Future Generation Computer Systems 160 (2024) 577–597

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Quantum-empowered federated learning and 6G wireless networks for IoT security: Concept, challenges and future directions

Danish Javeed [a], Muhammad Shahid Saeed [b], Ijaz Ahmad [c], Muhammad Adil [d], Prabhat Kumar [e,*], A.K.M. Najmul Islam [e]

[a] Software College, Northeastern University, Shenyang 110169, China
[b] School of Software Technology, Dalian University of Technology (DUT), Dalian 116024, Liaoning, China
[c] Institute of Business and Management Sciences (IBMS), The University of Agriculture, 25130 Peshawar, Pakistan
[d] College of Intelligence and Computing, Tianjin University, Tianjin, China
[e] Department of Software Engineering, LUT School of Engineering Science, LUT University, 53850 Lappeenranta, Finland

ARTICLE INFO

Keywords:
Federated learning
Cyber threats
Internet of Things
Privacy
Security
Quantum computing
Wireless networks
6G

ABSTRACT

The Internet of Things (IoT) has revolutionized various sectors by enabling seamless device interaction. However, the proliferation of IoT devices has also raised significant security and privacy concerns. Traditional security measures often fail to address these concerns due to the unique characteristics of IoT networks, such as heterogeneity, scalability, and resource constraints. This survey paper adopts a thematic exploration approach for a comprehensive analysis to investigate the convergence of quantum computing, federated learning, and 6G wireless networks. This novel intersection is explored to significantly improve security and privacy within the IoT ecosystem. Quantum computing can enhance encryption algorithms to make IoT data more secure for intelligent IoT applications. Federated learning, a decentralized machine learning approach, allows IoT devices to learn a shared model while keeping all the training data on the original device, thereby enhancing privacy. This synergy becomes even more crucial when integrated with the high-speed, low-latency capabilities of 6G networks, which can facilitate real-time, secure data processing and communication among many IoT devices. Second, we discuss the latest developments, offering an up-to-date overview of advanced solutions, available datasets, and key performance metrics and summarizing the vital insights, challenges, and trends in securing IoT systems. Third, we design a conceptual framework for integrating quantum computing in federated learning, adapted for 6G networks. Finally, we highlight the future advancements in quantum technologies and 6G networks and summarize the implications for IoT security, paving the way for researchers and practitioners in the field of IoT security.

1. Introduction

The Internet of Things (IoT) refers to the concept of connecting everyday physical objects to the Internet, thereby enabling these objects to collect and share data with other devices or centralized systems. Utilizing sensors and communication technology, IoT devices are capable of communicating and interacting with their environment without the necessity for human intervention [1]. IoT has emerged as a disruptive force across various sectors and industries, primarily enhancing productivity and efficiency. By facilitating automation and real-time monitoring through the interconnectedness of diverse systems and devices, IoT reduces the need for human input and streamlines operations [2]. For example, IoT sensors can detect anomalies in machinery and initiate repairs, thereby minimizing downtime and enhancing the operational efficiency of industrial processes. Additionally, the vast data collection and analysis capabilities of IoT are instrumental in supporting informed decision-making. Organizations can access valuable insights into market trends, consumer behavior, and operational performance, which aids in the development of effective strategies and the enhancement of customer experiences [3]. This data-driven approach also allows for the creation of new products and services tailored to customer needs, promoting innovation.

However, the widespread implementation of IoT is not without its challenges, particularly in the areas of security, privacy, and interoperability [4]. The inherent vulnerabilities of IoT devices, many of which possess limited memory and processing capabilities, pose significant

* Corresponding author.
E-mail addresses: 2027016@stu.neu.edu.cn (D. Javeed), ShahidSaeedRana@mail.dlut.edu.cn (M.S. Saeed), Ijazahmad@ieee.org (I. Ahmad), 6122000014@tju.edu.cn (M. Adil), prabhat.kumar@lut.fi (P. Kumar), najmul.islam@lut.fi (A.K.M.N. Islam).

https://doi.org/10.1016/j.future.2024.06.023
Received 20 December 2023; Received in revised form 24 May 2024; Accepted 12 June 2024
Available online 13 June 2024

security risks. The rush by manufacturers to market these products often results in insufficient attention to robust security measures, leaving devices susceptible to a variety of cyber-attacks, including Brute Force, Botnets, Denial of Service (DoS), Spoofing, and Phishing attacks [5]. Data privacy represents another major concern within IoT networks, as these devices often collect and transmit sensitive and private information, from health data captured by wearables to footage from home security cameras. Ensuring the privacy and confidentiality of this sensitive data is paramount, as unauthorized access or breaches can have dire consequences for individuals and businesses alike [6]. Moreover, IoT devices may employ a variety of communication protocols, such as Message Queuing Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), Wi-Fi, Bluetooth, Zigbee, etc., and are produced by different vendors. This diversity can complicate the assurance of safe and seamless integration into IoT networks. Device incompatibilities and security vulnerabilities may be exploited by malicious actors, underscoring the importance of addressing these issues [7]. Furthermore, the distributed nature of IoT, with countless devices connected to networks, provides hackers with a larger attack surface. This increases the risk of widespread Distributed Denial of Service (DDoS) attacks, where compromised IoT devices flood networks or services with traffic, aiming to disrupt normal operations and cause outages [8].

Federated Learning (FL) represents a decentralized approach to machine learning with significant implications for IoT applications. In the IoT paradigm, various devices, such as smartphones, sensors, and smart appliances, continually generate data [9]. FL enables these devices to collectively learn a shared prediction model while retaining all the training data on the original device, thereby preserving data privacy and reducing the need for data transmission. In an IoT context, this means each IoT device in the network can autonomously train an AI model using its data and then share the model parameters (not the data itself) with a central server. The server consolidates these parameters to create a global model, which is then sent back to the devices for further local updates. This process repeats until the model's performance meets the desired criteria [10]. This approach is particularly advantageous for IoT networks as it enables the utilization of real-time data residing on edge devices, potentially leading to more accurate and robust models. Furthermore, since raw data never leaves the user's device, it addresses privacy concerns and reduces the risk of data leakage [11]. However, implementing FL in IoT networks also presents several challenges, including dealing with Independent and Identically Distributed data (non-IID) due to the diverse nature of IoT devices, handling device dropouts due to intermittent connectivity, and ensuring the robustness of the global model against potential adversarial attacks.

Quantum computing is an advancing field that utilizes the principles of quantum mechanics to process information. Unlike classical computers that use bits (0s and 1s), quantum computers use quantum bits or qubits, which can exist in multiple states simultaneously due to their superposition property [12]. This allows quantum computers to process a vast number of possibilities at the same time. Entanglement is another principle of quantum mechanics used in quantum computing. When qubits become entangled, the state of one qubit becomes linked with the state of another, regardless of the distance between them. This interconnectedness can significantly speed up computational processes. In the context of IoT security, quantum computing offers substantial benefits. For example, quantum key distribution (QKD) uses quantum mechanics principles to secure communication information [13,14]. It enables two parties to generate a shared random secret key known only to them, which can be used to encrypt and decrypt messages. The security of QKD lies in the fact that any attempt to eavesdrop on the key will disturb the system and can be detected. Furthermore, quantum computing can potentially address the challenges of Federated Learning (FL) in IoT networks in several ways. Firstly, quantum computing's ability to process a vast number of possibilities simultaneously could help in dealing with non-IID data, enabling more efficient processing and analysis of diverse datasets, leading to more accurate and robust models. Secondly, quantum computing could enhance the robustness of FL against device dropouts [15]. Quantum error correction techniques could be used to mitigate the effects of lost updates due to device dropouts [16]. Additionally, quantum computing could also enhance the security of FL. Quantum Key Distribution (QKD) could be used to secure the transmission of model updates, making it harder for adversaries to launch attacks.

The sixth generation of wireless networks, or 6G, is set to take digital communication to the next level, especially in the context of the IoT. With billions of IoT devices interconnected worldwide, the need for faster, more reliable, and more secure networks is paramount, and 6G is poised to meet these demands }citeal2023edge. One of the key features of 6G is its use of higher frequency bands, which allows for greater data rates and capacity. This is particularly beneficial for IoT devices, which generate vast amounts of data that need to be transmitted efficiently. The high-frequency bands of 6G could enable faster and more reliable data transmission, enhancing the performance of IoT applications [17]. 6G is also expected to offer lower latency compared to its predecessors. In the IoT context, this means that the delay between sending a command to an IoT device and receiving a response could be significantly reduced. This is crucial for applications that require real-time responses, such as autonomous vehicles and industrial automation systems [18]. The integration of Quantum Computing, Federated Learning, and 6G Networks presents a promising frontier for enhancing the security and efficiency of IoT systems [19,20]. With its superior computational capabilities and secure communication protocols, Quantum Computing can potentially address the challenges of implementing Federated Learning in IoT networks. Meanwhile, the advent of 6G Networks promises unprecedented levels of connectivity, speed, and reliability, which are crucial for the effective functioning of IoT devices [16,21]. In conclusion, the future of IoT security looks promising with the advent of Quantum-Empowered Federated Learning and 6G Wireless Networks. This paper aims to contribute to this ongoing effort and we look forward to the exciting developments that lie ahead.

1.1. Related studies and surveys for IoT security

FL has emerged as a foundational element of every state-of-the-art privacy-preserving communication framework for the IoT in the current decade. FL introduces a remarkable innovation in traditional ML training strategies by establishing a decentralized and iterative training mechanism. As a consequence, not only does the training process become more robust and responsive, but it also enhances the accuracy of the training process, leading to highly reliable security frameworks. This idea is widely acknowledged, and the application circle of FL-driven approaches is continuously expanding. Researchers in [22] provide a comprehensive survey regarding the integration of FL-driven security approaches for IoT. The study describes a broader variety of FL-based security models designed to investigate major malware in the concerned IoT communication scenarios. Similar efforts are made in [23], where authors elaborate on FL-enabled schemes to countermeasure emerging cyber threats in large-scale IoT networks. The impact of FL on large volumes of IoT data, communication latencies, resource utilization, etc. is also addressed. The study also provides an extensive overview of the recent advances and challenges associated with the implications of FL in sensitive IoT communications.

Quantum computing is a significant technology that has a considerable influence on the security of IoT systems. It effectively optimizes network resources, communication streams, and interaction patterns, thereby facilitating the implementation of complex security frameworks for IoT devices. In [24], researchers discussed a wide range of quantum-based solutions to ensure security in medium- to large-scale IoT networks. The research also analyzes the existing challenges and future hazards while implementing quantum-driven security schemes in the concerned area. The FL also welcomes inter-coupling with quantum

Table 1
The summary of existing surveys.

Ref	Year	Domain	Pros	Cons
[22]	2023	FL for IoT security	A comprehensive survey is conducted to describe FL-based malware detection schemes for the IoT.	The study should also include other major attack categories in IoT networks.
[23]	2022	FL for IoT security	Recent advances in the utilization of FL to achieve cyber security in the IoT are addressed.	The futuristic insight does not focus on implementing FL for a particular segment of IoT.
[24]	2023	Quantum Computing for IoT Security	The authors discuss the role of quantum computing in maintaining IoT security.	The study could become more effective by including many relevant articles.
[25]	2022	Quantum-empowered FL for IoT security	The significance of quantum-empowered FL in all possible aspects is addressed.	The study does not offer futuristic insight to overcome concerns.
[26]	2023	Quantum cryptography for FL model training	The study environs several cryptographic ways where quantum computing allows FL model training on encrypted IoT data.	There must be some overview of the current challenges to implementing such complex cryptographic computations for FL-based IDS in the IoT.
[27]	2021	6G towards IoT security	A generalized outlook about 6G is provided for improving IoT security.	This survey does not indicate the futuristic scope of this strategic intervention.
[19]	2022	Quantum-driven 6G for IoT security	The study examines recent advancements regarding quantum-enabled 6G-based secure communication for IoT.	There should be a comprehensive explanation regarding the key factors responsible for the hierarchical integration of these technologies.

computing, which reflects the significant potential to ensure futuristic security models for next-generation IoT communications. Quantum-empowered FL models will undoubtedly be a ground-breaking idea because of the countless privileges that come with this integration. Quantum bits are the integral characteristic of quantum computing, which offers simultaneous consideration of multiple states. Quantum FL can boost the training mechanism of FL, resulting in improved accuracy and maximum reliability. Moving forward, the cryptographic aspects of quantum computing can impressively safeguard the privacy and integrity of IoT data. The researchers in [25] provide a summary of scientific studies that highlight the importance and challenges regarding quantum FL to increase security in IoT communication systems. In quantum FL-oriented threat detection models, there are several prominent cryptographic schemes that ensure the privacy of the data used to train the central model. In [26], authors have explained such mechanisms, e.g., blind quantum computing, Quantum Key Distribution (QKD), Quantum Random Number Generation (QRNG), etc. The training process on encrypted data exponentially maximizes the unwanted exposure of training data to suspicious entities associated with the system. The IoT can also be strategically interlaced with sixth-generation wireless communications networks (6G) to embrace a new space of revolutionary communication operations. The authors [27] explore the unmatchable strengths of 6G in IoT applications like edge intelligence, reconfigurable intelligent surfaces, reduced latencies, and minimal risks to security threats. The researchers in [19] cover a review of 6G technology, encompassing its prerequisites, challenges, and role in IoT security in an in-depth manner. The review of existing survey literature is summarized in Table 1:

Although there have been some recent surveys on the integration of FL, quantum computing, and 6G technologies in enhancing IoT security, these studies predominantly examine each technology in isolation rather than exploring their combined potential. The literature often misses the opportunity to examine the integrated benefits of combining FL's decentralized learning mechanisms, quantum computing's unparalleled computational and security capabilities, and 6G's advanced communication technologies for IoT security. Furthermore, challenges such as security, privacy, practical implementation, and regulatory issues associated with this integrated approach remain insufficiently explored. Addressing these gaps requires a shift in research focus towards the collaborative potential of these technologies, aiming to develop a more robust, efficient, and secure framework for IoT systems that leverages their collective strengths.

1.2. Contributions of this survey

The primary contributions of this survey paper can be summarized as follows: A thematic exploration approach is used to conduct a comprehensive analysis of the complex interplay between quantum computing, federated learning, 6G networks, and IoT security. This methodology allows for the identification and highlighting of the mutual dependencies and collective influence these technologies have on the future of secure IoT ecosystems. Within the thematic exploration framework, the latest advancements are presented, offering a synthesized view of sophisticated solutions, accessible datasets, crucial performance indicators, and summarizing essential insights, challenges, and trends in securing IoT systems. A novel framework is proposed that leverages quantum computing, federated learning, and 6G wireless networks for securing the IoT ecosystem. This framework is not only grounded in the thematic analysis of current research but also incorporates projections of how these technologies can be synergistically implemented to address emerging security challenges. Finally, a roadmap of future directions is offered, inspired by the themes uncovered through the exploration. This includes advancements in quantum technologies, the evolution of 6G networks, and emerging paradigms critical for shaping the secure IoT landscape.

1.3. Paper outline

The rest of the paper is organized as follows. Section 2 provides a comprehensive background necessary for understanding the intersection of IoT security, 5G and 6G networks, Federated Learning, and Quantum Computing. In Section 3, we discuss the challenges of federated learning in IoT and discuss the importance of quantum computing and 6G for enhancing security and privacy in the IoT ecosystem. Section 4 presents the most recent developments to overcome identified challenges. The paper's structure and flow are presented in Fig. 1.

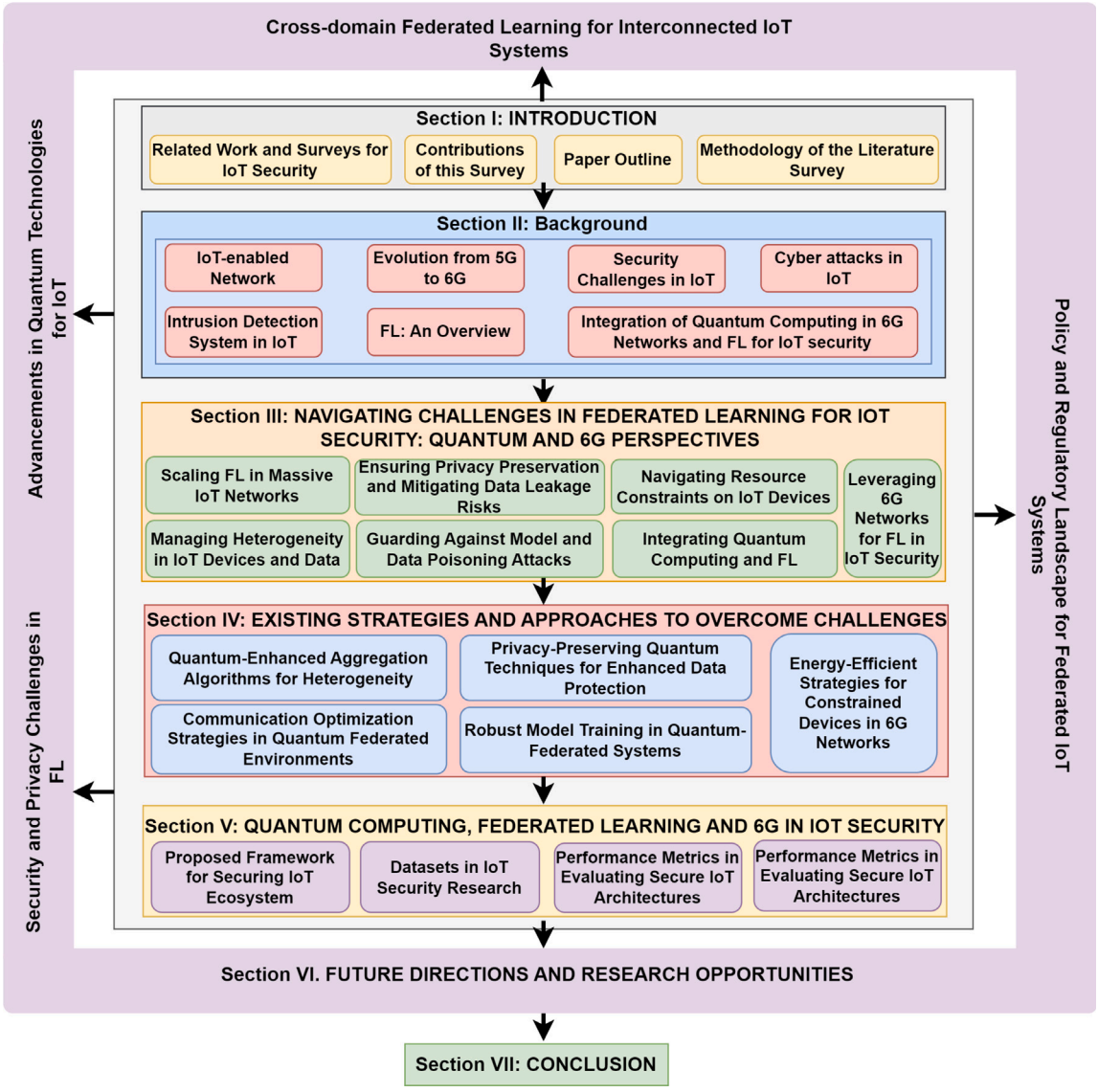

Fig. 1. Structure and the outline of this paper.

1.4. Methodology of the literature survey

This survey employs a thematic exploration approach to systematically review and analyze the literature at the intersection of FL, quantum computing, and 6G technologies within the IoT security domain. Our methodology is designed to uncover and synthesize themes emerging from the integration of advanced technologies in this interdisciplinary area. Below, we detail the process of our thematic exploration, including search strategies and selection criteria to navigate through the complex landscape of existing research.

Search Strategy: Our search strategy was implemented across multiple academic databases, including IEEE Xplore, ScienceDirect, Scopus, and Google Scholar, to ensure a comprehensive collection of relevant literature. The search utilized a combination of keywords such as "Federated Learning and IoT", "Quantum Computing for Security", "6G and IoT Security", and "Integration of FL, Quantum Computing, and 6G", among others. The aim was to capture a broad spectrum of studies that contribute to the dialogue on how these technologies converge to enhance IoT security. The temporal scope of the search was left open to include seminal works and the most recent publications, acknowledging the rapid development in these fields.

Selection Criteria: We included studies that offered significant insights into the application of FL, quantum computing, or 6G technologies in the context of IoT security. This encompassed theoretical explorations, empirical studies, practical applications, and reviews that directly or indirectly hinted at these technologies' benefits, challenges, or future directions in securing IoT ecosystems. Studies that did not specifically contribute to the understanding of these technologies' impact on IoT security were excluded. This focused approach ensured that our analysis remained pertinent to the survey's goals.

2. Background

This section provides a comprehensive background necessary for understanding the intersection of IoT-enabled networks, evolution from 5G to 6G, security challenges in IoT, intrusion detection systems in IoT, federated learning, and quantum computing.

2.1. IoT-enabled networks

The rise of the IoT is significantly influencing both the industrial and academic sectors with its potential to enable smart, autonomous

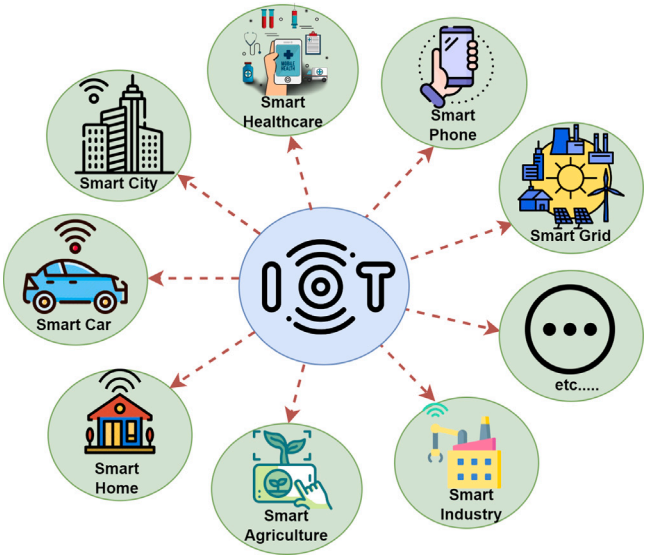

Fig. 2. IoT Applications.

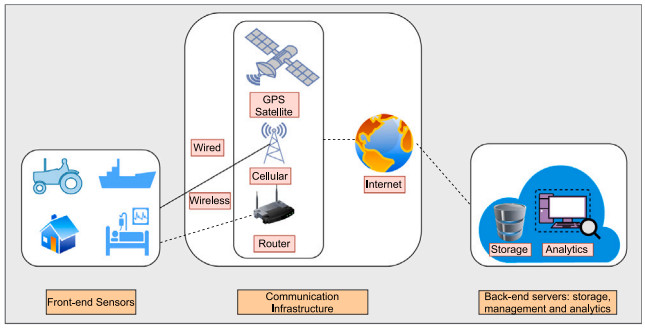

Fig. 3. A 3-tier IoT architecture [28].

interconnectivity among a wide array of devices without human intervention [1]. Globally, billions of devices are now part of the IoT, equipped with sensors, software, and other technologies for connecting and exchanging data via the Internet [1,29]. Some of the key applications of IoT are shown in Fig. 2. These IoT-enabled networks support the seamless communication of a diverse range of devices, from basic sensors and actuators to more complex systems, facilitating uninterrupted data sharing. With the exponential increase in the number of IoT devices [2], the networks are engineered to manage far more connections than traditional network systems. Furthermore, applications like autonomous vehicles and industrial automation systems necessitate extremely low response times. To meet these requirements, IoT networks are designed to minimize latency, ensuring swift and reliable communication for time-critical operations [30]. Many IoT devices, particularly those that are battery-operated, are made to last long periods without the need for frequent recharging. These devices typically support low-power communication protocols, extending battery life and operational duration to achieve this. IoT networks also adopt technologies designed to provide extensive coverage, including penetrating obstacles and effectively reaching remote locations. Given the critical nature of the data collected and the potential threat of cyber-attacks [5], these networks prioritize strong security measures to safeguard data integrity and maintain user privacy. Integration with cloud computing and edge computing infrastructures is common, enabling the processing, analysis, and storage of the vast data volumes generated by IoT devices [31]. The diversity of IoT devices and the range of manufacturers necessitate that IoT networks are developed with standards and protocols to ensure interoperability across different devices. This interoperability is essential in the design of IoT architectures, whether they adopt a three-tier, five-tier, or edge/fog computing model [32]. The network or communication layer plays a pivotal role in these architectures, acting as the conduit between the device layer, which collects data, and the higher levels where data processing and analysis are performed [28]. A typical 3-tier architecture is illustrated in Fig. 3 [28].

2.2. Evolution from 5G to 6G networks

The progression from 5G to 6G networks represents a significant leap in the field of telecommunications, characterized by enhanced connectivity, throughput, and a broad spectrum of technological innovations [21]. While 5G networks have laid the groundwork for higher data transmission rates, substantially reduced latency, and augmented connectivity across an expanding array of devices, 6G is poised to extend these capabilities further by leveraging cutting-edge technologies such as artificial intelligence (AI) and edge computing [33]. 6G networks are anticipated to offer data speeds reaching the terabit-per-second (Tbps) range, drastically minimizing latency to near-zero levels for real-time communications and enhancing network performance's overall reliability and efficiency. This leap is not merely incremental; it embodies a paradigm shift in network infrastructure, emphasizing the integration of AI for network optimization, management, and security. Furthermore, 6G aims to advance the concept of ubiquitous computing by enhancing the support for Internet of Things (IoT) ecosystems [17], where edge computing becomes a cornerstone, enabling data processing closer to the source and thus, reducing response times and bandwidth usage. The architecture of 6G networks is also expected to introduce novel communication technologies, including the use of higher frequency bands in the sub-terahertz (THz) and visible light communication (VLC) spectrum, to accommodate the increasing demand for bandwidth and support the vast data flows characteristic of next-generation digital applications. Moreover, 6G envisions a comprehensive integration of satellite networks to ensure seamless global coverage, particularly in areas where traditional cellular network deployment is challenging. As illustrated in Fig. 4, the evolution from 1G to 6G showcases a continuous strive for technological excellence, with each generation introducing transformative features that redefine the telecommunications landscape. The transition to 6G, in particular, is set to herald a new era of hyper-connectivity, facilitating advanced applications in virtual and augmented reality, autonomous systems [18], and smart cities, among others, thus underscoring the pivotal role of next-generation networks in shaping the future of digital society.

2.3. Security challenges in IoT

Considering the IoT acceptance rate, several devices connected to IoT are increasing every day [2]. Despite their significance, this increasing expansion of IoT networks and their devices results in serious security challenges. Some of them are shown in Fig. 5 and discussed as follows:

2.3.1. Interoperability

In the IoT ecosystem, devices utilize a wide array of communication protocols and originate from numerous manufacturers, introducing significant interoperability challenges [28]. The heterogeneity of these devices and protocols complicates the establishment of seamless and secure integration within IoT networks. Ensuring interoperability involves addressing compatibility across diverse hardware platforms and software standards, a task that requires the alignment of device communication methods and data formats. Moreover, the need for secure interactions further complicates interoperability, as each device and protocol may implement security measures differently, potentially leading to vulnerabilities at the points of interaction. This diversity

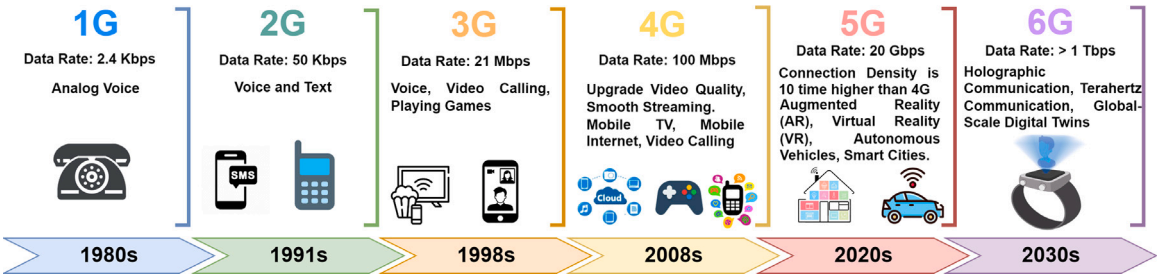

Fig. 4. Evolution of 6G.

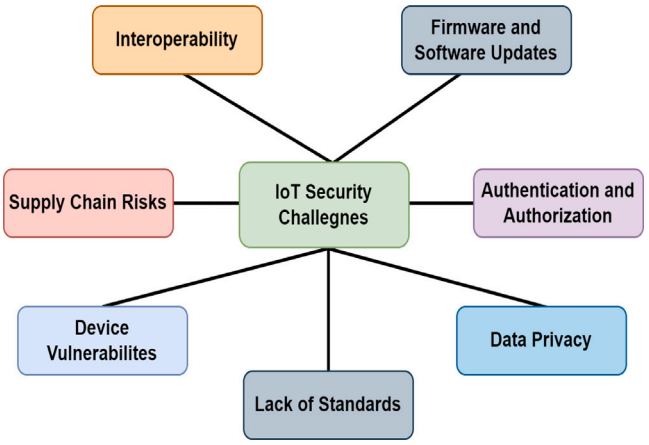

Fig. 5. IoT Security Challenges.

demands a robust framework for protocol translation and security policy enforcement to facilitate the safe and efficient operation of interconnected devices. Achieving such interoperability is crucial for realizing the full potential of IoT applications, necessitating ongoing technical efforts to develop universal standards and protocols that can accommodate the vast and varied landscape of IoT devices.

2.3.2. Device vulnerabilities

The IoT significantly expands digital connectivity, linking a vast array of devices within extensive networks. This expansion, however, introduces substantial security challenges, notably due to the varied capabilities of IoT devices and their inherent vulnerabilities [7]. Many IoT devices operate with limited computational resources, which, while promoting energy efficiency and cost-effectiveness, also limit the implementation of comprehensive security measures directly on the devices [7]. Advanced encryption methods, for example, may be too resource-heavy for numerous IoT devices, leading to a scenario where high-standard security features are not universally implementable. Manufacturers face the challenge of balancing these constraints with the necessity for adequate security. Security feature prioritization across the IoT spectrum is influenced by several factors, including device use purpose, cost, and the risk level associated with the device's data or operational context. In instances where devices are designed to be cost and energy-efficient, security features may be minimal, especially in applications deemed to have a lower risk of security breach. Nevertheless, securing IoT devices against breaches and attacks is critical [22]. Networks connecting these devices often incorporate additional security layers to counteract device-level vulnerabilities. These measures include network encryption, secure bootstrapping, and periodic software updates to patch identified security flaws.

2.3.3. Authentication and authorization

Authentication and authorization present significant challenges within the IoT realm. Authentication is the process of verifying a device or user identity. The diverse nature of IoT devices, which range from basic sensors to sophisticated gateways with differing security capabilities, makes the authentication of a device or user—more difficult. However, authorization defines what resources or actions within an IoT network credentialed entities can access. It is difficult to create strong authorization policies because of the dynamic nature of IoT environments and the requirement for fine-grained access control [6].

2.3.4. Data privacy

The enormous volume of data created and shared by networked devices is a serious barrier to data privacy in the IoTs [6]. Its devices gather private data about people and organizations. These devices can be anything from industrial sensors to smart household appliances. The variety of devices and communication protocols, sometimes insufficient security measures, and the sheer amount of data gathered make it difficult to ensure the privacy of this data [7].

2.3.5. Supply chain risks

Regarding IoT, supply chain risks are possible weaknesses and attacks that might jeopardize the dependability and security of IoT devices and the data they produce throughout their whole supply chain trip. These issues are especially important as IoT components frequently come from different manufacturers and vendors; therefore, resolving these risks is essential to guaranteeing IoT systems' overall security and quality.

2.3.6. Lack of standards

The development of IoT technologies is marked by rapid innovation and diversification, leading to a vibrant but fragmented landscape of devices and systems. One of the critical hurdles in this domain is the absence of universally established standards and protocols, which complicates the seamless integration and secure communication among devices from different manufacturers [34]. While many IoT-enabled networks strive to implement standards and protocols to ensure device interoperability, the reality is that the IoT ecosystem is too varied and evolves too quickly for a single set of standards to cover all aspects effectively. Devices are designed with certain standards in mind, but the fast pace of technological advancements and the broad spectrum of applications often outstrip these efforts, resulting in disparities in device compatibility and security protocols. This lack of uniform standards does not stem from an oversight but reflects the inherent challenges in standardizing an ecosystem as diverse and dynamic as the IoT. Efforts to establish and adopt global standards are ongoing, with industry groups, standardization bodies, and IoT communities working towards frameworks that can enhance security, data consistency, and interoperability across the ecosystem.

2.3.7. Firmware and software updates

Maintaining up-to-date firmware and software is critical for IoT device security. However, the geographical dispersion and often remote or physically inaccessible locations of these devices pose significant challenges for timely security updates and patches. Devices situated in

hard-to-reach areas may experience delays in receiving updates, leaving them vulnerable to newly identified threats for extended periods. This issue is compounded by the diverse nature of IoT ecosystems, where devices may operate on different update schedules and protocols, complicating the synchronization of updates across the network. Technical strategies to address these challenges include the implementation of over-the-air (OTA) update mechanisms, which allow for remote transmission and installation of updates without the need for physical access. Nevertheless, ensuring the reliability and security of OTA updates, particularly in constrained network environments or over limited bandwidth connections, requires sophisticated update management systems. These systems must support differential updating techniques, where only the changes between software versions are transmitted to minimize data transfer, and robust authentication protocols to prevent the introduction of malicious firmware. Effective management of firmware and software updates in remote IoT devices is essential, demanding innovative solutions to safeguard against security vulnerabilities while accommodating the logistical constraints of widespread IoT deployments.

2.4. Cyber attacks in IoT

The IoT has transformed the digital ecosystem by interconnecting billions of devices worldwide, from household appliances to industrial sensors [2]. This interconnectedness, while enabling a multitude of innovative applications, also exposes numerous vulnerabilities to cyber-attacks. IoT devices, often constrained by limited processing capabilities and prioritizing cost-efficiency over security, present attractive targets for cybercriminals [4]. Due to their ubiquitous nature and integration into critical processes, these devices can have far-reaching implications when compromised. We have discussed a few prominent attacks with their commonly used launch mechanism below:

2.4.1. Denial of service (DoS) attack

A Denial of Service (DoS) attack targets the availability of IoT devices or networks by overwhelming them with a flood of unsolicited requests [5]. This attack mechanism exploits the limited processing power and bandwidth inherent in many IoT devices, rendering them incapable of serving legitimate requests. DoS attacks can be launched through various means, including direct attacks from a single source or distributed attacks (DDoS) where the attack originates from multiple sources, complicating detection and mitigation efforts [8]. Vulnerabilities in network protocol implementations and insufficient rate-limiting measures on IoT devices often leave them exposed to such attacks.

2.4.2. Phishing attack

Phishing attacks in the IoT context often target the human element, deceiving device users or network administrators into disclosing sensitive information such as login credentials or network access keys [35]. Attackers launch phishing campaigns through seemingly trustworthy emails or websites, exploiting user awareness and security education vulnerabilities. These attacks are particularly effective in environments where IoT device authentication processes are tied to user-managed credentials, allowing attackers to gain unauthorized access to the network and connected devices.

2.4.3. Cross-site scripting (XSS)

Cross-site scripting (XSS) attacks are executed by injecting malicious scripts into web pages accessed by users of IoT management platforms. Once injected, these scripts can perform unauthorized actions on behalf of the users, such as data theft, session hijacking, or device control [36]. XSS attacks exploit vulnerabilities in web applications that fail to sanitize input from users or external sources properly. IoT ecosystems are particularly vulnerable to XSS attacks due to the reliance on web-based interfaces for device management and data visualization. Improper input validation and inadequate web application security measures expose these platforms to potential XSS exploits.

2.4.4. Radio frequency identification (RFID) spoofing

RFID Spoofing involves the unauthorized replication and transmission of RFID signals to impersonate legitimate RFID tags. Attackers use this method to bypass security measures in systems that rely on RFID for identification and access control, such as entry systems or inventory tracking in the IoT ecosystem [37]. The attack mechanism leverages the simplicity of many RFID communication protocols, which lack robust authentication and encryption processes. By mimicking the RFID signal of a legitimate tag, attackers can gain unauthorized access to secured areas or perform illicit operations within an IoT network. Vulnerabilities exploited in RFID Spoofing include weak or nonexistent cryptographic measures in the tag-reader communication process, allowing attackers to clone or simulate RFID tags without detection easily. Furthermore, many RFID systems do not implement measures to verify the physical proximity of the tag, making it possible for spoofed signals to be transmitted from a distance, increasing the attack's feasibility.

2.5. Intrusion detection system in IoT

An Intrusion Detection System (IDS) serves as a security mechanism, primarily functioning at the network layer within an IoT system [8]. For optimal performance in an IoT setting, an IDS deployed swiftly evaluates and responds to data packets, comprehends data across various layers and protocols in the IoT network, and remains compatible with the diverse technologies in the IoT environment [38]. Given the unique demands of IoT-based smart environments, they have minimal processing resources, quick response times, and handle large data volumes. Therefore, conventional IDSs might not be the best option for the IoT environment. There are various types of IDS that can be employed in IoT environments, each with its own mechanism for monitoring and protecting the network. The four primary types of IDS in the IoT are given below:

2.5.1. Signature-based IDS

The signature-based IDS is a security system used in IoT to detect threats by comparing network data against a database of known attack patterns, or "signatures" [38]. The IDS has a database known as threat signatures, which are patterns or characteristics of known malicious activities. The database is like a catalog of virus attacks in antivirus software, while the system continuously monitors the data passing through an IoT network, which includes incoming and outgoing traffic from various IoT devices like sensors, cameras, or smart appliances. For example, if an incoming data packet matches the signature of a known malware, the IDS will recognize it, while when the thread matches the signature database, the IDS generates alerts to notify administrators of the potential threat. Depending on the system setup, it may also take automatic actions to block suspicious activity.

2.5.2. Network-based IDS (NIDS)

In the context of IoT, a network-based IDS (NIDS) is a security tool that monitors all the network traffic of IoT devices for threats [38]. NIDS checks the data in the IoT network to identify signs of attacks or malware. If NIDS detects something unusual, it alerts network administrators about a potential security issue. NIDS is often deployed in critical network areas to monitor as much traffic as possible, similar to security cameras at major intersections, which is crucial in IoT networks with numerous devices. NIDS is effective for detecting known threats but may not be effective against new types of attacks.

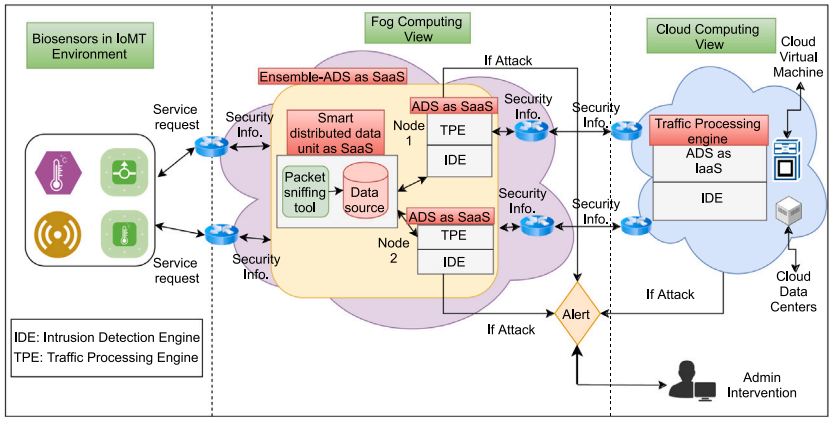

Fig. 6. Ensemble learning and fog–cloud architecture-driven anomaly-based IDS for Internet of Medical Things [40].

2.5.3. Host-based IDS (HIDS)

HIDS is a security mechanism that performs analysis and monitoring of a computer system's internals at the host level. Unlike NIDS, it acts directly on the host computer, scrutinizing actions like file accesses, system calls, and log entries, while NIDS concentrates on monitoring network traffic. Its core objective is to identify and handle security incidents that take place in the host environment [39]. A HIDS is essential to improving a system's overall security posture since it offers real-time monitoring and analysis of host actions. It aids in the early identification of security problems, enabling prompt action to reduce the effect of security breaches and mitigate any potential risks.

2.5.4. Anomaly-based IDS

Anomaly-based IDS (AIDS) was designed to address the limitations of signature-based IDS. In the initial training phase, AIDS establishes a model outlining the system's standard behavior. Once the IDS is deployed, it observes computer hosts and checks their activities against the nominal one. If the behavior significantly differs from the model, the IDS may trigger an alert. The approach allows AIDS to detect new, unknown attacks because it does not rely on pre-defined attack signatures [41]. Anomaly-based IDSs are categorized into three types based on their mechanism and detection methods: statistics-based, knowledge-based, and machine learning-based. Statistics-based and machine learning-based IDSs develop a model of typical host behavior, whereas knowledge-based systems focus on identifying anomalies in system data, like network protocols, guided by inputs from system administrators. For example, [40] proposed an ensemble learning and fog–cloud architecture-driven anomaly-based IDS for the Internet of Medical Things (IoMT) as shown in Fig. 6. The underlying approach combined machine learning algorithms using "stackingCVclassifier" to detect intrusions.

2.6. Federated learning (FL): An overview

FL is an ML technique that decentralizes the model training process and tackles privacy issues. Data collection and transmission to a central server for model training is common in classical ML. On the other hand, FL flips this paradigm by allowing model training to take place locally on servers or devices without requiring raw data to be sent outside those devices [42]. The Global Model (GM) is initialized on a Central Server (CS) to start the procedure. The learning process begins with this GM. The FL makes use of a variety of local device datasets rather than depending on a centralized dataset. The model is separately trained on each device using its local data, preventing sensitive data from being exposed to external servers and staying on the device. After combining the model updates it has received, the CS modifies the GM to take into account the combined knowledge of all involved devices. This iterative process delivers The modified GM back to local devices. Every time a model iteration is performed, the model gains from each dataset's many viewpoints. Furthermore, FL greatly reduces the quantity of data that must be communicated across the network by focusing only on the model changes. In situations when bandwidth is expensive or scarce, this method clearly excels. The schematic architecture of an FL system is shown in Fig. 7.

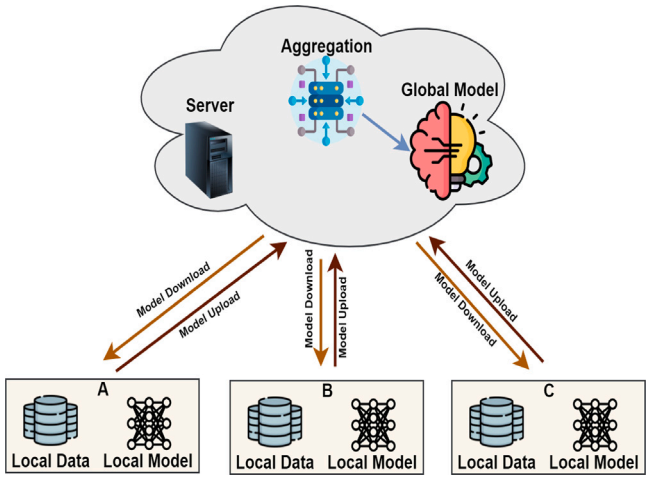

Fig. 7. Schematic Architecture of a Generic FL System.

2.7. Integration of quantum computing in 6G networks and FL for IoT security

With the advent of 6G networks quickly approaching, the telecom sector is investigating novel technologies to improve communication capacities. Integrating quantum-assisted communication protocols is one exciting area of research that uses the ideas of quantum mechanics to transform data transfer and security. Some key concepts are as follows: *(i) Quantum Superposition in Data Transmission (QSDT):* Multi-state simultaneous existence of Quantum Bits is made possible by quantum superposition. This might be used to send numerous data packets simultaneously, which could boost 6G network data transfer speeds. *(ii) Quantum Key Distribution (QKD):* QKD is, a quantum communication technique that secures communication channels by utilizing quantum features [14]. It might be used in 6G networks to allow for the safe exchange of encryption keys between parties, improving data transfer security. *(iii) Quantum Repeaters for Long-Distance Communication (QRLDC):* The purpose of Quantum Repeaters (QR) is to increase the long-distance capability of quantum communication. QR might be included in 6G networks to facilitate secure and smooth communication

over large geographic areas. *(iv) Quantum Entanglement for Teleportation (QET):* Particles can be associated by Quantum Entanglement (QE), regardless of their distance from one another, such that the state of one particle directly affects the state of another. This feature may be used to quantum teleport information, allowing 6G networks to transport data more quickly and effectively.

Furthermore, in the context of FL and IoT, utilizing quantum concepts can offer creative ways to handle the security and efficiency of communication concerns. For example, data is protected during transmission because of QKD's ability to create unbreakable encryption keys. By including QKD in the channels of communication used by FL and IoT devices, the risks of data breaches are reduced and sensitive information is kept private. Further, entanglement facilitates instantaneous quantum information transmission between far places via quantum teleportation. This technique may be used to maximize transmission efficiency when aggregating data from geographically scattered devices in FL settings. Moreover, IoT devices may be made more capable by using Quantum Sensors (QS), which make use of quantum features to provide extremely accurate measurements. QS can enhance the efficiency and dependability of IoT data in applications such as smart cities, healthcare, and environmental monitoring by offering previously unheard-of levels of precision.

3. Navigating challenges in federated learning for IoT security: Quantum and 6G perspectives

3.1. Scaling federated learning in massive IoT networks

In recent years, the fusion of AI and ML has ushered in a new era for the intelligence of massive IoT networks. Conventional methods involved centralizing the learning process at a single location, raising concerns about data sharing in potentially insecure environments and privacy issues. The introduction of FL has transformed this landscape, moving the AI functions from the data center to the network edge, involving a multitude of IoT devices to collaboratively train a globally shared model [43]. FL enables on-device learning, minimizing the need for extensive data transmission and preserving data privacy. This privacy-preserving paradigm opens new horizons for massive IoT networks such as smart cities, digital healthcare, and intelligent transportation, allowing for collaborative learning [44].

However, it becomes imperative to understand the novel challenges posed by the scale of these IoT networks. Scaling FL in massive IoT networks introduces distinctive hurdles, including system and data heterogeneity, communication overhead and latency, and the need for efficient strategies to ensure scalability while preserving security [45]. As the number of IoT devices participating in FL collaboration grows exponentially, the complexity of managing diverse computational capabilities and data types amplifies. This introduces a significant challenge in fostering effective collaboration within a FL environment. Moreover, communication overhead and latency become critical concerns, given the large sizes of data exchanged and the iterative nature of the learning process. Optimizing these aspects is crucial for maintaining efficient operations while upholding security standards. In addressing these challenges, an adaptive approach that accommodates the unique characteristics of massive IoT networks is essential to unlock the full potential of scalable and secure FL.

3.2. Managing heterogeneity in IoT devices and data

The participation of edge devices in the FL training process may vary from hundreds to millions in numbers, for instance, in the context of training a learning model for IoT application in the federated network might have millions of devices. However, the performance capabilities of those edge devices may vary with respect to their hardware specifications, such as computational power, memory, battery lifetime, and network connectivity [23,46]. It is highly likely that some devices may show diverse behavior due to system-related constraints, e.g., limited computation, low battery power, idle status, etc. As a consequence, participant devices become unreliable and can be dropped out at any time, leading to unequal participation and exerting great influence on the collaborative learning process of a global model, such as unreliable edge devices in a federated network called stragglers. System heterogeneity further exacerbates the challenges in FL. Several studies devised distinct methods, such as asynchronous communication by [47] to mitigate the effect of stragglers by robustly dropping out unreliable devices in the federated network. In [48], the authors proposed an adaptive client sampling algorithm in FL to minimize wall-clock convergence time by addressing system heterogeneity. Furthermore, the local performance of the predictive models also plays an important role, and the FL has the capability to improve the performance of these models [49].

3.3. Ensuring privacy preservation and mitigating data leakage risks

The primary goal of FL in large-scale IoT networks is to enable collaborative model training without compromising the privacy of individual device data. FL offers distinctive privacy advantages compared to centralized approaches, where the possession of even an "anonymized" dataset at an aggregation server poses risks to the privacy of devices in the network. Despite not explicitly sharing raw data, FL must address the risk of adversaries reconstructing the original data, especially in scenarios lacking complete protection for architecture and parameters [11]. Moreover, FL introduces potential privacy vulnerabilities through the exposure of intermediate results, such as parameter updates from optimization algorithms like stochastic gradient descent (SGD). The transmission of these gradients may inadvertently reveal private information, particularly when interacting with data structures like image pixels. Recent studies, such as [51], highlight the critical need for robust protection of parameters in FL design within the context of large-scale IoT networks. Additionally, the presence of malevolent devices in the FL environment can introduce additional security challenges, emphasizing the ongoing necessity for advancements in parameter protection in the FL framework for large-scale IoT deployments. Similarly, [50] proposed a deep privacy-encoding-based FL framework named PEFL, as referred to in Fig. 8. This approach adopts a perturbation-based encoding and long short-term memory-autoencoder technique to achieve the target of privacy and FL-based gated recurrent unit neural network for intrusion detection in IoT-based smart agriculture. Additionally, Human-centered AI can play an important role in smart agriculture. It can improve productivity and sustainability while also enhancing resource management and crop yields. The authors in [52] provided complete details about the security challenges and the future directions of Human-Centered AI for smart agriculture.

To mitigate the privacy and data leakage risk during the FL training process, each device can deploy some privacy-preserving technologies, including:

3.3.1. Differential privacy in FL

Differential Privacy The idea of Differential Privacy (DP) within FL [53] involves introducing controlled noise to perturb model parameters uploaded by edge devices. The primary goal is to obscure sensitive attributes, preventing a malicious server from distinguishing individual contributions and ensuring the impossibility of restoring the data, thereby safeguarding the privacy of edge devices. However, it is essential to acknowledge that the DP method introduces a trade-off between accuracy and privacy, necessitating careful adjustments to strike an optimal balance.

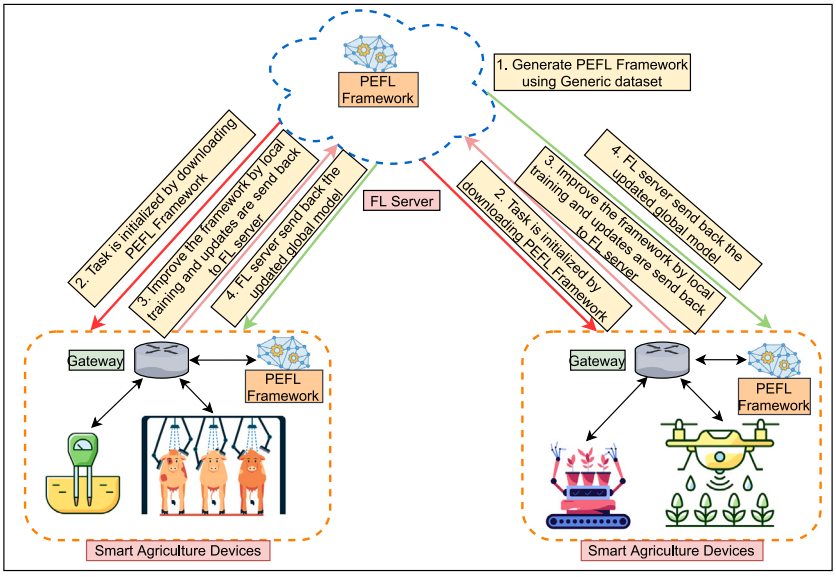

Fig. 8. Deep privacy-encoding-based FL framework for Smart Agriculture [50].

3.3.2. Secure multi-party computation (SMC) in FL

The essence of Secure Multi-Party Computation (SMC) lies in using encryption to protect individual device updates from scrutiny by the server. Rather than revealing each device's update, SMC ensures that only the aggregated sum is disclosed after a predefined number of updates [54]. This cryptographic protocol operates through a four-round interactive process, potentially activated during the training process's reporting phase of a specific communication round. In each round, the server gathers messages from all edge devices, utilizing these messages to compute an independent response, which is then returned to each respective device. During the first step, which is referred to as the Initialization step, all participants are verified and prepared for secure interactions as the server and edge devices exchange cryptographic keys and parameters to create a secure communication foundation. The server then gives edge devices, which carry out local computations, tasks, or models to complete during the second phase called the Distribution Phase. In order to enable collective model updating while maintaining security and privacy, devices prepare their encrypted changes for safe transmission back to the server. The third round, known as the commit phase, entails devices uploading model updates that are cryptographically masked to the server. Subsequently, in the finalization phase, devices reveal sufficient cryptographic secrets, enabling the server to unveil the aggregated model update. This process ensures robust privacy protection, establishing SMC as a critical component in safeguarding the confidentiality of model updates in FL scenarios.

3.3.3. Dummy approach for FL

The dummy approach, inspired by location privacy protection measures [55] can be used in FL to protect the edge device privacy during the FL training process. In this approach, dummy model parameters can be uploaded to the server along with true model parameters to conceal the contribution of an individual device during the training process. The aggregation process at the server ensures that system performance is maintained and guaranteed.

3.4. Guarding against model and data poisoning attacks

In FL, ensuring the integrity of the global model requires a careful examination of the potential threats posed by model and data poisoning attacks [56]. Model-stealing attacks represent a significant concern in the FL framework, where any rogue device may endeavor to embed hidden backdoor functionality into the shared global model, e.g., an attempt to ensure that the image classifier assigns specific labels to images chosen by the attacker with specific features, or in the context of natural language processing tasks, an attacker might seek to influence a word predictor to complete sentences according to their malicious intent. In response to these potential threats, robust security measures at the architectural level of FL become imperative. To further enhance the security of FL models, exploring and implementing effective countermeasures is essential. Understanding and addressing the nuances of poisoning attacks can strengthen the FL framework, ensuring a resilient defence against adversarial manipulations. Various protective measures can be implemented in the security design for FL, including:

3.4.1. Back-door defender

FL in IoT networks faces a notable threat from backdoor attacks, where malicious devices aim to embed covert functionalities into the shared global model. These attacks involve introducing subtle manipulations into the training data or model parameters, influencing the behavior of the model in unintended ways [57]. FL's susceptibility to backdoor attacks arises from its collaborative nature, allowing edge devices to contribute to the training process actively. The decentralized and collaborative framework of FL makes it challenging to detect and mitigate these attacks effectively [58]. To mitigate backdoor threats, a robust backdoor defense strategy should be adopted, it includes measures such as rigorous model verification [59], adversarial training, anomaly detection, robust aggregation protocols, specialized backdoor detection algorithms, and secure model initialization [60]. Integrating these strategies enhances the resilience of FL models in IoT networks, safeguarding against potential backdoor attacks and preserving the integrity of the collaborative learning process.

3.4.2. Homomorphic encryption

Homomorphic encryption (HE) in FL [61] is implemented to enhance the security of edge device data during parameter exchange. In this approach, first, model parameters are encoded before uploading to the server for aggregation, and then Both the public and private decoding keys are required for transmission. However, the adoption of homomorphic encryption introduces an additional communication cost [62]. For large-scale IoT networks, HE becomes crucial in preserving the privacy of edge device data, especially during the exchange of sensitive parameters. While it provides a robust security layer and mitigates data exposure during the training process, the associated

increase in communication cost emphasizes the need for efficient and optimized protocols to ensure the scalability and practicality of the FL framework in IoT networks [11].

3.5. Navigating resource constraints on IoT devices

The term "Resource-Constrained" is used to describe the availability of limited resources. The resource-constrained nature of IoT devices indicates small devices with less computation power, storage, and processing units [32]. To effectively collaborate in the FL-based models, the devices must be compatible enough to interact and process with standard mechanisms [63]. However, IoT devices sometimes suffer from severe concerns that hinder their way to shaking hands with FL approaches. The first major challenge is communication overhead. As these devices come with limited computation resources, their processing units cannot combat the continuous working overhead in FL models. As a result of this, the IoT device may partially or fully malfunction, causing a disturbance in the entire working chain [64]. The FL welcomes the training stage on multiple devices, which may be from different product generations. As a result, a network of disparate devices with varying capacities for memory, processing power, and battery life is created. Therefore, the duration of training may vary considerably between clients making it an inappropriate approach to evaluate all participants using the same scale [65]. There are two main categories into which this training phase may be divided: synchronous and asynchronous training. Talking about the synchronous training phase, a certain number of clients perform a task in each iteration. The server needs to wait until enough clients respond due to device or network issues. If such problems occur for a long time, the server skips that epoch and moves toward the next iteration [66]. In contrast, the asynchronous training pattern allows FL participants to send gradients directly to the FL server after each local update, whereas synchronous FL optimization does not permit this. While running an FL process, it is essential to schedule the training phase that the participants will go through referred to as scheduling. In the case of resource-constrained consumer devices, and when frequent interaction with the server uses up more resources, scheduling becomes an explicitly important consideration. Optimal scheduling may result in several advantages such as less energy consumption and reduced bandwidth [67].

3.6. Integrating quantum computing and federated learning

FL security might be greatly improved by QC through numerous aspects. One key feature is that quantum computers can do complicated calculations tenfold quicker than traditional computers. This may be used to fortify encryption systems. Due to the decentralized nature of data across several devices in FL, privacy and security become crucial problems [68]. QC can improve its security by developing cryptographic approaches like Post-Quantum Cryptography (PQC). In contrast to conventional cryptographic algorithms that may be susceptible to quantum computer attacks, PQC makes use of mathematical structures that are considered to remain secure even when strong quantum algorithms are present [69]. Consequently, FL systems can protect device-to-device data exchanges against future quantum attacks by employing PQC techniques. Furthermore, QC can improve the security of FL systems using QKD. It uses the ideas of quantum physics to make it possible for parties to exchange encryption keys in a secure manner. Theoretically, an eavesdropper cannot intercept the quantum key without being detected due to the intrinsic features of quantum systems, such as the uncertainty principle and the no-cloning theorem. By incorporating QKD into FL protocols, the overall security of the FL system can be strengthened by ensuring a more reliable and secure key exchange procedure [70]. Moreover, the idea of quantum-resistant algorithms, which can fend off attacks from both classical and quantum computers is also introduced by the QC. The integration of quantum-resistant algorithms into FL systems helps anticipate and mitigate security risks that may arise from the development of highly potent quantum computers. This proactive strategy guarantees that FL security will withstand new technology developments. The integration of QC into FL can enhance the overall security of the IoT systems. However, it poses several challenges, ranging from practical and technological considerations. Some of the key challenges are as follows: **Challenges:** The following are some of the key challenges: *Quantum-Safe FL Protocols:* Quantum-safe protocols must be developed and integrated in order to guarantee the security of FL in a QC environment. Quantum attacks may potentially exploit traditional cryptography methods. *Interoperability and Standards:* It can be difficult to establish compatibility between various IoT devices and QC platforms because each has its own hardware and communication protocols. *Quantum Resource Constraints:* Currently, extremely low temperatures and carefully regulated settings are necessary for quantum computers. Given the constraints on size, power, and environmental conditions on IoT devices, integrating quantum capabilities into such devices may be difficult. *Scalability and Communication Overheads:* FL requires inter-device communication, and as the number of IoT devices rises, scalability problems with the quantum entanglement that permits quantum communication may arise.

3.7. Leveraging 6G networks for federated learning in IoT security

In the current era of 5G networks, FL within the IoT ecosystem grapples with a set of challenges that requires a paradigm shift toward the next generation of 6G networks. The limitations of 5G, including limited data rate and higher latency, pose significant hurdles for the seamless operation of FL models in massive IoT networks [71]. The restricted bandwidth and increased latency in 5G networks impede the swift exchange of model updates between edge devices and aggregation servers, potentially compromising the real-time efficiency and reliability crucial for IoT applications e.g. a minor delay in the intelligent transportation system can result in unfavorable situations. Furthermore, security concerns within the 5G infrastructure demand enhanced measures to safeguard the privacy and integrity of data transmission during FL processes. These challenges underscore the need for a more advanced and capable network infrastructure. Next-generation 6G networks, anticipated as the next evolutionary step, promise to address and overcome the limitations inherent in 5G. With unprecedented data transfer speeds and reduced latency, 6G networks are poised to play an indispensable role in addressing challenges and enhancing the security of FL within the IoT ecosystem. As the next generation of wireless communication technology, it brings forth specific capabilities that contribute significantly to the efficiency and reliability of FL implementations. The capabilities of next-generation 6G networks are as follows:

3.7.1. Ultra-fast data rate

One notable aspect is the potential for increased data transfer speeds in 6G networks, one of the crucial Key Performance Indicators (KPIs) for evaluating network performance. It is anticipated that the data rate of 6G networks will surpass 1 Tbps, marking a more than 50 times increase compared to current cellular technology, a substantial improvement in the data transfer speeds. This remarkable enhancement in data rates, referred to as Massive Enhanced Mobile Broad Band (meMBB) in 6G [17], is essential for the FL training process. The ultra-fast data rates of 6G networks facilitate quicker and more efficient communication between edge devices and aggregation servers, thereby alleviating issues associated with prolonged communication overhead. Furthermore, ultra-fast data rates in 6G could also contribute to reducing the time required for FL model training, enabling quicker convergence and improving overall efficiency. In essence, 6G, with its impressive KPIs, contributes significantly to improving the overall performance of the FL process in large-scale IoT networks.

3.7.2. Ultra-PlusPlus-reliability

The reliability and connectivity enhancements introduced by 6G networks, utilizing advanced technologies like mobile broadband reliable and low latency communication (MBRLLC), are poised to effectively address issues, i.e., latency problems in FL. With 6G's commitment to achieving unprecedented reliability levels exceeding ≥99. 99999%, marking a ≥100 times improvement compared to its predecessor [72]. Thus, the challenges associated with the exchange of model updates are significantly mitigated and result in a more robust and timely collaborative learning environment, underscoring its transformative capabilities in shaping the future of FL for massive IoT networks. Moreover, ultra-plusplus-reliability can enhance the security of FL by ensuring the integrity and privacy of model updates and communication in scenarios where security is critical.

3.7.3. Edge-native intelligence

6G networks facilitate the integration of edge intelligence, enabling edge devices to process and analyze data locally [73]. This capability reduces the need for transmitting large volumes of raw data to central servers, addressing bandwidth constraints and enhancing privacy. In the context of FL, edge intelligence can be leveraged to perform initial model training and inference locally, minimizing the amount of sensitive information transmitted over the network [21]. This decentralized approach enhances security and efficiency in FL implementations.

3.7.4. Dynamic network slicing

Dynamic network slicing is a key capability of 6G [74], enable the creation of isolated and customizable network segments for specific FL applications. This slicing capability ensures dedicated resources and optimal performance for FL services. For example, a network slice can be configured to prioritize FL model training traffic, guaranteeing high data transfer speeds and low latency. Dynamic network slicing enhances the overall reliability and efficiency of FL processes in large-scale IoT networks.

3.7.5. Quantum-safe cryptography

The advanced security features of 6G networks are another critical factor. Considering the evolving landscape of cybersecurity, 6G networks incorporate quantum-safe cryptography to protect against potential threats from quantum computers [18]. This advanced encryption ensures the long-term security of FL communications in IoT networks. Quantum-safe cryptography algorithms, resistant to quantum attacks, contribute to the resilience of FL implementations, safeguarding sensitive information exchanged during collaborative learning.

4. Existing strategies and approaches to overcome challenges

In this section, we provide complete details about the current strategies and approaches of quantum computing to overcome the challenges faced by federated learning for IoT security.

4.1. Quantum-enhanced aggregation algorithms for heterogeneity

While designing an FL-enabled threat detection approach, the aggregation algorithm is considered an integral element as it vividly plays a significant role in accumulating the local model updates transmitted from local nodes to the CS. In the case of widely expanded IoT networks containing a diversified variety of heterogeneous devices, the algorithm must be capable enough to cope with the heterogeneity challenges. The array of such challenges comprises of non-identical distribution of data, non-uniform traffic flows, limitations in computational resources of devices, diverse network conditions, communication overhead, and many more [82]. Quantum computing offers substantial insights to overcome such challenges by leveraging the domain with state-of-the-art methodologies to strengthen the accumulation mechanism of FL-oriented aggregation algorithms. The core charisma is embedded in the execution architecture of quantum computing in the form of a superposition phenomenon that enables quantum bits to exist simultaneously in multiple states. The implementation of this superposition property in the aggregation algorithm clearly empowers quantum computers to monitor all the heterogeneous traffic streams with diversified models. This process supports a synchronized supervision of multiple local model updates. It provides a smooth pathway to enforce aggregation standards along with the model-update checks, leading toward more comprehensive aggregation strategies [75].

Quantum entanglement is another consequential property of quantum computing that ensures logical correlation between the qubits, ignoring the distance among them. The integration of quantum entanglement with the aggregation algorithm is another remarkable assistance that contributes towards improving the aggregation mechanism of the algorithm. It enables the aggregation algorithm to maintain a highly logical correlation among the model updates originating from the heterogeneous devices, resulting in more authentic and accurate updates in the global model [12]. This technique also performs notably well in swear scenarios where the local devices are equipped with different datasets, causing a hectic task for the aggregation algorithm to align the segregated model updates into an assembled one. There are multiple other aspects where quantum computing enhances the potential of FL by yielding an appropriate framework to cope with the managerial challenges caused by heterogeneous devices and different data types. Quantum computing is leveraged with distributed computing properties, enabling efficient computations of processes streaming at various ends of the network. It also supports mutual coordination among such assorted spaces of processes, mitigating the negative influence of heterogeneity among large-scale IoT networks [76].

4.2. Communication optimization strategies in quantum federated environments

Communication optimization is an indispensable aspect heading toward exceedingly responsive FL systems with reduced communication overhead, negligible latencies, less consumption of system resources, better communication quality, etc. Quantum computing has the potential to intensively invigorate FL environments by furnishing a generous framework for efficiently optimized communication architecture. Quantum-inspired algorithms boosted with superposition property are capable of compressing big-sized conventional messages and representing them in different states at the same time. Such integration directly reduces communication overhead, making communication more responsive, robust, and durable. Quantum-empowered algorithms can also systematically configure the communication pathways to design an appropriate and optimized communication channel in FL-oriented systems [77]. Such phenomenal practices return appreciable outcomes such as unnecessary occupancy of transmission channels, shorter latencies, vigorous communication, etc.

The FL-oriented security approaches designed for IoT networks more frequently suffer from complex computations demanding proportionate computational resources. While dealing with diversified local model updates transmitted from heterogeneous devices having different datasets, the circumstances become more uncongenial, triggering the need for proper countermeasures to be taken. Quantum principles tackle such situations by offering edge-computing optimization techniques that make the system resources synchronized and aligned for certain communicational objectives [83]. It further reduces superfluous communication overhead, allowing a plain computational space to return more productive outcomes. Quantum-oriented algorithms are privileged with quantum error correction techniques capable of correcting communication errors by drawing a logical correlation among the heterogeneous traffic flows containing local model updates. This process alleviates the demand for data redundancy, reducing communication overhead and unnecessary burden on system resources [78].

Table 2
Impact of quantum principles on federated learning.

Ref	Quantum Principle	How it Works?	Impact on FL	Advantages
[75]	Superposition	Quantum bits simultaneously exist in multiple states	Aggregation algorithms at CS can be improved	The CS can simultaneously monitor all the segregated traffic streams.
[12]	Quantum Entanglement	It ensures a logical correlation between the quantum bits	Local model updates can be analyzed at the CS	The logical correlation between the local model updates can reduce the possibility of error to improve communication quality.
[76]	Parallel Computing	It maintains synchronized computations among diversified nodes	The heterogeneity among the local nodes can be overcome	The heterogeneity among the local model updates can be uniform.
[77]	Quantum Optimization	Capacious data volumes are compressed	Optimized communication between CS and the local nodes	It can provide smooth execution on extensive data and can also perform balanced configuration on different datasets for local model updates.
[78]	Quantum Algorithms	This property helps to optimize routing paths effectively	Optimized routing paths can reduce communication latencies	Robust communications, reduced communication overhead.
[79]	Quantum Tokenization	It allows secure privacy-preserving communication architecture	Secure communication can be established in FL systems	It enables secure feature extraction from the raw data. It also protects the identity of local nodes sharing data with the CS.
[80]	QSMPC	It enables local nodes to perform computations on encrypted data	Data encryption can lead to impressively secure communications	Data privacy can be achieved. It can also reduce the chances of data-related attacks.
[70]	QKD	This approach allows the safe distribution of keys	It may establish an encrypted gateway between the CS and edge nodes	It can protect the model updates being shared in FL-based systems.
[81]	Optimization Training	It effectively optimizes network entities to achieve specific objectives	The training processes in FL can be improved	The robust FL training can be maintained without overburdening the system resources.

4.3. Privacy-preserving quantum techniques for enhanced data protection

Quantum principles also perk FL approaches in privacy-preserving perspectives by introducing several meaningful and influential schemes. Starting with the Quantum Tokenization (QT) technique that permits secure feature extraction from the raw data precisely prohibits the exposure of sensitive content to heterogeneous edge nodes. The quantum principles are surprisingly competent to implement differential privacy strategies that stimulate CS to protect the privacy of individual nodes [79]. While integrating such schemes, the global model at the CS is dynamically updated without revealing the identification of participant nodes taking part in the updating process. The nodes provided with local data to generate the local model updates are supposed to hand it over to the CS for accumulation processes. Once the local model is updated, the identity of contributing nodes is anonymized, and outputs are shared with the CS, where the global model is updated by addressing the provided details.

In the cryptographic domain, whether they are symmetric or asymmetric, quantum algorithms will have a significant amount of impact on them. The quantum principles assure a meticulous communication infrastructure allowing parallel computations on encrypted data [84]. The end nodes can perform training on the encrypted data without accessing the plain data, ensuring an extraordinarily privacy-maintaining communication environment. The Quantum Secure Multi-Party Secure computation (QSMPC) is a majorly recommended technique adopted for this purpose [80]. The multi-facet computations on encrypted data safeguard the privacy of different data types used to generate local model updates. The quantum principles can also facilitate traditional FL systems by establishing an encrypted gateway to perform secure end-to-end communications. The QKD mechanism allows the safe distribution of communication keys between edge devices and the CS. Hence, it protects the local model updates transmitted to the central server, and the global model updates shared backward to end devices. It further lessens the probability of gateway attacks and data-oriented suspicious activities, e.g., sniffing, eavesdropping, and data breaching [70].

4.4. Robust model training in quantum-federated systems

Along with numerous other sustainable benefits, the quantum principle also influences the training mechanism of FL-inspired systems by reducing the computational complexities returning in productive outcomes, e.g., rapid training process, increased training quality, etc. FL mechanisms are sometimes susceptible to gradient descent challenges that hinder or partially slow the training process. Quantum computing legitimizes the training process by generically optimizing the hyperparameter used for the training process. This hyperparameter tuning may include optimizing learning rates, modifying the number of epochs, and variations in batch size. This integration boosted the model training processes without overburdening computational units. Quantum-based techniques tend to remodel the system configuration in challenging situations by aiding with an increasingly optimized communication infrastructure to sustain robust and delay-resistant training processes [81].

The prodigious strengths of quantum computing can also contribute towards the durability of FL by securing it against a multifarious cluster of security threats. The conventional FL models are vulnerable to two major attacking categories, i.e., data-concerning attacks and architectural-related attacks. The first category comprises eavesdropping, data sniffing, data breaching, false data injection, model inversion attacks, poisoning attacks, label flipping attacks, etc. Quantum principles grant the implementation of leading cryptographic techniques that bring forward the steady execution of FL training processes on

encrypted data and diminish the probable encounter with the mentioned data-related security challenges [85]. Quantum approaches upsurge optimization techniques in FL environments by formulating an admirable communication infrastructure to organize network entities intelligently. Once the framework is standardized, quantum methods deliver supervisory insights to regularize the communication infrastructure. This practice is regarded as an impactful choice to narrow the possibilities of architectural attacks such as routing attacks, backdoor attacks, and sybil attacks [86]. The impact of quantum principles on FL is also summarized in Table 2.

4.5. Energy-efficient strategies for constrained devices in 6G networks

In the futuristic realm of 6G networks, energy optimization in resource-constrained devices is undoubtedly a noteworthy research domain. Some imperative research approaches suggest considering the use of effective energy management strategies such as installing low-power hardware components, power switching techniques among participant nodes, etc. Designing energy-efficient communication protocols is another highly recommended scheme to regulate energy utilization in the system. This kind of protocol seeks to provide a sustainable energy-saving mechanism by effectively managing auxiliary communication streams and unnecessary bandwidth occupation. Some research studies also suggest adopting energy-efficient techniques to enjoy diversified energy benefits [87–89]. Energy optimization conceptualizes considering other sustainable and persistent energy-supply options, e.g., solar energy, kinetic energy, and economical thermal energy, rather than depending on traditional battery-powered technologies. In the context of FL networks, the advanced potential of 6G can progressively contribute to developing energy optimization techniques. The 6G communication patterns were designed to support maximized communication with advanced beamforming, high data rates, and ignorable latencies. In FL systems, this belief could improve the communicational efficiencies between the CS and edge devices to ensure an energy-efficient networking framework [21].

5. Quantum computing, federated learning and 6G in IoT security

This section presents a conceptual framework based on quantum-empowered FL and 6G for IoT security. It then provides a synopsis of the accessible public datasets and a range of performance metrics that play a vital role in the creation and evaluation of secure IoT infrastructures.

5.1. Proposed framework for securing IoT ecosystem

The field of IoT encompasses a broad spectrum of advanced technologies, meaning that no single reference architecture can adequately represent all potential implementations of a secure IoT ecosystem. However, this article uses 3 layered IoT architecture encompassing (i) End user layer; (ii) Mobile edge computing or processing layer and (iii) Centralized cloud server layer.

- **End User Layer:** This is the layer where the actual IoT devices reside. These devices, such as sensors, actuators, or smart appliances, collect data from their environment and perform actions based on instructions received. The data collected by these devices is sent to the Mobile Edge Computing Layer for further processing.
- **Mobile Edge Computing or Processing Layer:** This layer is responsible for processing the data collected by the end-user devices. It can involve tasks like data filtering, aggregation, and analysis. The goal is to reduce the amount of data that needs to be sent to the cloud, thereby reducing latency and bandwidth usage.

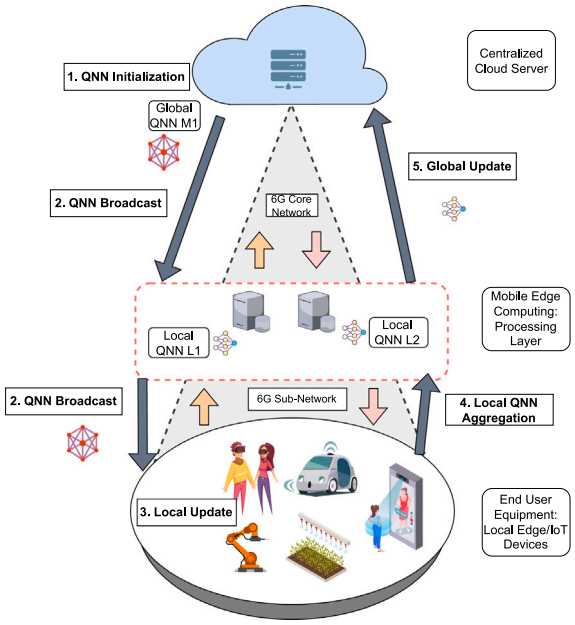

Fig. 9. Proposed conceptual framework based on quantum-empowered FL and 6G for IoT security.

- **Centralized Cloud Server Layer:** This is the layer where data is stored, managed, and further analyzed. It provides the computational power and storage capacity needed for advanced data analytics, machine learning, and other complex tasks. It also provides an interface for users to interact with the system, such as dashboards or APIs.

Fig. 9 presents the proposed conceptual framework based on quantum-empowered FL and 6G for IoT security. Once the gathered data from the end-user layer is forwarded to the mobile edge computing layer for further processing, the local Quantum Neural Networks (QNNs), L1 and L2, are used to process the data in an asynchronous federated learning manner. The processed data is then encrypted using homomorphic encryption to ensure data privacy and security. The encrypted data is then sent to the cloud server layer for further processing. This layer has a global QNN, m1, which is used to process the encrypted data received from the mobile edge computing layer. The data is decrypted using homomorphic encryption and then processed using the global QNN in an asynchronous federated learning manner. The entire process takes place within a 6G sub-network. There can be multiple such sub-networks, each handling a different set of IoT devices and data. The use of 6G sub-networks ensures efficient and secure communication between the various layers and components of the system. The asynchronous federated learning allows for decentralized and asynchronous learning across the local QNNs (L1 and L2) and the global QNN (m1), thereby improving the efficiency and effectiveness of the learning process. The use of homomorphic encryption ensures that data privacy and security are maintained throughout the process.

5.2. Datasets in IoT security research

In the realm of IoT security research, intrusion datasets play a pivotal role. These datasets, which record instances of unauthorized access or attacks on IoT devices or networks, are integral to various critical tasks such as vulnerability assessment, security testing, and the development of security solutions. (i) Vulnerability Assessment: Intrusion datasets provide a wealth of information about potential weak points in IoT systems. By analyzing these datasets, researchers can identify patterns of vulnerabilities, understand their root causes, and

Table 3
Overview of IoT-related attacks within network-based datasets [90–101].

DataSet	Attack Types
AWID [90]	Popular attacks on 802.11 (e.g., authentication request, ARP flooding, injection, probe request)
BoT-IoT [91]	DoS, DDoS, OS Fingerprinting, Service Scanning, Data Ex-filtration, Keylogging
ToN-IoT [92]	backdoor, injection, Distributed Denial of service (DDoS), ransomware, password, scanning, Man in the middle (MITM) and cross-site scripting (XSS)
CICIDS 2017 [93]	Botnet (Ares), cross-site-scripting, DoS (executed through Hulk, GoldenEye, Slowloris, and Slowhttptest), DDoS (executed through LOIC), heartbleed, infiltration, SSH brute force, SQL injection
CIDDS-001 [94]	DoS, port scans (ping-scan, SYN-Scan), SSH brute force
CIDDS-002 [94]	Port scans (ACK-Scan, FIN-Scan, ping-Scan, UDP-Scan, SYN-Scan)
CTU-13 [95]	Botnets (Menti, Murlo, Neris, NSIS, Rbot, Sogou, Virut)
DARPA [96]	DoS, privilege escalation (remote-to-local and user-to-root), probing
DDoS 2019 [97]	DDoS (HTTP flood, SIDDOS, smurf ICMP flood, UDP flood)
ISCX 2012 [98]	Four attack scenarios (1: Infiltrating the network from the inside; 2: HTTP DoS; 3: DDoS using an IRC botnet; 4: SSH brute force)
KDD CUP 99 [99]	DoS, privilege escalation (remote-to-local and user-to-root), probing
NSL-KDD [99]	DoS, privilege escalation (remote-to-local and user-to-root), probing
UNSW-NB15 [100]	Backdoors, DoS, exploits, fuzzers, generic, port scans, reconnaissance, shellcode, spam, worms
X-IIoTID [101]	Bruteforce, C&C, Dictionary, Crypto_ransom, Vulnerability Scan, MiTM, etc

develop strategies to mitigate them. (ii) Security Testing: For security testing, intrusion datasets are invaluable. They allow researchers to simulate real-world intrusion scenarios, thereby enabling them to evaluate the effectiveness of security measures under conditions that closely mimic actual intrusion attempts and (iii) Solution Development: When it comes to the development of security solutions, intrusion datasets serve as the raw data that machine learning algorithms need to train on. By learning from these datasets, these algorithms can develop models to detect anomalies, predict vulnerabilities, and provide proactive security measures. Table 3 gives a holistic view of the most recent publicly available datasets and attack types present in the dataset.

5.3. Performance metrics for evaluating secure IoT architectures

When evaluating the effectiveness of secure IoT architectures incorporating Quantum Neural Networks (QNN), Federated Learning, and 6G communication, several key performance metrics can provide insights into their performance. Table 4 shows a comprehensive overview of essential metrics for evaluation.

5.4. Performance metrics in evaluating secure IoT architectures

Performance evaluation is critical in the development of secure IoT architectures that include 6G communication, FL, and QC. A comprehensive understanding is necessary to assess the effectiveness of these systems, which use modern technology to improve security. As essential benchmarks, performance metrics provide information about the strength and effectiveness of these sophisticated security systems. An extensive overview of how well these systems handle security issues is given by performance metrics when evaluating secure IoT designs. They enable stakeholders to gauge the architecture's real-time responsiveness, reliability, and adaptability in the face of evolving threats. By delving into these metrics, one can ascertain the system's strengths, identify areas for improvement, and make informed decisions to fortify IoT security. Referencing Table 4 presents a detailed overview of essential metrics, each offering unique perspectives on the architecture's capabilities. These metrics collectively contribute to a holistic understanding of the secure IoT ecosystem, guiding stakeholders in optimizing security measures for a dynamic and interconnected digital landscape.

6. Future directions and research opportunities

This section evaluates the discussed research and offers concluding remarks on the evolving themes, accomplishments, and present challenges that require additional focus in the realm of quantum-empowered FL and 6G for IoT security.

6.1. Security and privacy challenges in FL

FL has surprisingly revolutionized the training pattern of AI algorithms by familiarizing them with a decentralized learning approach, where AI algorithms are trained via multiple independent learning sessions. That strategy treats both AI algorithms and data in an anonymous way where each session uses its training dataset irrespective of one another [64]. On the contrary side, traditional ML approaches use a centralized dataset to train the entire algorithm. This model is considered superior to the conventional learning approach and it is widely acknowledged in several application areas. A typical architecture of a federated recommender system has five main layers, namely the data layer, algorithm layer, service layer, interface layer, and application layer [104]. IoT is inspired by these novel concepts of FL and is potentially being used in various aspects of our lifestyle such as e-commerce, energy management, healthcare monitoring, and smart electronics [105]. IoT helps to effectively analyze a large amount of data streams, and then these systems recommend relevant suggestions generated by the recommendation engines.

6.1.1. Privacy issues

Federated Learning (FL) has transformed AI model training strategies, offering significant advantages in training outcomes. However, it introduces critical privacy risks that threaten the Confidentiality, Integrity, and Availability (CIA) of client data and systems, as described by [106]. The privacy status of FL-based systems should need to be evaluated on the CIA triad scale. That demands the system to fulfill the foundations of privacy in which confidentiality describes the information to be more secure and protected [107]. Integrity describes the system to ensure data synchronization at the both sender and the receiver end. Availability investigates the system to showcase the data when and where it is needed [108]. The involvement of heterogeneous clients may increase the probability of malicious interaction with the system especially in the training phase. In the FL training phase, the local data from certain clients is collected against pre-defined parameters, the data is then aggregated and the centralized model is updated. The attackers can monitor these parameters but are also able to contribute to the training mechanism. In this way, they have full access to explore the modifications in the updated global model to shake the confidentiality of the communication system [109]. Such a situation triggers the possibility of model inversion attacks that may result in decreasing the computation efficiency and might make it possible for the attackers to introduce backdoors into current systems [110].

The attackers may manipulate the training process as well generally referred to as model poisoning attacks. Such attacks manipulate training by supplying poisoned local model updates to the servers. Model poisoning generally occurs on the client side, where an adversary controls a small number of participants for common combative objectives. This kind of adversarial aggregation commonly known as Generative Adversarial Network (GAN) is harmful to the system . The GAN is more likely to induce unwanted streams of data by producing a dummy local model against the given parameters. In this way, they will negatively take part in the training phase resulting in the tempering

Table 4
Performance metrics for secure IoT architectures [102].

Metric	Parameters	Rationale
Quantum Computing Speed [16]	Quantum processing speed	Enables rapid real-time analysis and response to IoT security threats for proactive defence.
Federated Learning Accuracy [43]	Model accuracy in a federated learning environment	Ensures precise threat detection and response, enhancing overall IoT security posture and reliability.
Data Privacy Preservation [44]	Level of data privacy maintained during federated learning	Preserves individual user data confidentiality, fostering trust in the IoT ecosystem's security measures.
6G Network Latency [72]	Network latency in 6G communication	Facilitates swift responses to security events by enabling low-latency communication in the 6G network.
Security Robustness [70]	Robustness against quantum attacks	Ensures long-term protection by identifying and mitigating vulnerabilities to quantum threats in the architecture.
Device-to-Device Communication Speed [17]	Speed of communication between IoT devices	Establishes a responsive and interconnected IoT network through faster device-to-device communication for enhanced security.
Adaptive Security Response Time [22]	Time taken to adapt security measures based on detected threats	Reflects system agility in responding to emerging security challenges with a shorter response time.
Resource Utilization [23]	Quantum computing and federated learning resource consumption	Ensures efficient resource usage, optimizing sustainability and longevity of the secure IoT architecture.
Scalability [11]	System performance as the number of IoT devices increases	Accommodates a growing number of devices, maintaining performance and security in expanding IoT ecosystems.
Quantum Neural Network Training Time [25]	Time required to train Quantum Neural Networks	Influences adaptability to changing security needs, with shorter training times for faster integration.
Energy Consumption [102]	Power usage of the secure IoT system	Assess energy consumption for understanding sustainability and environmental impact, optimizing the IoT system's viability.
Interoperability [28]	Compatibility with diverse IoT devices and platforms	Ensures broad applicability and ease of deployment across diverse ecosystems through secure architecture interoperability.
Latency in Quantum Model Updates [71]	Time taken to update quantum models across the IoT network	Critical for maintaining security relevance by swiftly minimizing latency in updating quantum models.
Reliability of Quantum Key Distribution [26]	Reliability of quantum key distribution for secure communication	Evaluates the effectiveness of secure communication channels through reliable quantum key distribution in IoT.
Resilience to Adversarial Attacks [103]	Ability to withstand and recover from adversarial attacks	Assesses robustness against intentional security breaches, ensuring the system can withstand and recover promptly.
End-to-end encryption	Effectiveness of end-to-end encryption for data in transit	Evaluate the safeguarding of data during transmission, contributing to the overall integrity of IoT communications.

of data and a central global model. Such circumstances create an alarming situation where data integrity is at stake [11]. These activities have some severe outcomes as well where the system becomes non-responsive and unavailable to normal processes as well. Apart from the CIA triad, the system architecture of FL allows more compelling hazards i.e. SQL injection, extra consumption of system resources, and intensified communication delays [68]. The privacy-preserving approaches in FL are provided in Table 5.

6.1.2. Secure data sharing issues

The decentralized approach, while having multiple clients for training, makes the system vulnerable to a wide variety of security issues. As the number of clients increases, anonymity increases as well, which provides room for cyber threats to occur [115]. There are several sources of such vulnerabilities. The first potential concern comes from the communication mechanisms. FL protects operational data from other entities to ensure data privacy. However, there is still a possibility of partially disclosing the actual training data of clients by utilizing the model parameters that have been updated within the centralized global scheme [116]. The second concern arises from the presence of malicious clients. In some cases, the client intends to inject a suspicious process within the FL model to interrupt the operational processes of the system. This type of attack may result in serious consequences e.g. lack of training accuracy, excessive consumption of system resources, and lack of reliability. Early detection of such threats ensures smooth operations of FL models [117]. The third major source of threats also comes from the client side and is associated with the landscape of FL. In the FL landscape, some adversarial clients can apply old local data to update the global model once and attempt to deduce other clients' information. That phenomenon shakes the confidentiality and privacy of other clients and casts a questionable impact on the reliability of the overall system [118]. The FL clients can be better classified into two major categories: active and passive. The active clients work according to the regulations, on the contrast side, the passive clients do not contribute to the training process. These passive clients may infuse fake parameters to update the centralized global model. That activity complicates the running processes and puts other clients' stacks at risk [114]. Cloud servers are an excellent choice to get this job done. However, the quality of the server should be considered twice before the operations [57]. When multiple clients are involved, they are more likely to transmit their local data according to the provided parameters. The aggregation algorithm is also a major component of the system and can be an active reason for security threats. The aggregation algorithm is responsible for collecting and aggregating this local data. The centralized global model is then updated and the updates are shared with other clients. The aggregation algorithm must be intelligent enough to ignore the local data provided by suspicious clients. In the worst scenario, the system may malfunction by easily inserting abnormal data [119]. Moving forward, the next security threat arises from the server side. In an FL model, the centralized server is responsible for

Table 5
Privacy-preserving approaches in FL [111–113].

Ref	Operational Scenario	Approach	Dataset	Achievements	Limitations
[114]	IoT-enabled Smart communications	GRU	Modbus-based network dataset	Privacy preservation Investigation and classification of possible security threats	The notable increase in training time
[111]	Edge computing is driven intelligent communication environments	CNN	Customized dataset	Effective strength to stop retrieval of irrelevant information.	Significant computational overhead is witnessed
[112]	Generic FL training phases	Blockchain (Smart Contract)	N/A	Introduced a secure agreement concept between the client and the FL Server	Requires higher computational resources.
[9]	IoT empowered networks	Blockchain	KDDCUP99	Timely detection of malicious events	Not suitable for resource-constrained scenarios
[113]	Smart communications	Secure Boost	N/A	Competencies in privacy preservation	-

handling multiple tasks such as obtaining and aggregating local models, sharing the updates of global models, etc. Therefore, the server must be compatible enough to handle the workload to perform the given tasks more efficiently [120].

6.2. Cross-domain federated learning for interconnected IoT systems

In IoT systems, where devices are networked and produce massive volumes of data across several domains, Cross-domain Federated Learning (CD-FL) has multiple crucial functions. These functions demonstrate the value of CD-FL in resolving issues and maximizing the advantages of IoT systems. Some of the key roles of CD-FL in the IoT systems context are as follows:

6.2.1. Privacy preservation

In IoT systems, privacy is critical, particularly when handling sensitive or personal data [121]. CD-FL ensures that data never leaves the local devices. Only model updates do. Methods such as secure aggregation and FL with differential privacy offer an additional degree of privacy protection [42,122]. This keeps private sensitive data while allowing it to be used to enhance the model.

6.2.2. Enhanced security

Security mechanisms are incorporated into CD-FL to guarantee the accuracy of model updates and defend against adversarial attacks. To prevent model updates from being altered during transmission, CD-FL uses authentication and encryption techniques [103]. It also defends the network against threats that can jeopardize the system's dependability and credibility by compromising the integrity of the learning process.

6.2.3. Scalability enhancement

There has been an enormous increase in the IoT ecosystems in the past few years. CD-FL expands to support a growing variety of IoT domains and devices [123]. New devices and domains may be added to CD-FL without causing a corresponding rise in communication overhead because of its scalable architecture. Large-scale IoT deployments require this scalability [124], in order to maintain the efficacy and efficiency of the FL process as the system expands.

6.2.4. Data collaboration and knowledge sharing

Data is produced in IoT ecosystems by a variety of devices, each of which belongs to a distinct domain (e.g., healthcare [125], transportation [126], smart cities [31], and smart industries). These devices include sensors, cameras, and actuators. CD-FL enables cross-domain collaborative model training among IoT devices by allowing them to collaboratively train ML and DL models without centralizing the data [127]. The partnership aims to improve the accuracy and prediction potential of the model by utilizing insights from a variety of data sources and areas.

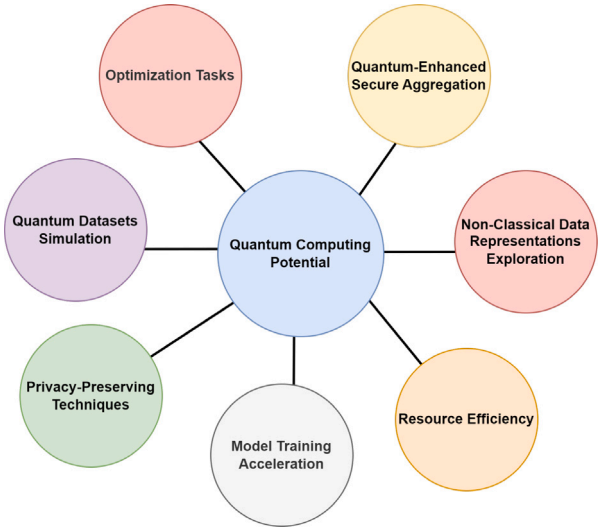

Fig. 10. Quantum Computing Potential in Enhancing FL for IoT.

6.2.5. Resource optimization

IoT devices frequently have limited memory, battery life, and processing power [128]. These constraints of IoT devices are taken into account by CD-FL through the use of model structures and resource-efficient algorithms and optimizes the training process of the model to be resource-efficient [129]. To guarantee that IoT devices may participate in FL without placing a strain on their resources, this involves employing lightweight model designs, lowering communication overhead, and decreasing computation requirements.

6.3. Advancements in quantum technologies for IoT

Quantum computing (QC) has the potential to significantly enhance FL for IoT in several ways as shown in Fig. 10. Although QC technology is still in its early stages and has numerous obstacles to overcome, it has special capabilities that can help FL in IoT environments:

6.3.1. Optimization tasks

Quantum computing (QC) introduces significant advancements in optimization tasks for Federated Learning (FL) in IoT by utilizing quantum algorithms, such as the Quantum Approximate Optimization Algorithm (QAOA). These algorithms are designed to tackle complex combinatorial optimization problems more efficiently than their classical counterparts [130]. In FL, this means enhanced capability in finding optimal model parameters with greater speed, potentially reducing computational costs and improving model accuracy while maintaining privacy standards.

6.3.2. Quantum datasets simulation

The ability of quantum computers to simulate quantum systems has far-reaching implications for IoT. Particularly in scenarios where IoT devices, like quantum sensors, generate complex data, quantum computers can simulate and process these datasets to improve the accuracy of predictive models and decision-making processes [13]. This capability is crucial for applications such as environmental monitoring and healthcare diagnostics, where precise data analysis can lead to better outcomes.

6.3.3. Privacy-preserving techniques

Quantum cryptography offers groundbreaking improvements in securing data transfers within IoT networks. Technologies such as Quantum Key Distribution (QKD) ensure secure communication channels, impervious to traditional and quantum attacks, by allowing the distribution of keys with a security level guaranteed by the laws of quantum mechanics. This method significantly enhances the security of FL by safeguarding the data exchanged between IoT devices from eavesdropping or tampering.

6.3.4. Quantum-enhanced secure aggregation

Secure aggregation in FL is critical to preserve the privacy of the model's updates from individual devices. Quantum-enhanced secure aggregation utilizes quantum secure multi-party computation (SMPC), which allows multiple parties to jointly compute a function over their inputs while keeping those inputs private [131]. This not only secures the aggregation process but also enhances trust among participants, a crucial aspect in decentralized environments like IoT.

6.3.5. Non-classical data representations exploration:

QC enables the exploration of non-classical data representations, which can lead to the discovery of new insights from IoT data that classical analytics methods might miss. This capability can be particularly beneficial in complex systems where data interactions are non-linear and highly interconnected, such as smart grids or autonomous vehicular networks. Quantum-enhanced analytics could reveal more effective strategies for system optimization and fault detection.

6.3.6. Resource efficiency

Large-scale FL deployments may benefit from resource-efficient solutions provided by quantum computers. Quantum-inspired algorithms and quantum annealers may be able to assist in controlling the computing resources needed for FL.

6.3.7. Accelerate model training

Compared to traditional computers, quantum computers can solve some mathematical problems far more quickly. In the FL context, IoT devices may converge on a global model faster if quantum computers could accelerate the model training process.

6.4. Policy and regulatory landscape for federated IoT systems

Federated IoT system policy and regulatory environments are always changing as new issues and technological advancements arise. To combine innovation with the defense of people's rights, security, and public interests, organizations and legislators must collaborate to ensure the policies and regulations.

7. Conclusion

This survey paper provided a detailed description of how integrating quantum computing, federated learning, and 6G wireless networks can enhance IoT security and privacy. Quantum computing strengthened encryption algorithms, making IoT data more secure, while federated learning enhanced privacy by allowing IoT devices to learn a shared model without sharing the training data. The integration of these technologies with the high-speed, low-latency capabilities of 6G networks facilitated real-time, secure data processing and communication among IoT devices. The paper also provided an up-to-date overview of the latest developments, challenges, and trends in IoT security and designed a conceptual framework for integrating quantum computing in federated learning for 6G networks. This will assist researchers and practitioners in developing new security frameworks, design regulations, and standards to ensure the safe and ethical use of these technologies.

CRediT authorship contribution statement

Danish Javeed: Writing – original draft, Data curation. **Muhammad Shahid Saeed:** Writing – original draft, Visualization, Data curation. **Ijaz Ahmad:** Writing – original draft, Visualization. **Muhammad Adil:** Writing – original draft, Data curation. **Prabhat Kumar:** Writing – original draft, Visualization, Supervision, Data curation, Conceptualization. **A.K.M. Najmul Islam:** Writing – review & editing, Supervision, Data curation.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgment

This work was supported by the Research Council of Finland with CHIST-ERA, grant agreement no - 359790, Di4SPDS-Distributed Intelligence for Enhancing Security and Privacy of Decentralized and Distributed Systems.

References

[1] K. Rose, S. Eldridge, L. Chapin, The internet of things: An overview, Internet Soc. (ISOC) 80 (2015) 1–50.
[2] M. Wollschlaeger, T. Sauter, J. Jasperneite, The future of industrial communication: Automation networks in the era of the internet of things and industry 4.0, IEEE Ind. Electron. Mag. 11 (1) (2017) 17–27.
[3] L. Georgios, S. Kerstin, A. Theofylaktos, Internet of things in the context of industry 4.0: An overview, Int. J. Entrepreneurial Knowl (2019).
[4] D. Javeed, M.S. Saeed, I. Ahmad, P. Kumar, A. Jolfaei, M. Tahir, An intelligent intrusion detection system for smart consumer electronics network, IEEE Trans. Consum. Electron. (2023).
[5] P. Kumari, A.K. Jain, A comprehensive study of ddos attacks over IoT network and their countermeasures, Comput. Secur. (2023) 103096.
[6] F. Al-Turjman, H. Zahmatkesh, R. Shahroze, An overview of security and privacy in smart cities' IoT communications, Trans. Emerg. Telecommun. Technol. 33 (3) (2022) e3677.
[7] R. Ramadan, Internet of things (IoT) security vulnerabilities: A review, PLOMS AI 2 (1) (2022).
[8] S. Prajapati, A. Singh, Cyber-attacks on internet of things (IoT) devices, attack vectors, and remedies: A position paper, IoT Cloud Comput. Societal Good (2022) 277–295.
[9] L. Cui, Y. Qu, G. Xie, D. Zeng, R. Li, S. Shen, S. Yu, Security and privacy-enhanced federated learning for anomaly detection in IoT infrastructures, IEEE Trans. Ind. Inform. 18 (5) (2021) 3492–3500.

[10] S. AbdulRahman, H. Tout, H. Ould-Slimane, A. Mourad, C. Talhi, M. Guizani, A survey on federated learning: The journey from centralized to distributed on-site learning and beyond, IEEE Internet Things J. 8 (7) (2020) 5476–5497.

[11] Q. Li, Z. Wen, Z. Wu, S. Hu, N. Wang, Y. Li, X. Liu, B. He, A survey on federated learning systems: Vision, hype and reality for data privacy and protection, IEEE Trans. Knowl. Data Eng. (2021).

[12] N. Singh, A. Tiwari, V. Khaneja, Federated machine learning architecture for heterogeneous quantum devices, in: International Conference on Emerging Trends and Technologies on Intelligent Systems, Springer, 2023, pp. 21–31.

[13] V. Hassija, V. Chamola, A. Goyal, S.S. Kanhere, N. Guizani, Forthcoming applications of quantum computing: Peeking into the future, IET Quantum Commun. 1 (2) (2020) 35–41.

[14] E. Diamanti, H.-K. Lo, B. Qi, Z. Yuan, Practical challenges in quantum key distribution, npj Quantum Inf. 2 (1) (2016) 1–12.

[15] C. Wang, A. Rahman, Quantum-enabled 6G wireless networks: Opportunities and challenges, IEEE Wirel. Commun. 29 (1) (2022) 58–69.

[16] S.J. Nawaz, S.K. Sharma, S. Wyne, M.N. Patwary, M. Asaduzzaman, Quantum machine learning for 6G communication networks: State-of-the-art and vision for the future, IEEE Access 7 (2019) 46317–46350.

[17] C.-X. Wang, X. You, X. Gao, X. Zhu, Z. Li, C. Zhang, H. Wang, Y. Huang, Y. Chen, H. Haas, et al., On the road to 6G: Visions, requirements, key technologies and testbeds, IEEE Commun. Surv. Tutor. (2023).

[18] V. Ziegler, P. Schneider, H. Viswanathan, M. Montag, S. Kanugovi, A. Rezaki, Security and trust in the 6G era, IEEE Access 9 (2021) 142314–142327.

[19] K. Prateek, N.K. Ojha, F. Altaf, S. Maity, Quantum secured 6G technology-based applications in internet of everything, Telecommun. Syst. 82 (2) (2023) 315–344.

[20] M. Alsabah, M.A. Naser, B.M. Mahmmod, S.H. Abdulhussain, M.R. Eissa, A. Al-Baidhani, N.K. Noordin, S.M. Sait, K.A. Al-Utaibi, F. Hashim, 6G wireless communications networks: A comprehensive survey, Ieee Access 9 (2021) 148191–148243.

[21] M. Al-Quraan, L. Mohjazi, L. Bariah, A. Centeno, A. Zoha, K. Arshad, K. Assaleh, S. Muhaidat, M. Debbah, M.A. Imran, Edge-native intelligence for 6G communications driven by federated learning: A survey of trends and challenges, IEEE Trans. Emerg. Top. Comput. Intell. (2023).

[22] M. Venkatasubramanian, A.H. Lashkari, S. Hakak, IoT malware analysis using federated learning: A comprehensive survey, IEEE Access (2023).

[23] B. Ghimire, D.B. Rawat, Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things, IEEE Internet Things J. (2022).

[24] D. Chawla, P.S. Mehra, A survey on quantum computing for internet of things security, Procedia Comput. Sci. 218 (2023) 2191–2200.

[25] H.T. Larasati, M. Firdaus, H. Kim, Quantum federated learning: Remarks and challenges, in: 2022 IEEE 9th International Conference on Cyber Security and Cloud Computing (CSCloud)/2022 IEEE 8th International Conference on Edge Computing and Scalable Cloud, EdgeCom, IEEE, 2022, pp. 1–5.

[26] S. Cherbal, A. Zier, S. Hebal, L. Louail, B. Annane, Security in internet of things: A review on approaches based on blockchain, machine learning, cryptography, and quantum computing, J. Supercomput. (2023) 1–79.

[27] D.C. Nguyen, M. Ding, P.N. Pathirana, A. Seneviratne, J. Li, D. Niyato, O. Dobre, H.V. Poor, 6G internet of things: A comprehensive survey, IEEE Internet Things J. 9 (1) (2021) 359–383.

[28] P. Kumar, Towards Design and Development of Secure and Privacy-Preserving Frameworks for IoT-enabled Networks, GRIN Verlag, 2022.

[29] D. Javeed, T. Gao, M.S. Saeed, P. Kumar, R. Kumar, A. Jolfaei, A softwarized intrusion detection system for IoT-enabled smart healthcare system, ACM Trans. Internet Technol. (2023).

[30] V.P.S. Achari, Z. Khanam, A.K. Singh, A. Jindal, A. Prakash, N. Kumar, I 2 UTS: An IoT based intelligent urban traffic system, in: 2021 IEEE 22nd International Conference on High Performance Switching and Routing, HPSR, IEEE, 2021, pp. 1–6.

[31] R. Minu, G. Nagarajan, A. Munshi, K. Venkatachalam, W. Almukadi, M. Abouhawwash, An edge based attack detection model (EBAD) for increasing the trustworthiness in IoT enabled smart city environment, IEEE Access 10 (2022) 89499–89508.

[32] D. Javeed, T. Gao, M.S. Saeed, M.T. Khan, FOG-empowered augmented intelligence-based proactive defensive mechanism for IoT-enabled smart industries, IEEE Internet Things J. (2023).

[33] A. Malik, V. Parihar, B. Bhushan, R. Chaganti, S. Bhatia, P.N. Astya, Security services for wireless 5G internet of things (IoT) systems, in: 5G and beyond, Springer Nature Singapore Singapore, 2023, pp. 169–195.

[34] J. Saleem, M. Hammoudeh, U. Raza, B. Adebisi, R. Ande, IoT standardisation: Challenges, perspectives and solution, in: Proceedings of the 2nd International Conference on Future Networks and Distributed Systems, 2018, pp. 1–9.

[35] D. Javeed, T. Gao, Z. Jamil, Artificial intelligence (AI)-based intrusion detection system for IoT-enabled networks: A state-of-the-art survey, in: Protecting User Privacy in Web Search Utilization, IGI Global, 2023, pp. 269–289.

[36] J. Kaur, U. Garg, G. Bathla, Detection of cross-site scripting (XSS) attacks using machine learning techniques: A review, Artif. Intell. Rev. 56 (11) (2023) 12725–12769.

[37] A. Maatallaoui, H. Touil, L. Setti, The impact of radio frequency (RF) attacks on security and privacy: A comprehensive review, in: Proceedings of the 6th International Conference on Networking, Intelligent Systems & Security, 2023, pp. 1–23.

[38] T. Sowmya, E.M. Anita, A comprehensive review of AI based intrusion detection system, Measurement: Sensors (2023) 100827.

[39] I. Martins, J.S. Resende, P.R. Sousa, S. Silva, L. Antunes, J. Gama, Host-based IDS: A review and open issues of an anomaly detection system in IoT, Future Gener. Comput. Syst. 133 (2022) 95–113.

[40] P. Kumar, G.P. Gupta, R. Tripathi, An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks, Comput. Commun. 166 (2021) 110–124.

[41] M. Bhavsar, K. Roy, J. Kelly, O. Olusola, Anomaly-based intrusion detection system for IoT application, Discov. Internet Things 3 (1) (2023) 5.

[42] D. Javeed, M.S. Saeed, P. Kumar, A. Jolfaei, S. Islam, A.N. Islam, Federated learning-based personalized recommendation systems: An overview on security and privacy challenges, IEEE Trans. Consum. Electron. (2023).

[43] L.U. Khan, W. Saad, Z. Han, E. Hossain, C.S. Hong, Federated learning for internet of things: Recent advances, taxonomy, and open challenges, IEEE Commun. Surv. Tutor. 23 (3) (2021) 1759–1799.

[44] S. Savazzi, M. Nicoli, V. Rampa, Federated learning with cooperating devices: A consensus approach for massive IoT networks, IEEE Internet Things J. 7 (5) (2020) 4641–4654.

[45] L.G.F. da Silva, D.F. Sadok, P.T. Endo, Resource optimizing federated learning for use with IoT: A systematic review, J. Parallel Distrib. Comput. (2023).

[46] A. Muhammad, K. Lin, J. Gao, B. Chen, Robust multi-model personalized federated learning via model distillation, in: International Conference on Algorithms and Architectures for Parallel Processing, Springer, 2021, pp. 432–446.

[47] A. Sahu, T. Li, M. Sanjabi, M. Zaheer, A. Talwalkar, V. Smith, On the convergence of federated optimization in heterogeneous networks (vol. 3), 2018, arXiv preprint arXiv:1812.06127.

[48] B. Luo, W. Xiao, S. Wang, J. Huang, L. Tassiulas, Tackling system and statistical heterogeneity for federated learning with adaptive client sampling, in: IEEE INFOCOM 2022-IEEE Conference on Computer Communications, IEEE, 2022, pp. 1739–1748.

[49] A.-C. Hauschild, M. Lemanczyk, J. Matschinske, T. Frisch, O. Zolotareva, A. Holzinger, J. Baumbach, D. Heider, Federated random forests can improve local performance of predictive models for various healthcare applications, Bioinformatics 38 (8) (2022) 2278–2286.

[50] P. Kumar, G.P. Gupta, R. Tripathi, PEFL: Deep privacy-encoding-based federated learning framework for smart agriculture, IEEE Micro 42 (1) (2022) 33–40, http://dx.doi.org/10.1109/MM.2021.3112476.

[51] S. Moriai, Privacy-preserving deep learning via additively homomorphic encryption, in: 2019 IEEE 26th Symposium on Computer Arithmetic, ARITH, IEEE, 2019, 198–198.

[52] A. Holzinger, A. Saranti, A. Angerschmid, C.O. Retzlaff, A. Gronauer, V. Pejakovic, F. Medel-Jimenez, T. Krexner, C. Gollob, K. Stampfer, Digital transformation in smart farm and forest operations needs human-centered AI: Challenges and future directions, Sensors 22 (8) (2022) 3043.

[53] K. Wei, J. Li, M. Ding, C. Ma, H.H. Yang, F. Farokhi, S. Jin, T.Q. Quek, H.V. Poor, Federated learning with differential privacy: Algorithms and performance analysis, IEEE Trans. Inf. Forensics Secur. 15 (2020) 3454–3469.

[54] Y. Li, Y. Zhou, A. Jolfaei, D. Yu, G. Xu, X. Zheng, Privacy-preserving federated learning framework based on chained secure multiparty computing, IEEE Internet Things J. 8 (8) (2020) 6178–6186.

[55] H. Kido, Y. Yanagisawa, T. Satoh, Protection of location privacy using dummies for location-based services, in: 21st International Conference on Data Engineering Workshops, ICDEW'05, IEEE, 2005, 1248–1248.

[56] E. Bagdasaryan, A. Veit, Y. Hua, D. Estrin, V. Shmatikov, How to backdoor federated learning, in: International Conference on Artificial Intelligence and Statistics, PMLR, 2020, pp. 2938–2948.

[57] X. Gong, Y. Chen, Q. Wang, W. Kong, Backdoor attacks and defenses in federated learning: State-of-the-art, taxonomy, and future directions, IEEE Wirel. Commun. (2022).

[58] C. Wu, X. Yang, S. Zhu, P. Mitra, Mitigating backdoor attacks in federated learning, 2020, arXiv preprint arXiv:2011.01767.

[59] H. Hosseini, H. Park, S. Yun, C. Louizos, J. Soriaga, M. Welling, Federated learning of user verification models without sharing embeddings, in: International Conference on Machine Learning, PMLR, 2021, pp. 4328–4336.

[60] A. Reisizadeh, F. Farnia, R. Pedarsani, A. Jadbabaie, Robust federated learning: The case of affine distribution shifts, Adv. Neural Inf. Process. Syst. 33 (2020) 21554–21565.

[61] C. Zhang, S. Li, J. Xia, W. Wang, F. Yan, Y. Liu, {BatchCrypt}: Efficient homomorphic encryption for {cross-silo} federated learning, in: 2020 USENIX Annual Technical Conference, USENIX ATC 20, 2020, pp. 493–506.

[62] X. Yin, Y. Zhu, J. Hu, A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions, ACM Comput. Surv. 54 (6) (2021) 1–36.

[63] J. Liu, H. Xu, L. Wang, Y. Xu, C. Qian, J. Huang, H. Huang, Adaptive asynchronous federated learning in resource-constrained edge computing, IEEE Trans. Mob. Comput. (2021).

[64] A. Imteaj, U. Thakker, S. Wang, J. Li, M.H. Amini, A survey on federated learning for resource-constrained IoT devices, IEEE Internet Things J. 9 (1) (2021) 1–24.
[65] C. Shen, J. Xu, S. Zheng, X. Chen, Resource rationing for wireless federated learning: Concept, benefits, and challenges, IEEE Commun. Mag. 59 (5) (2021) 82–87.
[66] Y. Zhan, P. Li, Z. Qu, D. Zeng, S. Guo, A learning-based incentive mechanism for federated learning, IEEE Internet Things J. 7 (7) (2020) 6360–6368.
[67] H. Cao, H. Zhao, A. Jindal, G.S. Aujla, L. Yang, Energy-efficient virtual resource allocation of slices in vehicles-assisted b5g networks, IEEE Trans. Green Commun. Netw. 6 (3) (2022) 1408–1417.
[68] V. Mothukuri, R.M. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, G. Srivastava, A survey on security and privacy of federated learning, Future Gener. Comput. Syst. 115 (2021) 619–640.
[69] D.J. Bernstein, T. Lange, Post-quantum cryptography, Nature 549 (7671) (2017) 188–194.
[70] R. Kaewpuang, M. Xu, D. Niyato, H. Yu, Z. Xiong, X.S. Shen, Adaptive resource allocation in quantum key distribution (QKD) for federated learning, in: 2023 International Conference on Computing, Networking and Communications, ICNC, IEEE, 2023, pp. 71–76.
[71] J. Pei, S. Li, Z. Yu, L. Ho, W. Liu, L. Wang, Federated learning encounters 6G wireless communication in the scenario of internet of things, IEEE Commun. Stand. Mag. 7 (1) (2023) 94–100.
[72] W. Jiang, B. Han, M.A. Habibi, H.D. Schotten, The road towards 6G: A comprehensive survey, IEEE Open J. Commun. Soc. 2 (2021) 334–366.
[73] Y. Xiao, G. Shi, Y. Li, W. Saad, H.V. Poor, Toward self-learning edge intelligence in 6G, IEEE Commun. Mag. 58 (12) (2020) 34–40.
[74] W. Wu, C. Zhou, M. Li, H. Wu, H. Zhou, N. Zhang, X.S. Shen, W. Zhuang, AI-native network slicing for 6G networks, IEEE Wirel. Commun. 29 (1) (2022) 96–103.
[75] S.I. Rayhan, An approach to work with quantum data in federated learning, 2023.
[76] D. Ferrari, A.S. Cacciapuoti, M. Amoretti, M. Caleffi, Compiler design for distributed quantum computing, IEEE Trans. Quantum Eng. 2 (2021) 1–20.
[77] Q. Xia, Q. Li, Quantumfed: A federated learning framework for collaborative quantum training, in: 2021 IEEE Global Communications Conference, GLOBECOM, IEEE, 2021, pp. 1–6.
[78] X. Wei, L. Fan, Y. Guo, Y. Gong, Z. Han, Y. Wang, Quantum assisted scheduling algorithm for federated learning in distributed networks, in: 2023 32nd International Conference on Computer Communications and Networks, ICCCN, IEEE, 2023, pp. 1–10.
[79] O. Shmueli, Semi-quantum tokenized signatures, in: Annual International Cryptology Conference, Springer, 2022, pp. 296–319.
[80] S. Yang, Y. Chen, S. Tu, Z. Yang, A post-quantum secure aggregation for federated learning, in: Proceedings of the 2022 12th International Conference on Communication and Network Security, 2022, pp. 117–124.
[81] M. Chehimi, S.Y.-C. Chen, W. Saad, D. Towsley, M. Debbah, Foundations of quantum federated learning over classical and quantum networks, IEEE Netw. (2023).
[82] M. Chehimi, W. Saad, Quantum federated learning with quantum data, in: ICASSP 2022-2022 IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP, IEEE, 2022, pp. 8617–8621.
[83] B. Narottama, S.Y. Shin, Federated quantum neural network with quantum teleportation for resource optimization in future wireless communication, IEEE Trans. Veh. Technol. (2023).
[84] S. Bhatt, B. Bhushan, T. Srivastava, V. Anoop, Post-quantum cryptographic schemes for security enhancement in 5G and B5G (beyond 5G) cellular networks, in: 5G and beyond, Springer Nature Singapore Singapore, 2023, pp. 247–281.
[85] Q. Xu, L. Zhao, Z. Su, D. Fang, R. Li, Secure federated learning in quantum autonomous vehicular networks, IEEE Netw. (2023).
[86] D. Gurung, S.R. Pokhrel, G. Li, Secure communication model for quantum federated learning: A post quantum cryptography (PQC) framework, 2023, arXiv preprint arXiv:2304.13413.
[87] U.M. Malik, M.A. Javed, S. Zeadally, S. ul Islam, Energy-efficient fog computing for 6G-enabled massive IoT: Recent trends and future opportunities, IEEE Internet Things J. 9 (16) (2021) 14572–14594.
[88] A. Mukherjee, P. Goswami, M.A. Khan, L. Manman, L. Yang, P. Pillai, Energy-efficient resource allocation strategy in massive IoT for industrial 6G applications, IEEE Internet Things J. 8 (7) (2020) 5194–5201.
[89] N. Hu, Z. Tian, X. Du, M. Guizani, An energy-efficient in-network computing paradigm for 6G, IEEE Trans. Green Commun. Netw. 5 (4) (2021) 1722–1733.
[90] C. Kolias, G. Kambourakis, A. Stavrou, S. Gritzalis, Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset, IEEE Commun. Surv. Tutor. 18 (1) (2016) 184–208.
[91] N. Koroniotis, N. Moustafa, E. Sitnikova, B. Turnbull, Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-IoT dataset, Future Gener. Comput. Syst. 100 (2019) 779–796.
[92] N. Moustafa, A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets, Sustainable Cities Soc. 72 (2021) 102994.
[93] I. Sharafaldin, A.H. Lashkari, A.A. Ghorbani, Toward generating a new intrusion detection dataset and intrusion traffic characterization, ICISSp 1 (2018) 108–116.
[94] M. Ring, S. Wunderlich, D. Landes, A. Hotho, CIDDS-001, 2022, http://dx.doi.org/10.34740/KAGGLE/DSV/4061966, URL https://www.kaggle.com/dsv/4061966.
[95] S. Garcia, M. Grill, J. Stiborek, A. Zunino, An empirical comparison of botnet detection methods, Comput. Secur. 45 (2014) 100–123.
[96] C. Thomas, V. Sharma, N. Balakrishnan, Usefulness of DARPA dataset for intrusion detection system evaluation, in: Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2008, vol. 6973, SPIE, 2008, pp. 164–171.
[97] I. Sharafaldin, A.H. Lashkari, S. Hakak, 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.
[98] A. Shiravi, H. Shiravi, M. Tavallaee, A.A. Ghorbani, Toward developing a systematic approach to generate benchmark datasets for intrusion detection, Comput. Secur. 31 (3) (2012) 357–374.
[99] M. Tavallaee, E. Bagheri, W. Lu, A.A. Ghorbani, A detailed analysis of the KDD CUP 99 data set, in: 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ieee, 2009, pp. 1–6.
[100] N. Moustafa, J. Slay, UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set), in: 2015 Military Communications and Information Systems Conference, MilCIS, IEEE, 2015, pp. 1–6.
[101] M. Al-Hawawreh, E. Sitnikova, N. Aboutorab, X-IIoTID: A connectivity-agnostic and device-agnostic intrusion data set for industrial internet of things, IEEE Internet Things J. 9 (5) (2021) 3962–3977.
[102] Y. Zhan, J. Zhang, Z. Hong, L. Wu, P. Li, S. Guo, A survey of incentive mechanism design for federated learning, IEEE Trans. Emerg. Top. Comput. 10 (2) (2021) 1035–1044.
[103] S. Singh, S. Rathore, O. Alfarraj, A. Tolba, B. Yoon, A framework for privacy-preservation of IoT healthcare data using federated learning and blockchain technology, Future Gener. Comput. Syst. 129 (2022) 380–388.
[104] B. Tan, B. Liu, V. Zheng, Q. Yang, A federated recommender system for online services, in: Proceedings of the 14th ACM Conference on Recommender Systems, 2020, pp. 579–581.
[105] Y. Himeur, A. Sayed, A. Alsalemi, F. Bensaali, A. Amira, I. Varlamis, M. Eirinaki, C. Sardianos, G. Dimitrakopoulos, Blockchain-based recommender systems: Applications, challenges and future opportunities, Comp. Sci. Rev. 43 (2022) 100439.
[106] M. Alazab, S.P. RM, M. Parimala, P.K.R. Maddikunta, T.R. Gadekallu, Q.-V. Pham, Federated learning for cybersecurity: Concepts, challenges, and future directions, IEEE Trans. Ind. Inform. 18 (5) (2021) 3501–3509.
[107] H. Gao, Y. Wang, Algorithm-level confidentiality for average consensus on time-varying directed graphs, IEEE Trans. Netw. Sci. Eng. 9 (2) (2022) 918–931.
[108] M.S.M. Shah, Y.-B. Leau, M. Anbar, A.A. Bin-Salem, Security and integrity attacks in named data networking: A survey, IEEE Access 11 (2023) 7984–8004.
[109] O. Aouedi, A. Sacco, K. Piamrat, G. Marchetto, Handling privacy-sensitive medical data with federated learning: Challenges and future directions, IEEE J. Biomed. Health Inf. (2022).
[110] A. Holzinger, E. Weippl, A.M. Tjoa, P. Kieseberg, Digital transformation for sustainable development goals (sdgs)-a security, safety and privacy perspective on ai, in: International Cross-Domain Conference for Machine Learning and Knowledge Extraction, Springer, 2021, pp. 1–20.
[111] A. Makkar, U. Ghosh, D.B. Rawat, J.H. Abawajy, Fedlearnsp: Preserving privacy and security using federated learning and edge computing, IEEE Consum. Electron. Mag. 11 (2) (2021) 21–27.
[112] A.R. Short, H.C. Leligou, M. Papoutsidakis, E. Theocharis, Using blockchain technologies to improve security in federated learning systems, in: 2020 IEEE 44th Annual Computers, Software, and Applications Conference, COMPSAC, IEEE, 2020, pp. 1183–1188.
[113] K. Cheng, T. Fan, Y. Jin, Y. Liu, T. Chen, D. Papadopoulos, Q. Yang, Secureboost: A lossless federated learning framework, IEEE Intell. Syst. 36 (6) (2021) 87–98.
[114] V. Mothukuri, P. Khare, R.M. Parizi, S. Pouriyeh, A. Dehghantanha, G. Srivastava, Federated-learning-based anomaly detection for iot security attacks, IEEE Internet Things J. 9 (4) (2021) 2545–2554.
[115] C. Ma, J. Li, M. Ding, H.H. Yang, F. Shu, T.Q. Quek, H.V. Poor, On safeguarding privacy and security in the framework of federated learning, IEEE Netw. 34 (4) (2020) 242–248.
[116] R. Gosselin, L. Vieu, F. Loukil, A. Benoit, Privacy and security in federated learning: A survey, Appl. Sci. 12 (19) (2022) 9901.
[117] X. Liu, H. Li, G. Xu, Z. Chen, X. Huang, R. Lu, Privacy-enhanced federated learning against poisoning adversaries, IEEE Trans. Inf. Forensics Secur. 16 (2021) 4574–4588.
[118] J. Gao, B. Hou, X. Guo, Z. Liu, Y. Zhang, K. Chen, J. Li, Secure aggregation is insecure: Category inference attack on federated learning, IEEE Trans. Dependable Secure Comput. (2021).

[119] S. Li, E.C.-H. Ngai, T. Voigt, An experimental study of Byzantine-robust aggregation schemes in federated learning, IEEE Trans. Big Data (2023).
[120] M. Song, Z. Wang, Z. Zhang, Y. Song, Q. Wang, J. Ren, H. Qi, Analyzing user-level privacy attack against federated learning, IEEE J. Sel. Areas Commun. 38 (10) (2020) 2430–2444.
[121] Z. Zeng, Y. Liu, L. Chang, A robust and optional privacy data aggregation scheme for fog-enhanced IoT network, IEEE Syst. J. 17 (1) (2022) 1110–1120.
[122] A.P. Kalapaaking, I. Khalil, M.S. Rahman, M. Atiquzzaman, X. Yi, M. Almashor, Blockchain-based federated learning with secure aggregation in trusted execution environment for internet-of-things, IEEE Trans. Ind. Inform. 19 (2) (2022) 1703–1714.
[123] D.C. Nguyen, M. Ding, P.N. Pathirana, A. Seneviratne, J. Li, H.V. Poor, Federated learning for internet of things: A comprehensive survey, IEEE Commun. Surv. Tutor. 23 (3) (2021) 1622–1658.
[124] G.S. Ramachandran, B. Krishnamachari, Towards a large scale iot through partnership, incentive, and services: A vision, architecture, and future directions, Open J. Internet Things (OJIOT) 5 (1) (2019) 80–92.
[125] D.C. Nguyen, Q.-V. Pham, P.N. Pathirana, M. Ding, A. Seneviratne, Z. Lin, O. Dobre, W.-J. Hwang, Federated learning for smart healthcare: A survey, ACM Comput. Surv. 55 (3) (2022) 1–37.
[126] Y. Wu, H.-N. Dai, H. Wang, Z. Xiong, S. Guo, A survey of intelligent network slicing management for industrial IoT: Integrated approaches for smart transportation, smart energy, and smart factory, IEEE Commun. Surv. Tutor. 24 (2) (2022) 1175–1211.
[127] P. Zhao, Y. Huang, J. Gao, L. Xing, H. Wu, H. Ma, Federated learning-based collaborative authentication protocol for shared data in social IoV, IEEE Sens. J. 22 (7) (2022) 7385–7398.
[128] A. Imteaj, K. Mamun Ahmed, U. Thakker, S. Wang, J. Li, M.H. Amini, Federated learning for resource-constrained IoT devices: Panoramas and state of the art, Federated Transf. Learn. (2022) 7–27.
[129] L.U. Khan, M. Alsenwi, I. Yaqoob, M. Imran, Z. Han, C.S. Hong, Resource optimized federated learning-enabled cognitive internet of things for smart industries, IEEE Access 8 (2020) 168854–168864.
[130] N. Ngoenriang, M. Xu, J. Kang, D. Niyato, H. Yu, X.S. Shen, DQC2O: Distributed quantum computing for collaborative optimization in future networks, IEEE Commun. Mag. (2023).
[131] D. Wu, M. Pan, Z. Xu, Y. Zhang, Z. Han, Towards efficient secure aggregation for model update in federated learning, in: GLOBECOM 2020-2020 IEEE Global Communications Conference, IEEE, 2020, pp. 1–6.

Danish Javeed is currently pursuing a Ph.D. degree in Software Engineering, specializing in Information Security with the Software College, Northeastern University, China under the prestigious fellowship of Ministry of Education funded by the Government of China. He got his M.E degree in Computer Applied Technology from Changchun University of Science and Technology, China, under the same fellowship in 2020. He is also working on various research projects with researchers from the LUT School of Engineering Science, LUT University, Lappeenranta, Finland. He has many research contributions in Deep Learning, Cybersecurity, Intrusion Detection and Prevention Systems, the Internet of Things, Software-defined Networking, and Edge Computing. He has authored or coauthored over 15+ publications in high-ranked journals and conferences. He is also an IEEE Student Member.

Muhammad Shahid Saeed is currently pursuing a Ph.D. degree in Software Engineering, with the Dalian University of Technology, PR China under the prestigious fellowship of Ministry of Education funded by the Government of China. He is also working on various projects in collaboration with researchers from Northeastern University, China. He has a few research contributions in Intrusion Detection and Prevention Systems, the Internet of Things, Industry 4.0, Software-defined Networking, and Edge Computing.

Ijaz Ahmad is currently pursuing Ph.D. degree in pattern recognition and intelligence system from Shenzhen Institute of Advanced Technology (SIAT), Chinese Academy of Sciences (CAS) under the ANSO Scholarship for young scientists. He got his M.E degree in Computer Applied Technology from Changchun University of Science and Technology, China, under the prestigious fellowship of the Ministry of Education funded by the Government of China in 2020. He has many research contributions in pattern recognition, applied machine intelligence, biomedical signal processing, biomedical imaging, clinical decision support systems and the Internet of Things (IoT). He has authored or co-authored over 20+ publications in high-ranked journals and conferences. He is also an IEEE Student Member.

Muhammad Adil received master's degree in computer science and technology from Dalian University of Technology, China in 2022. He is currently pursuing PhD in computer science and technology from Tianjin university, China. His main research includes privacy-preserved distributive machine learning, time sensitive networking, and 5G for industrial networks.

Prabhat Kumar received his Ph.D. degree in Information Technology, National Institute of Technology Raipur, Raipur, India, under the prestigious fellowship of Ministry of Human Resource and Development (MHRD) funded by the Government of India in 2022. Thereafter, he worked with Indian Institute of Technology Hyderabad, India as a Post-Doctoral Researcher under project "Development of Indian Telecommunication Security Assurance Requirements for IoT devices". He is currently working as Post-Doctoral Researcher with the Department of Software Engineering, LUT School of Engineering Science, LUT University, Lappeenranta, Finland. He has many research contributions in Machine Learning, Deep Learning, Federated Learning, Big Data Analytics, Cybersecurity, Blockchain, Cloud Computing, Internet of Things and Software Defined Networking. He has authored or coauthored over 40+ publications in high-ranked journals and conferences, including 15+ IEEE TRANSACTIONS paper. One of his Ph.D. publications was recognized as a top cited article by WILEY in 2020–21. He is also an IEEE Member.

A.K.M. Najmul Islam is a Full Professor at LUT University, Finland. He conducts crossdisciplinary research in digitalization and its impact on citizens, organizations, and society. He is a docent of Information Systems at Tampere University. Islam's publication has appeared in top Information Systems outlets such as Journal of Strategic Information Systems, European Journal of Information Systems, and Information Systems Journal. He has published in other highly ranked interdisciplinary journals such as IEEE Access, Computers & Education, Technological Forecasting and Social Change, International Journal of Information Management, Information Technology & People, Computers in Human Behavior, Computers in Industry, Internet Research, Communications of the AIS, among others. He is currently serving as a Senior Editor for Information Technology & People journal.