federated learning system. The combination of efficient resource utilization, enhanced privacy preservation, and fault tolerance in the 6G-SECUREIDS algorithm establishes a powerful and robust framework for collaborative learning in distributed IDS environments.

3.4 Experimental Evaluation

In this section we discuses our implementation of the learning phase of the 6G-SECUREIDS system.

3.4.1 Experimental Setup

We conducted our experiments using Google Colab, PyTorch, and the AIJack framework to evaluate the learning process of 6G-SECUREIDS. We also used the MNIST dataset for testing and evaluation. The experimental setup consisted of four client models, each with its own architecture. Table 3.2 provides an overview of the architecture details for each client model.

Table 3.2: Client Model Architectures

Client	Number of Nodes	Number of Layers
Client 1	784-10	2
Client 2	784-160-10	3
Client 3	784-140-10	3
Client 4	784-150-10	3

3.4.2 Results

The experimental results substantiate the efficacy of the proposed model, with all clients demonstrating comparable performance on both their local datasets and the validation dataset, irrespective of their distinct model architectures. This uniformity in results underscores the model's robustness and its capacity to perform consistently across diverse architectural configurations. Notably, Client 1, which employed the simplest model architecture comprising only a single linear layer, attained an accuracy of 90.14% on its private dataset and 90.42% on the validation dataset, as illustrated in Fig. 3.3 and Fig. 3.4, respectively. These findings indicate that even a basic model structure is capable of yielding competitive results.

Clients 2, 3, and 4 utilized more complex architectures with additional hidden layers, thereby enabling the learning of more sophisticated representations that capture intricate data patterns and relationships. Despite the increased complexity, the accuracy achieved by these clients—90.59%, 90.40%, and 90.51% on their local datasets, respectively—remained closely aligned with that of Client 1. This consistency across various architectures highlights the model's exceptional generalization capabilities; it demonstrates an ability to effectively learn and adapt to varying levels of complexity, thereby extracting pertinent features and producing accurate predictions. Consequently, the model's performance appears to be less contingent on specific architectural details and more reliant on its capacity to learn meaningful data representations.

The observed consistency in performance across heterogeneous architectures not only attests to the model's robustness but also suggests its potential for broad applicability. The ability to deliver reliable results across different architectural choices renders the model versatile and adaptable to a range of practical scenarios. Overall, the experimental findings reinforce the model's strength in achieving competitive accuracy across diverse configurations, thereby confirming its reliability and suitability for deployment in various real-world applications.

3.5 Conclusion

In this chapter, we introduced 6G-SECUREIDS, an intrusion detection system engineered specifically for the demands of 6G wireless networks. The architecture harnesses advanced machine learning techniques, including knowledge transfer-based federated learning, to enable the real-time detection and mitigation of security threats. In addition, a private blockchain is integrated into the system to ensure transparency and safeguard the integrity

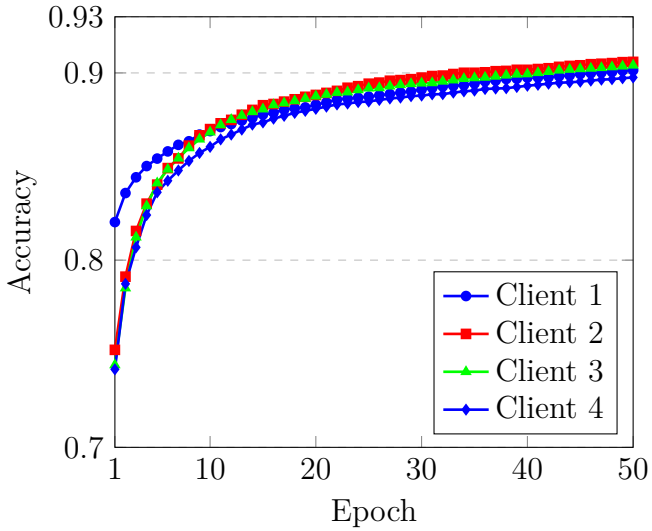


Figure 3.3: Accuracy of Clients on their private datasets over 50 Rounds

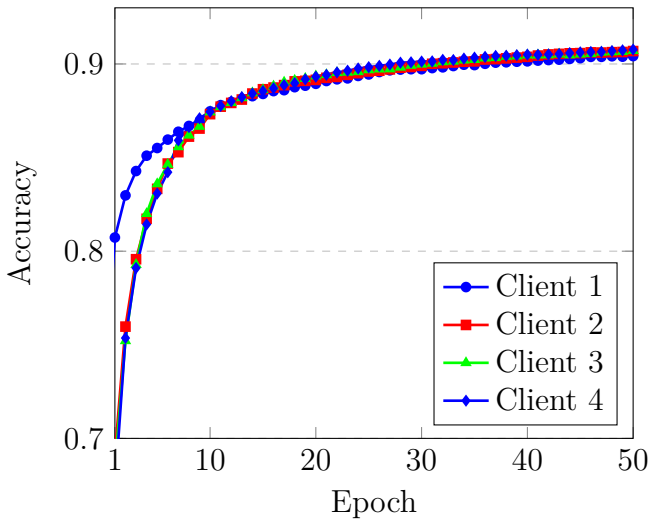


Figure 3.4: Accuracy of Clients on the validation dataset over 50 Rounds

of the shared data. Experimental results demonstrate that, irrespective of differing model architectures, clients consistently achieved high accuracy scores—ranging from 90.14% to 90.59%—which underscores both the reliability and versatility of 6G-SECUREIDS. The system effectively classifies and identifies security threats, as evidenced by the steady improvement in accuracy across training epochs. In summary, the findings presented in this chapter validate 6G-SECUREIDS as a robust and effective intrusion detection solution tailored for 6G wireless networks.

Chapter 4

FBMP-IDS: FL-based Blockchain-powered Lightweight MPC-secured IDS for 6G networks

The future 6G wireless network is expected to provide record-high data rates, ultra-low latency, and transparent coexistence with new technologies such as artificial intelligence and the Internet of Everything. With these rapid technological advancements are enormous security challenges, primarily intrusion detection and prevention. Centralized detection approaches grow less effective in countering such challenges, calling for decentralized, privacy-oriented solutions.

To help solve some of these problems, we propose a new secure gradients exchange algorithm for distributed intrusion detection in 6G networks. Our approach combines Federated Learning with secure multi-party computation and blockchain technology, thereby enabling collaborative model training while preserving the privacy of data from each entity. Additionally, the application of gradient compression and adaptive secure aggregation methods further enhances communication overhead and computational complexity to make our solution robust and efficient despite the high data rates and ubiquitous connectivity offered by 6G networks.

Experimental evaluations conducted using the CICIoT2023 dataset indicate that our federated learning-based hybrid model, comprising a one-dimensional convolutional neural network (CNN1D) and a multi-head attention mechanism, outperforms some of the popular deep learning models. Specifically, it achieves an average accuracy of 79.92%, an average detection rate of 77.41%, and a false alarm rate of just 2.55%.

4.1 Introduction

Wireless technology has been at the forefront of society's advancement, ranging from transmitting basic sound signals to advanced information transmission via radio waves. The industry has seen explosive expansion and groundbreaking leaps in the past couple of decades, beginning with the groundbreaking breakthrough by Bell Labs of the Advanced Mobile Phone System, or 1G. Subsequent generations—2G, 3G, 4G, and more recently

5G networks—have continued to offer increasingly advanced capabilities [11]. Although 5G was envisioned to deliver transformational capabilities, like the Internet of Everything (IoE) and enhanced broadband for machine-type communications, among some of its most eagerly sought goals, like wireless interconnectivity of machines without any human intervention, are still elusive [47]. This gap between promise and reality necessitates critical examination of whether or not 5G can live up to its early promises for technologies like the IoE, and whether subsequent 6G networks will be able to show the level of flexibility and efficiency required in order to facilitate the high-level expectations predicted for 2030 [11].

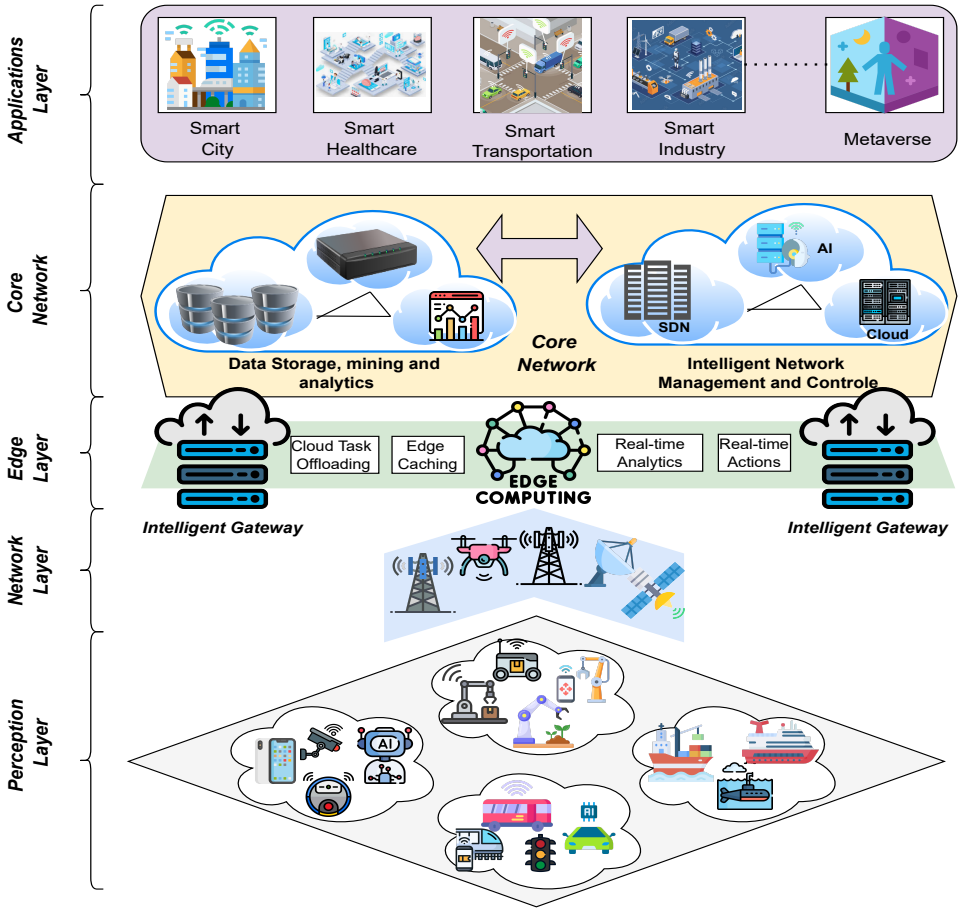


Figure 4.1: Vizualization of connected intelligence for future 6G Networks

Figure 4.1 provides an overview of connected intelligence for future 6G networks. Compared to preceding generations, the sixth-generation (6G) network is expected to deliver a transformative leap in communication capabilities by offering faster data speeds, lower latency, and the capacity to connect an exponentially larger number of devices [11]. In pursuit of these advancements, 6G is anticipated to adopt a layered network architecture, with each layer dedicated to distinct functionalities. The perception layer will focus on signal transmission and modulation techniques, potentially utilizing frequency bands beyond the millimeter waves to achieve even higher capacity [181]. The Edge layer will incorporate intelligent devices capable of performing sophisticated routing and processing functions, such as cloud task offloading and edge caching, thereby optimizing performance [182]. The core network, serving as the operational hub, will be endowed with enhanced

processing and storage capabilities to handle power-intensive tasks such as data mining and analytics, while the application layer will support the deployment of futuristic services, including real-time, mission-critical applications like intelligent transportation systems and smart healthcare services.

The network layer is tasked with routing and addressing, likely leveraging intelligent algorithms and machine learning to optimize traffic flow in the complex 6G ecosystem. It is envisioned that self-configuring networks will dynamically adjust routing based on real-time traffic patterns and congestion levels [183]. The transport layer will establish and manage data communication sessions between applications, potentially employing novel protocols to guarantee data delivery across diverse network conditions and device types, ranging from conventional smartphones to autonomous vehicles [182]. Meanwhile, the application layer will provide end-user services, delivering ultra-high-definition video streaming with near-instantaneous response times, seamless augmented and virtual reality experiences that blend the virtual and physical realms, and ultra-reliable, low-latency communications for critical industrial automation tasks [11].

The integration of artificial intelligence within 6G network frameworks is heralded as a key driver for innovation and real-time decision-making. Nonetheless, this integration also introduces significant security challenges, necessitating robust measures to protect the integrity and privacy of these advanced systems [47]. Intrusion detection systems (IDS), whether implemented as software or hardware solutions, analyze network traffic and system logs to identify security policy violations [184]. The application of AI, particularly through machine learning and deep learning, is critical in enhancing IDS capabilities in IoT environments [185]. Given the evolving nature of 6G—with its dramatic increase in data rates, proliferation of IoT devices, and deeper AI integration—traditional IDS approaches are being challenged. Consequently, novel intrusion detection strategies and secure collaborative learning techniques are required. Federated learning has emerged as a promising paradigm in this context, as it enables collaborative machine learning on distributed datasets without necessitating data sharing, thereby addressing privacy concerns inherent in centralized approaches [125]. However, the deployment of federated learning in 6G networks also brings forth new security issues, such as the exposure of model gradients during training.

To address these challenges, this chapter proposes a secure gradients exchange-based IDS that synergistically combines federated learning, secure multi-party computation (MPC), and blockchain technology, specifically tailored for 6G wireless networks. The proposed algorithm facilitates decentralized and secure aggregation of gradients, incorporates techniques such as gradient compression and quantization, and employs adaptive secure aggregation strategies to optimize communication overhead and computational complexity. Moreover, the algorithm is designed for integration with 6G network slicing and virtualization, thereby ensuring efficient resource allocation and maintaining Quality of Service (QoS) during secure gradient exchange. The architecture of the FBMP-IDS leverages a hybrid deep learning model that fuses the robust feature extraction capabilities of convolutional neural networks (CNNs) with the contextual analysis provided by a multi-head attention mechanism. This multi-head attention component is instrumental in capturing long-range dependencies inherent in the data [186], enabling the model to analyze not only individual data points but also the interrelationships among them.

Table 4.1: Comparison of Related Works

Study	Year	Approach	Used dataset	Results	Strengths	Limitations
Rezvy et al. [187]	2019	Deep auto-encoded dense neural network for intrusion detection in 5G and IoT networks	Aegean Wi-Fi Intrusion dataset [188]	Accuracy (99.9%)	High detection rate	Detects only 3 types of attacks
Moudoud et al. [189]	2020	Stochastic Markov-based model for detecting and predicting false data injection and DDoS attacks in 5G-enabled IoT	Real log activity from [190]	Detection rate >95% for DDoS	Lightweight; No complex computing	Considers only two types of attacks
Abdulqadder et al. [191]	2020	Multi-layer IDPS system for 6G networks with game theory and Four-Q-Curve technique	Own Dataset	High Detection Rate (96.08%)	Detects and mitigates various attacks	Centralized learning; Privacy issues
Zhang et al. [192]	2021	Ensemble machine learning algorithm for intrusion detection in 6G vehicular CAN bus networks	CAN intrusion dataset[193]	AUC(77.83%), Fmeasure (75.33%)	Addresses dynamic and heterogeneous vehicular networks; Improves AUC and F-measure	Centralized deployment; - High False Positive Rate (FPR) (10.46%)
Almiani et al. [194]	2021	Kalman backpropagation neural network IDS model for detecting DDoS attacks in 5G-enabled IoT	CICDDoS 2019 [195]	Acc. (94%), FPR (0.09%), DR (97.49%)	Good detection performances	Considers only one type of attack (DDoS)
Chen et al. [196]	2022	Fuzzing-based evaluation of Network Intrusion Detection Systems (NIDS) rules	Own Dataset	Analyzing phase time cost from 1ms to 1min	Evaluates effectiveness of rule implementations	Inefficient processing time variability; Signature-based detection shortcomings
Alotaibi et al. [197]	2023	Software-driven FL-based IDS (IDSoft) with hierarchical FL framework	MNIST [198]	Accuracy (94.17%)	Reduces communication rounds; Leverages 6G technologies	Lack of security against malicious nodes; -Dataset may not be suitable for the task
Vinita et al. [199]	2023	FL-based IDS for 6G Internet of Vehicles (IoV) with three-tier model weight aggregation	Sybil attack dataset [200]	Accuracy (87%)	High detection rate; Sybil attack detection	Does not consider malicious clients
Prasad et al. [201]	2023	Fuzzy Logic System (FLS) and ML-based IDS for securing mobile ad-hoc networks	Own Dataset	BRS: TPR (100%) and Accuracy (99.7%) on Wormhole	Evaluates performance reliability; Potential for network security solutions	Centralized learning; Privacy concerns; Only two attacks (Blackhole and Wormhole)

As a result, the model attains a holistic understanding of network behavior, effectively distinguishing between normal traffic patterns and potential intrusions.

4.2 Related Works

The pursuit of strengthening the security infrastructure in 6G networks has prompted a series of significant studies that explore innovative methods for intrusion detection and prevention. These investigations span diverse network environments—including vehicular networks, IoT settings, and more generalized network scenarios—each addressing unique challenges while contributing novel insights to the evolving landscape of network security.

For instance, Rezvy et al. [187] developed a deep auto-encoded dense neural network approach for detecting intrusions in 5G and IoT networks, evaluated using the Aegean Wi-Fi Intrusion dataset. Their method, which targets three specific types of attacks (Flooding/DoS, Injection, and Impersonation), demonstrated an impressive detection accuracy of 99.9

Abdulqadder et al. [191] proposed a multi-layer Intrusion Detection and Prevention System (IDPS) that secures various network components—including switches, domain controllers, and NFV infrastructure—by employing multiple levels of security. In a related vein, Zhang et al. [192] introduced an ensemble machine-learning algorithm based on weighting techniques tailored for dynamic, heterogeneous vehicular networks, with experimental evaluations showing notable improvements in AUC and F-measure metrics. However, their approach was confined to centralized deployments, which raises scalability

concerns for 6G environments.

Almiani et al. [194] utilized a Kalman-backpropagation neural network to construct an IDS for detecting DDoS attacks in 5G-enabled IoT networks, achieving an average detection accuracy of 94% on the CICDDoS2019 dataset, albeit for a single type of attack. In contrast, Chen et al. [196] advocated for the use of fuzzing techniques to evaluate Network Intrusion Detection Systems (NIDS) rules, though they noted inefficiencies in processing time compared to anomaly-based IDS approaches.

Alotaibi et al. [197] advanced the field by proposing a software-driven, FL-based IDS integrated into the network architecture. Their hierarchical federated learning framework, which incorporates both synchronous and asynchronous aggregation techniques alongside an offloading mechanism, demonstrated significant reductions in communication rounds. Nonetheless, the framework did not address the potential security risks associated with malicious nodes compromising the entire system. Vinita et al. [199] presented a federated learning-based IDS for the Internet of Vehicles (IoV) compatible with 6G networks, achieving a detection accuracy of 87% and incorporating mechanisms to differentiate normal data from Sybil attacks, though it did not account for the possibility of normally benign nodes being subverted.

Prasad et al. [201] proposed an approach utilizing a Fuzzy Logic System in conjunction with machine learning to secure mobile ad-hoc networks (MANETs) against attacks such as black-hole and wormhole intrusions in a simulated virtual network environment. Recent research has also examined emerging paradigms such as over-the-air computation [202], which efficiently encodes and decodes information via superimposed waveforms to mitigate interference and maintain data integrity. Other studies have underscored challenges related to the management and exchange of information within blockchain-based IDSs secured by Multi-Party Computation (MPC) in real-world scenarios. Additionally, the role of Software-Defined Networking (SDN) in optimizing network resource allocation has been recognized as a promising avenue for overcoming practical hurdles [203].

Table 4.1 provides a summary of these approaches, outlining their primary methodologies, key strengths, and inherent limitations. Overall, while many current approaches leverage deep learning and machine learning techniques to achieve high detection rates, they are often constrained by factors such as limited attack scope, reliance on centralized learning architectures that pose privacy and scalability issues, high false positive rates, and datasets that may not fully capture the complex attack landscapes anticipated in 6G networks.

The major contributions of the proposed system are:

- *Decentralized and Secure Gradient Aggregation:* The proposed system eliminates the reliance on a centralized aggregation server by distributing the gradient aggregation process across a blockchain network and individual client devices. Secure multi-party computation (MPC) protocols are employed to ensure that individual gradients remain confidential while still enabling the accurate computation of global model updates.

- *Gradient Compression* To address the challenges posed by high data rates and extensive connectivity in 6G networks, the system incorporates gradient compression

and quantization techniques. This approach significantly reduces the communication overhead associated with transmitting gradients, thereby improving efficiency without materially compromising model accuracy.

- *Adaptive Secure Aggregation Strategies* The system is equipped with a suite of MPC protocols that vary in complexity, communication overhead, and security guarantees. Based on real-time network conditions and the specific characteristics of participating entities, the system dynamically selects the most appropriate MPC protocol in each federated learning round. This adaptive strategy optimally balances security, communication overhead, and computational complexity.

  Blockchain-enabled Decentralization and Transparency Blockchain technology is integrated into the system to decentralize the federated learning process, ensuring that it remains transparent and immutable. The blockchain network collectively manages the global state of the model, verifies the authenticity and integrity of gradient data, and disseminates updated model weights to all participating clients, thereby reinforcing overall trust in the system.

- *Hybrid Model Based on CNN1D and Multi-Head Attention* To optimize detection performance and minimize false alarm rates, the system introduces a hybrid deep learning model that fuses the efficiency of one-dimensional convolutional neural networks (CNN1D) with the contextual analytical power of multi-head attention mechanisms. This combination enhances feature extraction and facilitates a more comprehensive analysis of network traffic, resulting in superior learning efficiency and more robust intrusion detection compared to models based on a single learning paradigm.

4.3 The FBMP-IDS: An Overview

In this chapter, we have proposed a secure gradients exchange-based IDS for FL in a 6G wireless network environment, as provided in Alg. 1. The algorithm uses the synergy of FL, secure MPC, and blockchain to enable privacy-preserving and secure collaborative model training in a decentralized manner.

4.3.1 Motivation

The motivation for this work is grounded in the anticipated challenges and requirements of 6G wireless networks, including massive connectivity, stringent latency and reliability constraints, and the need for efficient resource utilization and network slicing [47, 11]. Moreover, the increasing reliance on collaborative machine learning and data sharing raises critical concerns regarding privacy and security [154]. By integrating Federated Learning (FL), Multi-Party Computation (MPC), and blockchain technology into our proposed system, we address these challenges in a comprehensive and innovative manner. This integration enables secure and privacy-preserving collaborative model training while capitalizing on the distinctive characteristics of 6G networks, such as network slicing, virtualization, and high data rates, alongside the potential for blockchain-enabled

infrastructure. The distributed nature of our algorithm further enhances resilience by eliminating single points of failure, while adaptive secure aggregation strategies and gradient compression techniques optimize the trade-offs between security, communication overhead, and computational complexity [191]. Overall, the present work contributes toward the realization of privacy-preserving and secure FL-based intrusion detection systems for next-generation wireless networks, thereby enabling collaborative and distributed machine learning across a wide array of applications and services in the 6G era.

4.3.2 Threat Model

In constructing a distributed intrusion detection system for 6G networks, it is imperative to rigorously assess the range of potential threats and vulnerabilities that could undermine the system's integrity and effectiveness. Developing a comprehensive threat model enables a deeper understanding of the adversarial landscape and informs the design of robust countermeasures.

Malicious Intrusion Detection Agents:

Intrusion Detection Agents (IDAs) play a critical role by providing local network traffic data and computational resources to support the collaborative training process. However, if some of these agents are compromised or fall under adversarial control, several risks emerge:

- Poisoning attacks: Adversaries can inject corrupted or manipulated data into the training process, thereby degrading the performance of the intrusion detection model [154].
- Model extraction attacks: By exploiting the gradients or model updates exchanged during training, attackers may attempt to extract or reconstruct the global intrusion detection model [204].
- Privacy violations: Malicious agents could analyze exchanged gradients or model updates to infer sensitive information regarding other participants' network traffic data [205].

Insecure Communication Channels:

The secure exchange of gradients and model updates is fundamental to maintaining the integrity of the federated learning process within the 6G-SECUREIDS framework. This process depends on communication channels connecting Intrusion Detection Agents, Security Edge Nodes, and the Blockchain Network. However, these channels are susceptible to several significant threats. Some of the potential threats include:

- Eavesdropping attacks: Adversaries may intercept and monitor the communication channels to gain unauthorized access to sensitive information, such as gradients or model updates, thereby compromising confidentiality [204].

- Man-in-the-middle attacks: Attackers can position themselves between communicating entities to intercept, alter, or inject malicious payloads into the data being exchanged, potentially corrupting gradients or model updates and undermining the integrity of the learning process [206].

4.3.3 Network Model

The network architectures should be customized to address the distributed intrusion detection challenges arising from the integration of artificial intelligence and federated learning in 6G wireless networks. The architecture presented in this paper relies on significant functionalities of 6G—i.e., virtualization, edge computing, and network slicing—to effectively distribute resources, ensure low latencies, as well as ensure strong security features during collaborative intruder detection model training. In this network structure, we utilize the inherent characteristics of 6G infrastructure to create several logical instances of networks by network slicing, each for various security services or applications [49]. Moreover, each network slice can be further partitioned into several dynamic sub-slices that are allocated and orchestrated based on the specific requirements of the distributed intrusion detection system [49]. The whole network comprises three primary components: the Intrusion Detection Agents, the Security Edge Nodes, and the Blockchain Network, as indicated in Figure 4.2.

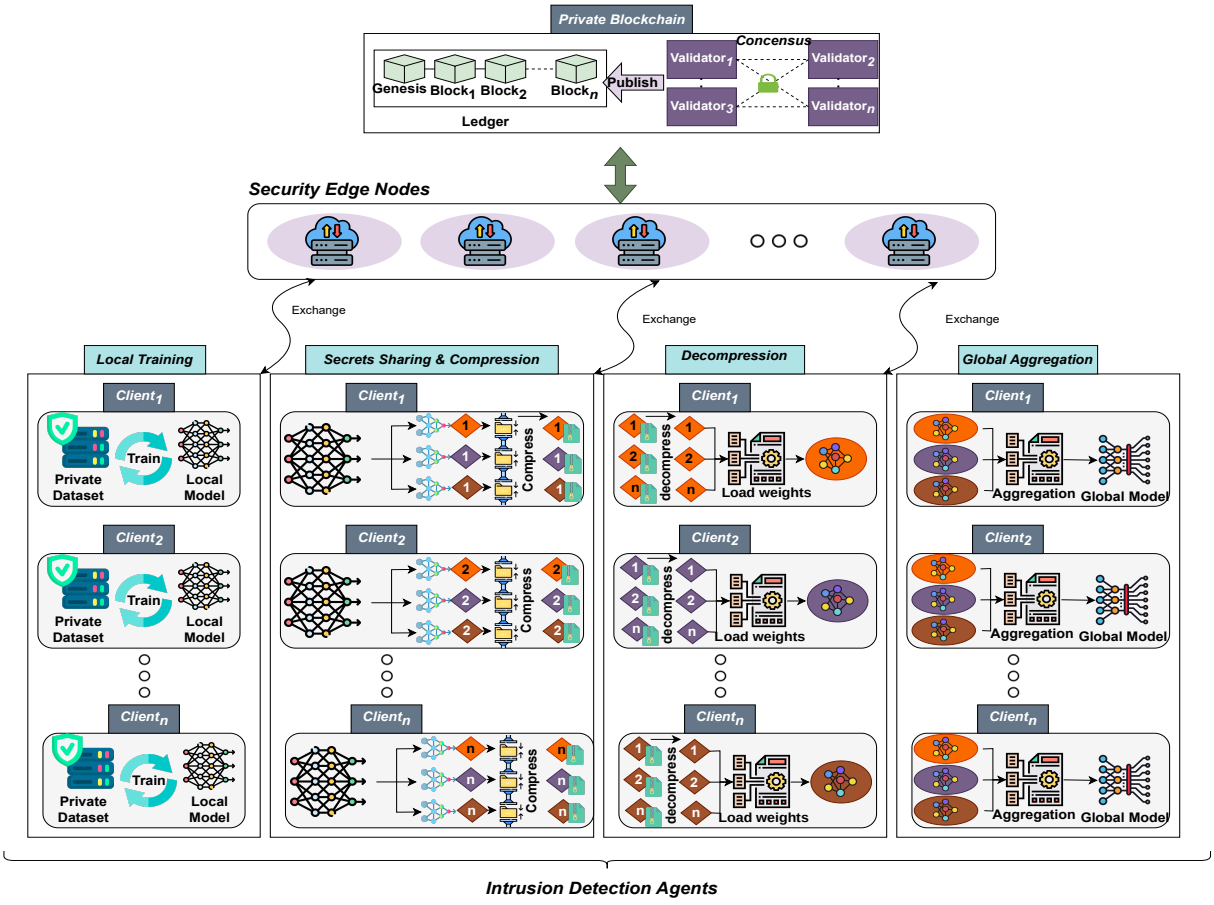


Figure 4.2: Network Model for the FBMP-IDS system

Intrusion Detection Agents

The devices that participate in our model are referred to as Intrusion Detection Agents. The agents exchange their local network traffic data and computing resources to facilitate the collaborative training of intrusion detection models. As such, they can be any connected device—including IoT devices, network routers, firewalls, and other devices capable of capturing network traffic and performing local model training and gradient computation [204]. Moreover, a separate sub-slice of the network slice is allocated to each agent solely for intrusion detection purposes. The sub-slice offers isolated and secured communication channels for gradient exchange and resource allocation while guaranteeing the satisfaction of Quality of Service (QoS) demands.

Security Edge Nodes

The Security Edge Nodes are edge computation nodes that reside near the edge of the network, in close proximity to the Intrusion Detection Agents. They are used as secure points to relay the gradients formed during the process of federated training based on the techniques of edge computing in order to decrease latency and communication overhead [204]. They are responsible for coordinating the secure gradients exchange algorithm, which allows aggregation of gradients from agents within their own sub-slices. These nodes are also responsible for the integration with the Blockchain Network by announcing the aggregated gradients for validation and updating the global model [205].

Blockchain Network

The Blockchain Network is a secure, decentralized, and immutable gradients aggregation and global intrusion detection model management platform. In the network, every node participates in maintaining and verifying the blockchain ledger and hence ensuring transparency, traceability, and single points of failure resistance [207]. Smart contracts are deployed in the Blockchain Network to encode the secure gradients exchange algorithm; the contracts allow for the verification of gradients, calculation of global model updates, and distribution of the updated intrusion detection model to all agents [207]. Seamless communication between the Blockchain Network, Security Edge Nodes, and Intrusion Detection Agents ensures a secure, decentralized collaborative training process, while preserving the integrity and privacy of network traffic data for each entity at the same time [204].

By incorporating network slicing, virtualization, edge computing, and blockchain technologies, the novel network paradigm provides a robust and secure framework for deploying distributed intrusion detection in 6G wireless networks. The comprehensive architecture is especially effective at addressing problems related to resource allocation, latency, and security, as well as facilitating efficient, privacy-preserving collaborative training of intrusion detection models—thereby significantly enhancing the overall security of future wireless networks.

Algorithm 1 FL-based Blockchain-powered Lightweight MPC-secured IDS for 6G networks

Require: Participants $P_1, P_2, \ldots, P_n$, Blockchain BC, Global Model M_G, Compression Function $Q(\cdot)$, Set of MPC Protocols $\mathcal{P}$

Initialize M_G with random weights
Perform MPC setup: establish secure channels and generate shared secrets
for each round r **do**
    Select MPC protocol $\mathcal{P}_r \in \mathcal{P}$ based on network conditions and participant characteristics
    for each participant P_i **do**
        Initialize local model M_i with same architecture as M_G
        Copy weights of M_G to M_i
        Train M_i on local data of P_i using optimization algorithm and loss function
        Compute gradients ∇_i of M_i with respect to initial weights from M_G
        Compress gradients: $Q(\nabla_i)$
        Secret-share $Q(\nabla_i)$ using $\mathcal{P}_r$ to obtain shares $[Q(\nabla_i)]_1, [Q(\nabla_i)]_2, \ldots, [Q(\nabla_i)]_n$
    end for
    Execute secure aggregation protocol in $\mathcal{P}_r$ to compute $[\overline{Q(\nabla)}]_i = \frac{1}{n}\sum_{j=1}^{n}[Q(\nabla_j)]_i$ for each P_i
    Reconstruct average compressed gradients $\overline{Q(\nabla)}$ from shares $[\overline{Q(\nabla)}]_1, [\overline{Q(\nabla)}]_2, \ldots, [\overline{Q(\nabla)}]_n$
    Broadcast $\overline{Q(\nabla)}$ to BC and verify using participants' signatures
    Update M_G weights using $\overline{Q(\nabla)}$: $W_{M_G}^{(t+1)} = W_{M_G}^{(t)} - \eta\overline{Q(\nabla)}$
end for

Figure 4.3: Algorithm

4.3.4 System Model

Initialization

- **a.** The global model M_G is initialized with random weights.
- **b.** Participants $P_1, P_2, \ldots, P_n$ engage in an MPC setup phase, establishing secure communication channels and generating shared secrets or cryptography keys necessary for MPC computations.
- **c.** A set of MPC protocols $\mathcal{P}$ with varying levels of complexity, communication overhead, and security guarantees are defined.

Round Preparation

For each round r of FL, an MPC protocol $\mathcal{P}_r \in \mathcal{P}$ is selected based on the current network conditions and participant characteristics.

Client Training

- **a.** Each participant P_i initializes a local model M_i with the same architecture as the global model M_G.
- **b.** P_i copies the current weights of M_G to M_i.
- **c.** P_i trains M_i on their local data using a suitable optimization algorithm and loss function.
- **d.** P_i computes the gradients ∇_i of M_i with respect to the initial weights copied from M_G.
- **e.** P_i compresses the gradients ∇_i using the compression function $Q(\cdot)$ to obtain compressed gradients $Q(\nabla_i)$.
- **f.** P_i secret-shares the compressed gradients $Q(\nabla_i)$ using the selected MPC protocol $\mathcal{P}_r$, obtaining shares $[Q(\nabla_i)]_1, [Q(\nabla_i)]_2, \ldots, [Q(\nabla_i)]_n$.

Secure Aggregation using MPC

- **a.** Participants execute the secure aggregation protocol defined by $\mathcal{P}_r$, where each P_i holds shares $[Q(\nabla_j)]_i$ of every other participant's compressed gradients $Q(\nabla_j)$.
- **b.** Through the secure aggregation protocol, participants jointly compute the sum of their shared compressed gradients without revealing individual values, yielding shares $[\overline{Q(\nabla)}]_i = \frac{1}{n}\sum_{j=1}^{n}[Q(\nabla_j)]_i$ of the average compressed gradients for each P_i.

Reconstruction and Blockchain Integration

- **a.** Participants reconstruct the final average compressed gradients $\overline{Q(\nabla)}$ from the shares $[\overline{Q(\nabla)}]_1, [\overline{Q(\nabla)}]_2, \ldots, [\overline{Q(\nabla)}]_n$ using the MPC reconstruction protocol defined by $\mathcal{P}_r$.
- **b.** $\overline{Q(\nabla)}$ is broadcasted to the blockchain network BC.
- **c.** The authenticity and integrity of $\overline{Q(\nabla)}$ are verified using the participants' digital signatures.

Global Model Update

- **a.** Once the average compressed gradients $\overline{Q(\nabla)}$ are verified on the blockchain, the global model M_G weights are updated using the verified gradients:

$$W_{M_G}^{(t+1)} = W_{M_G}^{(t)} - \eta\overline{Q(\nabla)}$$

where η is the learning rate, and t represents the current round of FL.

4.3.5 Gradient Compression Approach

DNN quantization has emerged as a pivotal technique in optimizing the deployment of neural networks on resource-constrained devices [208]. DNN quantization is defined as the process of reducing the precision in weights and activations of neural networks from higher bit-widths (e.g., 32-bit floating point) to lower bit-widths (e.g., 8-bit integers) [209, 210]. This reduction is strongly driven by the quest for improvements in computational efficiency and memory footprint, with an additional inference speed boost and no large losses in terms of model accuracy [211]. In our framework we implemented this stage using the QKeras quantization library from Google [211, 212, 213]. The library is built upon the work of [214], in creating Quantized Neural Networks (QNNs), where during training, all activations and weights are quantized to Q bits in a fixed point representation. The quantization function in the forward pass can be formulated by [214]:

$$q = clip(\frac{round(2^{Q-1}W)}{2^{Q-1}}, -1, 1 - 2^{-(Q-1)}) \tag{4.1}$$

The quantization function is a mathematical transformation applied to the weights of the neural network during the training process. The equation provided describes how a weight W is quantized to Q bits using a fixed-point representation.

- **Rounding and Scaling**: The expression $round(2^{Q-1}W)$ scales the weight W by 2^{Q-1} and then rounds it to the nearest integer.
- **Normalization**: The result is then divided by 2^{Q-1} to normalize it back to the range of the original weight values.

Algorithm 2 Dynamic Selection and Execution of MPC Protocols

Require: Set of MPC Protocols $\mathcal{P}$, Network Conditions NC, Participant Characteristics PC

function SelectMPCProtocol($\mathcal{P}$, NC, PC)
  Define a scoring function $\mathrm{S}(\mathcal{P}_\mathrm{r}, \mathrm{NC}, \mathrm{PC})$ that evaluates the suitability of each protocol $\mathcal{P}_\mathrm{r} \in \mathcal{P}$ based on current network conditions NC and participant characteristics PC
  Initialize an empty list scores
  for each protocol $\mathcal{P}_\mathrm{r} \in \mathcal{P}$ **do**
    Compute the score $\mathrm{s_r} = \mathrm{S}(\mathcal{P}_\mathrm{r}, \mathrm{NC}, \mathrm{PC})$
    Append $(\mathcal{P}_\mathrm{r}, \mathrm{s_r})$ to scores
  end for
  Sort scores based on $\mathrm{s_r}$ in descending order
  Select the protocol with the highest score: $\mathcal{P}_{\mathrm{best}} = \mathrm{scores}[0][0]$
  return $\mathcal{P}_{\mathrm{best}}$
end function

Figure 4.4: Algo

- **Clipping**: The *clip* function ensures that the quantized value q stays within the range $[-1, 1 - 2^{-(Q-1)}]$. This prevents the values from exceeding the re-presentable range for the given bit-width Q.

By quantizing the weights and activations to lower bit-widths, significant improvements in computational efficiency and memory usage are achieved, making it feasible to deploy complex neural networks on resource-constrained devices without substantial loss in accuracy. This has been proven by several works including [213, 209].

4.3.6 Dynamic Selection and Execution of MPC Protocols

The secure aggregation protocol within our system is crucial for ensuring that the gradients from participants are aggregated securely without revealing individual contributions. The dynamic selection of MPC protocols is based on current network conditions and participant characteristics, as presented in Alg. 2.

The scoring function $S(\mathcal{P}_r, NC, PC)$ can be defined based on various factors such as communication overhead, computational complexity, and security guarantees. The scoring function can be defined as:

$$S(\mathcal{P}_r, NC, PC) = \alpha \cdot \mathrm{s}(\mathcal{P}_r) - \beta \cdot \mathrm{o}(\mathcal{P}_r, NC) - \gamma \cdot \mathrm{c}(\mathcal{P}_r, PC) \tag{4.2}$$

where s is the security guarantees, o is the communication overhead, c is the computational complexity, and α, β, γ are weights assigned to each factor based on their

importance.

4.3.7 Advantages

Through the integration of secure multi-party computation (MPC) techniques, the system is provided with an additional level of security and privacy for gradient exchange process [215]. MPC protocols ensure that gradients of each participant remain confidential during computation but are still able to allow correct aggregation of gradients even when participants are compromised or act maliciously [216]. Besides, the system also applies gradient compression to lower communication overhead, and adaptive secure aggregation methods adaptively select the most appropriate MPC protocol according to real-time network status and attributes of participating nodes. All these integrated mechanisms make the algorithm particularly effective in coping with the unique challenges in 6G wireless networks while ensuring both security and privacy.

4.3.8 Our system Vs. Traditional FL-based IDSs

Our system is a decentralized secure gradients exchange algorithm designed specifically for 6G networks, eliminating the need for a centralized aggregation server [125]. Instead, the traditional role of the central server is distributed among the blockchain network and the participating clients [207]. This decentralized approach ensures that key functionalities, which would typically be handled by a central server, are instead managed collectively. In our framework, the global model M_G is initially randomly generated, and its weights are iteratively updated using the aggregated gradients received from the clients during each training round. Importantly, these activities are not performed by a single server; rather, they are orchestrated by the blockchain network through consensus mechanisms and smart contracts, thereby enhancing transparency and robustness. Gradient aggregation is executed in a decentralized manner through the integration of secure multi-party computation (MPC) protocols and the blockchain network. Each client secret-shares its compressed gradients using the selected MPC protocol [216]. The participating entities then collaboratively compute the average of these compressed gradients without revealing any individual values. This secure aggregation process is facilitated by the combined strength of the MPC protocols and the consensus mechanisms inherent in the blockchain network.

After updating the global model weights, the new global model state must be disseminated to all participating clients for the subsequent round of training. In our approach, the updated global model weights are broadcast as transactions on the blockchain, thereby ensuring transparency and immutability [207]. Furthermore, the updated model can be stored in a distributed file system, making it readily accessible to all participants [204]. By eliminating the need for a centralized aggregation server, our algorithm avoids potential single points of failure and enhances the overall security, resilience, and decentralization of the federated learning process. The blockchain network thus serves as a decentralized and transparent platform for secure gradient aggregation and global model management, leveraging its inherent properties of decentralization, immutability, and consensus mechanisms.

Table 4.2: The CICIoT2023 dataset classes distribution

Category	Attack	Number of Instances
DDoS (72.7%)	DDoS-ICMP_Flood	7,200,504
	DDoS-UDP_Flood	5,412,287
	DDoS-TCP_Flood	4,497,667
	DDoS-PSHACK_Flood	4,094,755
	DDoS-SYN_Flood	4,059,190
	DDoS-RSTFINFlood	4,045,285
	DDoS-SynonymousIP_Flood	3,598,138
	DDoS-HTTP_Flood	28,790
	DDoS-UDP_Fragmentation	286,925
	DDoS-ACK_Fragmentation	285,104
	DDoS-SlowLoris	23,426
	DDoS-ICMP_Fragmentation	452,489
DoS (17.3%)	DoS-UDP_Flood	3,318,595
	DoS-HTTP_Flood	71,864
	DoS-TCP_Flood	2,671,445
	DoS-SYN_Flood	2,028,834
Recon (0.75%)	Recon-PingSweep	2262
	Recon-HostDiscovery	134,378
	Recon-OSScan	98,259
	Recon-PortScan	82,284
Mirai (5.64%)	Mirai-greeth_flood	991,866
	Mirai-udpplain	890,576
	Mirai-greip_flood	751,682
Spoofing (1.04)	DNS_Spoofing	178,911
	MITM-ArpSpoofing	307,593
Web (0.05%)	Uploading_Attack	1252
	DictionaryBruteForce	13,064
	BrowserHijacking	5859
	CommandInjection	5409
	SqlInjection	5245
	XSS	3846
	Backdoor_Malware	3218
BruteForce (0.02%)	DictionaryBruteForce	13,064
Benign (2.3%)	BenignTraffic	1,098,195

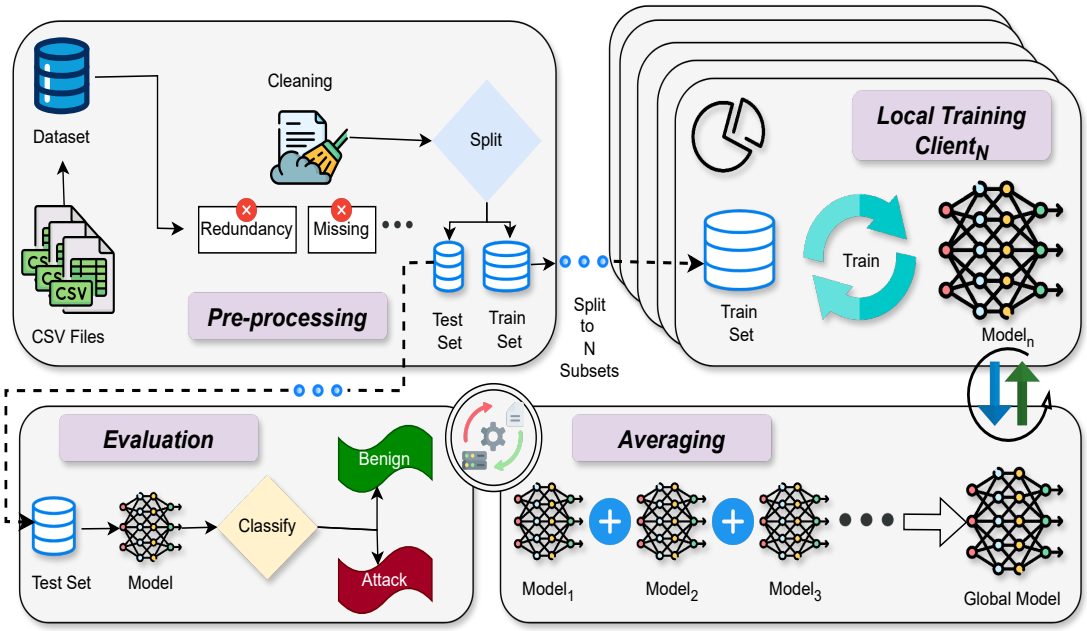


Figure 4.5: Simplified illustration of dataset pre-processing, model training, and evaluation

4.4 Computational Complexity Analysis

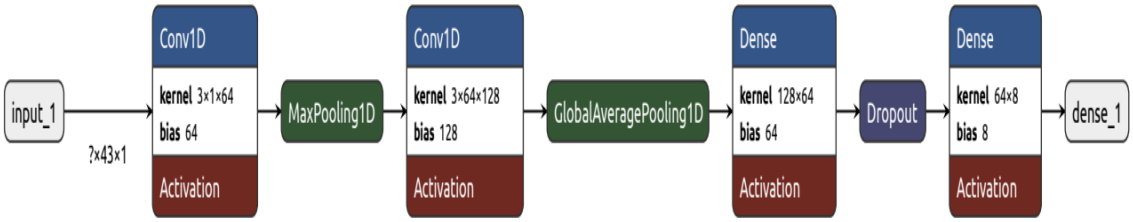
The computational complexity of the algorithm proposed can be decomposed into communication overhead, compression overhead, and the number of training rounds.

4.4.1 Communication Complexity

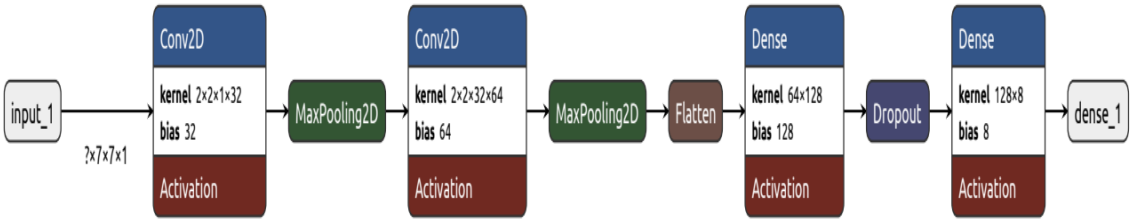
The choice of MPC protocol in each round ($\mathcal{P}_r$) is highly influential in the choice of the time complexity. Popular MPC protocols typically have communication complexity scaling with $\mathcal{O}(n^d.K)$, where n is the number of participants and d and K are variable factors depending on the exact protocol used. [217, 218].

4.4.2 Compression Overhead

Employment of the compression function $Q(\cdot)$ comes with some computational overhead compared to uncompressed gradients. However, the compression ratio attained will directly impact communication overhead. An efficient compression function with a higher ratio can hugely reduce the amount of data transmitted during secure aggregation. This, therefore, calls for care in the choice of the compression function, since there is a trade-off between the overhead incurred in compression and the reduction of communication.



(a) CNN 1D



(b) CNN 2D

Figure 4.6: Models used for the Experimental Evaluation: CNN 1D and 2D

Table 4.3: Confusion matrix.

		Predicted class	
		Negative (Benign)	Positive (Attack)
Effective class	Negative (Benign)	True negative	False positive
	Positive (Attack)	False negative	True positive

4.4.3 Training Rounds

The global model is then iterated with many rounds of training to achieve convergence. Total communication cost scales with the number of rounds, linearly (R).

Time Complexity

Now, this complexity can be written in Big O notation as: $\mathcal{T} = O(R \cdot C_{MPC} + C_{compression})$ where:

- R is the number of rounds of training.
- C_{MPC} denotes the communication complexity of the MPC protocol chosen for each round.
- $C_{compression}$ denotes the computational cost associated with the application of the compression function $Q(\cdot)$.

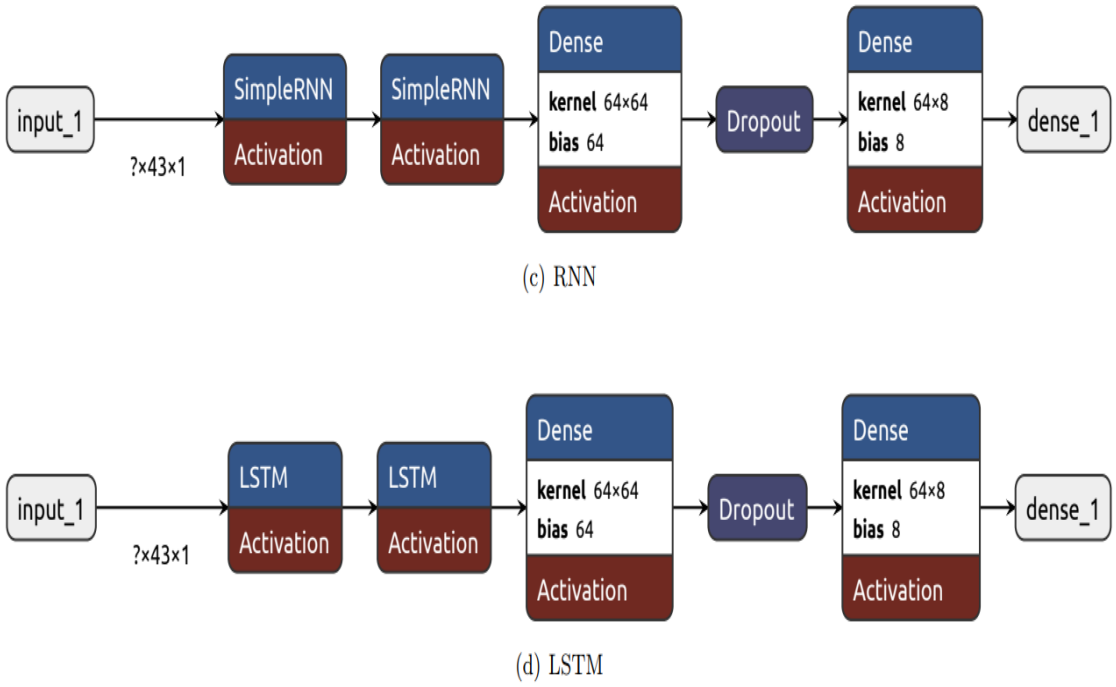


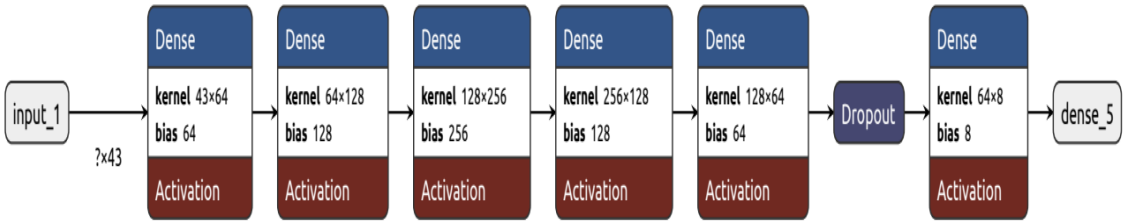
Figure 4.7: Models used for the Experimental Evaluation: RNN and LSTM

Table 4.4: Hyperparamaters of the different models used for the experimental evaluation

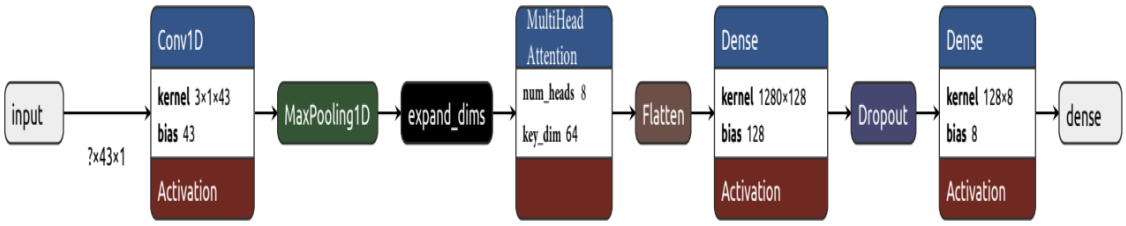
Hyperparameters		CNN1D	CNN2D	RNN	LSTM	DNN	Hybrid Model
Client parameters	Learning rate	0.001	0.001	0.001	0.001	0.001	0.001
	Batch size	64	64	64	64	64	256
	Number of epochs	70	70	20	15	70	70
	Optimizer	adam	adam	adam	adam	adam	adam
	Loss function	sparse categorical crossentropy	sparse categorical crossentropy	sparse categorical crossentropy	sparse categorical crossentropy	sparse categorical crossentropy	sparse categorical crossentropy
Server Parameters	Number of Round	40	40	10	10	40	70
	Number of clients	5	5	5	5	5	5
	Fraction of clients per round	100%	100%	100%	100%	100%	100%
	Aggregation method	FedAvg	FedAvg	FedAvg	FedAvg	FedAvg	FedAvg
	Client selection strategy	Both	Both	Both	Both	Both	Both

4.5 Experimentation

In order to conduct our experiments, we proceeded as per the procedure laid out in Figure 4.5. We first conducted data pre-processing followed by dividing the training dataset into five individual subsets—each of which would be used to train a single federated client. After conducting several rounds of federated learning, a client's model was selected to test against the test dataset. We tested various architectures of deep neural networks, including a simple deep neural network (DNN), convolutional neural networks (CNNs), long short-term memory (LSTM) networks, and a combined architecture with 1D CNN and a Multi-Head Attention mechanism. These experiments were simulated through the Flower framework and TensorFlow for federated learning training [219]. We used the CICIoT2023 dataset [220] for training and testing, chosen because it has realistic traffic content and is a real-world representation of contemporary IoT network traffic.



(e) DNN



(f) The hybrid model

Figure 4.8: Models used for the Experimental Evaluation: DNN and Our model

The CICIoT2023 dataset [220]

The CICIoT2023 dataset is a recent dataset that was designed to support security analytics development for IoT environments. It provides a comprehensive collection of data generated from a wide range of IoT attack scenarios. The authors developed a complex IoT network topology with over 100 devices and exposed them to 33 various attack types to create this dataset. These attacks belonged to different types, such as Distributed Denial-of-Service (DDoS), Denial-of-Service (DoS), reconnaissance (Recon), web-based attacks, brute-force attacks, spoofing attacks, and Mirai botnet-based attacks. What is more important, all of these attacks originated from the compromised IoT devices on other devices in the network.

The data collection process involved three primary phases: generation, extraction, and labeling. Firstly, several attack scenarios were simulated on the prepared IoT network to generate corresponding network traffic. This traffic was then captured in pcap format using the Wireshark network protocol analyzer. In the final phase, the captured data was annotated meticulously based on the specific attack scenario each segment illustrated. The resulting pcap files were an enormous amount of data, over approximately 548 GB in size. To make the analysis simpler to perform later on, the dataset was divided into 10-MB chunks so that parallel pcap to CSV conversion—a more analysis-friendly format—was possible. Then, the DPKT library was utilized to extract an extensive feature set from the traces of traffic.

Pre-processing

As depicted in Figure 4.5, our experimental procedure began by concatenating all CSV files from the CICIoT2023 dataset into a single data frame. We then performed data clean-

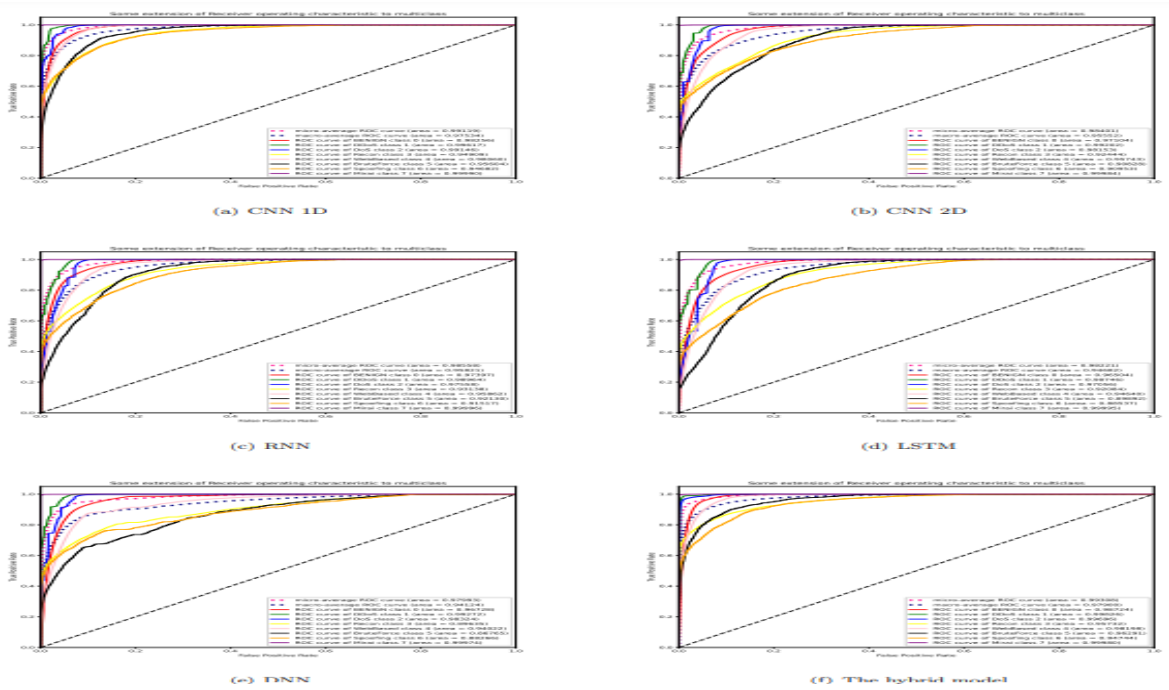


Figure 4.9: ROC curve and AUC ROC of the different Models using Federated learning.

ing by eliminating redundant entries, removing rows with missing values, and discarding columns that contained the same value across all rows. Following these preprocessing steps, we balanced the dataset by selecting a fixed number of rows corresponding to each attack type as well as benign activity. Next, normalization was applied to every value in each column, as described by Equation 4.3. The refined dataset was then partitioned into a training set and a test set. Finally, the training set was further divided into multiple training subsets, with each subset allocated to train the model deployed on an individual node.

$$\overline{x_i(j)} = \frac{x_i(j) - min(x(j))}{max(x(j)) - min(x(j))} \tag{4.3}$$

4.5.1 Used Mectrics

To assess the performance of our proposed models, we utilized several metrics including the True Positive Rate (TPR) for each class, Global Accuracy, Average Detection Rate, False Alarm Rate, and Average Accuracy, which are formally defined in Equations 4.4 through 4.8. These metrics are computed based on the confusion matrix shown in Table 4.3.Additionally, we incorporated the Receiver Operating Characteristic (ROC) curve and the Area Under the Curve (AUC) as further performance evaluation measures. Also, the communication overhead that is presented in Equation 4.9, where R represents training rounds, N represents the total number of clients, and CMS or the Compressed Model Size, which represents the final model size, after introducing the 8bit quantization using the TensorFlow Model Optimization Toolkit [221] and optimizing for resource constraints via the TensorFlow Lite Framework [222].

$$TPR_{classX} = \frac{TP_{classX}}{TP_{classX} + FN_{classX}} \tag{4.4}$$

$$Accuracy_{Global} = \frac{\sum^{NBclass} \text{TP}}{\sum^{NBclass} (\text{TP} + \text{FP})} \tag{4.5}$$

$$DR_{Average} = \frac{\sum TPR_{AttackX}}{NB_{OfAttackX}} \tag{4.6}$$

$$\text{FAR} = 1 - \frac{TP_{Benign}}{TP_{Benign} + FN_{Benign}} \tag{4.7}$$

$$ACC_{Average} = \frac{1}{NBClass} \sum TPR_X \tag{4.8}$$

$$\text{Overhead} = R \cdot N \cdot (N-1) \cdot \text{CMS} \tag{4.9}$$

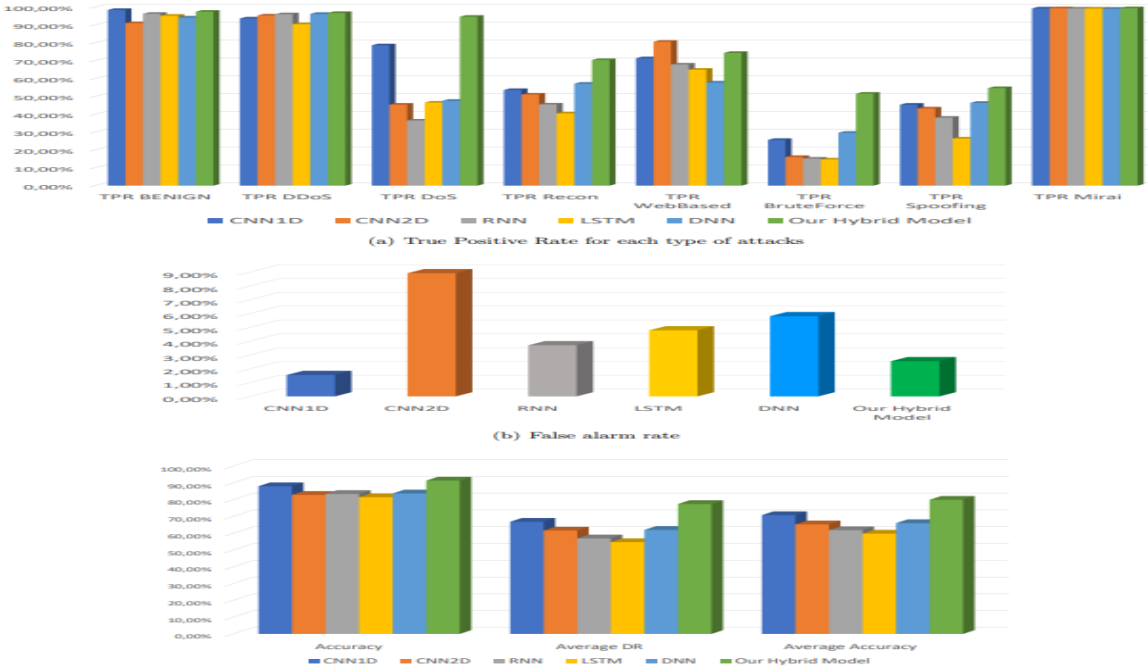


Figure 4.10: TPR and Global metrics for the different used models.

4.5.2 Models used for Federated learning

Figure 4.6 provides an overview of the initial models deployed for federated learning, which are subsequently broadcast to all participating clients. The models employed in our experiments are described as follows:

- *CNN1D model:* This model adopts a sequential architecture that utilizes two one-dimensional convolutional (Conv1D) layers. The first Conv1D layer uses a kernel size of 3×1 with 64 filters and an associated bias of 64, followed by a max pooling layer to reduce the dimensionality of the feature maps. The second Conv1D layer

Table 4.5: Obtained results for the different used models

		CNN1D	CNN2D	RNN	LSTM	DNN	Hybrid Model
Specific Metrics	TPR BENIGN	98,45%	91,09%	96,30%	95,22%	94,20%	97,45 %
	TPR DDoS	93,68%	95,34%	96,06%	90,49%	96,25%	96,76 %
	TPR DoS	78,67%	45,42%	36,54%	46,58%	47,58%	94,65 %
	TPR Recon	53,64%	51,07%	45,52%	40,52%	57,15%	70,39%
	TPR WebBased	71,40%	80,63%	67,90%	64,96%	57,82%	74,39%
	TPR BruteForce	25,68%	16,10%	15,17%	14,70%	29,67%	51,56%
	TPR Spoofing	45,41%	43,30%	38,12%	26,45%	46,42%	54,70 %
	TPR Mirai	99,29%	99,40%	99,25%	99,23%	99,14%	99,43%
Global Metrics	Accuracy	88,00%	82,85%	83,39%	81,45%	83,70%	91,35 %
	FAR	1,55%	8,91%	3,70%	4,78%	5,80%	2,55 %
	Average DR	66,82%	61,61%	56,94%	54,70%	62,01%	77,41 %
	Average Accuracy	70,78%	65,30%	61,86%	59,77%	66,03%	79,92%

applies a kernel size of 3×64 with 128 filters and a bias of 128, and a non-linear activation function is then applied. Subsequently, a global average pooling layer is employed to aggregate the features along the spatial dimension, followed by a dropout layer to mitigate overfitting. The architecture is completed with a fully connected layer.

- *CNN2D Model:* This model begins with a two-dimensional convolutional layer that employs a kernel size of 2×2, 32 filters, and a bias of 32. A 2D max pooling layer is then applied to reduce the data dimensionality. A subsequent 2D convolutional layer with a kernel size of 2×2, 64 filters, and a bias of 64 is employed, followed by an activation layer. Additional 2D max pooling is performed to further reduce the dimensionality, and the resulting feature maps are flattened into a one-dimensional vector before passing through a fully connected layer. A dropout layer is included to prevent overfitting, and the model concludes with a final fully connected layer.

- *RNN Model:* The recurrent neural network (RNN) model features a sequential structure beginning with an input layer that processes a vector corresponding to the first element in the sequence. It includes two SimpleRNN layers to capture temporal dependencies, followed by dense layers that apply non-linear activation functions to transform the sequential data into the desired output vector.

- *LSTM Model:* This model mirrors the architecture of the RNN model, with the key distinction that the SimpleRNN layers are replaced by Long Short-Term Memory (LSTM) layers. This modification is intended to better capture long-range dependencies and mitigate issues such as vanishing gradients.

- *Hybrid Model:* The hybrid model combines the strengths of a one-dimensional CNN with a Transformer block. In this architecture, the CNN1D component is tasked

Table 4.6: Models Sizes and the Network Overhead

	CNN1D	CNN2D	RNN	LSTM	DNN	Our Hybrid Model
Original model Total params	33,736 (131.78 KB)	17,768 (69.41 KB)	17,160 (67.03 KB)	54,600 (213.28 KB)	85,832 (335.28 KB)	206,602 (807.04 KB)
Original model Trainable params	33,736 (131.78 KB)	17,768 (69.41 KB)	17,160 (67.03 KB)	54,600 (213.28 KB)	85,832 (335.28 KB)	206,602 (807.04 KB)
Compressed model size	42.29 KB	22.21 KB	32.66 KB	77.96 KB	101 KB	251 KB
Network Overhead	33.04 MB	17.35 MB	6.38 MB	15.23 MB	78.91 MB	343.16 MB

with extracting salient features from network traffic data, while the multi-head attention mechanism in the Transformer block analyzes interdependencies between data points over long sequences. This fusion allows the model to capture both local features and long-range contextual relationships, enhancing its ability to detect complex attack patterns.

Used Hyperparamaters

To reach our purpose and achieve high performance of the FBMP-IDS system, different values of various hyper-parameters were tried. After several attempts, we identified the optimal hyper-parameters and their corresponding models, which are detailed in Table 4.4.

4.5.3 Results

The effectiveness of the FBMP-IDS architecture is assessed in this part. In the process of evaluation, we used the different training sub-datasets for the training steps of the different nodes, and the test sub-set for the test step. Table 4.5 and Figure 4.10 summarize the results obtained for the various deep learning models.

Specific Metrics

The table groups the True Positive Rates (TPRs) that each model has achieved in detecting various intrusion categories. Results can be seen in the FBMP-IDS with the Hybrid Model, attaining the highest overall performance and highest detection rate with 99.43% in Mirai attacks, 70.39% in Recon-based attacks, and 96.76% in DDoS-based attacks while being powerful in the identification of other attack types. As depicted in Figure 4.10, the following are the comparisons of the models based on the TPR obtained:

- *Benign Traffic:* The majority of models obtained high TPR values, demonstrating how these models are capable of distinguishing between normal and malicious traffic. The best of these models was CNN1D with a TPR of 98.45% and the second one is the Hybrid Model with a TPR of 97.45%.
- *Distributed Denial-of-Service Attacks:* Again, the Hybrid Model was better than the rest with a TPR of 96.76%. The DNN and RNN models performed very well in detecting DDoS attacks, with TPR values of 96.25% and 96.06% respectively.

- *Denial-of-Service (DoS) Attack:* As in the DDoS attack, the Hybrid Model was the best of all models, with a TPR of 94.65%. While CNN2D, RNN, and others had lower rates.

- *Reconnaissance Attacks:* The Hybrid Model achieved the highest TPR (70.39%) in the case of reconnaissance attack detection. A good TPR value was received by DNN at 57.15%. All other models showed lower performance.

- *Web-based Attack:* Again, the Hybrid Model showed strong performance at 74.39% in the case of web-based attack detection. A notable TPR (80.63%) is achieved by CNN2D, too, while others showed lower detection rates.

- Brute-Force Attack: Hybrid Models showed significant improvement in the case of brute-force attack detection over the other models and achieved a TPR of 51.56%. While all others showed much lower TPR.

- Spoofing Attack: Again, the Hybrid model showed the best performance at a TPR of 54.70% in the case of spoofing attack detection. Also, moderate TPRs are shown by CNN1D and DNN models, while others showed lower detection rates.

- Mirai Botnet Attack: All models achieved exceptionally high TPRs for detecting Mirai botnet attacks and obtained values over 99%, demonstrating how these are very capable of finding that threat. And the best among them was the hybrid model at 99.43%.

Global Performance Metrics

As detailed in Table 4.5, the global performance metrics evaluated in this study include Accuracy, False Alarm Rate (FAR), Average Detection Rate (DR), and Average Accuracy. Figure 4.10 illustrates that the Hybrid Model achieves the highest overall Accuracy of 91.35% and an Average Accuracy of 79.92%, accompanied by a very low FAR of 2.55%. These results demonstrate that the Hybrid Model strikes an effective balance between accurately detecting intrusions and minimizing false alarms.

ROC Analysis for the Different Models

In addition to the true positive rates for each intrusion class, Receiver Operating Characteristic (ROC) curves were constructed for each deep learning model deployed within the FBMP-IDS framework, as shown in Figure 4.9. The ROC curves, which depict the trade-off between the True Positive Rate (TPR) and the False Positive Rate (FPR) across various classification thresholds, provide further insight into model performance.

Micro-averaged ROC curves reveal overall performance differences among the models. Notably, the Hybrid Model achieved the highest micro-averaged ROC score of 0.993%, indicating superior classification performance and robust handling of class imbalances. However, while micro-averaged metrics offer a general performance overview, they can obscure weaknesses at the level of individual classes.

A closer examination of class-specific ROC curves reveals that several models, including CNN2D (Figure 4.9(b)), LSTM (Figure 4.9(d)), and DNN (Figure 4.9(e)), exhibit lower AUC values and less defined curves for certain classes. For example, although the CNN1D model (Figure 4.9(a)) achieved a commendable micro-averaged ROC score of 0.991%, its performance was notably limited in the "Recon" class. Similarly, the CNN2D model underperformed in both the "Recon" and "Spoofing" classes. In contrast, the Hybrid Model consistently delivered strong performance across individual classes, outperforming the LSTM model in the "Bruteforce" class with an AUC of 0.96% compared to 0.89%. Conversely, DNN models exhibited the poorest performance, with AUC values below 0.9 for the "Recon," "Bruteforce," and "Spoofing" classes.

These observations underscore the importance of evaluating both micro-averaged and class-specific ROC curves. While a model may demonstrate high overall performance, it may still struggle with specific classes due to inherent architectural limitations or potential biases in the training data. Recognizing such nuances is critical for real-world applications, where the relative importance of correctly classifying certain types of intrusions—such as "DoS" attacks—may outweigh others, like "Recon" activities.

4.5.4 Comparisons

Comparisons presented in Figure 4.10 clearly demonstrate that, across various evaluation metrics, the FBMP-IDS architecture—particularly its Hybrid Model—effectively detects a wide range of intrusion types. The Hybrid Model consistently outperforms other individual deep learning models within the framework, achieving superior results in most intrusion categories and exhibiting exceptional flexibility and robustness. Notably, the Hybrid Model also registers the highest AUC-ROC scores across different intrusion types, further reinforcing its overall superiority. Table 4.6 details the communication overhead associated with each model; while the Hybrid Model incurs the highest overhead due to its larger parameter set, this disadvantage must be considered alongside its performance benefits. By synergistically combining the strengths of CNNs and Multi-Head Attention mechanisms, the hybrid architecture is capable of capturing complex relationships in the data, thereby delivering optimal performance in scenarios where high accuracy is essential. Consequently, if the primary objective is to achieve optimal detection performance, the marginally increased communication overhead of the Hybrid Model is a justified trade-off given the substantial gains in detection accuracy and overall robustness.

4.6 conclusion

The advent of 6G wireless networks brings with it unparalleled opportunities as well as significant challenges in network security and privacy. The integration of advanced artificial intelligence into 6G connectivity necessitates the development of scalable and adaptive intrusion detection and prevention mechanisms that can respond dynamically to the continuously evolving network topology and distributed nature of these systems. In this work, we introduce a novel secure gradients exchange algorithm for distributed intrusion detection in 6G networks that synergistically combines federated learning with

secure multi-party computation and blockchain technology. Our proposed system enables the collaborative training of intrusion detection models while maintaining data privacy and ensuring secure gradient aggregation through the use of MPC protocols.

This approach supports adaptive secure aggregation that optimizes both communication overhead and computational complexity in real time. Furthermore, blockchain technology underpins the system by providing a decentralized, transparent, and tamper-proof framework for the federated learning process. In addition, we present a hybrid model architecture that employs Convolutional Neural Networks for effective feature extraction and Multi-Head Attention mechanisms for enhanced contextual analysis, thereby improving detection rates and reducing false alarm occurrences. The feasibility and efficacy of the proposed approach have been validated through extensive experimental evaluations and comparisons against several baseline models.

Chapter 5

TL2AB : Trusted Lightweight Authentication using AI and Blockchain for 6G Networks

5.1 Introduction

The globe is entering one of the quickest transforming ages, from 5G to 6G wireless networks [12]. Compared to its ancestor, 6G is expected to offer unprecedented connectivity via ultra-low latency and support gigantic IoT ecosystems that allow for transformational use cases such as smart cities, autonomous systems, and even next-generation AR and VR [11]. New threats to security come with new innovations, however. While this trend comes with augmented network complexity, exposure to cyberattacks goes through the roof, leaks of data, and privacy invasions [28]. In response, lightweight and efficient authentication protocols capable of securing communication in highly dynamic and resource-scarce environments need to be designed to enhance trustworthiness and security.

Most of the existing authentication protocols, which were initially designed for both 4G and 5G [223], are not effective enough to meet high-performance and security requirements for 6G [224]. They are either too resource-intensive to execute on the small, low-power devices pervasive in IoT, or too rigid to be flexible to the dynamic nature of 6G wireless networks that require real-time decision-making and context-awareness. Besides, the centralized nature of most current security architectures creates bottlenecks and single points of failure, and these are also vulnerable to attack.

In this chapter, we propose TL2AB, a novel authentication framework combining blockchain with Artificial Intelligence (AI) strength in an effort to provide strong, light, and distributed security for 6G networks. TL2AB utilizes the immutability of blockchain and its distributed trust model to develop a tamper-resistant, decentralized authentication framework. Meanwhile, AI-powered continuous authentication is watching that device's activity in real-time-responding to the growing threat. The marriage of the decentralized architecture of blockchain and the adaptive learning aspect of AI, empowers TL2AB with the following significant advantages:

- *Lightweight Architecture:* computation-lightweight architecture is designed to coexist in harmonious bliss with resource-constrained IoT devices making up most of the 6G ecosystem.

- *Decentralized Trust:* The blockchain removes a single point of failure, hence enhancing security, scalability, and resilience to cyberattack.

- *AI-based Adaptive Security:* The AI continuously looks out for threats and continually updates the real-time risk assessment to modify security measures without any extra overhead.

- *Scalability:* Such a system would scale to the enormous 6G scale towards constant authentication of billions of devices that interact with each other.

This work introduces the TL2AB architecture, describing in detail its elements and the interaction among AI, blockchain, and 6G edge nodes. The architecture proposed herein seeks to support not only device-to-network communication but also device-to-device authentication, critical in such a decentralized environment as is 6G. We will outline the mathematical model, the consensus algorithm, and the continuous AI-based risk profiling driving the dynamic nature of authentication.

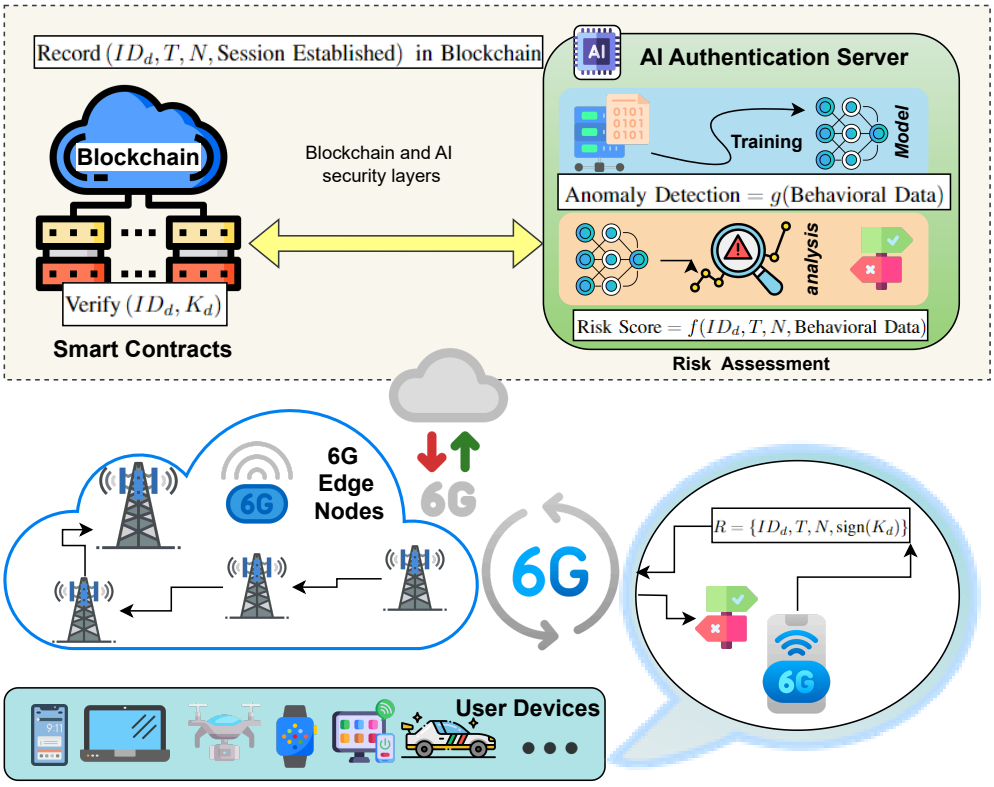


Figure 5.1: TL2AB architecture

5.2 Related Works

6G technology have attracted a significant interest of research into enhancing security and authentication mechanisms in the way of wide-scale applications, including: healthcare satellite networks, and blockchain-based systems [225, 226, 227]. The section below review a selected set of related literature on the security challenges pertaining to 6G networks and different proposed solutions, as provided in Tab. 5.1.

Paper	**Application Domain**	**Security Mechanism**	**Authentication Approach**	**Technological Focus**
Le et al. [225]	Healthcare	Data Privacy, System Cost Optimization	Three-factor authentication (Smart Card, Password, Biometric)	Healthcare Networks, Authentication Protocols
Chaudhry et al. [227]	Maritime Transportation Systems	GPS Spoofing, Unauthorized Data Access	Lightweight Authentication Protocol	Maritime Security, GPS-based Systems
Tao et al. [226]	Satellite Networks	Privacy Preservation, Energy Efficiency	Bilinear Pairing-based Group Signature, Batch Authentication	Satellite-ground Integrated Networks
Asim et al. [100]	Blockchain	Multi-Factor Authentication (MFA), Cyber Attack Prevention	MFA in Blockchain Systems	Blockchain-based Security, Cybersecurity
Fang et al. [228]	IoT Networks	Security Management, Authentication Efficiency	AI-enabled Lightweight Authentication, Holistic Access Control	IoT Networks, AI-enhanced Security
Garabato et al. [229]	General (Authentication Systems)	Continuous Authentication, Activity Monitoring	AI-based Continuous Authentication (SVM, MLP, Deep Learning)	AI-driven Authentication, Continuous User Verification

Table 5.1: Summary of Related Works on Security and Authentication in 6G Networks

The authors in [225] proposed CL-UCSSO, a three-factor authentication mechanism-based authentication protocol based on a smart card, password, and biometric authentication. Further, it accommodates network communication among healthcare providers and patients in an effective manner. Then, it addresses issues and challenges related to data privacy and system cost. The authors validated the suggested protocol through extensively used verification tools, proving its superior performance and features compared to the existing protocols. Another article in [227] analyzed the security and privacy vulnerabilities in 6G-enabled Maritime Transportation Systems. The authors therein propose a lightweight authentication protocol to protect against security attacks through GPS spoofing and illegal data access. The formal method of security analysis allows the authors to prove that their protocol guarantees enhanced features of security compared to traditional authentication protocols. This work emphasizes the need for adaptable security solutions for each individual sector within the 6G ecosystem. The paper in [226] suggested some authentication protocols for preserving privacy in heterogeneous satellite-ground integrated network. The authors suggest a bilinear pairing-based short group

signature algorithm that will offer unlinkable authentication and a lightweight batch authentication protocol of low-energy nodes with DoS attack resistance with efficiency. They also illustrate one of the issues during roaming across different operator networks and the necessary implementations towards efficient cross-domain authentication protocols with reduced latency. The work in [100] that demonstrated a survey of security issues in 6G networks illustrates high expectation on the use of blockchain technology to improve both security and authentication. The paper also conveys the use of MFA mechanisms within a blockchain network to prevent different types of sophisticated cyber-attacks. This study demonstrates that the management of certain vulnerabilities associated with applications is in need, and blockchain is expected to be one of the most promising solutions for future security needs.

Besides increasing security in these environments with the strength of AI, two additional solutions are crafted that can be achieved using AI: a light-weight authentication protocol and an extensive access control protocol. The biggest discovery was that AI can make security management easier and might support IoT's dynamic environment, pointing out a few potential future research paths such as collaborative access control, advanced machine learning algorithms, and game theory-based defense mechanisms.

There has been a lot of research on the use of AI techniques to improve authentication and authorization in large-scale IoT networks. In one such work, the authors outlined the characteristics of IoT networks and the constraints of conventional authentication approaches [228]. Having enumerated the advantages of utilizing AI to improve security in such environments, the authors went on to outline two new AI-enabled solutions: a light-weight authentication protocol and a full-fledged access control protocol. The main point was that AI could make security management easier and would adapt to the changing IoT landscape. It also depended on future research directions, including cooperative access control, new machine learning algorithms, and game theory for defense mechanisms.

Another work explored the feasibility of AI-based continuous authentication in [229]. The authors developed a custom application to gather user activity data in a guided setting and also utilized an open dataset for benchmarking in a non-guided setting. They designed key features from the data and trained three AI models: Support Vector Machines, Multi-Layer Perceptrons, and a Deep Learning-based solution. These were actually successful AI-based techniques for authentication of users in guided and unguided environments. They then developed a continuous authentication system based on weighted sliding windows to detect impostor sessions in real-world settings.

For a general comparison, Tab. 5.2 summarizes the key security features, authentication techniques, technical focus, and limitations of the selected state of the art works and our TL2AB proposal. As can be seen from the comparison, the limitations of the existing solutions – i.e., scalability problems, computational costliness, or lack of complete continuous monitoring – are what TL2AB aims to address by the integration of decentralized blockchain-based trust with AI-driven dynamic risk assessment for 6G networks.

Table 5.2: Comparison of Security Features and Authentication Approaches in Related Schemes

Reference	**App. Domain**	**Security Mechanism**	**Authentication Approach**	**Tech. Focus**	**Key Security Features and Limitations**
[230]	Healthcare IoT	Implicit Certificate-based	Three-factor (Smart Card, Password, Biometric)	6G Healthcare	Robust multi-factor security; high computational cost and limited scalability.
[231]	Smart Home IoT	Implicit Certificate-based	Lightweight Device-to-Device Authentication	Smart Home IoT	Optimized for resource-constrained devices; resists replay and MITM attacks.
[232]	General IoT Systems	Blockchain-based	Decentralized Authentication	IoT Networks	Leverages decentralized trust; may incur processing overhead.
[233]	IoT Networks	Blockchain-inspired	Cluster-based Authentication with Consensus	IoT Networks	Novel consensus algorithm with low computational overhead; challenges with heterogeneous integration.
[234]	IoT Systems	PUF-based	Lightweight Mutual Authentication	IoT	High efficiency and robust resilience against physical and side-channel attacks; tailored for constrained environments.
[235]	Health Informatics	Blockchain-enabled	Probabilistic Authentication and Authorization	Healthcare IoT	Robust mutual authentication with enhanced access control and lower overhead; designed specifically for health informatics.
TL2AB (Proposed)	**6G Networks, IoT**	**AI-driven Continuous Authentication with Blockchain**	**Dynamic, Adaptive Multi-factor Authentication**	**6G, IoT**	**Integrates decentralized trust with AI-driven risk assessment for real-time, scalable, and resource-efficient authentication; introduces continuous monitoring and dynamic adaptation to emerging threats.**

Variable	Description
ID_d	A unique identifier assigned to each device in the network.
K_d	The cryptographic key generated for each device, used to sign authentication requests and secure communications.
R	The authentication request message, which includes ID_d, T, N, and $sign(K_d)$.
T	The timestamp indicating when the authentication request is generated; used to prevent replay attacks.
N	A unique nonce included in each authentication request to ensure its uniqueness and counter replay attacks.
$sign(K_d)$	The digital signature produced using the device's key K_d, ensuring the authenticity and integrity of the request.
RS	The risk score computed by the AI Authentication Server, normalized between 0 and 1 to reflect the likelihood of a security threat.
$T_{\text{threshold}}$	The predefined risk score threshold above which additional authentication measures are required.
P(MITM)	The estimated probability of a successful Man-in-the-Middle attack on the system.
P(Impersonation)	The estimated probability of a successful impersonation attack on the system.
P(DoSTL2AB)	The estimated probability of a successful Denial-of-Service attack against the TL2AB framework.
P(DoScentralized)	The estimated probability of a successful Denial-of-Service attack against a centralized authentication system, provided for comparison.
$P(E)$	The estimated probability of a privacy breach event occurring within the system.

Table 5.3: Symbols Definition

5.3 System and Network Model

Here, the architecture and operational processes of TL2AB are presented as in Fig. 5.1. The proposed framework is founded on blockchain technology and AI to develop a secure, efficient, and self-tuning authentication mechanism for 6G networks.

5.3.1 TL2AB Architecture

The TL2AB architecture includes some key components implemented in operation in collaboration, enabling secure authentication in 6G environments:

- User Devices That is, the IoT devices, mobile phones, and sensors would have to obtain authentication prior to joining the network. All the user devices must have a one-of-a-kind cryptographic key in a secure element of the device.
- *6G Edge Nodes* These are device-to-rest-of-the-network user device interfaces. They act as intermediaries between the rest of the network and the device, relaying authentication responses as well as requests.
- *AI Authentication Server* This is an AI-powered server based on machine learning algorithms. It inspects the authentication requests from the user-side device and behavioral pattern to create a verdict regarding the risk that the device carries and modify their authentication requirements according to real-time threats.
- *Blockchain Network* The decentralized blockchain constitutes the foundation of the TL2AB Authentication Framework. The network provides trust in the guise of immutability, hence retaining all the authentication requests and their outcomes. It therefore also includes the qualities of transparency and traceability.
- *Smart Contracts* Smart contracts running on the blockchain, make this authentication automatic by specifying a list of rules or conditions under which authentication can be successful. They make sure that the service terms are satisfied before access is allowed.

5.3.2 System Assumptions

The key assumptions underlying the TL2AB framework are as follows:

- The underlying blockchain network is secure against 51% attacks and other consensus-related vulnerabilities, considering the fact that a majority of nodes comprising it are honest.
- In the user's devices, use a secure element which securely store the unique cryptographic keys used by users without compromising security.
- The AI Authentication Server can collect enough behavioral data to model the activities of users with high accuracy and also spot anomalies.

Algorithm 1 TL2AB Authentication Algorithm (Part 1)

procedure RegisterDevice(ID_d, K_d)
    Generate cryptographic key K_d and store (ID_d, K_d) in Blockchain.
    return "Device Registered"
end procedure
procedure AuthenticationRequest(ID_d, K_d)
    Generate timestamp T and nonce N.
    $R \leftarrow \{ID_d, T, N, \text{Sign}(K_d)\}$
    return R
end procedure
procedure AssessRisk(R)
    Analyze behavioral data associated with ID_d.
    $RS \leftarrow f(ID_d, T, N, \text{BehavioralData})$
    return RS
end procedure
procedure ExecuteSmartContract(R)
    if Verify(ID_d, K_d) in Blockchain **then**
        Record authentication attempt in Blockchain.
        return "Authentication Successful"
    else
        return "Authentication Failed"
    end if
end procedure

Figure 5.2: TL2AB Authentication Algorithm (Part 1)

- There might be some adversaries which can intercept and manipulate the messages of communication and might compromise individual devices or nodes in the network.
- The AI models are trained using clean data that has not been compromised in any way, making them quite reliable in the risk assessment process.

Step 1: Registration

The smart contract on the blockchain is accountable for the authentication of this request. The authentication process includes:

- **Uniqueness check:** The smart contract checks if the identifier ID_d is not registered by looking at the state of the ledger.
- **Hash format validation:** Format and length of $H(K_d)$ are validated against predefined parameters (e.g., 256-bit SHA-256 output).
- **Replay protection:** A nonce or timestamp is appended to the transaction in order to thwart replay attacks.
- **Authenticity assurance (optional):**Optional: if needed, an off-chain verifier (e.g., TEE attestation service or PKI server) can verify that K_d was calculated within a trusted module and associated with the device ID_d.

Algorithm 2 TL2AB Authentication Algorithm (Part 2)

```
1:  procedure AdjustAuthentication(RS)
2:      if RS > T_threshold then
3:          Require additional factors (Biometric, OTP).
4:          if additional factors are provided then
5:              return "Authentication Successful"
6:          else
7:              return "Authentication Failed"
8:          end if
9:      else
10:         return "Authentication Successful"
11:     end if
12: end procedure
13: procedure EstablishSession(ID_d)
14:     Encrypt Data and record session in Blockchain.
15:     return "Session Established"
16: end procedure
17: procedure MonitorSession(ID_d)
18:     while session is active do
19:         Check for anomalies in behavioral data.
20:         if AnomalyDetected() then
21:             TerminateSession(ID_d) and require re-authentication.
22:         end if
23:     end while
24: end procedure
25: procedure TerminateSession(ID_d)
26:     Record session termination in Blockchain.
27:     return "Session Terminated"
28: end procedure
29: procedure Main
30:     // Register Device
31:     RegisterDevice(ID_d, H(K_d))
32:     // Authentication Process
33:     R ← AuthenticationRequest(ID_d, KH(K_d))
34:     RS ← AssessRisk(R)
35:     if RS < T_threshold then
36:         if ExecuteSmartContract(R) == "Authentication Successful" then
37:             AdjustAuthentication(RS)
38:             EstablishSession(ID_d)
39:             MonitorSession(ID_d)
40:         else
41:             return "Authentication Failed"
42:         end if
43:     else
44:         Require additional authentication.
45:     end if
46: end procedure
```

Figure 5.3: TL2AB Authentication Algorithm (Part 2)

If all checks pass, the pair $\{ID_d, H(K_d)\}$ is recorded immutably on the blockchain, enabling only registered devices to initiate authentication requests in future sessions. The formal notation of the registration operation is:

$$\text{RegisterDevice}(ID_d, H(K_d)) \Rightarrow \text{Blockchain Entry}$$

Authentication Request Generation

When a device attempts to authenticate, it generates an authentication request containing its identity ID_d, a timestamp T, and a nonce N. To ensure integrity and authenticity, the device signs a specific set of values using its private key K_d stored in the TEE.

The digital signature is computed over the concatenation of the request components as follows:

$$\text{Sign}(K_d, M) \quad \text{where } M = \{ID_d \parallel T \parallel N\}$$

This signature proves the origin and integrity of the message without revealing K_d. The smart contract or authentication server then verifies the signature using the stored $H(K_d)$ or a public key (if asymmetric cryptography is used).

The full authentication request sent to the system is:

$$R = \{ID_d, T, N, \text{Sign}(K_d, ID_d \parallel T \parallel N)\}$$

Step 3: AI-Driven Risk Assessment

- Upon the attempt of a registered device to join the network, it issues an authentication request R. This request identifies the device identifier ID_d, a timestamp T, a nonce N (to prevent replay When the AI Authentication Server receives an authentication request, it evaluates the security risk of the request. A machine learning model processes various contextual factors, including previous user behavior, device type, network type, and geolocation. The computed *risk score* RS determines the authentication level to be executed: attacks), and a digital signature produced using K_d. The authentication request is then transmitted securely to the authentication server to be verified:

  $$RS = f(ID_d, T, N, \text{Behavioral Data})$$

  where f is a Random Forest Regressor trained on authentication logs. If the computed *risk score* is *below* the predefined threshold $T_{\text{threshold}}$, the request proceeds to blockchain validation. Otherwise, additional authentication steps are required. In our implementation, the function f computes the risk score RS for an authentication attempt. This function is realized using a Random Forest Regressor that is trained on historical authentication data. The inputs to f include the device identifier (ID_d), timestamp (T), nonce (N), and a set of behavioral features ($\mathbf{X}$), such as the number of login attempts and time since the last login. The risk score RS is normalized to fall between 0 and 1, with higher values indicating greater risk. This approach allows the AI Authentication Server to quickly assess risk and adjust authentication measures in real time.

Step 4: Smart Contract Execution

- The authentication request is cross-checked with blockchain data to confirm that the requesting device is registered and that its credentials have not been breached. The smart contract confirms the identity of the device by verifying if ID_d and the saved hash of K_d equals recorded values stored on the blockchain:

$$\text{Verify}\,(ID_d, H(K_d)) \Rightarrow \text{Blockchain Lookup}$$

- If the verification is successful, the authentication request proceeds to the next step. Otherwise, the authentication attempt is rejected.

Step 5: Adaptive Multi-Factor Authentication (MFA)

Based on the *risk score evaluatio*n, the system dynamically adjusts the authentication requirements:

- If $RS < T_{\text{threshold}}$, the request is considered low-risk, and authentication proceeds without additional verification.
- If $RS \geq T_{\text{threshold}}$, the system enforces an additional authentication factor, such as biometric authentication or a one-time password (OTP):

$$\text{Require(Biometric, OTP)}$$

- If the user successfully completes MFA verification, authentication is granted. Otherwise, access is denied.

Step 6: Secure Session Establishment

Once authentication is approved, the device establishes a secure session using encryption protocols to protect subsequent communications. The authentication event, along with the session details, is recorded immutably on the blockchain:

$$\text{Encrypt}\,(\text{Session Data}) \Rightarrow \text{Secure Session}$$

$$\text{Record}\,(ID_d, T, N, \text{Session Established}) \Rightarrow \text{Blockchain Entry}$$

Step 7: Continuous Monitoring and Anomaly Detection

During the authenticated session, the AI Authentication Server continuously monitors user behavior to detect anomalies. If any suspicious activity is detected, the system dynamically adjusts authentication requirements or terminates the session. The anomaly detection function is defined as:

$$\text{Anomaly Detection} = g(\text{Behavioral Data})$$

where g is a machine learning-based anomaly detection model.

Step 8: Secure Session Termination

When the user completes their activities, the session is securely terminated, and an entry is recorded on the blockchain:

$$\text{TerminateSession}(ID_d) \Rightarrow \text{Record}\,(ID_d, T, N, \text{Session Terminated}) \Rightarrow \text{Blockchain Entry}$$

This ensures a secure log of all authentication events, maintaining an immutable audit trail.

In summary, the TL2AB framework integrates advanced technologies to create a robust, lightweight authentication solution that addresses the unique challenges posed by 6G networks. The following sections will provide more details on the mathematical models that are used in the framework and discuss its security and performance evaluations.

5.4 Experimental Evaluation

5.4.1 Dataset

The dataset we have created has rich key attributes capturing, for each authentication request, important information in the form of device details, user behavior metrics, and network characteristics. All these attributes are necessary to construct a predictive model to determine the risk associated with each authentication attempt. Tab. 5.4 describes each feature in the dataset, including its importance and usability for the analysis in this work. This complete data set is the basis of our machine learning model from which meaningful observation regarding patterns in authentication and possible breaches in security can be extrapolated.

Analysis of Authentication Dataset

Here, we provid a series of visualizations that develops the authentication data against various dimensions, including, risk score distribution, network types, device types, authentication methods, and relationships between login attempts, time since last login, and the calculated risk score.

- *Distribution of Risk Scores*: Fig. 5.4 illustrates the risk score distribution of authentication attempts. The histogram is right-skewed, indicating that there are lots of low-risk scores in most authentication cases and high-risk ones are relatively uncommon. This distribution informs us that there would be majority authentication attempts that would fall into low-risk classes with a minority that would have to be examined in depth. The superimposed density curve plotted over the histogram provides a smoothed approximation of the probability distribution, in support of the observation that risk scores are highly dense within the lower range. This observation substantiates the research aim by demonstrating how the authentication

Feature	Description	Type
Timestamp	The timestamp when the authentication event occurred, randomly generated within a month.	DateTime
Device_ID	Unique identifier for each device.	String (ID)
IP_Address	Randomly generated IP address (e.g., 192.168.1.1).	String (IPv4)
Location	Geographical coordinates (latitude, longitude) of the device's location, randomly generated.	String (Latitude,Longitude)
Network_Type	Type of network being used (WiFi, 4G, or 5G).	Categorical (WiFi, 4G, 5G)
Device_Type	Type of device used for authentication (smartphone, IoT sensor, laptop, or tablet).	Categorical (smartphone, IoT, laptop, tablet)
OS_Version	The version of the operating system on the device (e.g., iOS_15, Android_12).	Categorical (OS Version)
App_Version	Version of the application used for authentication (e.g., 1.2, 2.5).	String (Version)
Authentication_Method	Authentication method used (password, biometric, token, 2FA).	Categorical (password, biometric, token, 2FA)
Login_Attempts	The number of login attempts made during this session (between 1 and 10).	Integer (1–10)
Time_Since_Last_Login	Time in hours since the last successful login, ranging from 0 to 168 hours (7 days).	Numeric (Continuous)
Unusual_Activity_Flag	Flag indicating whether unusual activity was detected during the session (1: Yes, 0: No).	Binary (0, 1)
Is_Roaming	Flag indicating whether the user is roaming (1: Yes, 0: No).	Binary (0, 1)
Is_VPN	Flag indicating whether the user is using a VPN (1: Yes, 0: No).	Binary (0, 1)
Risk_Score	A calculated risk score based on multiple factors such as login attempts, time since last login, etc.	Numeric (0–1)

Table 5.4: Feature Descriptions

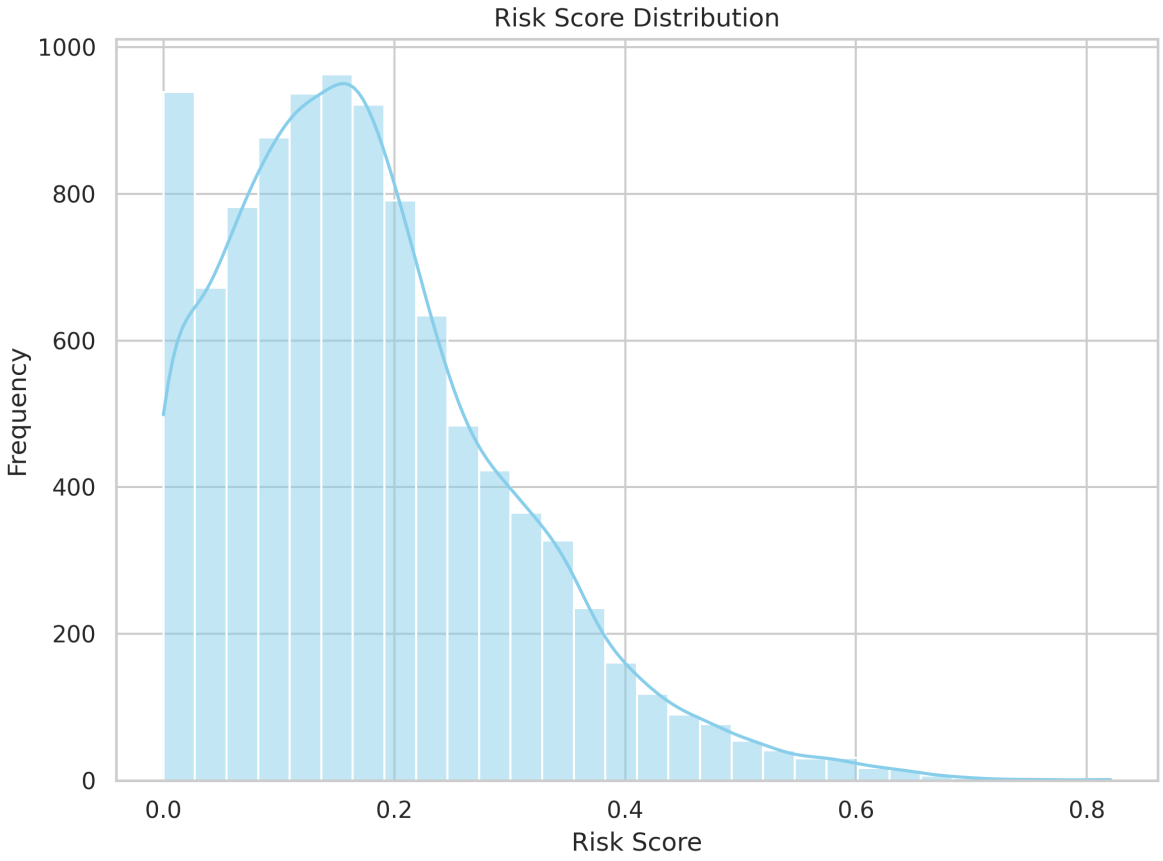


Figure 5.4: Risk Score Distribution

process clearly identifies and classifies low-risk and high-risk authentication processes. The mostly minor high-risk event rate indicates that the proposed approach does not incur unnecessary security measures without relaxing its vigilance against potential fraudulent login attempts. The risk score, as calculated from login attempts, time elapsed since last login, suspicious behavior, roaming, and VPN use, has the distribution as depicted in Tab.5.5.

Statistic	**Value**
Count	100,000
Mean	0.1769
Standard Deviation	0.1237
Minimum	0.0000
25th Percentile (Q1)	0.0863
50th Percentile (Median)	0.1590
75th Percentile (Q3)	0.2431
Maximum	0.8794

Table 5.5: Risk Score Statistics

These numbers show that the risk scores are low in general, with a mean of 0.1769 and most values concentrated below 0.25. The high point of 0.8794 indicates the presence of high-risk users, but they are few. A very small fraction of the entire dataset (5.03%) is suspected of suspicious activity. And Only 0.10% of the users are labeled high-risk, with risk scores greater than 0.7. This indicates that the overwhelming majority of users do have low risk scores but that there is a very small subgroup with behavior perhaps indicating a higher security issue.

- *Network Type Distribution:* Figure 5.5 shows the distribution of network types used in authentication attempts. The 4G, 5G, and WiFi networks are the three types considered. As seen from the results, authentication attempts are evenly distributed among network types so that the testing of the authentication framework accounts for different network conditions. This diversity is required for studying the impact of network variability on authentication performance, particularly for 6G networks. By adding network diversity to the evaluation, the study ensures that the proposed model is robust to network-level variations. This is consistent with the research objective of developing a flexible authentication system that works efficiently under heterogeneous network conditions, a key characteristic of 6G security.

- *Device Type Distribution:* Fig. 5.6 shows the distribution of device types in the dataset, presenting the relative frequency of authentication attempts from various device types, ranging from laptops, smartphones, to IoT sensors, and tablets. The findings demonstrate a fairly even distribution across device types, revealing that the dataset covers a wide range of device types. This distribution is essential to determining the generalizability of the proposed authentication framework across various device ecosystems in a 6G network system. These findings validate the ability of the framework to generalize since it is being trained and tested on a wide range of devices. The diversified coverage of device types prevents a single category

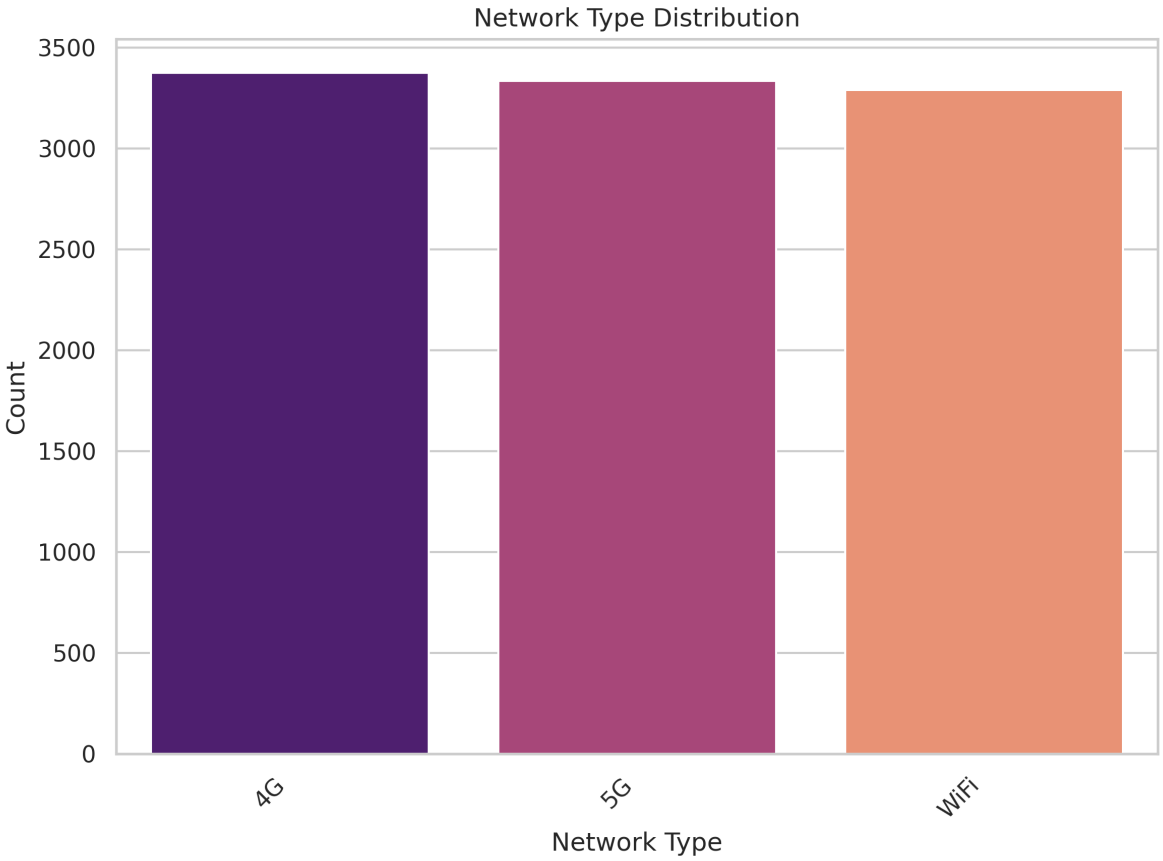


Figure 5.5: Network Type Distribution

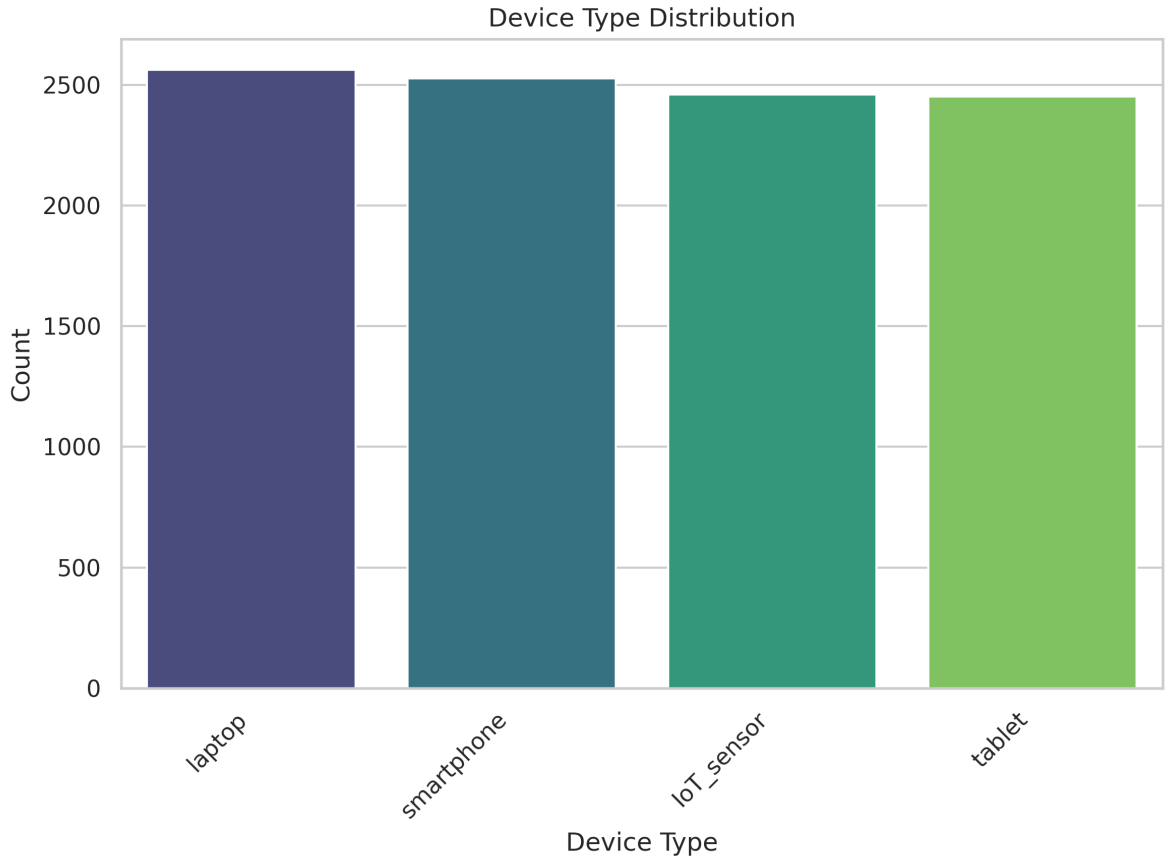


Figure 5.6: Device Type Distribution

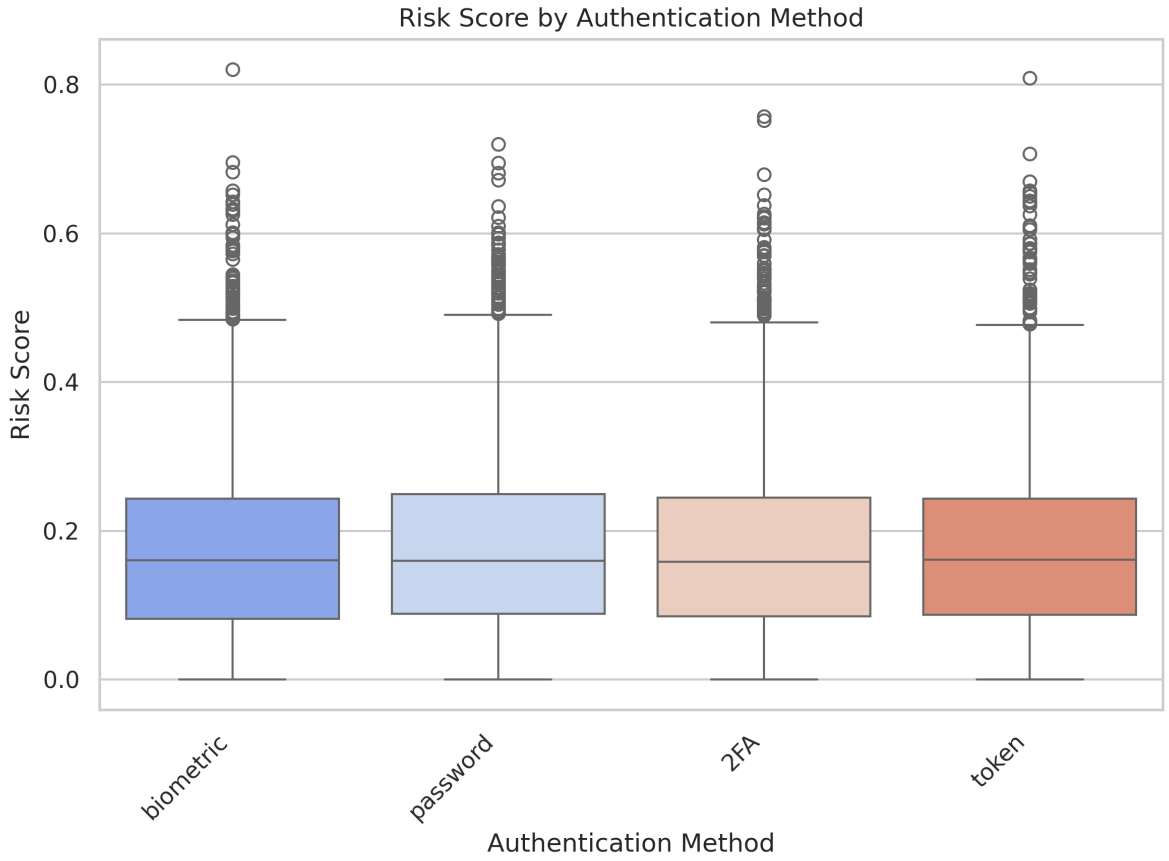


Figure 5.7: Risk Score by Authentication Method

from overwhelming the authentication model and thus making it more deployable in real-world applications.

- *Risk Score by Authentication Method* Fig. 5.7 illustrates comparative risk score analysis for different authentication mechanisms, including biometric authentication, passwords, two-factor authentication (2FA), and token-based authentication. The box plot illustrates the risk score distribution for each authentication mechanism, with indication of outliers and risk level variation. Findings reveal that some authentication mechanisms possess lower median risk scores, whereas other authentication mechanisms possess greater risk variability. This contrast highlights the necessity for the selection of robust authentication methods in order to secure 6G networks.

- *Login Attempts vs. Risk Score* Fig. 5.8 shows the daily variation in the risk scores and login attempts. The two-axis plot shows the trajectory of the average risk score (left y-axis) and login attempt frequency (right y-axis) during a day over 24 hours. The patterns show periodic peaks in login attempts after risk score changes. The findings highlight the significance of time being considered during authentication risk evaluation. The findings suggest that authentication requests at certain time intervals can be riskier in nature, and hence dynamic security policies may be required. This result strongly supports the research objective of creating a risk-

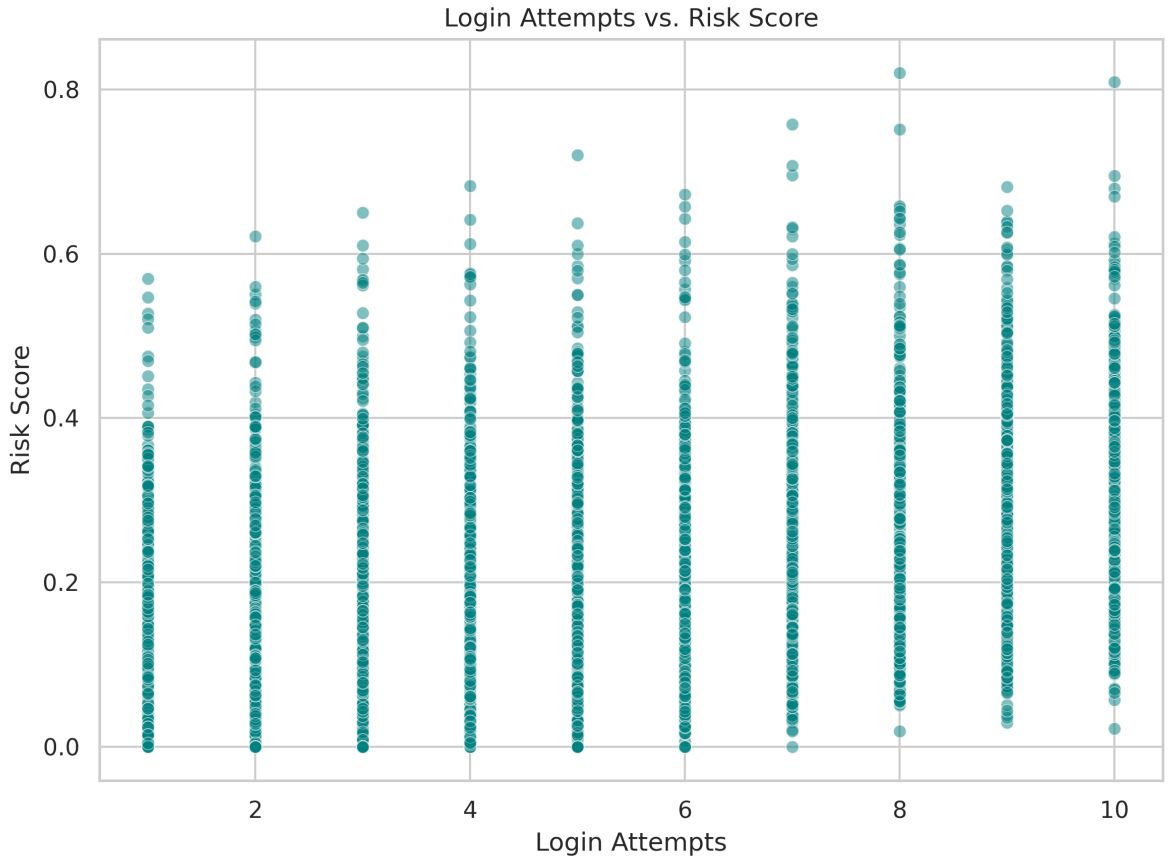


Figure 5.8: Login Attempts vs. Risk Score

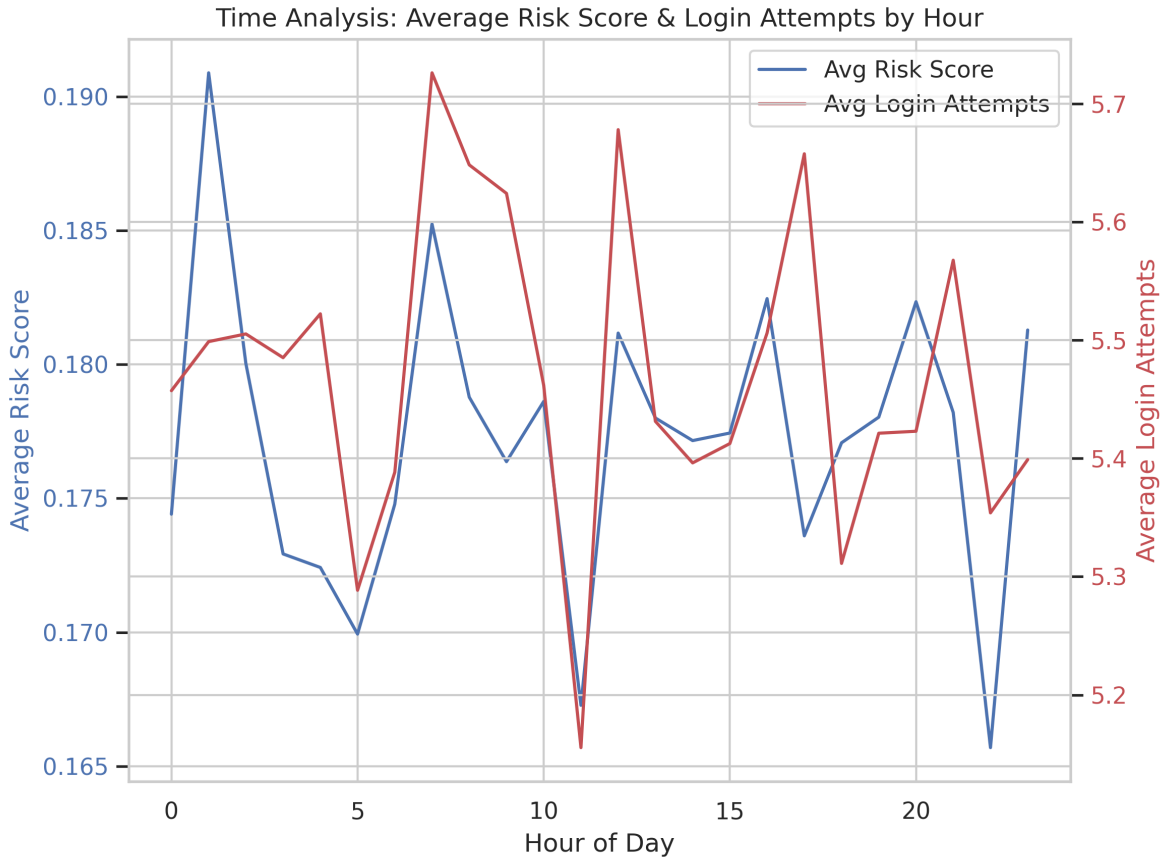


Figure 5.9: Login Attempts vs. Risk Score

aware authentication system. The ability to identify and flag suspicious activity based on failed login attempts enhances the performance of the system in blocking unauthorized access with minimal impact on legitimate users.

- *Temporal Analysis of Risk Scores and Login Attempts* Fig. 5.9 displays the time evolution of risk scores and login attempts during a day. The two-axis figure illustrates the oscillations in the mean risk score (left y-axis) and number of login attempts (right y-axis) on a 24-hour cycle. The periodic regular maxima in login attempts are found to always coincide with risk score oscillations. This temporal examination casts critical lights upon authentication behavior, and time-aware security controls can be designed to react to the change of user activity patterns based on this temporal examination.this includes the attempt location or the user profile. These results emphasize the necessity of including temporal factors in authentication risk assessment. The trends in observations indicate that authentication requests during some time windows can be riskier in terms of nature, requiring dynamic security policies. This aligns with the research interest by indicating that there is a need for time-aware risk countermeasures in 6G authentication systems.

  Some login attempt thresholds (e.g., 3, 5, and 8) have a couple of instances of higher risk scores (above 0.6), which can reflect unusual behavior patterns at these attempt numbers. The average login attempts by device type are as follows:

Device Type	Average Login Attempts
IoT Sensor	5.50
Laptop	5.51
Smartphone	5.49
Tablet	5.45

Table 5.6: Login Attempts by Device Type

The average number of login attempts for each device type is close to 5.5, as presented in Tab. 5.6 indicating that users across different devices and locations tend to make a similar number of attempts.

5.4.2 AI Authentication Server Evaluation

This section specifies the AI model that, in TL2AB context, forecasts the danger of authentication attempts. The model uses an ensemble learning algorithm known as *Random Forest* [236], wherein predictions of multiple decision trees are combined to improve the accuracy and credibility of predictions. Unlike linear regression-based models, Random Forest does not rely on one hypothesis but applies an ensemble of several decision trees for prediction. Our model utilizes a *Random Forest Regressor* to make a prediction of a risk score based on several features extracted from the authentication request data. According to this, the AI model loads data, preprocesses, trains the model, and conducts performance tests.

Data Preprocessing and Feature Engineering

Before training the Random Forest model, several preprocessing steps are performed on the data to ensure that the model receives high-quality input. The preprocessing pipeline includes timestamp conversion, feature extraction, and one-hot encoding of categorical variables.

The data preprocessing pipeline consists of several steps aimed at preparing the authentication data for model training. The main steps are:

- **Timestamp Conversion**: The ‘Timestamp‘ field is converted to a datetime format to extract useful time-based features.
- **Feature Extraction**: Additional features, such as the hour of the day (‘Hour‘) and the day of the week (‘DayOfWeek‘), are derived from the ‘Timestamp‘.
- **Categorical Encoding**: Categorical variables such as ‘Network_Type‘, ‘Device_Type‘, ‘OS_Version‘, and ‘Authentication_Method‘ are converted to one-hot encoded columns to make them suitable for machine learning models.
- **Feature Selection**: Non-numeric columns like ‘Timestamp‘, ‘Device_ID‘, ‘IP_Address‘, ‘Location‘, and ‘App_Version‘ are dropped from the dataset.

Parameter	Value
Number of Trees (n_estimators)	100
Number of Features Used	23
Details of the first tree in the forest	
Tree depth	30
Number of leaves	4974
Number of nodes	9947

Table 5.7: Model Architecture

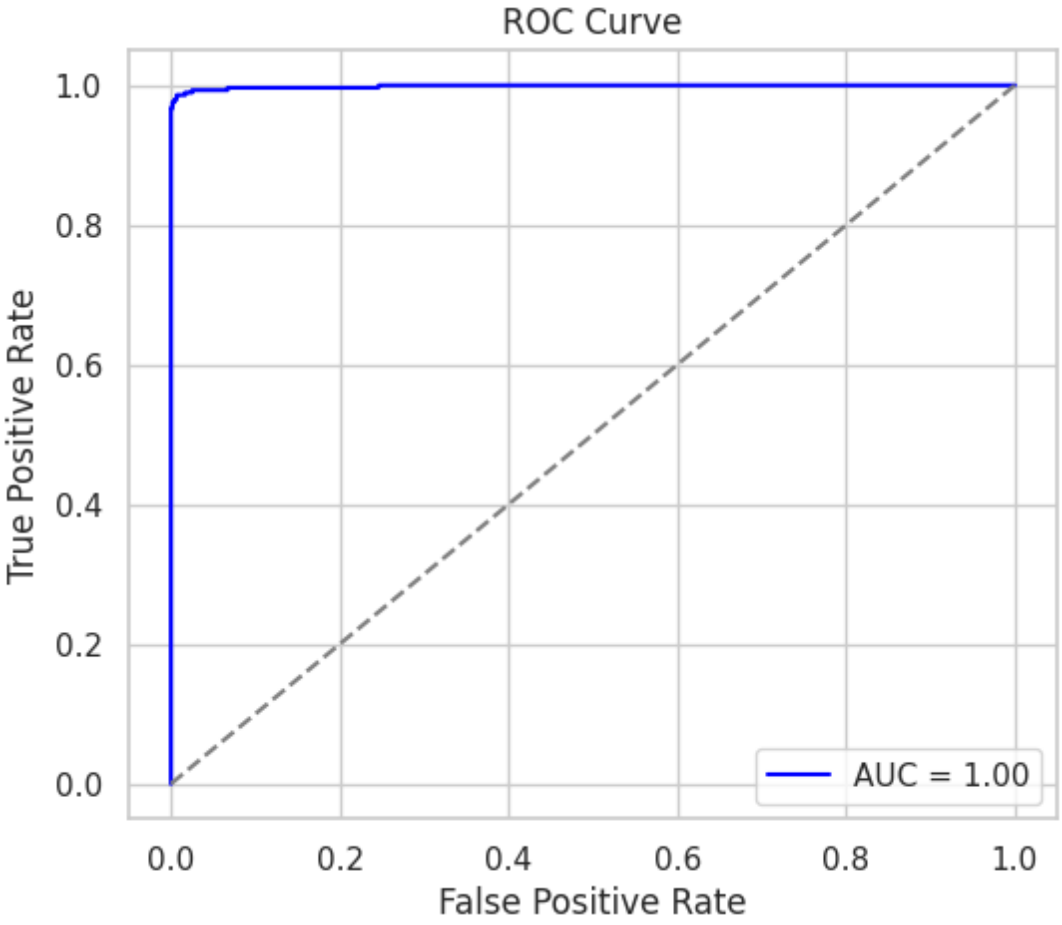


Figure 5.10: RoC Curve

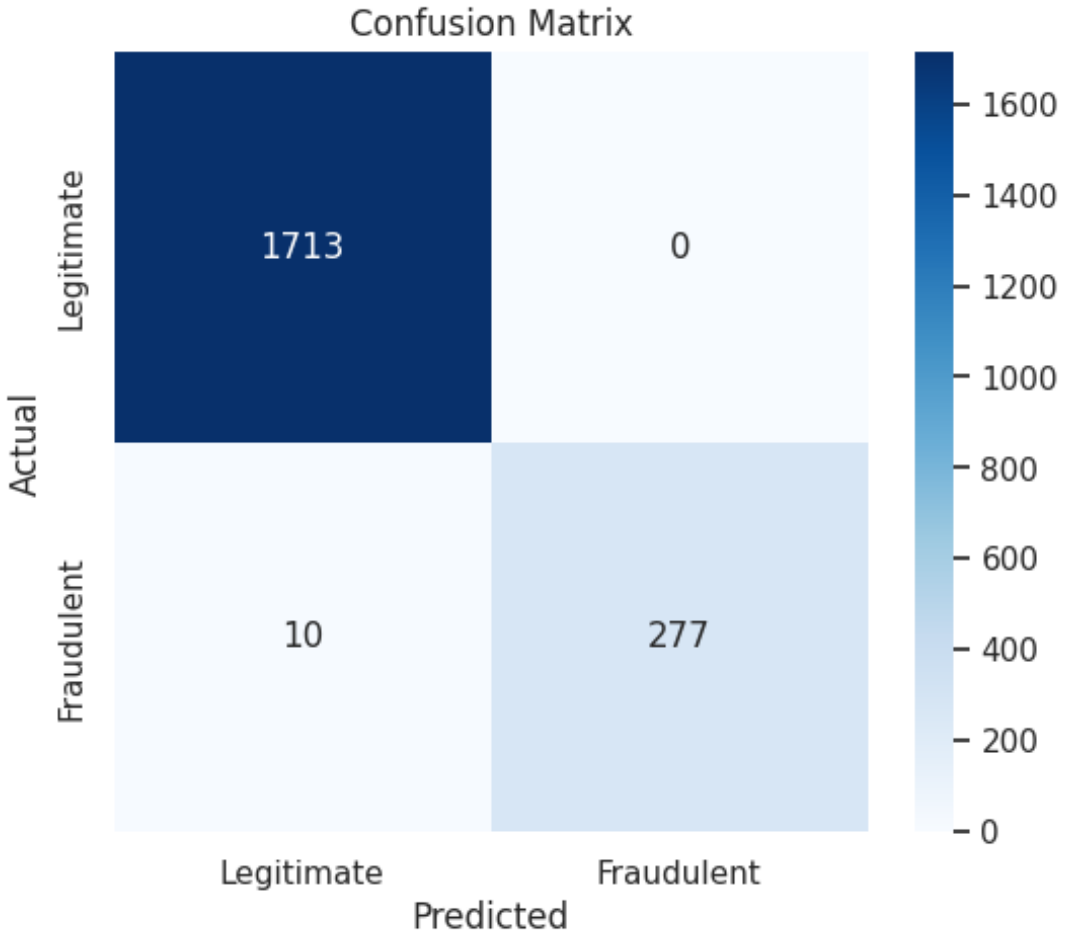


Figure 5.11: Confusion Matrix

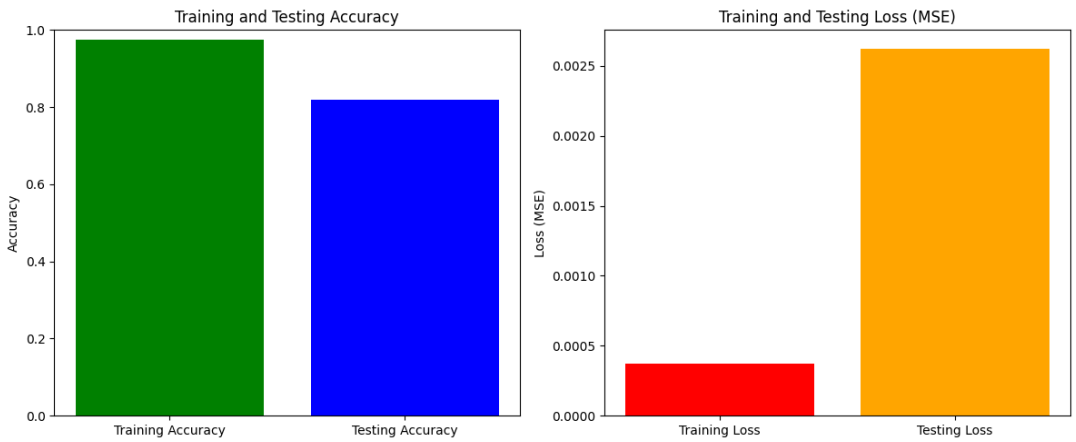


Figure 5.12: Training and Testing Accuracy and Loss

The trained model was a Random Forest Regressor (Tab. 5.7), accuracy and loss metrics were used to test its performance throughout both training and testing stages, as illustrated in Fig. 5.12, Fig. 5.10, and Fig. 5.11. High training accuracy of the fraud detection model is 97.51%„ as illustrated in Fig. 5.12, indicating that it learns well from the training data. This trend also accompanies a training loss of 0.0004 and a test loss of 0.0026. Though the training loss is unexpectedly small, greater test loss guarantees that the model isn't overgeneralizing but is capable of bettering itself.

On accuracy in fraudulent cases detection, accuracy 99% means zero false positive and no true case being flagged as fraudulent. But the 0.965 recall means 3.5% true cases that are actual cases of fraud are missed. The value 0.997 for AUC-ROC guarantees the capability of the model to effectively identify fraudulent as compared to non-fradulent cases.

False Negative Rate (FNR) of 0.035, i.e., only 3.5% of fraudulent transactions are missed. The False Positive Rate (FPR) is 0.001, which is good as it avoids unnecessary disruptions for legitimate users.

These metrics indicate that the lightweight Random Forest Regressor inside the AI authentication server can give accurate predictions and good performance on the training dataset and very commendable accuracy on the test dataset. The results are therefore suggestive of the model's effectiveness in capturing the underlying relationships in the data while making sure of a decent level of generalization.

5.5 Security Analysis

This section evaluates the TL2AB authentication system in its entirety, from the viewpoint of its insusceptibility to various critical security vulnerabilities that are commonly prevalent in 6G network systems.

5.6 Threat Model

TL2AB protocol has been designed keeping in mind that big 6G networks have an adversarial nature. Both internal and external attackers have been considered by us in our threat model and we estimate these attacks based on the strength of our multi-layer defense mechanism. The system is tailored to be immune to the following main attack vectors:

Insider Threats: Malicious insiders, such as valid-credential users or compromised machines, may attempt to exploit access privileges or steal sensitive data. To counter this, TL2AB ensures that cryptographic keys (K_d) are generated within and secured by Trusted Execution Environments (TEEs) or Hardware Security Modules (HSMs), thereby reducing the risk of credential exposure. In addition, real-time anomaly detection systems leveraging AI monitor access behavior and report alarms on the detection of anomalous patterns. Access is controlled tightly by means of role-based and attribute-based controls to uphold the least privilege principle.

Sybil Attacks: Sybil attacks involve attackers trying to generate multiple fake identities to induce blockchain consensus disruptions or spam the network with invalid authentication requests. TL2AB averts this by introducing a stringent identity verification protocol at device registration, which securely ties each cryptographic key (K_d) to a physical device identifier. The resource-intensive cost of producing numerous spurious identities, in addition to a supermajority consensus requirement (typically over $\frac{2}{3}$ active nodes), also reduces the viability of the attack.

Collusion and Compromise of Multiple Nodes: Colluding attackers or compromise of multiple nodes attempting to destroy the blockchain or the AI-based authentication server is addressed by the decentralized nature of TL2AB. The authentication responsibilities are distributed among spatially and logically different nodes. Majority consensus (e.g., 67% honest participation) is induced by the protocol's consensus mechanism before any transaction is authenticated, thereby decreasing the colluding success probability.

Replay Attacks: Replay attacks are based on intercepted valid authentication requests for making unauthorized access. TL2AB prevents such attacks by adding timestamps (T) and nonces (N) to all authentication messages. These are checked cross-wise within a finite window of time and against a list of recognized previously seen messages to avoid stale or repeated attempts. Dynamic session management adds protection by periodically updating authentication parameters.

5.6.1 Security Requirements

For purposes of delivering strong resilience to the threats outlined above, TL2AB is designed architecturally to satisfy stringent security requirements. *Confidentiality* is achieved with strong encryption and secure key management. *Integrity* is provided by executing digital signatures on every authentication action, which are securely stored in a blockchain ledger such that tamper evidence is afforded. The solution provides support for multi-factor authentication as well as AI-based behavior authentication for facilitating

good *authentication* and *non-repudiation*. Its distributed nature and consensus algorithm with decentralization offer high *availability* and defense against Denial-of-Service (DoS) attacks. *Forward secrecy* is achieved through dynamic session key generation with unique session keys for each authentication session, limiting the impact of key compromise. Real-time surveillance and adaptive countermeasures endow TL2AB with the capability to rapidly detect and neutralize arising threats.

Man-in-the-Middle (MITM) Attacks

Claim 1: We claim that the probability of success of an Man-in-the-Middle (MITM) attack is negligible.

Proof: To prove that a successful MITM attack has a negligible probability, we look in detail at the steps that an attacker, A, would have to go through. For this, it would intercept the message R, $ID_d, T, N, \text{sign}(K_d)$, where ID_d is the identity, T is the timestamp, N is a nonce, and $sign(K_d)$ is the cryptographic signature. Having intercepted R, he would then need to modify this message in such a way as to do it without modification being detected through the security mechanisms involved. After that, the attacker would have to breach the AI-based risk assessment layer, which is in constant monitoring of the system for anomalies. Finally, this would involve compromising the blockchain to change the stored authentication record associated with R. The overall probability of a successful MITM attack, denoted as $P(\text{MITM})$, can therefore be expressed as the product of the probabilities of successfully completing each of these steps: $P(\text{MITM}) = P(\text{Intercept}) \cdot P(\text{Modify}) \cdot P(\text{Bypass AI}) \cdot P(\text{Compromise Blockchain})$.

Given the cryptographic protection afforded by the signing of R, the on-going AI monitoring of the system, along with the immutability of the blockchain, the probabilities of successfully completing each of these steps are extremely small. Hence, we consider the overall probability of a successful MITM attack, $P(\text{MITM})$, to be negligible.

Replay Attacks

TL2AB includes both timestamps (T) and nonces (N) in every authentication request for resisting replay attacks.

Claim 2: TL2AB is secure against replay attacks.

Proof: An adversary intercepts a valid authentication request $R = \{ID_d, T, N, \text{sign}(K_d)\}$ at time t;. For such a replay attack to be effective at any later time $t + \Delta t$, two conditions have to be met by the adversary.

First, the timestamp T must still be accepted as current at time $t + \Delta t$. This is already ameliorated in TL2AB, since the system uses a small acceptance window over timestamps. If the time difference Δt is larger than this acceptance window, the system will reject the request for being outdated, which prevents the replay. Second, the nonce N shall not have been used in any previous authentication request. TL2AB enforces every nonce is unique; so even if an adversary replays the captured message, the system will find the duplication of nonce value and discard the replay request.

As the window for accepting timestamps is decreasing while the uniqueness of nonces is still strictly enforced, the success probability of a replay attack decreases. Therefore, this implies security against that kind of attack.

Impersonation Attacks

TL2AB detects impersonation attacks through the device-specific cryptographic keys, K_d, and the AI-driven behavior analysis approach.

Claim 3: In TL2AB, the success rate for an impersonation attack is close to zero.

Proof: To conduct a successful impersonation attack, the adversary has to successfully pass several conditions: First, it must acquire or forge a valid cryptographic key K_d that uniquely maps to the respective device. This would specifically entail an adversary creating an authentication request R. Inaddition, the adversary has to be able to impersonate the legitimate user's behavioral patterns as analyzed by the AI-driven system such that the AI-based behavioral checks are bypassed.

The overall probability of a successful impersonation attack, denoted as $P(\text{Impersonation})$, may be written as: $P(\text{Impersonation}) = P(\text{Obtain}K_d) \cdot P(\text{Pass Crypto}) \cdot P(\text{Mimic Behavior})$.

Because the solution assumes the use of secure key generation and storage within a TEE, an adversary's chance of obtaining or forging the cryptographic key K_d is minimized; therefore, $P(\text{Obtain } K_d)$ is considered negligible. This is further enforced by the fact that continuous AI-driven behavioral analysis monitors the unique behavioral pattern of the legitimate user to an extent that makes the likelihood of successfully mimicking the behavior, $P(\text{Mimic Behavior})$, very low. In light of such formidable security measures, we conclude that the overall probability of success in impersonation attack $P(\text{Impersonation})$ is negligible.

5.6.2 Formal Security Analysis using BAN Logic

To further assure the security guarantees of TL2AB, we provide a formal analysis of the authentication protocol using BAN logic. The logic allows us to reason about the beliefs that are established between communicating principals after the execution of a cryptographic protocol. In our scenario, we have two principals: the user device D and the authentication server or smart contract S. The message of interest is the authentication request:

$$D \rightarrow S : \{ID_d, T, N, \text{Sign}_{K_d}(ID_d \parallel T \parallel N)\}$$

We define the following BAN logic primitives:

- P **believes** X: Principal P believes statement X
- P **sees** X: Principal P receives message X
- P **once-said** X: Principal P said message X at some point in the past

- **fresh**(X): Message X is fresh
- **pubkey**(K, P): K is the public key of principal P

The following assumptions are made: (1) the server S believes it knows the authentic public key of the device D, i.e., S **believes pubkey**(K_d, D); (2) the server believes that the nonce N is fresh, i.e., S **believes fresh**(N); and (3) the server receives the signed message, i.e., S **sees** $\text{Sign}_{K_d}(ID_d \parallel T \parallel N)$.

Based on these assumptions and the rules of BAN logic, the server concludes the following: from the digital signature and its belief in the key binding, S **believes** D **once-said** $(ID_d \parallel T \parallel N)$. Given the freshness of the nonce, it follows that S **believes** D **believes** $(ID_d \parallel T \parallel N)$, and therefore, S **believes** auth(D); that is, the server is convinced that the request originated recently and authentically from device D. This formal reasoning confirms that the authentication phase of TL2AB ensures origin authenticity and freshness, and is resilient to replay attacks.

Denial of Service (DoS) Attacks

The decentralized nature of blockchain and the adaptive risk assessment by AI provide inherent resistance to Denial of Service (DoS) attacks.

Claim 4: TL2AB significantly mitigates the impact of DoS attacks compared to centralized authentication systems.

Proof: In a traditional centralized authentication system, a successful DoS attack typically involves overwhelming the central server with an excessive amount of traffic, causing the system to become unavailable. The probability of a successful DoS attack in a centralized system can be expressed as:

$$P(\text{DoS}_{\text{centralized}}) = P(\text{Overwhelm\_central\_server}),$$

where P(Overwhelm_central_server) is the likelihood of overloading the single point of failure in a centralized system — the central server.

On the other hand, TL2AB employs a blockchain-driven decentralized architecture that spreads authentication work to multiple nodes. In order to even stand a chance of launching an effective DoS attack on TL2AB, the attacker would need to flood multiple blockchain nodes simultaneously. In addition, the attacker would need to bypass the AI adaptive risk assessment system, which detects abnormal traffic trends and changes defenses dynamically. As such, the probability of a successful DoS attack against TL2AB is represented by:

$$P(\text{DoS}_{\text{TL2AB}}) = P(\text{Hit\_multiple\_nodes}) \cdot P(\text{Bypass\_AI}),$$

where P(Hit_multiple_nodes) represents the difficulty of attacking multiple blockchain nodes concurrently, and P(Bypass_AI) accounts for the challenge of evading the AI's adaptive monitoring.

Due to the distributed nature of the blockchain network and the AI's ability to detect and respond to abnormal traffic patterns, the probability of a successful DoS attack in

TL2AB is significantly lower than that in a centralized system. Therefore, we can conclude that $P(\text{DoS}_{\text{TL2AB}}) \ll P(\text{DoS}_{\text{centralized}})$, which demonstrates TL2AB's superior resistance to DoS attacks.

5.6.3 Privacy Preservation

TL2AB protects users' privacy with a number of mechanisms. For starters, encryption keys are hosted in a Trusted Execution Environment (TEE) which shields against inappropriate access and hides sensitive information. Secondly, AI processing monitors the patterns of behaviour without keeping any raw user information, thus decreasing privacy risks surrounding data gathering. Lastly, the anonymity of blockchain-based transactions by their very nature provides an additional layer of privacy, rendering activity tracing hard to attribute to specific users. TL2AB design incorporates a combination of several layers of privacy-enabling mechanisms to protect sensitive information:

- **Key Privacy:** Cryptographic key K_d is never transmitted. A cryptographic hash $H(K_d)$ is stored on-chain, so it is computationally infeasible to derive the original key due to the one-way nature of hash functions. The key itself is stored securely within the Trusted Execution Environment (TEE).
- **Privacy of Behavioral Data:** Locally or by a privacy-oblivious AI model, the risk is assessed. Only the derived features such as login frequency or location region (and not raw behavioral logs) are employed so that raw user activity and personal data do not leak.
- **On-Chain Privacy:** Information that is stored on-chain is limited and minimal in scope and includes hashed or insensitive values only. No personally identifiable information (PII) is ever stored on-chain.

These measures collectively ensure that TL2AB protects user privacy across three fronts: device identity, behavioral context, and cryptographic material, even in an adversarial environment with partial visibility into the network or blockchain.

Claim 5: TL2AB preserves user privacy with high probability.

Proof: Let E represent the event of a privacy breach. The probability of event E occurring can be expressed as: $P(E) = P(\text{TEE\_compromised}) \cdot P(\text{AI\_data\_leaked}) \cdot P(\text{Blockchain\_deanonymized})$. Given the strong security properties of the TEE, the data minimization approach utilized in the AI analysis, and the pseudonymous nature of blockchain transactions, each of these probabilities is very low. Therefore, the overall probability of a privacy breach, $P(E)$, is negligible.

5.6.4 Forward Secrecy

TL2AB ensures forward secrecy through dynamic session key generation and continuous risk assessment.

Claim 6: TL2AB provides forward secrecy. **Proof:** Let S_i and S_j denote two distinct sessions, where $i < j$. The compromise of the session key K_j does not reveal any information about the session key K_i. This is due to several factors: First, session keys are generated independently for each session, ensuring that the compromise of one does not affect the others. Second, the AI component continuously updates the risk assessment, which influences the key generation process, further enhancing security. Lastly, the blockchain records each authentication event separately, making it more challenging for an adversary to link compromised keys across sessions.

As a result, we can express the relationship between the probabilities as: $P(\text{Compromise\_}S_i|\text{Compro}$ $P(\text{Compromise\_}S_i)$, with proof that breaking one session key does not break others and thus offers forward secrecy.

Finally, this security formal analysis offers proof that TL2AB offers a security guarantee against a multitude of attack channels relevant to 6G networks. The integration of AI and blockchain technologies synergistically creates an enhanced effect to boost the overall security posture of the authentication model.

5.6.5 Comprehensive Analysis of TL2AB Capabilities

We provide here a close analysis of the benefits of TL2AB in terms of its security, privacy guarantee, adaptability in dynamic environments, and world scalability and responsiveness. We benchmark them against the equivalent state-of-the-art authentication models

Scalability and Performance

TL2AB is a light-weight architecture specifically suggested for computation-limited IoT devices for 6G networks. With the usage of decentralized blockchain technology, TL2AB distributes authentication processes over multiple nodes and thereby prevents single points of failure as well as provides high availability. Moreover, the use of AI-driven continuous risk analysis prevents computational overhead but maintains low latency even in the case of dynamic network conditions

Security Features

TL2AB achieves robust security by the concomitant usage of various defense layers. Use of blockchain implementation offers tamper-proof logging in addition to distributed trust, cryptographic signatures and safe key storage (in a Trusted Execution Environment using salted hash) protect precious credentials, whilst the AI Authentication Server constantly scans for device abnormality to dynamically assess risk and search for likely risks. The diversified method possesses extremely robust defense against attacks such as man-in-the-middle, replay, impersonation, and denial-of-service.

Privacy-Preserving Mechanisms

For preserving users' privacy, TL2AB incorporates a number of privacy-enabling practices. Privacy-sensitive information is protected by storing salted hashes of cryptographic keys rather than plaintext keys, and each blockchain transaction is pseudonymous to prevent directly linking to specific users. Additionally, the AI module processes the behavioral data in a minimal data approach without holding plaintext personal data, lowering privacy exposure accordingly.

Adaptability and Dynamic Response

TL2AB's one of its greatest assets is that it is highly dynamic. The AI-based risk assessment in the approach dynamically changes real-time, allowing the system to dynamically adjust authentication needs based on current threat levels. This provides the system responsiveness to real-time network dynamics and new threats with maintaining the equilibrium between security and usability without heavy computation.

Comparative Analysis with Related Frameworks

Table 5.9 summarizes a qualitative comparison of TL2AB and some relevant peer authentication schemes identified in the current literature along the four main factors of security strength, privacy protection, versatility, and scalability/performance.

This comprehensive assessment demonstrates that TL2AB not only surpasses security, privacy, and flexibility but also greatly improves scalability and performance over existing state-of-the-art frameworks. The synergy between blockchain technology and AI-based ongoing monitoring makes TL2AB a robust and multi-purpose instrument for 6G networks.

5.7 Advantages of TL2AB

While the works that have been reviewed above in the related works section contribute to some form of knowledge, TL2AB is unique insofar as it combines AI-driven continuous monitoring with blockchain to facilitate the creation of a decentralized authentication framework. Past solution architectures have been for specific applications or technologies, while TL2AB is intended to be implemented in its entirety in various 6G environments. With the additional advantages of:

- *Efficiency and Resource Utilization:* Unlike the three-factor mechanism as proposed in the healthcare industry [225], TL2AB is lightweight; hence, more ideal for resource-poor IoT devices prevalent in 6G networks.
- *Decentralization:* The reliance on a single, central system in the CL-UCSSO mechanism and other proposals is problematic because there is one point of failure [225, 227]. TL2AB is founded on a blockchain-based platform that will have a distributed framework of trust.

- *Adaptability:* The light-weight protocols advocated in satellite-ground networks and maritime shipping are premised primarily on specific contexts. TL2AB uses AI for real-time adaptation of the most recent threats with a more assertive security posture.

The comprehensive security framework TL2AB, combines multi-factor authentication and blockchain into one platform that facilitates dynamic and context-aware authentication in diversified 6G applications. The suggested TL2AB tends to fill those gaps achieved in the literature review by providing a robust and efficient, scalable authentication solution which would be able to scale up with growing demands of the 6G network without compromising security and privacy.

5.7.1 Scalability and Performance

Efficiency and scalability are significant issues in 6G networks, especially when handling billions of devices. Research like Tao et al. [226] and Fang et al. [228] talk about the necessity of optimizing protocols to handle massive-scale networks by reducing overhead, postponing latency, and ensuring fast authentication. This line of work is consistent with the goal of TL2AB, which is to provide a lightweight, scalable authentication mechanism that can accommodate large, dynamic 6G environments. Tab. 5.8 summarizes the most significant characteristics of the related works and their comparison with the TL2AB framework.

5.7.2 Computational and Communication Performance Comparison

Here, we compare the computation and communication cost of TL2AB with other authentication schemes. Tab. 5.10 shows a comparison of the reported computation and communication in different works.

The training time is 1.7202 seconds and inference per sample is 0.000375 seconds with optimal processing. Inference CPU consumption is 21% measured with a moderate cost of computation suitable for real-time authentication within 6G networks. TL2AB further has a low model size of 0.15 MB and therefore is light-weight in contrast to deep-learning-based authentications.

The total message length of the message sent using the authentication in the TL2AB protocol is 334 bytes, which include the authentication request (296 bytes), risk assessment response (5 bytes), smart contract verification response (1 byte), and session confirmation (32 bytes). The message length is still small in a step towards decreasing communication overhead without compromising security and scalability in high-speed networks. As much as communication efficiency is concerned, TL2AB sends 334 bytes while authenticating with near-zero overhead. Even though Aman et al. [234] has a minimal message length of 40 bytes, they are utilizing the conventional cryptographic schemes that are not necessarily more adaptable while dealing with dynamic 6G environments. In contrast, Al Ahmed et

al. [233] exhibit extremely high encryption delay (0.077642 sec) and decryption time (3.537678 sec), which would produce authentication delay in real-time systems.

Compared to Siddhartha et al. [230], with 102.059 mJ total computing energy consumption, TL2AB's AI-driven lightweight approach saves computation without increasing communication overhead. Similarly, Tahir et al. [235] obtained 5.2% reduction in computational overhead and 3.8% reduction in communication overhead, and TL2AB is a compromise among security, efficiency, and real-time flexibility. That is, TL2AB is an efficient authentication scheme with low computational and communication overhead, efficient, secure, and rapid authentication, and therefore well suited for future 6G networks.

5.8 Conclusion

TL2AB is a system that offers an emerging paradigm in answering the sophisticated security issues engendered by 6G technology. It leverages AI and blockchain technologies and proposes an effective, secure, and light authentication mechanism with implications for numerous applications in several sectors. TL2AB is much more secure and efficient compared to other prevailing different authentication methods. Future work will consider network scalability in the case of TL2AB and examine any potential enhancements available with the introduction of new technologies like quantum cryptography. In the long run, TL2AB should be a stepping stone towards enabling secure and user-friendly authentication protocols in upcoming 6G networks to further enable sophisticated applications requiring enhanced security and privacy.

Paper & Application Domain	**Security Mechanism**	**Authentication Approach**	**Technological Focus**	**Scalability & Performance**
Le et al. [225] (Healthcare)	Data Privacy, System Cost Optimization	3-Factor Authentication (Smart Card, Password, Biometric)	Healthcare Networks, Authentication Protocols	High cost, secure but computationally expensive
Chaudhry et al. [227] (Maritime)	GPS Spoofing, Unauthorized Data Access	Lightweight Authentication Protocol	GPS-based Systems, Maritime Security	Low overhead, lightweight, secure
Tao et al. [226] (Satellite Networks)	Privacy Preservation, Energy Efficiency	Bilinear Pairing-based Group Signature, Batch Authentication	Satellite-ground Integrated Networks	Energy-efficient, scalable, low-latency
Asim et al. [100] (Blockchain)	MFA, Cyber Attack Prevention	Multi-Factor Authentication (MFA)	Blockchain-based Security	Blockchain-enhanced security, scalable
Fang et al. [228] (IoT)	Security Management, Authentication Efficiency	AI-Enabled Lightweight Authentication	IoT Networks, AI-enhanced Security	Scalable, adaptive to dynamic environments
Garabato et al. [229] (General)	Continuous Authentication, Activity Monitoring	AI-based Continuous Authentication (SVM, MLP, Deep Learning)	AI-driven Authentication, Continuous User Verification	Scalable, adaptive, continuous verification
TL2AB Framework (6G Networks)	Device Security, Risk Assessment	Lightweight & Dynamic Authentication (Cryptographic Signatures, AI-based Risk Assessment)	6G Networks, AI-driven Security	Scalable, low-latency, real-time dynamic adjustments

Table 5.8: Comparison of Authentication Approaches in 6G Networks

Table 5.9: Comprehensive Comparison of Authentication Frameworks

Reference	Security Robustness	Privacy Preservation	Adaptability	Scalability & Performance
Siddhartha et al. [230]	High; robust multi-factor security	Moderate; traditional key management	Low; static authentication model	Low; high computational overhead
Kumar et al. [231]	Moderate-High; efficient for smart home IoT	Moderate; limited to specific domain	Low; limited dynamic adjustment	Moderate; optimized for smart home devices
Khalid et al. [232]	High; decentralized blockchain-based security	Moderate; standard blockchain privacy	Moderate; fixed protocol parameters	Moderate; blockchain overhead may limit scalability
Al Ahmed et al. [233]	High; innovative consensus algorithm enhances security	Moderate; privacy not extensively addressed	Moderate; cluster-based but less dynamic	Moderate; efficient clustering with integration challenges
Aman et al. [234]	High; PUF-based mechanism provides strong security	High; intrinsic hardware-level privacy	Low-Moderate; less emphasis on dynamic adaptation	Low; optimized for constrained devices only
Tahir et al. [235]	High; robust for health informatics	High; designed for sensitive data	Moderate; fixed policies	Moderate; balanced performance for specialized applications
TL2AB (Proposed)	**Very High; combines blockchain and AI for continuous, dynamic threat assessment**	**Very High; employs salted hashes and pseudonymous transactions**	**Very High; real-time AI-driven adaptation**	**High; lightweight design ensuring low latency and high scalability**

Table 5.10: Comparison of Computational and Communication Performance with Related Works

Scheme	**Reported Results (Computation)**	**Reported Results (Communication)**
Siddhartha et al. [230]	Total computational energy: 102.059 mJ	Transmission energy per bit: 0.72 µJ, Reception: 0.81 µJ
Aman et al. [234]	Hash operations: O(n), Modular exponentiation: O(n + M(l)k)	Message length: 40 bytes, Lower overhead than traditional methods
Tahir et al. [235]	Computational overhead reduced by 5.2%	Communication overhead reduced by 3.8%
Kumar et al. [231]	AES delay: 0.001975 ms, SHA-1 delay: 0.001135 ms	Reported security increase with minimal impact on communication
Al Ahmed et al. [233]	RSA Encryption: 0.077642 sec, Decryption: 3.537678 sec	Average network delay: 7 ms
Our Model (TL2AB)	Training Time: 1.7202 sec, Inference Time: 0.000375 sec, CPU Usage: 21%, Model Size: 0.15 MB	Message length: 334 bytes (minimal overhead)

General Conclusion

The evolution of wireless communication has reached a milestone with the advent of 6G networks, which have promised unprecedented advancements in speed, intelligence, and connectivity. But with these advancements come advanced security challenges that require a paradigm shift in network protection, privacy, and trust. This dissertation delved into the complexities of 6G security through a detailed study of its issues and proposing new solutions through blockchain, artificial intelligence, federated learning, and multi-party computation that enable a secure and trustworthy network architecture.

Through this research, we have established that current security models lack to cope with the hyper-connected, decentralized, and dynamically evolving nature of 6G. The connectivity of billions of devices ranging from smart sensors to autonomous machines raises the attack surface, and centralized security will be a thing of the past. The emergence of AI-powered cyberattacks, quantum computer-based attacks, and privacy concerns alongside mass data gathering makes the case even more intricate. To find solutions to all these problems, we explored how blockchain as an immutable decentralized security system can supply immutability, transparency, and trust within 6G systems. Combining AI and blockchain, we engineered a new harmony where artificial intelligence speeds up distributed security mechanism's performance and blockchain fortifies AI models against evasion attacks and poisoning. This overlap of technologies guarantees unprecedented security at the highest order of self-organization, defense mechanisms that fend off novel attacks.

One of the contributions of this thesis is the design and implementation of 6G-SecureIDS, a blockchain-based distributed system intrusion detection system. Unlike conventional IDS models that rely on centralized inspection, 6G-SecureIDS employs federated learning to enable cooperative threat detection without revealing raw data. The use of blockchain guarantees secure, verifiable, and tamper-proof knowledge exchange among IDS nodes. Our tests proved that it is possible to achieve high detection rates without breaking privacy and this system is an optimistic security framework for future 6G systems.

In addition, we developed FBMP-IDS as an advanced intrusion detection system integrated with federated learning, blockchain, and multi-party computation for boosting security and efficiency. With knowledge of the computation and communication delay in federated learning, gradient compression mechanisms have been utilized to reduce bandwidth usage and a dynamic protocol selection mechanism for MPC protocols to ensure secure data sharing with low latency. The benchmarking against existing available IDS frameworks ensured not just that FBMP-IDS improves detection but also significantly

reduces computation overhead, thus rendering it scalable and viable for deployment in real-world environments. Finally, the TL2AB authentication framework was developed to ensure trusted identity management across a hyper-connected 6G ecosystem.

The implications of this research extend beyond intrusion detection to serve as a guide to safe, smart, and privacy-preserving 6G networks. The decentralized nature of blockchain can be leveraged further to secure identity management, authentication, and data integrity in numerous applications ranging from smart cities and healthcare to autonomous transportation and industrial IoT. The use of AI for network security has both challenges and opportunities, and AI-based defense mechanisms must be robust against attacks from adversaries but also interpretable and compliant with regulations. Further, the arrival of quantum computing necessitates a transition to post-quantum cryptographic primitives to render 6G security mechanisms quantum-resistant against prospective computational threats.

Despite the encouraging innovations brought forth in this work, some challenges are left open for further research. Scalability remains a top concern, with blockchain and federated learning introducing computational complexities that must be optimized to address the massive scale of 6G networks. Growing energy efficiency in security measures is another pressing issue, particularly with green communication as an emerging concern in next-generation networks. Privacy protection should be reinforced even more using new cryptographic methods like zero-knowledge proofs and differential privacy, which will make the data of the users safe even in an extremely interconnected ecosystem. In addition, regulatory and ethical issues need to be tackled very carefully so that decentralization can be balanced with compliance, while international cooperation in the formulation of standardized security measures for 6G is promoted.

This thesis is an important milestone on the journey of securing 6G networks, but it is only the beginning of an active research ecosystem. The next decade will witness the explosion of AI, blockchain, and quantum computing, and there will be a need for constant innovation in security paradigms. By embracing decentralized intelligence, privacy-preserving architectures, and quantum-resistant security measures, we can lay the foundation for a future where 6G networks are not only faster and smarter but also inherently secure, resilient, and trustworthy. The vision of an entirely interconnected digital world depends on our ability to anticipate and counter security risks, so that future technologies are built on a foundation of trust, privacy, and security.

Bibliography

[1] K. B. Letaief, W. Chen, Y. Shi, J. Zhang, and Y.-J. A. Zhang, "The roadmap to 6g: Ai empowered wireless networks," *IEEE communications magazine*, vol. 57, no. 8, pp. 84–90, 2019.

[2] X. D. Duan, X. Y. Wang, L. Lu, N. X. Shi, C. Liu, T. Zhang, and T. Sun, "6g architecture design: From overall, logical and networking perspective," *IEEE Communications Magazine*, vol. 61, no. 7, pp. 158–164, 2023.

[3] H. Yang, A. Alphones, Z. Xiong, D. Niyato, J. Zhao, and K. Wu, "Artificial-intelligence-enabled intelligent 6g networks," *IEEE network*, vol. 34, no. 6, pp. 272–280, 2020.

[4] S. A. Abdel Hakeem, H. H. Hussein, and H. Kim, "Security requirements and challenges of 6g technologies and applications," *Sensors*, vol. 22, no. 5, p. 1969, 2022.

[5] Y. Zuo, J. Guo, N. Gao, Y. Zhu, S. Jin, and X. Li, "A survey of blockchain and artificial intelligence for 6g wireless communications," *IEEE Communications Surveys & Tutorials*, 2023.

[6] M. F. K. Sial, "Blockchain technology–prospects, challenges and opportunities," *IEEE Blockchain, Technical Briefs*, 2019.

[7] A. Kumari, R. Gupta, and S. Tanwar, "Amalgamation of blockchain and iot for smart cities underlying 6g communication: A comprehensive review," *Computer Communications*, vol. 172, pp. 102–118, 2021.

[8] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, "Ai and 6g security: Opportunities and challenges," in *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*. IEEE, 2021, pp. 616–621.

[9] H. Xu, P. V. Klaine, O. Onireti, B. Cao, M. Imran, and L. Zhang, "Blockchain-enabled resource management and sharing for 6g communications," *Digital Communications and Networks*, vol. 6, no. 3, pp. 261–269, 2020.

[10] Z. Zhou, O. Onireti, H. Xu, L. Zhang, and M. Imran, "Ai and blockchain enabled future wireless networks: A survey and outlook," *Distributed Ledger Technologies: Research and Practice*, 2024.

[11] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "What should 6g be?" *Nature Electronics*, vol. 3, no. 1, pp. 20–29, 2020.

[12] W. Jiang, B. Han, M. A. Habibi, and H. D. Schotten, "The road towards 6g: A comprehensive survey," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 334–366, 2021.

[13] C. Huang, S. Hu, G. C. Alexandropoulos, A. Zappone, C. Yuen, R. Zhang, M. Di Renzo, and M. Debbah, "Holographic mimo surfaces for 6g wireless networks: Opportunities, challenges, and trends," *IEEE wireless communications*, vol. 27, no. 5, pp. 118–125, 2020.

[14] W. Guo, "Explainable artificial intelligence for 6g: Improving trust between human and machine," *IEEE Communications Magazine*, vol. 58, no. 6, pp. 39–45, 2020.

[15] Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G. K. Karagiannidis, and P. Fan, "6g wireless networks: Vision, requirements, architecture, and key technologies," *IEEE vehicular technology magazine*, vol. 14, no. 3, pp. 28–41, 2019.

[16] H. Tataria, M. Shafi, A. F. Molisch, M. Dohler, H. Sjöland, and F. Tufvesson, "6g wireless systems: Vision, requirements, challenges, insights, and opportunities," *Proceedings of the IEEE*, vol. 109, no. 7, pp. 1166–1199, 2021.

[17] S. Naser, L. Bariah, S. Muhaidat, and E. Basar, "Zero-energy devices empowered 6g networks: Opportunities, key technologies, and challenges," *IEEE Internet of Things Magazine*, vol. 6, no. 3, pp. 44–50, 2023.

[18] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Toward 6g networks: Use cases and technologies," *IEEE communications magazine*, vol. 58, no. 3, pp. 55–61, 2020.

[19] L. Leyva, D. Castanheira, A. Silva, A. Gameiro, and L. Hanzo, "Cooperative multiterminal radar and communication: A new paradigm for 6g mobile networks," *IEEE Vehicular Technology Magazine*, vol. 16, no. 4, pp. 38–47, 2021.

[20] I. F. Akyildiz, A. Kak, and S. Nie, "6g and beyond: The future of wireless communications systems," *IEEE access*, vol. 8, pp. 133 995–134 030, 2020.

[21] S. Mavoungou, G. Kaddoum, M. Taha, and G. Matar, "Survey on threats and attacks on mobile networks," *IEEE Access*, vol. 4, pp. 4543–4572, 2016.

[22] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6g: A survey on prospective technologies and challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2384–2428, 2021.

[23] B. Dash, M. F. Ansari, P. Sharma, and A. Ali, "Threats and opportunities with ai-based cyber security intrusion detection: a review," *International Journal of Software Engineering & Applications (IJSEA)*, vol. 13, no. 5, 2022.

[24] D. Je, J. Jung, and S. Choi, "Toward 6g security: technology trends, threats, and solutions," *IEEE Communications Standards Magazine*, vol. 5, no. 3, pp. 64–71, 2021.

[25] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, "Security and privacy in 6g networks: New areas and new challenges," *Digital Communications and Networks*, vol. 6, no. 3, pp. 281–291, 2020.

[26] B. Mao, J. Liu, Y. Wu, and N. Kato, "Security and privacy on 6g network edge: A survey," *IEEE communications surveys & tutorials*, vol. 25, no. 2, pp. 1095–1127, 2023.

[27] M. Ylianttila, R. Kantola, A. Gurtov, L. Mucchi, I. Oppermann, Z. Yan, T. H. Nguyen, F. Liu, T. Hewa, M. Liyanage *et al.*, "6g white paper: Research challenges for trust, security and privacy," *arXiv preprint arXiv:2004.11665*, 2020.

[28] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The roadmap to 6g security and privacy," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1094–1122, 2021.

[29] T. S. Rappaport, Y. Xing, O. Kanhere, S. Ju, A. Madanayake, S. Mandal, A. Alkhateeb, and G. C. Trichopoulos, "Wireless communications and applications above 100 ghz: Opportunities and challenges for 6g and beyond," *IEEE access*, vol. 7, pp. 78 729–78 757, 2019.

[30] N. Y. Al-Matari, A. T. Zahary, and A. A. Al-Shargabi, "A survey on advancements in blockchain-enabled spectrum access security for 6g cognitive radio iot networks," *Scientific Reports*, vol. 14, no. 1, p. 30990, 2024.

[31] J. Wu, Y. Gao, L. Wang, J. Zhang, and D. O. Wu, "How to allocate resources in cloud native networks towards 6g," *IEEE Network*, 2023.

[32] M. E. Haque, F. Tariq, M. R. Khandaker, K.-K. Wong, and Y. Zhang, "A survey of scheduling in 5g urllc and outlook for emerging 6g systems," *IEEE access*, vol. 11, pp. 34 372–34 396, 2023.

[33] J. Zhang, C. Yang, R. Dong, Y. Wang, A. Anpalagan, Q. Ni, and M. Guizani, "Intent-driven closed-loop control and management framework for 6g open ran," *IEEE Internet of Things Journal*, 2023.

[34] E. Coronado, R. Behravesh, T. Subramanya, A. Fernàndez-Fernàndez, M. S. Siddiqui, X. Costa-Pérez, and R. Riggio, "Zero touch management: A survey of network automation solutions for 5g and 6g networks," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 4, pp. 2535–2578, 2022.

[35] M. A. Habibi, B. Han, A. Fellan, W. Jiang, A. G. Sánchez, I. L. Pavón, A. Boubendir, and H. D. Schotten, "Towards an open, intelligent, and end-to-end architectural framework for network slicing in 6g communication systems," *IEEE Open Journal of the Communications Society*, 2023.

[36] P. Bhattacharya, D. Saraswat, A. Dave, M. Acharya, S. Tanwar, G. Sharma, and I. E. Davidson, "Coalition of 6g and blockchain in ar/vr space: Challenges and future directions," *IEEE Access*, vol. 9, pp. 168 455–168 484, 2021.

[37] X. Wang, P. Jia, X. Shen, and H. V. Poor, "Intelligent and low overhead network synchronization for large-scale industrial iot systems in the 6g era," *IEEE Network*, vol. 37, no. 3, pp. 76–84, 2022.

[38] I. I. Ioannou, C. Christophorou, V. Vassiliou, M. Lestas, and A. Pitsillides, "Dynamic d2d communication in 5g/6g using a distributed ai framework," *IEEE Access*, vol. 10, pp. 62 772–62 799, 2022.

[39] G. P. Sharma, D. Patel, J. Sachs, M. De Andrade, J. Farkas, J. Harmatos, B. Varga, H.-P. Bernhard, R. Muzaffar, M. Ahmed *et al.*, "Toward deterministic communications in 6g networks: state of the art, open challenges and the way forward," *IEEE Access*, vol. 11, pp. 106 898–106 923, 2023.

[40] S. Wang, T. Sun, H. Yang, X. Duan, and L. Lu, "6g network: Towards a distributed and autonomous system," in *2020 2nd 6G wireless summit (6G SUMMIT)*. IEEE, 2020, pp. 1–5.

[41] N. Cheng, H. Jingchao, Y. Zhisheng, Z. Conghao, W. Huaqing, L. Feng, Z. Haibo, and S. Xuemin, "6g service-oriented space-air-ground integrated network: A survey," *Chinese Journal of Aeronautics*, vol. 35, no. 9, pp. 1–18, 2022.

[42] T. Nakano, Y. Okaie, S. Kobayashi, T. Hara, Y. Hiraoka, and T. Haraguchi, "Methods and applications of mobile molecular communication," *Proceedings of the IEEE*, vol. 107, no. 7, pp. 1442–1456, 2019.

[43] H. Guo, J. Li, J. Liu, N. Tian, and N. Kato, "A survey on space-air-ground-sea integrated network security in 6g," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 53–87, 2021.

[44] A. Ahad, Z. Jiangbina, M. Tahir, I. Shayea, M. A. Sheikh, and F. Rasheed, "6g and intelligent healthcare: Taxonomy, technologies, open issues and future research directions," *Internet of Things*, p. 101068, 2024.

[45] A. A. Barakabitze and R. Walshe, "Sdn and nfv for qoe-driven multimedia services delivery: The road towards 6g and beyond networks," *Computer Networks*, vol. 214, p. 109133, 2022.

[46] M. Beshley, M. Klymash, I. Scherm, H. Beshley, and Y. Shkoropad, "Emerging network technologies for digital transformation: 5g/6g, iot, sdn/ibn, cloud computing, and blockchain," in *IEEE lnternational Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering*. Springer, 2022, pp. 1–20.

[47] T. Nguyen, N. Tran, L. Loven, J. Partala, M.-T. Kechadi, and S. Pirttikangas, "Privacy-aware blockchain innovation for 6g: Challenges and opportunities," *2020 2nd 6G Wireless Summit (6G SUMMIT)*, pp. 1–5, 2020.

[48] S. Hu, Y.-C. Liang, Z. Xiong, and D. Niyato, "Blockchain and artificial intelligence for dynamic resource sharing in 6g and beyond," *IEEE Wireless Communications*, vol. 28, no. 4, pp. 145–151, 2021.

[49] W. Wu, C. Zhou, M. Li, H. Wu, H. Zhou, N. Zhang, X. S. Shen, and W. Zhuang, "Ai-native network slicing for 6g networks," *IEEE Wireless Communications*, vol. 29, no. 1, pp. 96–103, 2022.

[50] P. Porambage, G. Gür, D. P. M. Osorio, M. Livanage, and M. Ylianttila, "6g security challenges and potential solutions," in *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*. IEEE, 2021, pp. 622–627.

[51] M. A. Uusitalo, P. Rugeland, M. R. Boldi, E. C. Strinati, P. Demestichas, M. Ericson, G. P. Fettweis, M. C. Filippou, A. Gati, M.-H. Hamon *et al.*, "6g vision, value, use cases and technologies from european 6g flagship project hexa-x," *IEEE access*, vol. 9, pp. 160 004–160 020, 2021.

[52] X. Tang, C. Cao, Y. Wang, S. Zhang, Y. Liu, M. Li, and T. He, "Computing power network: The architecture of convergence of computing and networking towards 6g requirement," *China communications*, vol. 18, no. 2, pp. 175–185, 2021.

[53] Q. Mao, F. Hu, and Q. Hao, "Deep learning for intelligent wireless networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2595–2621, 2018.

[54] N. P. Kuruvatti, M. A. Habibi, S. Partani, B. Han, A. Fellan, and H. D. Schotten, "Empowering 6g communication systems with digital twin technology: A comprehensive survey," *IEEE access*, vol. 10, pp. 112 158–112 186, 2022.

[55] P. Szilagyi, L. M. Contreras-Murillo, D. R. Menéndez, P. Giardina, and A. De la Oliva, "6g architecture for enabling predictable, reliable and deterministic networks: the predict6g case," in *2024 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2024, pp. 1–6.

[56] T. Taleb, C. Benzaïd, M. B. Lopez, K. Mikhaylov, S. Tarkoma, P. Kostakos, N. H. Mahmood, P. Pirinen, M. Matinmikko-Blue, M. Latva-Aho *et al.*, "6g system architecture: A service of services vision," *ITU journal on future and evolving technologies*, vol. 3, no. 3, pp. 710–743, 2022.

[57] N. Panwar, S. Sharma, and A. K. Singh, "A survey on 5g: The next generation of mobile communication," *Physical Communication*, vol. 18, pp. 64–84, 2016.

[58] S. Sullivan, A. Brighente, S. A. Kumar, and M. Conti, "5g security challenges and solutions: a review by osi layers," *Ieee Access*, vol. 9, pp. 116 294–116 314, 2021.

[59] M. Moussaoui, E. Bertin, and N. Crespi, "5g shortcomings and beyond-5g/6g requirements," in *2022 1st International Conference on 6G Networking (6GNet)*. IEEE, 2022, pp. 1–8.

[60] A. I. Salameh and M. El Tarhuni, "From 5g to 6g—challenges, technologies, and applications," *Future Internet*, vol. 14, no. 4, p. 117, 2022.

[61] H. Viswanathan and P. E. Mogensen, "Communications in the 6g era," *IEEE access*, vol. 8, pp. 57 063–57 074, 2020.

[62] M. Ozger, I. Godor, A. Nordlow, T. Heyn, S. Pandi, I. Peterson, A. Viseras, J. Holis, C. Raffelsberger, A. Kercek *et al.*, "6g for connected sky: A vision for integrating terrestrial and non-terrestrial networks," in *2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*. IEEE, 2023, pp. 711–716.

[63] J. Zhao, "A survey of intelligent reflecting surfaces (irss): Towards 6g wireless communication networks," *arXiv preprint arXiv:1907.04789*, 2019.

[64] H. Li, S. Li, and G. Min, "Lightweight privacy-preserving predictive maintenance in 6g enabled iiot," *Journal of Industrial Information Integration*, vol. 39, p. 100548, 2024.

[65] Q. Wu, W. Wang, Z. Li, B. Zhou, Y. Huang, and X. Wang, "Spectrumchain: A disruptive dynamic spectrum-sharing framework for 6g," *Science China Information Sciences*, vol. 66, no. 3, p. 130302, 2023.

[66] K. Nassisid, T. David, and K. Muhammad, "Adaptive video streaming over 6g networks: Buffer control and user behavior analysis," *arXiv preprint arXiv:2407.05436*, 2024.

[67] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "5g security: Analysis of threats and solutions," in *2017 IEEE conference on standards for communications and networking (CSCN)*. IEEE, 2017, pp. 193–199.

[68] L. Qi, X. Xu, X. Wu, Q. Ni, Y. Yuan, and X. Zhang, "Digital-twin-enabled 6g mobile network video streaming using mobile crowdsourcing," *IEEE Journal on Selected Areas in Communications*, 2023.

[69] A. H. Sodhro, S. Pirbhulal, Z. Luo, K. Muhammad, and N. Z. Zahid, "Toward 6g architecture for energy-efficient communication in iot-enabled smart automation systems," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5141–5148, 2020.

[70] N. Kumar and R. Ali, "A smart contract-based robotic surgery authentication system for healthcare using 6g-tactile internet," *Computer Networks*, vol. 238, p. 110133, 2024.

[71] P. Whig, A. Velu, and R. R. Naddikatu, "The economic impact of ai-enabled blockchain in 6g-based industry," in *AI and blockchain technology in 6G wireless network*. Springer, 2022, pp. 205–224.

[72] K. David, J. Elmirghani, H. Haas, and X.-H. You, "Defining 6g: Challenges and opportunities [from the guest editors]," *IEEE Vehicular Technology Magazine*, vol. 14, no. 3, pp. 14–16, 2019.

[73] A. U. Gawas, "An overview on evolution of mobile wireless communication networks: 1g-6g," *International journal on recent and innovation trends in computing and communication*, vol. 3, no. 5, pp. 3130–3133, 2015.

[74] S. Bashir, M. H. Alsharif, I. Khan, M. A. Albreem, A. Sali, B. M. Ali, and W. Noh, "Mimo-terahertz in 6g nano-communications: Channel modeling and analysis." *Computers, Materials & Continua*, vol. 66, no. 1, 2021.

[75] R. Singh and D. Sicker, "Thz communications-a boon and/or bane for security, privacy, and national security," in *TPRC48: The 48th Research Conference on Communication, Information and Internet Policy*, 2020.

[76] G. Blinowski, "Security of visible light communication systems—a survey," *Physical Communication*, vol. 34, pp. 246–260, 2019.

[77] M. A. Arfaoui, A. Ghrayeb, and C. M. Assi, "Secrecy performance of the mimo vlc wiretap channel with randomly located eavesdropper," *IEEE Transactions on Wireless Communications*, vol. 19, no. 1, pp. 265–278, 2019.

[78] S. Soderi, "Enhancing security in 6g visible light communications," in *2020 2nd 6G wireless summit (6G SUMMIT)*. IEEE, 2020, pp. 1–5.

[79] S. Cho, G. Chen, and J. P. Coon, "Enhancement of physical layer security with simultaneous beamforming and jamming for visible light communication systems," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 10, pp. 2633–2648, 2019.

[80] Y. Hu, W. Kuang, Z. Qin, K. Li, J. Zhang, Y. Gao, W. Li, and K. Li, "Artificial intelligence security: Threats and countermeasures," *ACM Computing Surveys (CSUR)*, vol. 55, no. 1, pp. 1–36, 2021.

[81] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*. Ieee, 1994, pp. 124–134.

[82] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, 2017.

[83] S. Lal, T. Taleb, and A. Dutta, "Nfv: Security threats and best practices," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 211–217, 2017.

[84] C. Sandeepa, B. Siniarski, N. Kourtellis, S. Wang, and M. Liyanage, "A survey on privacy of personal and non-personal data in b5g/6g networks," *ACM Computing Surveys*, vol. 56, no. 10, pp. 1–37, 2024.

[85] M. Mitev, A. Chorti, H. V. Poor, and G. P. Fettweis, "What physical layer security can do for 6g security," *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 375–388, 2023.

[86] I. Mavridis, A.-I. Androulakis, A. Halkias, and P. Mylonas, "Real-life paradigms of wireless network security attacks," in *2011 15th Panhellenic Conference on Informatics*. IEEE, 2011, pp. 112–116.

[87] M. Pattaranantakul, R. He, Q. Song, Z. Zhang, and A. Meddahi, "Nfv security survey: From use case driven threat analysis to state-of-the-art countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3330–3368, 2018.

[88] R. Priyadarshani, K.-H. Park, Y. Ata, and M.-S. Alouini, "Jamming intrusions in extreme bandwidth communication: A comprehensive overview," *arXiv preprint arXiv:2403.19868*, 2024.

[89] T. Chen, J. Liu, Y. Xiang, W. Niu, E. Tong, and Z. Han, "Adversarial attack and defense in reinforcement learning-from ai security view," *Cybersecurity*, vol. 2, pp. 1–22, 2019.

[90] A. A. Ahmed, M. K. Hasan, I. Memon, A. H. M. Aman, S. Islam, T. R. Gadekallu, and S. A. Memon, "Secure ai for 6g mobile devices: Deep learning optimization against side-channel attacks," *IEEE Transactions on Consumer Electronics*, 2024.

[91] J. Suomalainen, I. Ahmad, A. Shajan, and T. Savunen, "Cybersecurity for tactical 6g networks: Threats, architecture, and intelligence," *Future Generation Computer Systems*, vol. 162, p. 107500, 2025.

[92] A. Chorti, A. N. Barreto, S. Köpsell, M. Zoli, M. Chafii, P. Sehier, G. Fettweis, and H. V. Poor, "Context-aware security for 6g wireless: The role of physical layer security," *IEEE Communications Standards Magazine*, vol. 6, no. 1, pp. 102–108, 2022.

[93] K. Ramezanpour, J. Jagannath, and A. Jagannath, "Security and privacy vulnerabilities of 5g/6g and wifi 6: Survey and research directions from a coexistence perspective," *Computer Networks*, vol. 221, p. 109515, 2023.

[94] T. Hewa, G. Gür, A. Kalla, M. Ylianttila, A. Bracken, and M. Liyanage, "The role of blockchain in 6g: Challenges, opportunities and research directions," *2020 2nd 6G Wireless Summit (6G SUMMIT)*, pp. 1–5, 2020.

[95] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the internet of things: Research issues and challenges," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2188–2204, 2018.

[96] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized business review*, p. 21260, 2008.

[97] S. Maalem, M. Derdour, A. Bennour, and A. Sahraoui, "A multi-level blockchain-based architecture for securing and controlling data flow in 6g networks," *SN Computer Science*, vol. 5, no. 8, pp. 1–15, 2024.

[98] A. K. Tyagi and S. Tiwari, "Blockchain-enabled smart healthcare applications in 6g networks," *Digital Twin and Blockchain for Smart Cities*, pp. 459–494, 2024.

[99] N. K. Jadav, R. Gupta, and S. Tanwar, "Blockchain and edge intelligence-based secure and trusted v2v framework underlying 6g networks," in *IEEE INFOCOM 2022-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2022, pp. 1–6.

[100] J. Asim, A. S. Khan, R. M. Saqib, J. Abdullah, Z. Ahmad, S. Honey, S. Afzal, M. S. Alqahtani, and M. Abbas, "Blockchain-based multifactor authentication for future 6g cellular networks: A systematic review," *Applied Sciences*, vol. 12, no. 7, p. 3551, 2022.

[101] Z. Sun, W. Liang, F. Qi, Z. Dong, and Y. Cai, "Blockchain-based dynamic spectrum sharing for 6g uiot networks," *IEEE Network*, vol. 35, no. 5, pp. 143–149, 2021.

[102] S. T. Muntaha, P. I. Lazaridis, M. Hafeez, Q. Z. Ahmed, F. A. Khan, and Z. D. Zaharis, "Blockchain for dynamic spectrum access and network slicing: A review," *IEEE Access*, vol. 11, pp. 17 922–17 944, 2023.

[103] A. Razaque, M. Khan, J. Yoo, A. Alotaibi, M. Alshammari, and M. Almiani, "Blockchain-enabled heterogeneous 6g supported secure vehicular management system over cloud edge computing," *Internet of Things*, vol. 25, p. 101115, 2024.

[104] M. Zawish, N. Ashraf, R. I. Ansari, S. Davy, H. K. Qureshi, N. Aslam, and S. A. Hassan, "Toward on-device ai and blockchain for 6g-enabled agricultural supply chain management," *IEEE Internet of Things Magazine*, vol. 5, no. 2, pp. 160–166, 2022.

[105] A. Jahid, M. H. Alsharif, and T. J. Hall, "The convergence of blockchain, iot and 6g: potential, opportunities, challenges and research roadmap," *Journal of Network and Computer Applications*, vol. 217, p. 103677, 2023.

[106] V. Srivastava, T. Mahara, and P. Yadav, "An analysis of the ethical challenges of blockchain-enabled e-healthcare applications in 6g networks," *International Journal of Cognitive Computing in Engineering*, vol. 2, pp. 171–179, 2021.

[107] D. Cuellar, M. Sallal, and C. Williams, "Bsm-6g: Blockchain-based dynamic spectrum management for 6g networks: Addressing interoperability and scalability," *IEEE Access*, 2024.

[108] R. Henry, A. Herzberg, and A. Kate, "Blockchain access privacy: Challenges and directions," *IEEE Security & Privacy*, vol. 16, no. 4, pp. 38–45, 2018.

[109] S. Kharche and P. Dere, "Interoperability issues and challenges in 6g networks." *J. Mobile Multimedia*, vol. 18, no. 5, pp. 1445–1470, 2022.

[110] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, and D. Mohaisen, "Exploring the attack surface of blockchain: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1977–2008, 2020.

[111] N. Sapra, I. Shaikh, and A. Dash, "Impact of proof of work (pow)-based blockchain applications on the environment: A systematic review and research agenda," *Journal of Risk and Financial Management*, vol. 16, no. 4, p. 218, 2023.

[112] O. Salman, A. Kayssi, A. Chehab, and I. Elhajj, "Multi-level security for the 5g/iot ubiquitous network," in *2017 Second International Conference on Fog and Mobile Edge Computing (FMEC)*. IEEE, 2017, pp. 188–193.

[113] M. Chelghoum, G. Bendiab, M. A. Labiod, M. Benmohammed, S. Shiaeles, and A. Mellouk, "Blockchain and ai for collaborative intrusion detection in 6g-enabled iot networks," in *2024 IEEE 25th International Conference on High Performance Switching and Routing (HPSR)*. IEEE, 2024, pp. 179–184.

[114] A. Ahmim, M. Derdour, and M. A. Ferrag, "An intrusion detection system based on combining probability predictions of a tree of classifiers," *International Journal of Communication Systems*, vol. 31, no. 9, p. e3547, 2018.

[115] M. S. Salek, S. Li, and M. Chowdhury, "A hybrid quantum-classical ai-based detection strategy for generative adversarial network-based deepfake attacks on an autonomous vehicle traffic sign classification system," *arXiv preprint arXiv:2409.17311*, 2024.

[116] B. Sun and Y. Zhao, "Tinynids: Cnn-based network intrusion detection system on tinyml models in 6g environments," *Internet Technology Letters*, p. e629, 2024.

[117] B. B. Gupta, A. Gaurav, V. Arya, and K. T. Chui, "Lstm-gru based efficient intrusion detection in 6g-enabled metaverse environments," in *2024 IEEE 25th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*. IEEE, 2024, pp. 118–123.

[118] D. Sirohi, N. Kumar, P. S. Rana, S. Tanwar, R. Iqbal, and M. Hijjii, "Federated learning for 6g-enabled secure communication systems: a comprehensive survey," *Artificial Intelligence Review*, vol. 56, no. 10, pp. 11 297–11 389, 2023.

[119] J. Zhang, C. Luo, Y. Jiang, and G. Min, "Security in 6g-based autonomous vehicular networks: Detecting network anomalies with decentralized federated learning," *IEEE Vehicular Technology Magazine*, 2025.

[120] D. Castelvecchi, "Can we open the black box of ai?" *Nature News*, vol. 538, no. 7623, p. 20, 2016.

[121] W.-x. Liu, J. Cai, Q. C. Chen, and Y. Wang, "Drl-r: Deep reinforcement learning approach for intelligent routing in software-defined data-center networks," *Journal of Network and Computer Applications*, vol. 177, p. 102865, 2021.

[122] I. H. Sarker, M. H. Furhad, and R. Nowrozy, "Ai-driven cybersecurity: an overview, security intelligence modeling and research directions," *SN Computer Science*, vol. 2, no. 3, p. 173, 2021.

[123] C. Shi, L. Yang, M. Zhang, M. Wu, B. Hou, H. Lu, F. Jia, F. Guo, W. Liu, Q. Yu *et al.*, "High-efficiency algan/gan/graded-algan/gan double-channel hemts for sub-6g power amplifier applications," *IEEE Transactions on Electron Devices*, vol. 70, no. 5, pp. 2241–2246, 2023.

[124] L. Jiao, Y. Shao, L. Sun, F. Liu, S. Yang, W. Ma, L. Li, X. Liu, B. Hou, X. Zhang *et al.*, "Advanced deep learning models for 6g: overview, opportunities and challenges," *IEEE Access*, 2024.

[125] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Artificial intelligence and statistics*. PMLR, 2017, pp. 1273–1282.

[126] V. N. Swamy, N. Naderializadeh, V. N. Ekambaram, S. Talwar, and A. Sahai, "Monitoring under-modeled rare events for urllc," in *2019 IEEE 20th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*. IEEE, 2019, pp. 1–5.

[127] H. W. Oleiwi, D. N. Mhawi, and H. Al-Raweshidy, "A secure deep autoencoder-based 6g channel estimation to detect/mitigate adversarial attacks," in *2023 5th Global Power, Energy and Communication Conference (GPECOM)*. IEEE, 2023, pp. 530–535.

[128] C. Ma, N. Wang, Q. A. Chen, and C. Shen, "Slowtrack: Increasing the latency of camera-based perception in autonomous driving using adversarial examples," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 38, no. 5, 2024, pp. 4062–4070.

[129] R. Meng, S. Gao, D. Fan, H. Gao, Y. Wang, X. Xu, B. Wang, S. Lv, Z. Zhang, M. Sun *et al.*, "A survey of secure semantic communications," *arXiv preprint arXiv:2501.00842*, 2025.

[130] S. He, C. Du, and M. S. Hossain, "6g-enabled consumer electronics device intrusion detection with federated meta-learning and digital twins in a meta-verse environment," *IEEE Transactions on Consumer Electronics*, 2023.

[131] R. Doriguzzi-Corin and D. Siracusa, "Flad: adaptive federated learning for ddos attack detection," *Computers & Security*, vol. 137, p. 103597, 2024.

[132] B. Li, P. Mo, H. You, J. Lu, M. Zhao, and L. Zhang, "Detection of hidden dangers in 6g power grid relay protection based on support vector machine," *Wireless Personal Communications*, pp. 1–21, 2024.

[133] E. Paolini, L. Valcarenghi, L. Maggiani, and N. Andriolli, "Real-time clustering based on deep embeddings for threat detection in 6g networks," *IEEE Access*, 2023.

[134] S. Sakraoui, A. Ahmim, M. Derdour, M. Ahmim, S. Namane, and I. B. Dhaou, "Fbmp-ids: Fl-based blockchain-powered lightweight mpc-secured ids for 6g networks," *IEEE Access*, 2024.

[135] A. Kuznetsov, P. Sernani, L. Romeo, E. Frontoni, and A. Mancini, "On the integration of artificial intelligence and blockchain technology: a perspective about security," *IEEE Access*, 2024.

[136] O. Odeyemi, C. C. Okoye, O. C. Ofodile, O. B. Adeoye, W. A. Addy, and A. O. Ajayi-Nifise, "Integrating ai with blockchain for enhanced financial services security," *Finance & Accounting Research Journal*, vol. 6, no. 3, pp. 271–287, 2024.

[137] S. Qiao, Y. Jiang, N. Han, W. Hua, Y. Lin, S. Min, and X. Wu, "Lbfl: A lightweight blockchain-based federated learning framework with proof-of-contribution committee consensus," *IEEE Transactions on Big Data*, 2024.

[138] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Low-latency federated learning and blockchain for edge association in digital twin empowered 6g networks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 7, pp. 5098–5107, 2020.

[139] L. Koch and E. Begoli, "Adversarial binaries: Ai-guided instrumentation methods for malware detection evasion," *ACM Computing Surveys*, vol. 57, no. 5, pp. 1–36, 2025.

[140] E. Nowroozi, I. Haider, R. Taheri, and M. Conti, "Federated learning under attack: Exposing vulnerabilities through data poisoning attacks in computer networks," *IEEE Transactions on Network and Service Management*, 2025.

[141] W. Yang, S. Wang, D. Wu, T. Cai, Y. Zhu, S. Wei, Y. Zhang, X. Yang, and Y. Li, "Deep learning model inversion attacks and defenses: A comprehensive survey," *arXiv preprint arXiv:2501.18934*, 2025.

[142] A. Aydeger and E. Zeydan, "Blockchain-based self-sovereign identity in 6g non-public networks: Enhanced security in industrial cyber-physical systems," in *2024 20th International Conference on Network and Service Management (CNSM)*. IEEE, 2024, pp. 1–7.

[143] A. Tankovic, T. Markesic, and E. Kaljic, "Blockchain-based protocol for active tracing of ip traffic in 5g/6g networks," in *2024 23rd International Symposium INFOTEH-JAHORINA (INFOTEH)*. IEEE, 2024, pp. 1–6.

[144] Z. Abou El Houda, H. Moudoud, and L. Khoukhi, "Blockchain meets o-ran: A decentralized zero-trust framework for secure and resilient o-ran in 6g and beyond," in *IEEE INFOCOM 2024-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2024, pp. 1–6.

[145] D. Girija, M. Rashmi, P. William, and N. Yogeesh, "Framework for integrating the synergies of blockchain with ai and iot for secure distributed systems," in *International Conference on Data Analytics and Insights*. Springer, 2023, pp. 257–267.

[146] B. Choudhury, P. K. Singh, P. Nath, U. Roy, and A. Kalla, "Blockchain and smart contract for decentralized and secure spectrum management toward 6g–beyond hype," *Intelligent Spectrum Management: Towards 6G*, pp. 211–236, 2025.

[147] M. B. Begum, B. Suganthi, P. Sivagamasundhari, S. Arunmozhi, and S. M. Suhail, "An enhanced heterogeneous local directed acyclic graph blockchain with recalling enhanced recurrent neural networks for routing in secure manet-iot environments in 6g," *International Journal of Communication Systems*, vol. 38, no. 4, p. e6110, 2025.

[148] R. Murugan, G. Yenduri, P. Maran, and T. Reddy Gadekallu, "The synergy of artificial intelligence and blockchain in 6g spectrum management," *Intelligent Spectrum Management: Towards 6G*, pp. 237–262, 2025.

[149] J. Zheng and Y. Zhang, "Trbft: An efficient blockchain consensus for edge computing-enabled iot systems," *IEEE Internet of Things Journal*, 2025.

[150] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for ai: Review and open research challenges," *IEEE access*, vol. 7, pp. 10 127–10 149, 2019.

[151] P. Li, Z. Xiao, H. Gao, X. Wang, and Y. Wang, "Reinforcement learning based edge-end collaboration for multi-task scheduling in 6g enabled intelligent autonomous transport systems," *IEEE Transactions on Intelligent Transportation Systems*, 2025.

[152] D. Ressi, R. Romanello, C. Piazza, and S. Rossi, "Ai-enhanced blockchain technology: A review of advancements and opportunities," *Journal of Network and Computer Applications*, p. 103858, 2024.

[153] O. Jogunola, B. Adebisi, A. Ikpehai, S. I. Popoola, G. Gui, H. Gačanin, and S. Ci, "Consensus algorithms and deep reinforcement learning in energy market: A review," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4211–4227, 2020.

[154] S. Sakraoui, M. Derdour, and A. Ahmim, "6g-secureids: Blockchain-enhanced secure knowledge transfer for distributed intrusion detection systems in advanced networks," in *2023 International Conference on Networking and Advanced Systems (ICNAS)*. IEEE, 2023, pp. 1–6.

[155] A. Bhandari, A. K. Cherukuri, and F. Kamalov, "Machine learning and blockchain integration for security applications," in *Big Data Analytics and Intelligent Systems for Cyber Threat Intelligence*. River Publishers, 2023, pp. 129–173.

[156] N. K. Parida, C. Jatoth, V. D. Reddy, M. M. Hussain, and J. Faizi, "Post-quantum distributed ledger technology: a systematic survey," *Scientific Reports*, vol. 13, no. 1, p. 20729, 2023.

[157] C. Chen, L. Wang, and Q. Shi, "A lattice-based certificateless secure data transmission scheme for internet of vehicles based-blockchain," *IEEE Transactions on Vehicular Technology*, 2024.

[158] L. Ouyang, W. Zhang, and F.-Y. Wang, "Intelligent contracts: Making smart contracts smart for blockchain intelligence," *Computers and Electrical Engineering*, vol. 104, p. 108421, 2022.

[159] L. Bindra, K. Eng, O. Ardakanian, and E. Stroulia, "Flexible, decentralised access control for smart buildings with smart contracts," *Cyber-Physical Systems*, vol. 8, no. 4, pp. 286–320, 2022.

[160] L. Axon, D. Panagiotakopoulos, S. Ayo, C. Sanchez-Hernandez, Y. Zong, S. Brown, L. Zhang, M. Goldsmith, S. Creese, and W. Guo, "Securing autonomous air traffic management: Blockchain networks driven by explainable ai," *arXiv preprint arXiv:2304.14095*, 2023.

[161] Z. Chang, Y. Cai, X. F. Liu, Z. Xie, Y. Liu, and Q. Zhan, "Anomalous node detection in blockchain networks based on graph neural networks," *Sensors*, vol. 25, no. 1, p. 1, 2024.

[162] L. McCormack and M. Bendechache, "Ethical ai governance: Methods for evaluating trustworthy ai," *arXiv preprint arXiv:2409.07473*, 2024.

[163] H. Chen, Y. Zhang, W. Li, X. Tao, and P. Zhang, "Confi: Convolutional neural networks based indoor wi-fi localization using channel state information," *Ieee Access*, vol. 5, pp. 18 066–18 074, 2017.

[164] S. K. Priya, N. Balaganesh, and K. P. Karthika, "Integration of ai, blockchain, and iot technologies for sustainable and secured indian public distribution system," in *AI Models for Blockchain-Based Intelligent Networks in IoT Systems: Concepts, Methodologies, Tools, and Applications*. Springer, 2023, pp. 347–371.

[165] V. Ziegler, H. Viswanathan, H. Flinck, M. Hoffmann, V. Räisänen, and K. Hätönen, "6g architecture to connect the worlds," *IEEE Access*, vol. 8, pp. 173 508–173 520, 2020.

[166] B. Samuel and V. T. Somasundaran, "Prevention of man-in-the-middle attacks using blockchain vpn."

[167] H. Chen, S. A. Asif, J. Park, C.-C. Shen, and M. Bennis, "Robust blockchained federated learning with model validation and proof-of-stake inspired consensus," *arXiv preprint arXiv:2101.03300*, 2021.

[168] A.-S. Shehu, "On the compliance of self-sovereign identity with gdpr principles: A critical review," *arXiv preprint arXiv:2409.03624*, 2024.

[169] R. de Filippis and A. Al Foysal, "Blockchain brains: Pioneering ai, ml, and dlt solutions for healthcare and psychology," *Open Access Library Journal*, vol. 11, no. 12, pp. 1–24, 2024.

[170] Z. Tolba, M. Derdour, M. A. Ferrag, S. Muyeen, and M. Benbouzid, "Automated deep learning black-box attack for multimedia p-box security assessment," *IEEE Access*, vol. 10, pp. 94 019–94 039, 2022.

[171] J. Pei, S. Li, Z. Yu, L. Ho, W. Liu, and L. Wang, "Federated learning encounters 6g wireless communication in the scenario of internet of things," *IEEE Communications Standards Magazine*, vol. 7, no. 1, pp. 94–100, 2023.

[172] F. Bouakkaz, W. Ali, and M. Derdour, "Forest fire detection using wireless multimedia sensor networks and image compression," *Instrum. Mes. Métrologie*, vol. 20, pp. 57–63, 2021.

[173] W. Schneble and G. Thamilarasu, "Attack detection using federated learning in medical cyber-physical systems," in *28th International conference on computer communications and networks (icccn)*, 2019, pp. 1–8.

[174] S. A. Rahman, H. Tout, C. Talhi, and A. Mourad, "Internet of things intrusion detection: Centralized, on-device, or federated learning?" *IEEE Network*, vol. 34, no. 6, pp. 310–317, 2020.

[175] O. Aouedi, K. Piamrat, G. Muller, and K. Singh, "Fluids: Federated learning with semi-supervised approach for intrusion detection system," in *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2022, pp. 523–524.

[176] Z. Zhang, Y. Zhang, D. Guo, L. Yao, and Z. Li, "Secfednids: Robust defense for poisoning attack against federated learning-based network intrusion detection system," *Future Generation Computer Systems*, vol. 134, pp. 154–169, 2022.

[177] M. Sarhan, S. Layeghy, N. Moustafa, and M. Portmann, "Cyber threat intelligence sharing scheme based on federated learning for network intrusion detection," *Journal of Network and Systems Management*, vol. 31, no. 1, p. 3, 2023.

[178] G. Hinton, O. Vinyals, and J. Dean, "Distilling the knowledge in a neural network," *arXiv preprint arXiv:1503.02531*, 2015.

[179] D. Li and J. Wang, "Fedmd: Heterogenous federated learning via model distillation," *arXiv preprint arXiv:1910.03581*, 2019.

[180] R. Khemaissia, M. Derdour, A. Djeddai, and M. A. Ferrag, "Sdgchain: When service dependency graph meets blockchain to enhance privacy," in *Proceedings of the 2021 ACM Workshop on Security and Privacy Analytics*, 2021, pp. 37–43.

[181] M. Matthaiou, O. Yurduseven, H. Q. Ngo, D. Morales-Jimenez, S. L. Cotton, and V. F. Fusco, "The road to 6g: Ten physical layer challenges for communications engineers," *IEEE Communications Magazine*, vol. 59, no. 1, pp. 64–69, 2021.

[182] K. B. Letaief, Y. Shi, J. Lu, and J. Lu, "Edge artificial intelligence for 6g: Vision, enabling technologies, and applications," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 1, pp. 5–36, 2021.

[183] A. Albanese, F. Devoti, V. Sciancalepore, M. Di Renzo, and X. Costa-Pérez, "Marisa: A self-configuring metasurfaces absorption and reflection solution towards 6g," in *IEEE INFOCOM 2022-IEEE Conference on Computer Communications*. IEEE, 2022, pp. 250–259.

[184] A. Ahmim and N. Ghoualmi-Zine, "A new fast and high performance intrusion detection system," *International Journal of Security and Its Applications*, vol. 7, no. 5, pp. 67–80, 2013.

[185] A. Ahmim, F. Maazouzi, M. Ahmim, S. Namane, and I. B. Dhaou, "Distributed denial of service attack detection for the internet of things using hybrid deep learning model," *IEEE Access*, vol. 11, pp. 119 862–119 875, 2023.

[186] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, Ł. Kaiser, and I. Polosukhin, "Attention is all you need," *Advances in neural information processing systems*, vol. 30, 2017.

[187] S. Rezvy, Y. Luo, M. Petridis, A. Lasebae, and T. Zebin, "An efficient deep learning model for intrusion classification and prediction in 5g and iot networks," in *2019 53rd Annual Conference on information sciences and systems (CISS)*. IEEE, 2019, pp. 1–6.

[188] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, "Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 184–208, 2015.

[189] H. Moudoud, L. Khoukhi, and S. Cherkaoui, "Prediction and detection of fdia and ddos attacks in 5g enabled iot," *IEEE Network*, vol. 35, no. 2, pp. 194–201, 2020.

[190] J. Zhu, S. He, J. Liu, P. He, Q. Xie, Z. Zheng, and M. R. Lyu, "Tools and benchmarks for automated log parsing," in *2019 IEEE/ACM 41st International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP)*. IEEE, 2019, pp. 121–130.

[191] I. H. Abdulqadder, S. Zhou, D. Zou, I. T. Aziz, and S. M. A. Akber, "Multi-layered intrusion detection and prevention in the sdn/nfv enabled cloud of 5g networks using ai-based defense mechanisms," *Computer Networks*, vol. 179, p. 107364, 2020.

[192] Z. Zhang, Y. Cao, Z. Cui, W. Zhang, and J. Chen, "A many-objective optimization based intelligent intrusion detection algorithm for enhancing security of vehicular networks in 6g," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, pp. 5234–5243, 2021.

[193] E. Seo, H. M. Song, and H. K. Kim, "Gids: Gan based intrusion detection system for in-vehicle network," in *2018 16th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2018, pp. 1–6.

[194] M. Almiani, A. AbuGhazleh, Y. Jararweh, and A. Razaque, "Ddos detection in 5g-enabled iot networks using deep kalman backpropagation neural network," *International Journal of Machine Learning and Cybernetics*, vol. 12, pp. 3337–3349, 2021.

[195] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (ddos) attack dataset and taxonomy," in *2019 international carnahan conference on security technology (ICCST)*. IEEE, 2019, pp. 1–8.

[196] H. Chen, B. Yuan, D. Zou, and H. Jin, "A fuzzing-based method for testing rules in intrusion detection systems in 6g networks," *IEEE Network*, vol. 36, no. 4, pp. 150–158, 2022.

[197] A. Alotaibi and A. Barnawi, "Idsoft: A federated and softwarized intrusion detection framework for massive internet of things in 6g network," *Journal of King Saud University-Computer and Information Sciences*, p. 101575, 2023.

[198] Y. LeCun, "The mnist database of handwritten digits," *http://yann. lecun. com/exdb/mnist/*, 1998.

[199] L. J. Vinita and V. Vetriselvi, "Federated learning-based misbehaviour detection on an emergency message dissemination scenario for the 6g-enabled internet of vehicles," *Ad Hoc Networks*, vol. 144, p. 103153, 2023.

[200] L. Jai Vinita and V. Vetriselvi, "Impact of sybil attack on software-defined vehicular fog computing (sdvf) for an emergency vehicle scenario," in *Inventive Communication and Computational Technologies: Proceedings of ICICCT 2022*. Springer, 2022, pp. 809–825.

[201] M. Prasad, S. Tripathi, and K. Dahal, "An intelligent intrusion detection and performance reliability evaluation mechanism in mobile ad-hoc networks," *Engineering Applications of Artificial Intelligence*, vol. 119, p. 105760, 2023.

[202] J. Du, T. Lin, C. Jiang, Q. Yang, C. F. Bader, and Z. Han, "Distributed foundation models for multi-modal learning in 6g wireless networks," *IEEE Wireless Communications*, vol. 31, no. 3, pp. 20–30, 2024.

[203] J. Du, C. Jiang, A. Benslimane, S. Guo, and Y. Ren, "Sdn-based resource allocation in edge and cloud computing systems: An evolutionary stackelberg differential game approach," *IEEE/ACM Transactions on Networking*, vol. 30, no. 4, pp. 1613–1628, 2022.

[204] M. A. Ferrag, O. Friha, L. Maglaras, H. Janicke, and L. Shu, "Federated deep learning for cyber security in the internet of things: Concepts, applications, and experimental analysis," *IEEE Access*, vol. 9, pp. 138 509–138 542, 2021.

[205] E. Ashraf, N. F. Areed, H. Salem, E. H. Abdelhay, and A. Farouk, "Fidchain: Federated intrusion detection system for blockchain-enabled iot healthcare applications," in *Healthcare*, vol. 10, no. 6. MDPI, 2022, p. 1110.

[206] H. Sedjelmaci and N. Ansari, "Zero trust architecture empowered attack detection framework to secure 6g edge computing," *IEEE Network*, 2023.

[207] W. Issa, N. Moustafa, B. Turnbull, N. Sohrabi, and Z. Tari, "Blockchain-based federated learning for securing internet of things: A comprehensive survey," *ACM Computing Surveys*, vol. 55, no. 9, pp. 1–43, 2023.

[208] J. Wu, C. Leng, Y. Wang, Q. Hu, and J. Cheng, "Quantized convolutional neural networks for mobile devices," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2016, pp. 4820–4828.

[209] R. Krishnamoorthi, "Quantizing deep convolutional networks for efficient inference: A whitepaper," *arXiv preprint arXiv:1806.08342*, 2018.

[210] B. Jacob, S. Kligys, B. Chen, M. Zhu, M. Tang, A. Howard, H. Adam, and D. Kalenichenko, "Quantization and training of neural networks for efficient integer-arithmetic-only inference," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2018, pp. 2704–2713.

[211] E. Wang, J. J. Davis, D. Moro, P. Zielinski, J. J. Lim, C. Coelho, S. Chatterjee, P. Y. Cheung, and G. A. Constantinides, "Enabling binary neural network training on the edge," in *Proceedings of the 5th international workshop on embedded and mobile deep learning*, 2021, pp. 37–38.

[212] C. N. Coelho, A. Kuusela, H. Zhuang, T. Aarrestad, V. Loncar, J. Ngadiuba, M. Pierini, and S. Summers, "Ultra low-latency, low-area inference accelerators using heterogeneous deep quantization with qkeras and hls4ml," *arXiv preprint arXiv:2006.10159*, p. 108, 2020.

[213] C. N. Coelho, A. Kuusela, S. Li, H. Zhuang, J. Ngadiuba, T. K. Aarrestad, V. Loncar, M. Pierini, A. A. Pol, and S. Summers, "Automatic heterogeneous quantization of deep neural networks for low-latency inference on the edge for particle detectors," *Nature Machine Intelligence*, vol. 3, no. 8, pp. 675–686, 2021.

[214] B. Moons, K. Goetschalckx, N. Van Berckelaer, and M. Verhelst, "Minimum energy quantized neural networks," in *2017 51st Asilomar Conference on Signals, Systems, and Computers*. IEEE, 2017, pp. 1921–1925.

[215] D. Byrd and A. Polychroniadou, "Differentially private secure multi-party computation for federated learning in financial applications," in *Proceedings of the First ACM International Conference on AI in Finance*, 2020, pp. 1–9.

[216] V. Mugunthan, A. Polychroniadou, D. Byrd, and T. H. Balch, "Smpai: Secure multi-party computation for federated learning," in *Proceedings of the NeurIPS 2019 Workshop on Robust AI in Financial Services*, vol. 21. MIT Press Cambridge, MA, USA, 2019.

[217] E. Sotthiwat, L. Zhen, Z. Li, and C. Zhang, "Partially encrypted multi-party computation for federated learning," in *2021 IEEE/ACM 21st International Symposium on Cluster, Cloud and Internet Computing (CCGrid)*. IEEE, 2021, pp. 828–835.

[218] Z. Beerliová-Trubíniová and M. Hirt, "Perfectly-secure mpc with linear communication complexity," in *Theory of Cryptography Conference*. Springer, 2008, pp. 213–230.

[219] Flower, "Flower: A friendly federated learning framework," 2024, accessed: 2024-01-11. [Online]. Available: https://flower.ai/

[220] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "Ciciot2023: A real-time dataset and benchmark for large-scale attacks in iot environment," *Sensors*, vol. 23, no. 13, p. 5941, 2023.

[221] "Tensorflow model optimization," 2024, accessed: 2024-01-11. [Online]. Available: https://www.tensorflow.org/model_optimization

[222] "Tensorflow lite," 2024, accessed: 2024-01-11. [Online]. Available: https://www.tensorflow.org/lite

[223] K. A. Alezabi, F. Hashim, S. J. Hashim, B. M. Ali, and A. Jamalipour, "Efficient authentication and re-authentication protocols for 4g/5g heterogeneous networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2020, pp. 1–34, 2020.

[224] A. S. Khan, M. A. Sattar, K. Nisar, A. A. A. Ibrahim, N. B. Annuar, J. b. Abdullah, and S. Karim Memon, "A survey on 6g enabled light weight authentication protocol for uavs, security, open research issues and future directions," *Applied Sciences*, vol. 13, no. 1, p. 277, 2022.

[225] T.-V. Le, C.-F. Lu, C.-L. Hsu, T. K. Do, Y.-F. Chou, and W.-C. Wei, "A novel three-factor authentication protocol for multiple service providers in 6g-aided intelligent healthcare systems," *IEEE Access*, vol. 10, pp. 28 975–28 990, 2022.

[226] Y. Tao, H. Du, J. Xu, L. Su, and B. Cui, "On-demand anonymous access and roaming authentication protocols for 6g satellite–ground integrated networks," *Sensors*, vol. 23, no. 11, p. 5075, 2023.

[227] S. A. Chaudhry, A. Irshad, M. A. Khan, S. A. Khan, S. Nosheen, A. A. AlZubi, and Y. B. Zikria, "A lightweight authentication scheme for 6g-iot enabled maritime transport system," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 2, pp. 2401–2410, 2021.

[228] H. Fang, A. Qi, and X. Wang, "Fast authentication and progressive authorization in large-scale iot: How to leverage ai for security enhancement," *IEEE network*, vol. 34, no. 3, pp. 24–29, 2020.

[229] D. Garabato, C. Dafonte, R. Santovena, A. Silvelo, F. J. Novoa, and M. Manteiga, "Ai-based user authentication reinforcement by continuous extraction of behavioral interaction features," *Neural Computing and Applications*, vol. 34, no. 14, pp. 11 691–11 705, 2022.

[230] V. Siddhartha, G. S. Gaba, and L. Kansal, "A lightweight authentication protocol using implicit certificates for securing iot systems," *Procedia computer science*, vol. 167, pp. 85–96, 2020.

[231] V. Kumar, N. Malik, J. Singla, N. Jhanjhi, F. Amsaad, and A. Razaque, "Light weight authentication scheme for smart home iot devices," *Cryptography*, vol. 6, no. 3, p. 37, 2022.

[232] U. Khalid, M. Asim, T. Baker, P. C. Hung, M. A. Tariq, and L. Rafferty, "A decentralized lightweight blockchain-based authentication mechanism for iot systems," *Cluster Computing*, vol. 23, no. 3, pp. 2067–2087, 2020.

[233] M. T. Al Ahmed, F. Hashim, S. J. Hashim, and A. Abdullah, "Authentication-chains: blockchain-inspired lightweight authentication protocol for iot networks," *Electronics*, vol. 12, no. 4, p. 867, 2023.

[234] M. N. Aman, K. C. Chua, and B. Sikdar, "A light-weight mutual authentication protocol for iot systems," in *GLOBECOM 2017-2017 IEEE Global Communications Conference*. IEEE, 2017, pp. 1–6.

[235] M. Tahir, M. Sardaraz, S. Muhammad, and M. Saud Khan, "A lightweight authentication and authorization framework for blockchain-enabled iot network in health-informatics," *Sustainability*, vol. 12, no. 17, p. 6960, 2020.

[236] S. J. Rigatti, "Random forest," *Journal of Insurance Medicine*, vol. 47, no. 1, pp. 31–39, 2017.