GSC Advanced Research and Reviews

eISSN: 2582-4597 CODEN (USA): GARRC2

Cross Ref DOI: 10.30574/gscarr

Journal homepage: https://gsconlinepress.com/journals/gscarr/

GSC Online Press INDIA

(Review Article)

Federated learning for secure and privacy preserving data analytics in heterogeneous networks

Mmasi Patience Robai *

Jaramogi Odinga Oginga University of Science and Technology 40601, Bondo, Kenya.

GSC Advanced Research and Reviews, 2024, 21(02), 527–555

Publication history: Received on 13 October 2024; revised on 24 November 2024; accepted on 26 November 2024

Article DOI: https://doi.org/10.30574/gscarr.2024.21.2.0451

Abstract

Federated Learning (FL) has emerged as a groundbreaking paradigm enabling collaborative machine learning across distributed nodes without centralizing data, thus addressing critical concerns in security and privacy. This survey explores the application of FL for secure and privacy-preserving data analytics in heterogeneous networks, where diverse devices, data distributions, and network conditions present unique challenges. This paper provides a comprehensive review of recent advancements in FL, focusing on its efficacy in safeguarding sensitive information while enabling effective analytics across varied domains such as healthcare, finance, and IoT systems. The paper delves into key methodologies for achieving privacy preservation, including differential privacy, secure multi-party computation, and homomorphic encryption, while analyzing their performance in dynamic and resource-constrained environments. Additionally, this paper examines strategies for managing heterogeneity, including personalized FL, model aggregation techniques, and adaptive optimization algorithms. Challenges such as scalability, communication efficiency, and adversarial robustness are discussed alongside potential solutions and future research directions. This survey aims to provide researchers and practitioners with an in-depth understanding of the state-of-the-art in FL for secure and privacy-preserving data analytics, fostering innovation and addressing emerging needs in increasingly complex network ecosystems.

Keywords: Federated learning; privacy; security; data analytics; HetNets

1. Introduction

The rapid proliferation of data-generating devices such as smartphones, sensors, and edge computing systems has ushered in a new era of data-driven decision-making [1], [2]. This unprecedented growth has led to significant advancements in machine learning and data analytics, enabling transformative applications across diverse domains such as healthcare, finance, and smart cities. However, as data continues to expand in volume, variety, and velocity, so do the challenges associated with ensuring its privacy and security [3]-[5]. Traditional centralized machine learning approaches, which require aggregating data at a central server, have become increasingly impractical due to rising concerns over data breaches [6], misuse, and stringent privacy regulations such as the General Data Protection Regulation (GDPR). Federated Learning (FL) has emerged as a revolutionary approach to overcome these challenges by facilitating collaborative model training across distributed devices while retaining data locally, ensuring privacy and security.

Federated learning, first introduced by Google in 2016, shifts the paradigm from centralized to decentralized model training [7], [8]. In FL, instead of transferring raw data to a central server, individual devices compute model updates based on their local data and share these updates with a central aggregator, as shown in Figure 1. The aggregator then integrates the updates to improve the global model iteratively [9]. This distributed approach addresses critical privacy concerns by ensuring that sensitive information [10] never leaves the local devices. FL's decentralized nature also aligns

* Corresponding author: Mmasi Patience Robai

well with the requirements of modern applications that involve sensitive data, making it particularly suitable for domains like personalized healthcare, financial fraud detection, and autonomous systems [11]. [12].

Despite its promise, the implementation of federated learning in real-world environments is fraught with challenges, particularly in heterogeneous networks. Such networks are characterized by a wide variety of devices with differing computational capabilities, network conditions, and data distributions [13], [14]. For instance, devices in an Internet of Things (IoT) environment may have highly imbalanced datasets, limited computational resources [15], and intermittent connectivity. These factors contribute to significant challenges, including inefficient communication, biased model updates, and slow convergence rates. Addressing these issues requires advanced algorithms and adaptive strategies to ensure robust and efficient FL deployment in diverse environments.

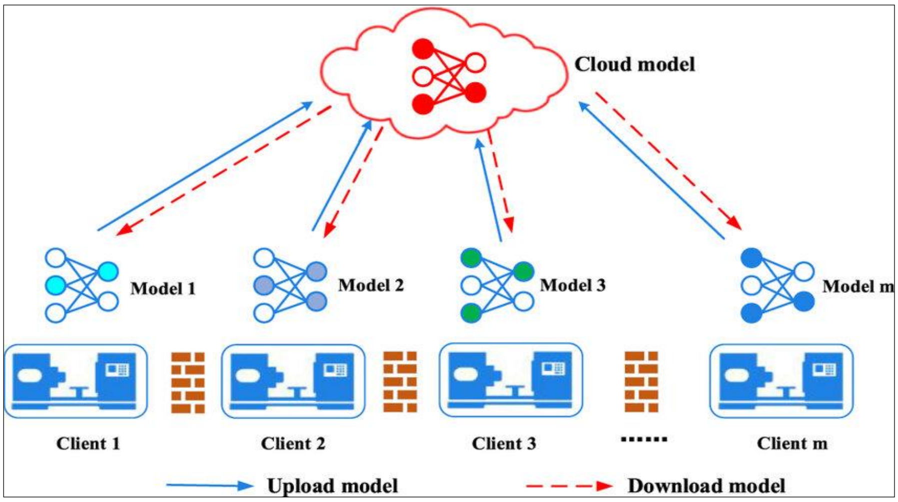

Figure 1 Federated learning

In addition to system heterogeneity, federated learning introduces unique security and privacy vulnerabilities. While the decentralized nature of FL inherently reduces the risks associated with centralizing sensitive data [16], it also creates new attack vectors. For example, adversaries may attempt to infer sensitive information from model updates through data reconstruction or membership inference attacks [17]-[19]. Moreover, malicious nodes can poison the global model by submitting incorrect or adversarial updates, undermining the reliability of the learning process. To address these risks, researchers have proposed various techniques such as differential privacy, secure multi-party computation, homomorphic encryption, and robust aggregation methods. These mechanisms aim to enhance the security and privacy [20] of FL systems while maintaining model utility.

Another critical challenge in federated learning arises from the heterogeneity of data across devices. Unlike traditional machine learning settings where data is assumed to be independent and identically distributed (IID), the data generated by devices in FL is often non-IID [21], [22]. This non-IID nature leads to skewed model updates, causing slower convergence and reduced performance of the global model [23], [24]. Additionally, the variation in device capabilities, ranging from high-performance edge servers to resource-constrained IoT sensors [25], exacerbates the problem, requiring efficient task scheduling and resource allocation strategies.

This survey paper aims to provide a comprehensive review of federated learning for secure and privacy-preserving data analytics in heterogeneous networks. It examines the latest advancements in privacy-preserving techniques, including differential privacy, encryption methods, and secure aggregation protocols. Furthermore, it explores strategies to address the challenges posed by heterogeneity, such as algorithmic adaptations for non-IID data, resource-efficient training methods, and robust communication protocols. The survey also highlights practical applications of Federated Learning across various domains, emphasizing the benefits and limitations of FL in real-world scenarios. Finally, the paper identifies open challenges and future research directions, providing a roadmap for advancing Federated Learning in increasingly complex and dynamic network environments. In a nutshell, this survey seeks to bridge the gap between theoretical advancements and practical implementations of Federated Learning. It aims to serve as a valuable resource for researchers and practitioners seeking to understand the state-of-the-art in FL and its potential to revolutionize secure and privacy-preserving data analytics in heterogeneous networks.

2. Basics of Federated learning

Federated learning is a decentralized machine learning paradigm that enables multiple participants (clients) to collaboratively train a global model while keeping their data localized on their devices [26], [27]. The basic architecture of federated learning revolves around a central server (often called the aggregator) and a set of distributed clients (devices such as smartphones, IoT devices, or computers). The goal is for the clients to collaboratively train a machine learning model without sharing their raw data with each other or with the central server [28], [29]. Instead, only model updates or gradients are exchanged, ensuring data privacy and security [30]. The following are the descriptions of the basic elements.

2.1. Central Server

The central server, also referred to as the aggregator, is responsible for coordinating the federated learning process [31], as depicted in Figure 2. It does not have access to the raw data but instead receives model updates (e.g., gradients or weights) from the clients. The key functions of the central server include:

- *Model initialization*: The central server initializes the global model, which will be trained collaboratively by the clients [32], [33]. This model typically consists of weights and biases, and it may start with random initialization or with pretrained weights from a previous model.

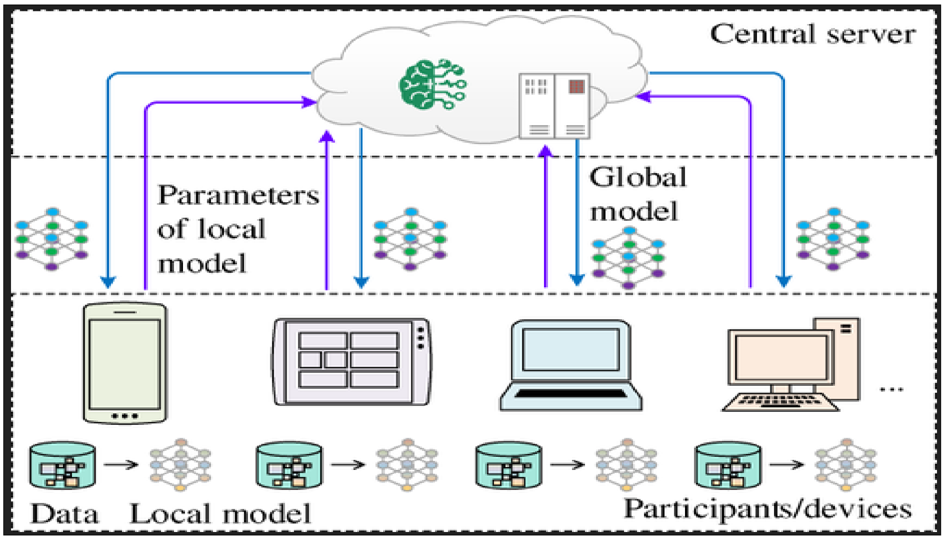

Figure 2 Federated learner elements

- *Model aggregation:* Once the clients perform local training, the server aggregates the model updates sent by the clients [34]. The aggregation process typically involves computing a weighted average of the model parameters or gradients from the participating clients [35]. This step is essential to combine the knowledge learned from the local datasets into a global model.
- *Model distribution:* After aggregating the model updates, the server sends the updated global model back to the clients for the next round of training.

2.2. Clients

The clients are the devices or entities that hold the local data and perform the actual model training. As shown in Figure 2, these devices could include smartphones, computers, IoT devices [36], or edge nodes, each with its own dataset. The key components and responsibilities of the clients include:

- *Local model training*: Each client performs local training on its own data [37]. Since data on the client devices is not shared with other clients or the central server, the local training is done independently [38]. The client computes updates (such as gradients) based on its local data and the model parameters it received from the server.

- *Model updates*: After local training, the client computes the model updates (gradients or weights) and sends them to the central server for aggregation [39], [40]. Importantly, clients only send model updates and not raw data, which preserves the privacy [41] of the data.
- *Participation control*: In some cases, not all clients participate in every round of training. Some clients may be excluded due to network connectivity issues, resource limitations, or voluntary opt-out [42], [43]. The central server can manage the number of participating clients to optimize the federated learning process.

2.3. Federated learning workflow

The federated learning process proceeds in multiple rounds, where each round consists of the following steps, which are summarized in Figure 3:

- *Initialization*: The central server initializes the global model and distributes it to participating clients [44].
- *Local training*: Clients receive the global model and train it locally on their own data [45]. This training typically involves multiple epochs or iterations of gradient descent [46] to adjust the model's parameters.
- *Model update transmission*: Model updates are transmitted by aggregating locally trained model parameters from multiple devices, rather than sharing raw data, to ensure privacy [47], [48]. These updates are sent to a central server, which combines them to improve the global model and distributes it back to the devices for further training..

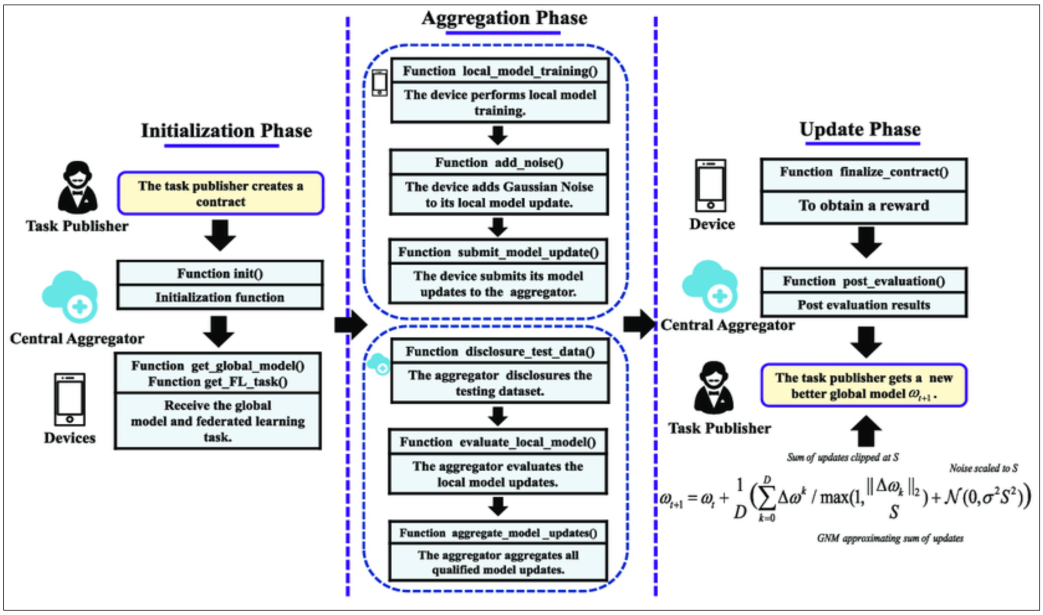

Figure 3 Federated learning workflow

- *Aggregation*: The server collects the model updates from all participating clients and aggregates them [49]. This aggregation usually involves averaging the weights or gradients in a manner that reflects the contribution of each client (e.g., weighted by the number of data points on each client).
- *Global model update*: Once the server aggregates the updates, it updates the global model [50]. This new global model is then sent back to the clients for the next round of local training.

Essentially, the basic architecture of federated learning is built around a central server and distributed clients, where local model training occurs on client devices, and model updates are aggregated at the server to improve the global model.

3. Federated learning and data analytics

Federated learning, as a decentralized approach to machine learning that has gained significant attention in data analytics due to its ability to train models collaboratively without requiring raw data to leave local devices [51]. This paradigm addresses critical privacy, security, and compliance challenges associated with traditional centralized learning [52], where data is aggregated at a central server. As shown in Figure 4, in FL, data remains on individual client devices, such as smartphones, IoT sensors, or edge systems, while model updates—rather than raw data—are exchanged with a central server [53]-[56]. This framework allows for efficient utilization of distributed data sources while minimizing privacy risks and ensuring compliance with data protection regulations like GDPR and HIPAA.

The core workflow of federated learning begins with a global model initialized by a central server and shared with participating clients. Each client uses its local data to train the model [57] independently, computing updates such as gradients or model weights. These updates are then sent back to the central server, where they are aggregated, typically using techniques like Federated Averaging (FedAvg). The aggregated updates are used to refine the global model, which is redistributed to the clients [58]-[61]. This iterative process continues until the global model achieves satisfactory performance or convergence. By focusing on local computation and limited data transfer, FL reduces communication overhead [62] and enhances scalability, making it ideal for large-scale systems.

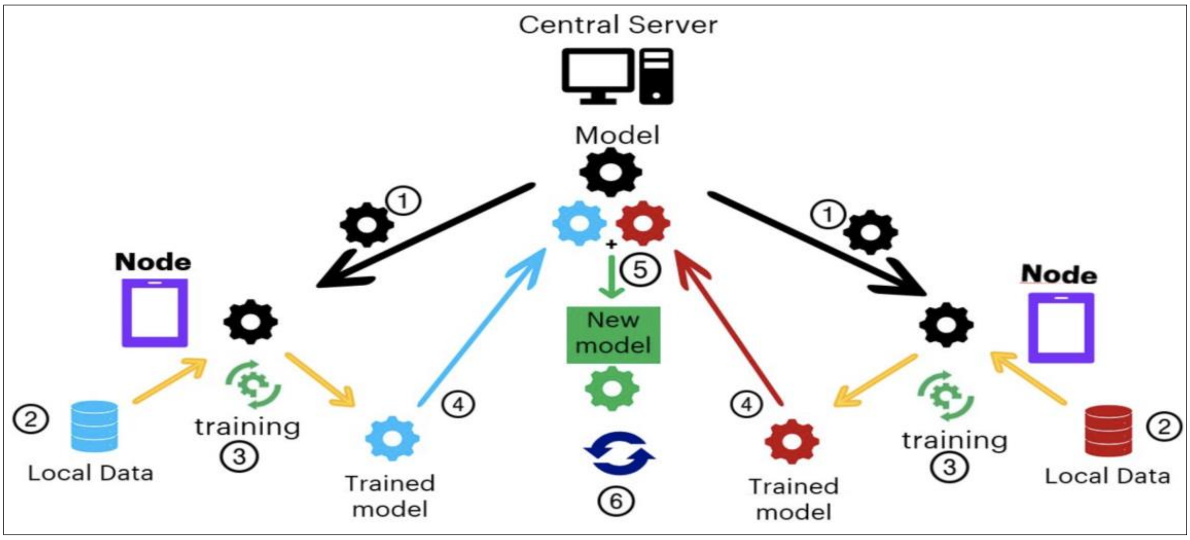

Figure 4 Federated learning – based data analytics

According to [63], federated learning offers numerous advantages for data analytics. Chief among these is privacy preservation, as sensitive data remains localized on devices, significantly reducing the risk of breaches or misuse [64]. FL also provides scalability by leveraging the computational power of distributed devices, enabling analytics across millions of clients. Additionally, FL supports personalization by allowing clients to tailor models to their unique data distributions, which is particularly valuable in domains such as healthcare and personalized services [65], [66]. Despite these benefits, implementing FL presents challenges, particularly in heterogeneous networks where devices may vary widely in computational power [67], network connectivity, and data distributions. Non-IID (non-independent and identically distributed) data across clients can lead to biased model updates, slower convergence, and reduced model performance.

Furthermore, FL introduces unique security risks. While decentralization mitigates data centralization risks, it also creates new vulnerabilities such as model poisoning [68], where malicious clients inject adversarial updates, and inference attacks [69], where attackers attempt to reconstruct sensitive information from model updates. To address these issues, researchers have developed techniques such as differential privacy, secure multi-party computation, and homomorphic encryption to enhance the security and privacy of FL systems [70], [71].

FL's transformative potential is evident in its applications across various domains. In healthcare, for example, FL enables hospitals to collaborate on predictive models without compromising patient data privacy. In IoT ecosystems, it facilitates real-time analytics while preserving the confidentiality of sensor data [72]. In finance, FL is used to develop fraud detection and risk assessment models while adhering to strict data protection laws [73]. Through the addressing of challenges such as data heterogeneity, system variability, and security threats, FL continues to evolve as a key enabler of secure, privacy-preserving, and scalable data analytics in distributed environments [74].

4. Security issues in heterogeneous networks

Heterogeneous networks (HetNets) refer to communication systems that integrate different types of network technologies, infrastructure, and devices, often with varying capabilities and characteristics [75]. As depicted in Figure

5, these networks typically combine cellular networks (such as 4G, 5G), Wi-Fi, IoT devices, and other wireless technologies, creating a diverse and complex environment for data transmission [76], [77]. HetNets are designed to improve coverage, capacity, and overall network performance by leveraging the strengths of different technologies, such as small cells, macro cells, and Wi-Fi offloading [79], [80]. Due to the varying scales, resource limitations, and diverse use cases of the different network components, HetNets face unique challenges in terms of coordination, management, and ensuring efficient, secure, and seamless connectivity across the entire network.

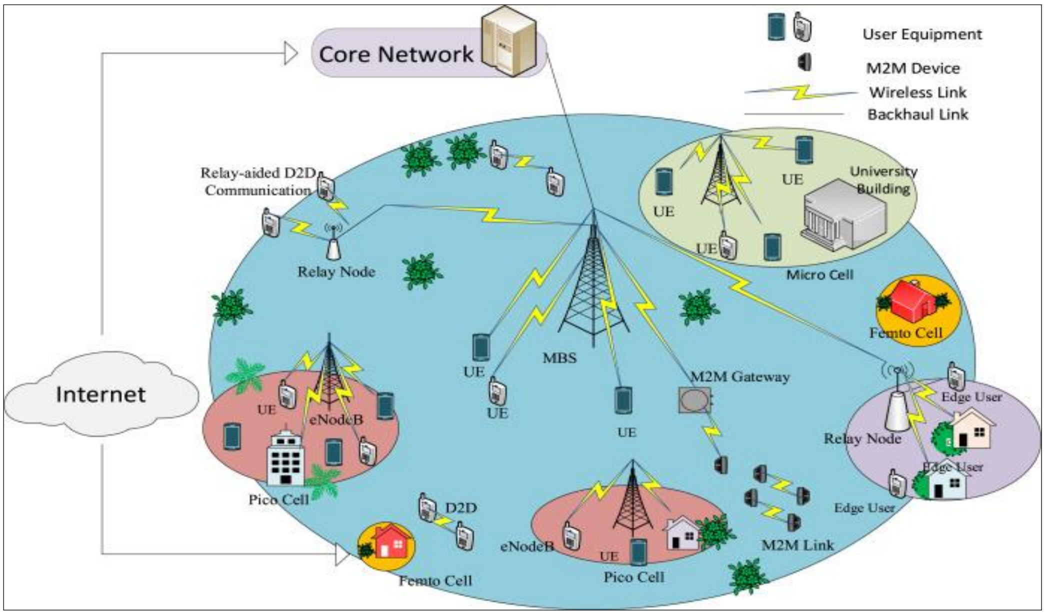

Figure 5 Heterogeneous network

Heterogeneous networks are characterized by a diverse set of devices, varying data distributions, and differing network conditions [81]. While these networks enable scalable and distributed data processing, they also introduce a range of security vulnerabilities. The complexity and variability inherent in HetNets create fertile ground for potential attacks, misconfigurations, and inefficiencies that compromise data integrity, confidentiality, and availability [82], [83]. This section extensively explores the key security issues in heterogeneous networks.

4.1. Data privacy breaches

In heterogeneous networks, data is often generated and stored on devices with varying levels of security capabilities [84]. Devices with lower security standards are more vulnerable to unauthorized access, leading to potential data breaches. For example, an IoT sensor with minimal encryption protocols can serve as an entry point for attackers to gain access to sensitive information in a connected system [85]-[87]. Additionally, the distributed nature of HetNets makes it challenging to implement consistent privacy-preserving mechanisms, as different devices may have incompatible security frameworks.

4.2. Adversarial attacks

Heterogeneous networks are particularly susceptible to adversarial attacks, where malicious entities aim to disrupt the network's operation or compromise its security. Key adversarial threats include:

Eavesdropping: Eavesdropping attacks occur when an unauthorized party intercepts and listens in on communications between two parties, typically to gain access to sensitive information [88], as depicted in Figure 6. This type of attack takes place without the knowledge of the communicating parties and can target data transmitted over various communication channels, such as unencrypted emails, network traffic, or wireless signals [89], [90]. The attacker can steal confidential information, including passwords, personal details, financial data, or intellectual property. Eavesdropping attacks are especially prevalent in unsecured networks, like public Wi-Fi, where attackers can exploit weak or absent encryption protocols to capture data in transit [91]. Preventing eavesdropping requires robust encryption and secure communication protocols to protect data privacy and integrity [92]. Unsecured communication channels in HetNets can be exploited by attackers to intercept sensitive information during transmission.

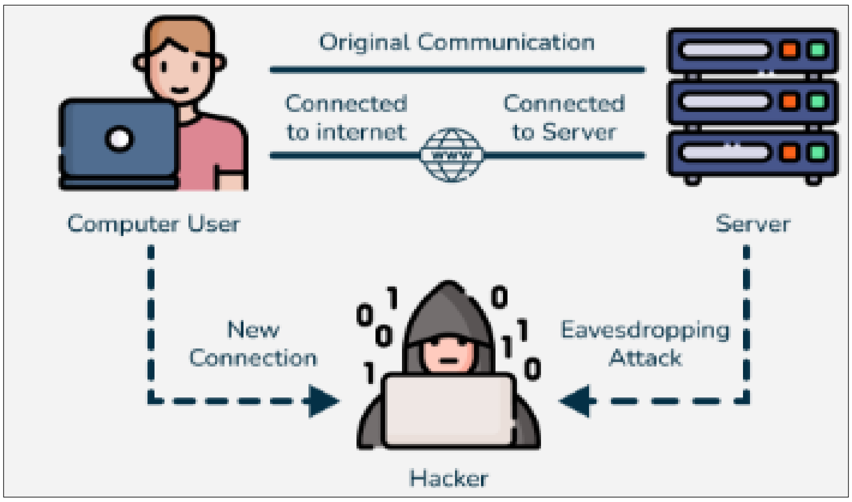

Figure 6 Eavesdropping attack

Man-in-the-Middle (MITM) attacks: Man-in-the-Middle (MitM) attacks are a type of cyberattack where an attacker intercepts and potentially alters the communication between two parties without their knowledge [93]. As demonstrated in Figure 7, the attacker secretly relays or modifies messages between the communicating entities, such as between a user and a website or between two devices in a network [94]. The attacker can eavesdrop on sensitive information, such as login credentials, financial data, or personal details, or inject malicious content to compromise the integrity of the communication [95]-[98]. MitM attacks are particularly dangerous in unsecured communication channels, such as public Wi-Fi networks, where encryption and authentication mechanisms [99] may be weak or absent. An attacker can intercept and alter communications between devices, compromising data integrity and authenticity.

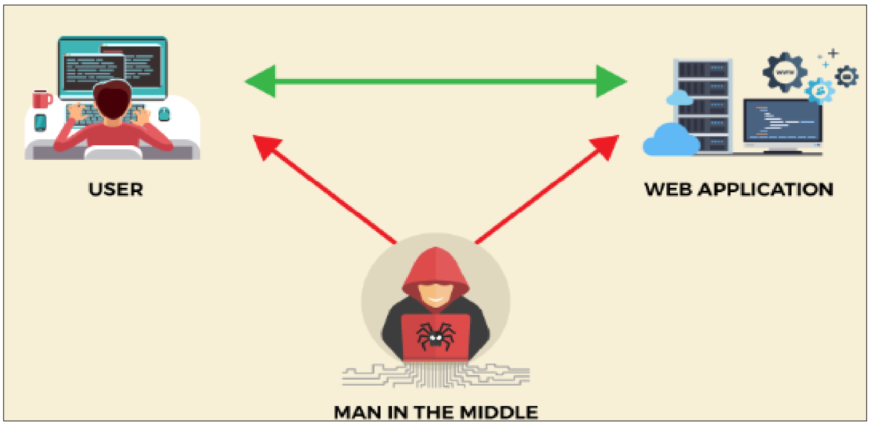

Figure 7 MITM attack

4.3. Device compromise and botnet attacks

Botnet attacks involve a network of compromised devices, often referred to as "bots" or "zombies," that are controlled by a central command-and-control server without the owners' knowledge [100], as depicted in Figure 8. These devices, which can include computers, IoT devices, and smartphones, are infected with malicious software, allowing the attacker to remotely control them [101], [102]. Once part of the botnet, the devices can be used to execute various types of malicious activities, such as launching Distributed Denial of Service (DDoS) attacks, stealing sensitive information, sending spam emails, or spreading malware to other systems [103]. Botnet attacks are particularly dangerous due to the scale and automation of the attack, as they can overwhelm targets, cause widespread damage, and operate under the radar for extended periods. Heterogeneous networks often consist of a mix of resource-constrained devices [104], such as IoT sensors, and high-performance devices, such as edge servers.

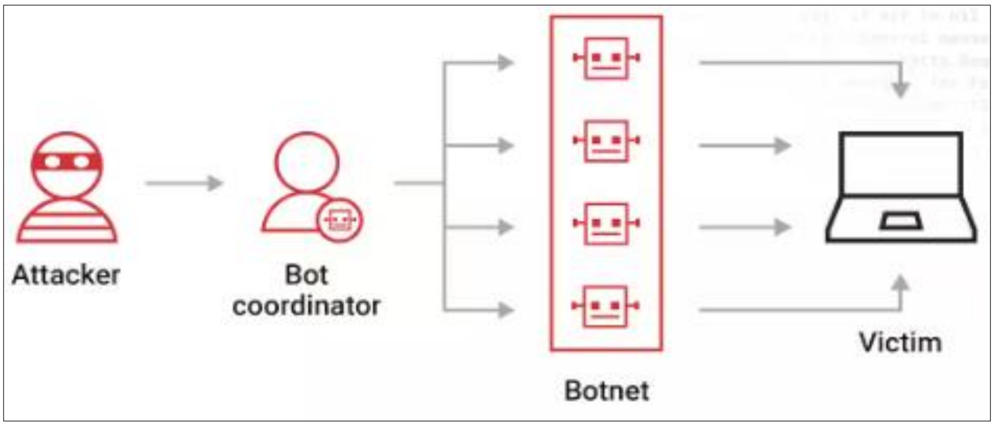

Figure 8 Botnet attack

The former are often less secure and easier to compromise. Once an attacker gains control of such devices, they can form botnets to launch distributed denial-of-service attacks, overwhelming the network and degrading its performance [105]. Device compromise also allows attackers to introduce malicious code or unauthorized updates into the system, undermining the integrity of the network.

4.4. Secure communication challenges

Secure communication in heterogeneous networks poses significant challenges due to the diverse mix of devices, technologies, and protocols involved [106]-[108]. The disparity in computational power, resource availability, and security capabilities among devices—ranging from IoT sensors to high-performance servers—creates vulnerabilities that attackers can exploit. Additionally, the dynamic and decentralized nature of HetNets, with devices constantly joining and leaving, complicates the establishment and maintenance of secure communication channels. Ensuring encryption, authentication, and data integrity across various technologies like cellular, Wi-Fi, and IoT protocols is further hindered by interoperability issues and resource constraints on low-power devices [109]. Furthermore, HetNets are susceptible to advanced threats, including man-in-the-middle (MitM) attacks, eavesdropping, and key management failures [110]-[113]. Addressing these challenges requires adaptive security frameworks that integrate lightweight encryption, scalable authentication mechanisms, and robust key distribution systems tailored to the unique characteristics of HetNets.

4.5. Insider threats

Insider threats in heterogeneous networks involve malicious or negligent actions by individuals with authorized access to the network, such as employees, administrators, or trusted devices, which compromise the network's security [114], [115]. Given the diverse and interconnected nature of HetNets, insiders can exploit their access to sensitive data, infrastructure, or communication channels across various technologies, including cellular, Wi-Fi, and IoT networks. These threats are particularly dangerous because insiders often bypass traditional security measures, such as firewalls and intrusion detection systems, to cause data breaches, disrupt operations, or introduce malware [116], [117]. The complexity of HetNets amplifies the risk, as it can be difficult to monitor and manage access across multiple platforms and devices. In collaborative environments like enterprise HetNets, insider threats pose a significant risk. Employees or trusted entities with access to sensitive systems may intentionally or unintentionally compromise security. The heterogeneity of access controls and policies across devices and platforms further exacerbates the challenge of identifying and mitigating insider threats [118].

4.6. Key management and authentication issues

Effective key management is critical for ensuring secure communication and data access in heterogeneous networks. However, the diversity of devices and protocols makes centralized key management infeasible. This leads to challenges such as:

Key distribution: Key distribution refers to the process of securely sharing cryptographic keys among different network entities, such as base stations, devices, and users, to enable secure communication and data exchange [119], [120]. This process is depicted in Figure 9, where KDC represents the key distribution center. Given the diverse and often decentralized nature of HetNets, which integrate various technologies (e.g., cellular, Wi-Fi, IoT), key distribution must ensure that each component can securely authenticate and encrypt communications across different network layers and devices [121].

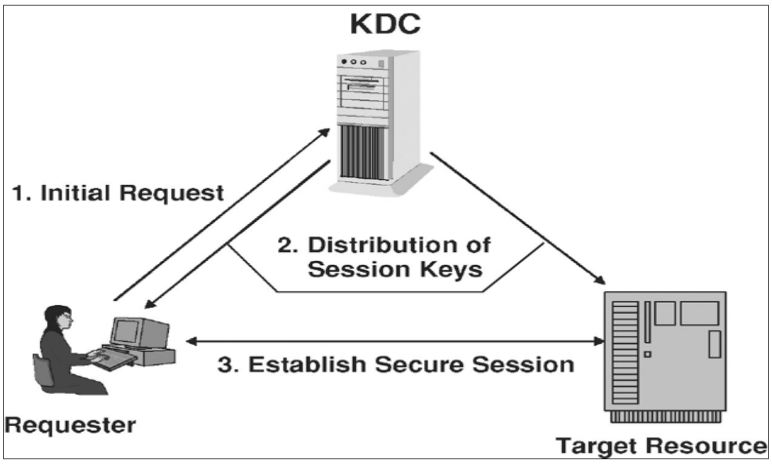

Figure 9 Key distribution

This process typically involves public-key infrastructure (PKI), symmetric or asymmetric encryption techniques, and secure key exchange protocols to prevent unauthorized access, eavesdropping, or tampering with sensitive data [122], [123]. Effective key distribution in HetNets is crucial for maintaining the confidentiality, integrity, and authenticity of communications, especially in the face of potential security threats like MitM attacks or eavesdropping.

Authentication: In heterogeneous networks, authentication is the process of verifying the identity of devices, users, or network components to ensure secure communication and prevent unauthorized access [124]-[126]. Figure 10 gives an illustration of the authentication process in a 6G hetnets In HetNets, where diverse technologies such as cellular networks, Wi-Fi, and IoT devices are interconnected, authentication mechanisms must accommodate the varied capabilities and security requirements of each component [127].

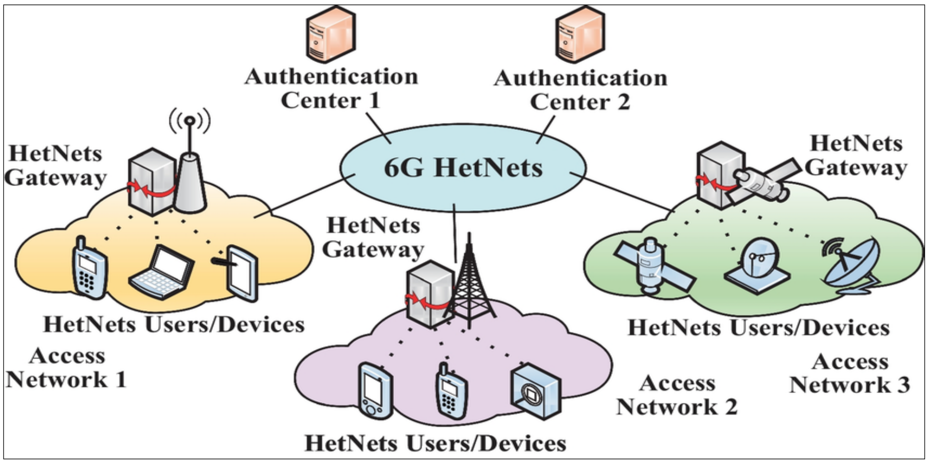

Figure 10 Authentication in 6G Hetnet

This involves using a combination of traditional techniques like username/password verification, as well as more advanced methods such as biometrics, certificates, token-based systems, and multi-factor authentication (MFA) [128], [129]. Secure authentication protocols are critical in HetNets to prevent identity spoofing, unauthorized access, and other security breaches, ensuring that only legitimate devices and users can participate in the network, thus maintaining data integrity, privacy, and overall network security [130], [131].

4.7. Non-uniform security policies

Non-uniform security policies in heterogeneous networks refer to the inconsistent application of security measures across the diverse technologies, devices, and protocols that make up these networks. Since HetNets integrate components like cellular networks, Wi-Fi, and IoT devices, each with distinct capabilities and requirements, enforcing uniform security standards becomes challenging [132], [133]. This disparity can create weak points in the network, as devices with lower security levels become entry points for attackers, compromising the entire system. For example, robust encryption might be used in cellular communication, while IoT devices in the same network rely on lightweight or outdated security measures due to resource constraints [134]- [136]. The lack of standardized policies can lead to vulnerabilities in authentication, data encryption, and access control. In a heterogeneous network, devices often belong to different administrative domains with varying security policies. This lack of uniformity creates gaps in the overall security framework. For instance, some devices may enforce strong encryption and multi-factor authentication [137], while others rely on basic security measures. Attackers can exploit these discrepancies to target the weakest links in the network.

4.8. Scalability and resource constraints

Scalability and resource constraints are significant challenges in heterogeneous networks due to the diverse range of devices and technologies with varying capabilities [138]-[140]. HetNets often integrate resource-constrained devices, such as IoT sensors and edge nodes, alongside more powerful infrastructure like cellular base stations and servers. These devices must communicate and collaborate efficiently despite differences in computational power, memory, and energy availability [141]. As HetNets grow in size and complexity, managing resources like bandwidth, processing power, and storage becomes increasingly difficult, leading to potential bottlenecks and degraded performance. The dynamic nature of HetNets, with devices frequently joining or leaving the network, further complicates scalability [142], [143]. Ensuring seamless operation and resource optimization requires efficient load-balancing algorithms, dynamic resource allocation techniques, and scalable security protocols tailored to the diverse and evolving requirements of HetNets.

4.9. Malware and ransomware attacks

Malware and ransomware attacks in heterogeneous networks involve malicious software that targets the diverse devices and systems connected across the network [144]. Malware, including viruses, worms, and Trojans, can infect IoT devices, smartphones, computers, or network infrastructure, often without detection, leading to system compromise, data theft, or disruption of services [145]. As illustrated in Figure 11, ransomware, a specific type of malware, encrypts a victim's files or locks access to critical systems and demands a ransom for restoration. In HetNets, the challenge is compounded by the variety of devices, operating systems, and communication protocols [146], which may have different levels of security, making them vulnerable to attacks.

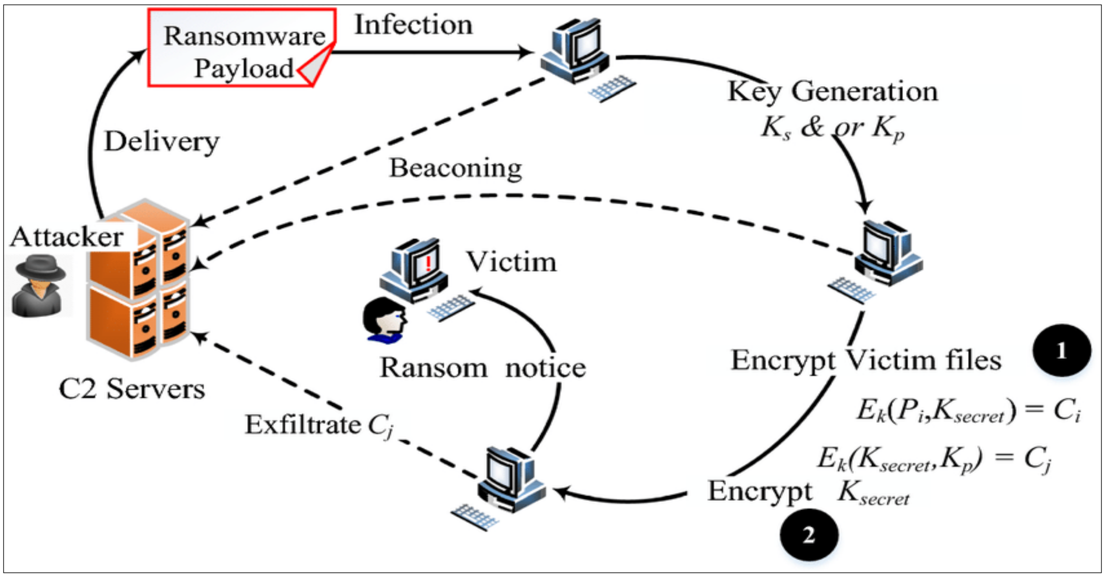

Figure 11 Ransomware attack

These threats can spread quickly across interconnected devices, leading to widespread disruption, financial loss, and loss of sensitive data. Effective prevention and mitigation strategies in HetNets include timely software updates, endpoint security, network monitoring, and user awareness to minimize the risk of malware and ransomware infections [147], [148]. As explained in [149], heterogeneous networks are prime targets for malware and ransomware attacks due to their distributed and interconnected nature. Attackers can introduce malware into less secure devices, which can then propagate across the network. Ransomware attacks can lock down critical systems, demanding payment for restoring access 150], and may have a cascading effect in HetNets, affecting multiple devices and services.

4.10. Lack of standardized security protocols

The lack of standardized security protocols in heterogeneous networks is a critical challenge stemming from the diverse technologies, devices, and communication standards within these networks [151], [152]. HetNets combine elements such as cellular networks, Wi-Fi, and IoT devices, each with its own security requirements and limitations. Without standardized protocols, ensuring consistent and interoperable security measures across these varied components becomes difficult [153], leaving gaps that attackers can exploit. This inconsistency complicates key management, authentication, and data encryption [154], as devices with differing capabilities may not support advanced or uniform security practices. Moreover, the absence of standards hinders collaboration among network providers, device manufacturers, and stakeholders. Addressing this issue requires developing universal security frameworks that are adaptable to diverse technologies while ensuring comprehensive protection and seamless integration in the HetNet ecosystem.

4.11. Physical security vulnerabilities

Physical security vulnerabilities in heterogeneous networks arise from the diverse and widely distributed components, such as IoT devices, base stations, and edge servers, many of which operate in remote or unsecured locations [155], [156]. Unlike centralized systems, HetNets often deploy small cells, access points, and sensors in public or outdoor environments, making them susceptible to physical tampering [157], theft, or destruction. Attackers can exploit these vulnerabilities to gain unauthorized access, disrupt services, or compromise the network by introducing malicious hardware or software [158]. For instance, physically tampered IoT devices can act as entry points for cyberattacks, impacting the broader network. Ensuring physical security in HetNets requires robust measures, such as tamper-resistant hardware, secure enclosures, regular maintenance checks, and the deployment of physical surveillance systems to protect critical infrastructure.

Security issues in heterogeneous networks stem from their intrinsic diversity and interconnected nature, making them complex and challenging to secure [159]. Attackers exploit the vulnerabilities arising from resource constraints, non-uniform policies, and outdated protocols to compromise data confidentiality, integrity, and availability. Mitigating these challenges requires a holistic approach that combines advanced security technologies [160], standardization efforts, and proactive policy enforcement. By addressing these issues, heterogeneous networks can achieve the resilience needed to support secure and robust data processing in increasingly interconnected environments.

5. Federated learning for security enhancement in heterogeneous networks

Federated learning is a decentralized approach to machine learning that enables multiple distributed devices (clients) to collaboratively train a global model without sharing their local data [161]. The rise of heterogeneous networks, characterized by a diverse set of devices, varying network conditions, and disparate data sources, has introduced complex challenges in both machine learning and security [162], [163]. FL presents an innovative way to address these challenges, not only enhancing privacy and efficiency but also strengthening security in such networks. By keeping sensitive data localized on devices, FL mitigates the risk of data breaches, while also enabling the development of robust models in environments where data is often sparse, non-IID (non-independent and identically distributed), and prone to security threats.

The sub-sections below explore how federated learning can be leveraged for security enhancement in heterogeneous networks, focusing on privacy preservation, resilience against adversarial attacks, secure communication, and model integrity.

5.1. Privacy preservation in heterogeneous networks

In traditional centralized machine learning models, data must be aggregated on a central server to train a model [164]. This centralization creates significant privacy risks as the raw data is exposed to potential breaches, leading to data misuse. Federated learning addresses this issue by allowing data to remain on individual devices. Only model updates, not raw data, are shared with a central server or coordinator [165], [166]. This decentralized approach minimizes the exposure of sensitive data, making it ideal for applications in privacy-sensitive domains like healthcare, finance, and IoT.

- *Differential privacy*: One of the key techniques used to further enhance privacy [167] in FL is differential privacy (DP). DP ensures that the information shared from the local models does not allow the reconstruction of sensitive individual data. In FL, differential privacy can be applied to the gradients or updates sent from the clients to the server [168, [169]. This prevents an attacker from inferring details about the local data, even if they gain access to model parameters or gradients. Differential privacy is crucial for securing personal information in heterogeneous networks, where data sources are often diverse and untrusted.
- *Homomorphic encryption*: Another technique used in FL to preserve privacy is homomorphic encryption [170], which allows computations to be performed on encrypted data without needing to decrypt it first. This ensures that even when malicious actors intercept the updates during transmission, the information remains confidential [171]. Homomorphic encryption, though computationally intensive, is gaining traction in FL systems, particularly in contexts requiring high privacy standards.

By utilizing these privacy-preserving techniques [172], FL ensures that even in a heterogeneous network with different security levels across devices, sensitive information is protected.

5.2. Resilience to adversarial attacks

Adversarial attacks are a major security concern in federated learning, especially in heterogeneous networks. Malicious actors may manipulate the model updates sent from clients to the central server to poison the global model, degrade its performance, or inject incorrect information [173], [174]. These attacks can be especially damaging in heterogeneous networks, where devices differ in computational capabilities, data quality, and reliability.

- *Federated averaging and robust aggregation*: To address the risks of adversarial poisoning, FL uses aggregation techniques like Federated Averaging (FedAvg), where the server averages the updates from clients to build a more accurate global model [175], [176]. However, when adversarial updates are present, simple averaging may not be robust enough. Several robust aggregation algorithms [177] have been developed, such as Trimmed Mean or Krum, which discard outlier updates from clients that deviate significantly from the majority, preventing malicious updates from contaminating the global model.
- *Secure federated learning*: In scenarios where adversarial clients can actively launch poisoning attacks, techniques like secure multi-party computation (SMC) and secure aggregation are used to ensure that the model updates remain confidential and that the global model is protected from malicious manipulation [178]-[180]. In secure aggregation, clients compute their updates in a way that prevents the server from learning individual updates until they are aggregated [181], thereby reducing the opportunity for attackers to target specific clients.

FL can also utilize Federated Adversarial Training (FAT), a technique where the model is trained to be more robust against adversarial inputs by including adversarial examples during the training process. This approach helps ensure that the model can resist attacks [182] when deployed in heterogeneous environments with a high risk of adversarial manipulation.

5.3. Secure communication in heterogeneous networks

Communication is a key component in federated learning systems, especially in heterogeneous networks, where devices have varying connectivity, bandwidth, and computational capabilities. The communication channels between devices and the central server are vulnerable to eavesdropping, man-in-the-middle attacks, and tampering [183]-[186].

- *Encryption and authentication*: To secure communication, FL incorporates end-to-end encryption protocols [187], ensuring that the updates sent from clients to the server are protected during transmission. This encryption prevents unauthorized entities from accessing the updates, thus protecting both the integrity of the global model and the privacy of the clients [188], [189]. Additionally, mutual authentication protocols are crucial for verifying the identity of both the clients and the server before the exchange of sensitive model updates, preventing unauthorized devices from participating in the federated learning process.
- *Lightweight encryption protocols*: Given the resource-constrained nature of many devices in heterogeneous networks (e.g., IoT sensors, mobile phones), using lightweight encryption protocols is vital [190], [191]. These protocols strike a balance between security and computational efficiency, enabling secure communication without heavily taxing the devices' limited computational resources [192]. Techniques such as elliptic curve cryptography (ECC) are commonly used for secure communication in such contexts.

By securing the communication process in federated learning, these measures reduce the likelihood of data leakage or attack, which is particularly critical in heterogeneous environments where devices may have varying security capabilities.

5.4. Model integrity and integrity verification

Maintaining the integrity of the global model is essential to the success of federated learning [193], especially in heterogeneous networks where devices have varying levels of trustworthiness. Clients in these networks may intentionally or unintentionally send inaccurate updates, which could harm the model's accuracy and reliability.

- *Model validation and checkpoints*: One approach to maintaining model integrity is checkpointing, where intermediate models are periodically validated before further aggregation [194]. This ensures that only models that meet specific performance or accuracy benchmarks are used for global aggregation [195]. In case of unexpected drops in performance, the system can revert to a previous model checkpoint to minimize the impact of potential tampering.
- *Blockchain for model auditing*: Another promising approach for ensuring model integrity is the use of blockchain technology [196]. Blockchain can be used to create an immutable audit trail of all model updates and transactions. This provides an additional layer of transparency and accountability [197], allowing the system to track and verify model changes, detect unauthorized modifications, and ensure that all updates are legitimate.

5.5. Defending against Sybil and DDoS attacks

In heterogeneous networks, especially when many low-cost, resource-constrained devices are involved, Sybil attacks (where a malicious actor creates multiple fake identities to manipulate the system) and Distributed Denial of Service (DDoS) attacks are potential threats [198], [199]. These attacks can overwhelm the system or skew the model's training process.

- *Client authentication and reputation systems*: A robust client authentication mechanism, combined with a reputation system, can help defend against Sybil attacks [200], [201]. Clients with a high reputation (i.e., historically reliable devices) can be given more weight in model aggregation, whereas suspicious or low-reputation clients can be excluded or down-weighted.
- *Rate limiting and traffic filtering*: To prevent DDoS attacks, rate limiting and traffic filtering mechanisms can be employed to detect and mitigate large volumes of malicious updates. These mechanisms can identify abnormal communication patterns and prevent malicious nodes [202] from overwhelming the server or the federated learning process.

It is clear that federated learning offers a powerful framework for enhancing security in heterogeneous networks by keeping sensitive data local, employing robust privacy-preserving techniques, and securing communication channels [203]. It enables secure, decentralized collaboration for model training while mitigating the risks posed by adversarial attacks, ensuring model integrity, and preventing data leakage. However, deploying FL in such environments requires careful consideration of security issues, including device heterogeneity, varying computational resources, and the presence of malicious actors [204]. By integrating advanced techniques such as differential privacy, secure aggregation, robust aggregation methods, and blockchain auditing, FL can significantly improve the security and reliability of data analytics in heterogeneous networks [205], paving the way for more secure, scalable, and privacy-preserving machine learning applications.

6. Research gaps and future research scopes

Federated learning has emerged as a promising solution to enhance data privacy and security, especially in the context of heterogeneous networks [206]. By keeping data localized on distributed devices, FL offers the advantage of avoiding centralized data collection, which can be vulnerable to security breaches. However, despite its potential, there are significant research gaps that need to be addressed to ensure the security and efficiency [207] of federated learning in heterogeneous networks. These gaps span multiple aspects, including model robustness, privacy-preserving techniques, secure communication, adversarial defense mechanisms, and system-level optimization.

This section identifies and extensively describes these research gaps in the context of Federated Learning for security enhancement in heterogeneous networks.

6.1. Model robustness in heterogeneous environments

Heterogeneous networks consist of devices with varying computational power, storage capacity, network bandwidth, and data characteristics [208]. These disparities introduce several challenges for Federated Learning, especially in terms of model robustness. Some key research gaps include:

6.1.1. Handling non-IID data

One of the most significant challenges in FL for heterogeneous networks is the issue of non-independent and identically distributed (Non-IID) data [209]. In many real-world scenarios, the data on different clients can be highly skewed, which can lead to biased or suboptimal model performance. Current FL algorithms often assume that the data on each device is IID, but this assumption is rarely true in heterogeneous environments [210], [211]. Further research is needed to develop more robust federated learning algorithms that can effectively [212] handle Non-IID data, ensuring that the global model performs well across diverse data distributions.

6.1.2. Dynamic device participation

In heterogeneous networks, devices may join and leave the learning process at any time due to issues like network connectivity, battery constraints, or resource availability [213]. This dynamic participation can lead to issues like model convergence delays or instabilities. Developing techniques that can adapt to the dynamic nature of device participation without compromising the model's performance or security is an important area of research.

6.1.3. Stragglers and delayed updates

Some clients in a heterogeneous network may have lower computational capabilities, resulting in slower training times [214]. These slower clients, known as "stragglers," can introduce delays in the aggregation process, slowing down convergence. Current FL systems often fail to account for the heterogeneous processing speeds of clients [215]. Research is needed to devise more efficient aggregation algorithms that can handle straggler issues and improve the convergence time in diverse device environments.

6.2. Security against adversarial attacks in heterogeneous networks

Federated learning in heterogeneous networks is particularly vulnerable to adversarial attacks [216], where malicious clients send poisoned updates to disrupt the global model's training. These attacks can significantly degrade model performance and compromise security [217]. Several research gaps in adversarial defense mechanisms need to be addressed:

6.2.1. Poisoning attacks and robust aggregation

While current methods like Federated Averaging (FedAvg) work well in ideal conditions, they are highly susceptible to poisoning attacks [218]. Malicious clients can inject inaccurate or malicious updates to corrupt the global model [219]. Research is needed to develop more robust aggregation techniques that can distinguish between legitimate and malicious updates, ensuring that the global model remains resilient to adversarial manipulation. Approaches such as Byzantine Fault Tolerance (BFT) and robust aggregation methods like Krum or Trimmed Mean need further refinement and optimization for heterogeneous environments.

6.2.2. Defending against model inversion and membership inference attacks

In federated learning, attackers can attempt to infer private data or membership information based on model updates [220]. Model inversion attacks aim to reconstruct private data from the model's outputs, while membership inference attacks attempt to determine whether a particular data point was used in training the model [221]. Addressing these types of attacks in heterogeneous networks, where the data is distributed across diverse devices, is a pressing research need. Techniques like differential privacy and secure multi-party computation (SMC) need to be integrated and optimized for these specific attack vectors.

6.2.3. Federated adversarial training

One area where federated learning could be enhanced is in the integration of adversarial training, which improves model robustness [222] by incorporating adversarial examples during training. However, adversarial training in FL is still in its infancy [223], and further research is required to develop decentralized adversarial training mechanisms that do not compromise privacy while defending against adversarial examples.

6.3. Privacy-preserving techniques in federated learning

While federated learning inherently improves privacy by keeping data localized [224], additional privacy-preserving techniques are necessary to protect sensitive information during model updates and aggregation. Key research gaps include:

6.3.1. Advanced Differential Privacy (DP) techniques

Differential privacy is one of the most widely adopted privacy-preserving techniques in FL [225]. However, ensuring strong privacy guarantees without significantly affecting model performance is a challenge. Research is needed to explore advanced DP techniques, such as local differential privacy, that can provide stronger privacy guarantees with minimal impact on the model's accuracy [226], [227]. There is also a need to develop adaptive DP mechanisms that can balance privacy and utility based on the privacy requirements of different clients.

6.3.2. Secure aggregation and homomorphic encryption

Secure aggregation ensures that the central server cannot access individual client updates, while homomorphic encryption allows computations to be performed on encrypted data without decryption [228], [229]. While both techniques have shown promise in federated learning, their implementation in heterogeneous networks remains a significant research challenge. The computational overhead required for these techniques can be prohibitive, particularly in resource-constrained devices. Research into more lightweight cryptographic techniques [230] that can enable secure aggregation and homomorphic encryption for heterogeneous devices is needed to ensure that these privacy mechanisms can be deployed at scale.

6.3.3. Privacy in cross-domain federated learning

Heterogeneous networks often consist of clients from different domains, each with its own privacy and security policies [231]. Cross-domain federated learning, where devices from different organizations or sectors collaborate without sharing sensitive data, poses additional privacy challenges. Research is needed to develop privacy-preserving techniques [232] that can facilitate secure cross-domain FL while ensuring that privacy regulations, such as GDPR and HIPAA, are met.

6.4. Secure communication in federated learning

In heterogeneous networks, secure communication is critical to prevent eavesdropping, man-in-the-middle attacks, and tampering of model updates during transmission [233]. Research gaps in secure communication protocols for FL include:

6.4.1. Lightweight cryptographic protocols

Many devices in heterogeneous networks, such as IoT sensors and mobile devices, have limited processing power and bandwidth [234]. While traditional encryption methods provide strong security, they can impose a significant computational and communication burden on such devices [235], [236]. Research is needed to develop lightweight cryptographic protocols [237] that can provide secure communication while minimizing overhead. Techniques like elliptic curve cryptography (ECC) and homomorphic encryption need to be optimized for low-power, resource-constrained devices in FL.

6.4.2. Efficient Secure Multi-Party Computation (SMC)

Secure multi-party computation allows multiple parties to compute a function without revealing their private data [238]. While SMC has been proposed as a way to secure federated learning, it suffers from significant computational and communication overheads [239]. Developing more efficient SMC protocols that are practical for heterogeneous networks with varying device capabilities is a key research gap.

6.4.3. Communication efficiency and privacy

As heterogeneous networks expand, communication efficiency becomes a major concern, especially when it comes to sending model updates from clients to the server [240]. Current FL approaches often require frequent communication, which can result in high latency and excessive bandwidth consumption [241]. Research is needed to design privacy-preserving techniques [242] that reduce the communication burden while still ensuring data security. Compression methods and federated distillation can help mitigate this issue by reducing the size of updates without compromising privacy.

6.5. System-level optimization and scalability

One of the critical challenges in deploying federated learning at scale in heterogeneous networks is ensuring system-level optimization. Some of the key research gaps in this area include:

6.5.1. Scalable federated learning architectures

In large-scale heterogeneous networks, the number of devices can reach millions or even billions, posing scalability challenges for FL [243]. Current FL algorithms struggle to scale efficiently as the number of devices grows [244]. Research is needed to design scalable architectures that can handle a large number of devices while maintaining security and performance. This includes techniques like asynchronous federated learning, model partitioning, and peer-to-peer federated learning that can scale without overwhelming the central server.

6.5.2. Resource-aware federated learning

Devices in heterogeneous networks have varying resources (e.g., battery, computational power, storage), which can impact the efficiency of the federated learning process [245], [246]. Research is needed to develop resource-aware federated learning algorithms that can dynamically adjust the participation of clients based on their available resources, network conditions, and computational capabilities. Such mechanisms will improve the overall efficiency and security of the system.

6.5.3. Fairness and incentivization

Federated learning relies on voluntary participation from clients, and ensuring fairness in the contribution of clients is essential for its success. Research on incentive mechanisms and fairness models is needed to ensure that clients contribute meaningful updates without being incentivized to engage in malicious behavior. These models must take into account the heterogeneity in devices [247], ensuring equitable contributions from clients with different capabilities.

While federated learning offers a promising approach to secure and privacy-preserving data analytics in heterogeneous networks [248], several research gaps remain in improving its security, efficiency, and scalability. These gaps include developing robust mechanisms for handling non-IID data, defending against adversarial attacks, optimizing privacy-preserving techniques, securing communication channels, and addressing system-level challenges such as scalability and resource constraints [249]-[253]. By addressing these challenges, Federated Learning can become a more effective and secure solution for distributed machine learning in heterogeneous networks, enabling the development of privacy-preserving and robust data analytics systems.

7. Conclusion

Federated learning has emerged as a revolutionary approach to distributed machine learning, particularly in heterogeneous networks, where data is dispersed across a diverse range of devices with varying capabilities. FL allows collaborative model training without the need to centralize sensitive data, offering significant benefits for privacy, security, and efficiency. However, as heterogeneous networks continue to expand and evolve, the security challenges associated with FL become increasingly complex. This survey has explored the various facets of Federated Learning for security enhancement in heterogeneous environments, focusing on privacy preservation, adversarial defenses, secure communication, and model integrity. Despite the advancements made in federated learning, significant research gaps still persist in ensuring robust security mechanisms across heterogeneous networks. These challenges include handling non-IID data, developing effective defenses against adversarial attacks, securing communication channels, and providing scalable, resource-efficient solutions. Additionally, the integration of advanced privacy-preserving techniques such as differential privacy, secure aggregation, and homomorphic encryption requires further optimization to balance privacy guarantees with model performance, especially when applied in resource-constrained devices. The future of Federated Learning in heterogeneous networks lies in addressing these security and privacy challenges while improving system efficiency and scalability. This will involve refining existing algorithms, developing novel techniques for secure aggregation and adversarial training, and enhancing the ability of FL systems to handle the dynamic and diverse nature of heterogeneous networks. Furthermore, interdisciplinary research that integrates cryptographic, machine learning, and networking techniques will be crucial in shaping secure and scalable Federated Learning systems.

Compliance with ethical standards

Disclosure of conflict of interest

The author holds no conflict of interest.

References

[1] Zhao C, Wang J, Wang Y, Liu W. Data-driven diabetes management: a statistical assessment information system leveraging big data. Smart Science. 2024 Oct 30:1-5.

[2] Hlophe MC, Maharaj BT. From cyber–physical convergence to digital twins: A review on edge computing use case designs. Applied Sciences. 2023 Dec 14;13(24):13262.

[3] Badshah A, Daud A, Alharbey R, Banjar A, Bukhari A, Alshemaimri B. Big data applications: overview, challenges and future. Artificial Intelligence Review. 2024 Sep 16;57(11):290.

[4] Sargiotis D. Overcoming Challenges in Data Governance: Strategies for Success. InData Governance: A Guide 2024 Sep 12 (pp. 339-363). Cham: Springer Nature Switzerland.

[5] Radhi BM, Hussain MA, Abduljabbar ZA, Nyangaresi VO. Secure and Fast Remote Application–Based Authentication Dragonfly Using an LED Algorithm in Smart Buildings. In2024 International Conference on Artificial Intelligence in Information and Communication (ICAIIC) 2024 Feb 19 (pp. 509-517). IEEE.

[6] Torres D, Castillo J. AI Techniques for Decentralized Data Processing: Advanced Methods for Enhancing Scalability, Efficiency, and Real-Time Decision-Making in Distributed Architectures. Journal of Artificial Intelligence and Machine Learning in Management. 2024 Feb 12;8(2):22-43.

[7] Banabilah S, Aloqaily M, Alsayed E, Malik N, Jararweh Y. Federated learning review: Fundamentals, enabling technologies, and future applications. Information processing and management. 2022 Nov 1;59(6):103061.

[8] Zhang C, Xie Y, Bai H, Yu B, Li W, Gao Y. A survey on federated learning. Knowledge-Based Systems. 2021 Mar 15;216:106775.

[9] AbdulRahman S, Tout H, Ould-Slimane H, Mourad A, Talhi C, Guizani M. A survey on federated learning: The journey from centralized to distributed on-site learning and beyond. IEEE Internet of Things Journal. 2020 Oct 12;8(7):5476-97.

[10] Nyangaresi VO, Alsolami E, Ahmad M. Trust-enabled Energy Efficient Protocol for Secure Remote Sensing in Supply Chain Management. IEEE Access. 2024 Aug 12.

[11] Bharati S, Mondal MR, Podder P, Prasath VS. Federated learning: Applications, challenges and future directions. International Journal of Hybrid Intelligent Systems. 2022 Feb;18(1-2):19-35.

[12] Drainakis G, Pantazopoulos P, Katsaros KV, Sourlas V, Amditis A, Kaklamani DI. From centralized to Federated Learning: Exploring performance and end-to-end resource consumption. Computer Networks. 2023 Apr 1;225:109657.

[13] Zhou N, Li YN, Mohajer A. Distributed capacity optimisation and resource allocation in heterogeneous mobile networks using advanced serverless connectivity strategies. International Journal of Sensor Networks. 2024;45(3):127-47.

[14] Sachin DN, Annappa B, Hegde S, Abhijit CS, Ambesange S. Fedcure: A heterogeneity-aware personalized federated learning framework for intelligent healthcare applications in iomt environments. IEEE Access. 2024 Jan 23.

[15] Alzaidi ZS, Yassin AA, Abduljabbar ZA, Nyangaresi VO. Development Anonymous Authentication Maria et al.'s Scheme of VANETs Using Blockchain and Fog Computing with QR Code Technique. In2024 10th International Conference on Control, Decision and Information Technologies (CoDIT) 2024 Jul 1 (pp. 2247-2252). IEEE.

[16] Hu K, Gong S, Zhang Q, Seng C, Xia M, Jiang S. An overview of implementing security and privacy in federated learning. Artificial Intelligence Review. 2024 Jul 11;57(8):204.

[17] Bai L, Hu H, Ye Q, Li H, Wang L, Xu J. Membership Inference Attacks and Defenses in Federated Learning: A Survey. ACM Computing Surveys. 2024.

[18] Hu H, Zhang X, Salcic Z, Sun L, Choo KK, Dobbie G. Source inference attacks: Beyond membership inference attacks in federated learning. IEEE Transactions on Dependable and Secure Computing. 2023 Oct 3.

[19] Ha T, Dang TK. Inference attacks based on GAN in federated learning. International Journal of Web Information Systems. 2022 Oct 25;18(2/3):117-36.

[20] Nyangaresi VO, Al-Joboury IM, Al-sharhanee KA, Najim AH, Abbas AH, Hariz HM. A Biometric and Physically Unclonable Function-Based Authentication Protocol for Payload Exchanges in Internet of Drones. e-Prime-Advances in Electrical Engineering, Electronics and Energy. 2024 Feb 23:100471.

[21] Ma X, Zhu J, Lin Z, Chen S, Qin Y. A state-of-the-art survey on solving non-iid data in federated learning. Future Generation Computer Systems. 2022 Oct 1;135:244-58.

[22] Zhu H, Xu J, Liu S, Jin Y. Federated learning on non-IID data: A survey. Neurocomputing. 2021 Nov 20;465:371-90.

[23] Wang H, Muñoz-González L, Eklund D, Raza S. Non-IID data re-balancing at IoT edge with peer-to-peer federated learning for anomaly detection. InProceedings of the 14th ACM conference on security and privacy in wireless and mobile networks 2021 Jun 28 (pp. 153-163).

[24] Zhang W, Wang X, Zhou P, Wu W, Zhang X. Client selection for federated learning with non-iid data in mobile edge computing. IEEE Access. 2021 Feb 3;9:24462-74.

[25] Jawad M, Yassin AA, Al-Asadi HA, Abduljabbar ZA, Nyangaresi VO. IoHT System Authentication Through the Blockchain Technology: A Review. In2024 10th International Conference on Control, Decision and Information Technologies (CoDIT) 2024 Jul 1 (pp. 2253-2258). IEEE.

[26] Alsharif MH, Kannadasan R, Wei W, Nisar KS, Abdel-Aty AH. A Contemporary Survey of Recent Advances in Federated Learning: Taxonomies, Applications, and Challenges. Internet of Things. 2024 Jun 14:101251.

[27] Farahani B, Monsefi AK. Smart and collaborative industrial IoT: A federated learning and data space approach. Digital Communications and Networks. 2023 Apr 1;9(2):436-47.

[28] Thota S, Vangoor VK, Reddy AK, Ravi CS. Federated Learning: Privacy-Preserving Collaborative Machine Learning. Distributed Learning and Broad Applications in Scientific Research. 2019 Aug 17;5:168-90.

[29] Satish S, Nadella GS, Meduri K, Gonaygunta H. Collaborative Machine Learning without Centralized Training Data for Federated Learning. International Machine Learning Journal and Computer Engineering. 2022 Jun 16;5(5):1-4.

[30] Nyangaresi VO. Extended Chebyshev Chaotic Map Based Message Verification Protocol for Wireless Surveillance Systems. InComputer Vision and Robotics: Proceedings of CVR 2022 2023 Apr 28 (pp. 503-516). Singapore: Springer Nature Singapore.

[31] Qi P, Chiaro D, Guzzo A, Ianni M, Fortino G, Piccialli F. Model aggregation techniques in federated learning: A comprehensive survey. Future Generation Computer Systems. 2024 Jan 1;150:272-93.

[32] Long G, Xie M, Shen T, Zhou T, Wang X, Jiang J. Multi-center federated learning: clients clustering for better personalization. World Wide Web. 2023 Jan;26(1):481-500.

[33] Pang J, Huang Y, Xie Z, Han Q, Cai Z. Realizing the heterogeneity: A self-organized federated learning framework for IoT. IEEE Internet of Things Journal. 2020 Jul 7;8(5):3088-98.

[34] Zheng Y, Lai S, Liu Y, Yuan X, Yi X, Wang C. Aggregation service for federated learning: An efficient, secure, and more resilient realization. IEEE Transactions on Dependable and Secure Computing. 2022 Jan 27;20(2):988-1001.

[35] Hu L, Yan H, Li L, Pan Z, Liu X, Zhang Z. MHAT: An efficient model-heterogenous aggregation training scheme for federated learning. Information Sciences. 2021 Jun 1;560:493-503.

[36] Al Sibahee MA, Abduljabbar ZA, Ngueilbaye A, Luo C, Li J, Huang Y, Zhang J, Khan N, Nyangaresi VO, Ali AH. Blockchain-Based Authentication Schemes in Smart Environments: A Systematic Literature Review. IEEE Internet of Things Journal. 2024 Jul 3.

[37] Ye R, Wang W, Chai J, Li D, Li Z, Xu Y, Du Y, Wang Y, Chen S. Openfedllm: Training large language models on decentralized private data via federated learning. InProceedings of the 30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining 2024 Aug 25 (pp. 6137-6147).

[38] Wu F, Li Z, Li Y, Ding B, Gao J. Fedbiot: Llm local fine-tuning in federated learning without full model. InProceedings of the 30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining 2024 Aug 25 (pp. 3345-3355).

[39] Nanayakkara SI, Pokhrel SR, Li G. Understanding global aggregation and optimization of federated learning. Future Generation Computer Systems. 2024 May 7.

[40] Dong Y, Wang Y, Gama M, Mustafa MA, Deconinck G, Huang X. Privacy-Preserving Distributed Learning for Residential Short-Term Load Forecasting. IEEE Internet of Things Journal. 2024 Feb 5.

[41] Nyangaresi VO. Provably secure authentication protocol for traffic exchanges in unmanned aerial vehicles. High-Confidence Computing. 2023 Sep 15:100154.

[42] Seyghaly R, Garcia J, Masip-Bruin X. A Comprehensive Architecture for Federated Learning-Based Smart Advertising. Sensors. 2024 Jan;24(12):3765.

[43] Thapa C, Camtepe S. Precision health data: Requirements, challenges and existing techniques for data security and privacy. Computers in biology and medicine. 2021 Feb 1;129:104130.

[44] Rosário AT, Raimundo R. Internet of Things and Distributed Computing Systems in Business Models. Future Internet. 2024 Oct 21;16(10):384.

[45] Wang H, Wang L. Fedkg: Model-optimized federated learning for local client training with non-iid private data. In2021 Ninth International Conference on Advanced Cloud and Big Data (CBD) 2022 Mar 26 (pp. 51-57). IEEE.

[46] Ali AH, Jasim HM, Abduljabbar ZA, Nyangaresi VO, Umran SM, Ma J, Honi DG. Provably Efficient and Fast Technique for Determining the Size of a Brain Tumor in T1 MRI Images. In2024 International Conference on Artificial Intelligence in Information and Communication (ICAIIC) 2024 Feb 19 (pp. 608-613). IEEE.

[47] Yin L, Feng J, Xun H, Sun Z, Cheng X. A privacy-preserving federated learning for multiparty data sharing in social IoTs. IEEE Transactions on Network Science and Engineering. 2021 Apr 20;8(3):2706-18.

[48] Lu Y, Huang X, Dai Y, Maharjan S, Zhang Y. Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. IEEE Transactions on Industrial Informatics. 2019 Sep 18;16(6):4177-86.

[49] Zhao L, Xie H, Zhong L, Wang Y. Multi-server verifiable aggregation for federated learning in securing industrial iot. In2024 27th International Conference on Computer Supported Cooperative Work in Design (CSCWD) 2024 May 8 (pp. 2692-2697). IEEE.

[50] Ganguly B, Hosseinalipour S, Kim KT, Brinton CG, Aggarwal V, Love DJ, Chiang M. Multi-edge server-assisted dynamic federated learning with an optimized floating aggregation point. IEEE/ACM Transactions on Networking. 2023 Apr 21;31(6):2682-97.

[51] Beltrán ET, Pérez MQ, Sánchez PM, Bernal SL, Bovet G, Pérez MG, Pérez GM, Celdrán AH. Decentralized federated learning: Fundamentals, state of the art, frameworks, trends, and challenges. IEEE Communications Surveys and Tutorials. 2023 Sep 15.

[52] Nyangaresi VO. Target Tracking Area Selection and Handover Security in Cellular Networks: A Machine Learning Approach. InProceedings of Third International Conference on Sustainable Expert Systems: ICSES 2022 2023 Feb 23 (pp. 797-816). Singapore: Springer Nature Singapore.

[53] Nguyen DC, Ding M, Pathirana PN, Seneviratne A, Li J, Poor HV. Federated learning for internet of things: A comprehensive survey. IEEE Communications Surveys and Tutorials. 2021 Apr 26;23(3):1622-58.

[54] Abreha HG, Hayajneh M, Serhani MA. Federated learning in edge computing: a systematic survey. Sensors. 2022 Jan 7;22(2):450.

[55] Zhang T, Gao L, He C, Zhang M, Krishnamachari B, Avestimehr AS. Federated learning for the internet of things: Applications, challenges, and opportunities. IEEE Internet of Things Magazine. 2022 Mar;5(1):24-9.

[56] Lim WY, Luong NC, Hoang DT, Jiao Y, Liang YC, Yang Q, Niyato D, Miao C. Federated learning in mobile edge networks: A comprehensive survey. IEEE communications surveys and tutorials. 2020 Apr 8;22(3):2031-63.

[57] Mohammed RJ, Ghrabat MJ, Abduljabbar ZA, Nyangaresi VO, Abduljaleel IQ, Ali AH, Honi DG, Neamah HA. A Robust Hybrid Machine and Deep Learning-based Model for Classification and Identification of Chest X-ray Images. Engineering, Technology and Applied Science Research. 2024 Oct 9;14(5):16212-20.

[58] Niu C, Wu F, Tang S, Hua L, Jia R, Lv C, Wu Z, Chen G. Billion-scale federated learning on mobile clients: A submodel design with tunable privacy. InProceedings of the 26th Annual International Conference on Mobile Computing and Networking 2020 Sep 21 (pp. 1-14).

[59] Eyuboglu S, Goel K, Desai A, Chen L, Monfort M, Ré C, Zou J. Model ChangeLists: Characterizing Updates to ML Models. InThe 2024 ACM Conference on Fairness, Accountability, and Transparency 2024 Jun 3 (pp. 2432-2453).

[60] Ma H, Wei J, Zhang G, Wang Q, Kong X, Du J. Heterogeneous Federated Learning: Client-side Collaborative Update Inter-Domain Generalization Method for Intelligent Fault Diagnosis. IEEE Internet of Things Journal. 2024 Nov 4.

[61] Shen L, Yang Q, Cui K, Zheng Y, Wei XY, Liu J, Han J. FedConv: A Learning-on-Model Paradigm for Heterogeneous Federated Clients. InProceedings of the 22nd Annual International Conference on Mobile Systems, Applications and Services 2024 Jun 3 (pp. 398-411).

[62] Nyangaresi VO, Moundounga AR. Secure data exchange scheme for smart grids. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[63] Babar M, Qureshi B, Koubaa A. Review on Federated Learning for digital transformation in healthcare through big data analytics. Future Generation Computer Systems. 2024 May 24.

[64] Ge L, Li H, Wang X, Wang Z. A review of secure federated learning: privacy leakage threats, protection technologies, challenges and future directions. Neurocomputing. 2023 Oct 4:126897.

[65] Rauniyar A, Hagos DH, Jha D, Håkegård JE, Bagci U, Rawat DB, Vlassov V. Federated learning for medical applications: A taxonomy, current trends, challenges, and future research directions. IEEE Internet of Things Journal. 2023 Nov 1.

[66] Siniosoglou I, Argyriou V, Fragulis G, Fouliras P, Papadopoulos GT, Lytos A, Sarigiannidis P. Applied federated model personalization in the industrial domain: a comparative study. IEEE Open Journal of the Communications Society. 2024 Sep 11.

[67] Duaa Fadhel Najem, Nagham Abdulrasool Taha, Zaid Ameen Abduljabbar, Vincent Omollo Nyangaresi, Junchao Ma and Dhafer G. Honi. Low-Complexity and Secure Clustering-Based Similarity Detection for Private Files. TEM Journal, 13(2), 2341-2349 (2024).DOI: 10.18421/TEM133-61

[68] Zheng R, Qu L, Chen T, Zheng K, Shi Y, Yin H. Poisoning decentralized collaborative recommender system and its countermeasures. InProceedings of the 47th International ACM SIGIR Conference on Research and Development in Information Retrieval 2024 Jul 10 (pp. 1712-1721).

[69] Rao B, Zhang J, Wu D, Zhu C, Sun X, Chen B. Privacy inference attack and defense in centralized and federated learning: A comprehensive survey. IEEE Transactions on Artificial Intelligence. 2024 Feb 8.

[70] Aziz R, Banerjee S, Bouzefrane S, Le Vinh T. Exploring homomorphic encryption and differential privacy techniques towards secure federated learning paradigm. Future internet. 2023 Sep 13;15(9):310.

[71] Xie Q, Jiang S, Jiang L, Huang Y, Zhao Z, Khan S, Dai W, Liu Z, Wu K. Efficiency optimization techniques in privacy-preserving federated learning with homomorphic encryption: A brief survey. IEEE Internet of Things Journal. 2024 Jul 8;11(14):24569-80.

[72] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Apr 1;142:103117.

[73] Balcıoğlu YS. Revolutionizing Risk Management AI and ML Innovations in Financial Stability and Fraud Detection. InNavigating the Future of Finance in the Age of AI 2024 (pp. 109-138). IGI Global.

[74] Karras A, Giannaros A, Theodorakopoulos L, Krimpas GA, Kalogeratos G, Karras C, Sioutas S. FLIBD: A federated learning-based IoT big data management approach for privacy-preserving over Apache Spark with FATE. Electronics. 2023 Nov 13;12(22):4633.

[75] Kandasamy M, Shanmugam R, Adesara H, Patel V, Dhanaraj RK. The impact of ubiquitous computing on heterogeneous next generation networks. InUbiquitous and Transparent Security 2024 Jun 4 (pp. 236-264). CRC Press.

[76] AbdlNabi MA, Hamza BJ, Abdulsadda AT. 6G optical-RF wireless integration: a review on heterogeneous cellular network channel modeling, measurements, and challenges. Telecommunication Systems. 2024 Sep 30:1-44.

[77] Ali ZA, Abduljabbar ZA, AL-Asadi HA, Nyangaresi VO, Abduljaleel IQ, Aldarwish AJ. A Provably Secure Anonymous Authentication Protocol for Consumer and Service Provider Information Transmissions in Smart Grids. Cryptography. 2024 May 9;8(2):20.

[78] Deebak BD. Cooperative Mobile Traffic Offloading in Mobile Edge Computing for 5G HetNet IoT Applications. Real-Time Intelligence for Heterogeneous Networks: Applications, Challenges, and Scenarios in IoT HetNets. 2021:43-58.

[79] Lorincz J, Klarin Z, Begusic D. Advances in improving energy efficiency of fiber–wireless access networks: a comprehensive overview. Sensors. 2023 Feb 16;23(4):2239.

[80] Mishra A, Swain A, Ray AK, Shubair RM. HetNet/M2M/D2D communication in 5G technologies. In5G IoT and Edge Computing for Smart Healthcare 2022 Jan 1 (pp. 45-87). Academic Press.

[81] Ma Y, Li T, Zhou Y, Yu L, Jin D. Mitigating Energy Consumption in Heterogeneous Mobile Networks Through Data-Driven Optimization. IEEE Transactions on Network and Service Management. 2024 Jun 19.

[82] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432). IEEE.

[83] Gupta SK, Gupta P, Singh P. Enhancing UAV-HetNet security through functional encryption framework. Concurrency and Computation: Practice and Experience. 2024 Sep 10;36(20):e8206.

[84] Mengistu TM, Kim T, Lin JW. A Survey on Heterogeneity Taxonomy, Security and Privacy Preservation in the Integration of IoT, Wireless Sensor Networks and Federated Learning. Sensors. 2024 Feb 1;24(3):968.

[85] Edwards DJ. Internet of Things (IoT) Security. InMastering Cybersecurity: Strategies, Technologies, and Best Practices 2024 Jul 1 (pp. 281-328). Berkeley, CA: Apress.

[86] Khan HU, Sohail M, Ali F, Nazir S, Ghadi YY, Ullah I. Prioritizing the multi-criterial features based on comparative approaches for enhancing security of IoT devices. Physical Communication. 2023 Aug 1;59:102084.

[87] Alshuraify A, Yassin AA, Abduljabbar ZA, Nyangaresi VO. Blockchain-based Authentication Scheme in Oil and Gas Industry Data with Thermal CCTV Cameras Applications to Mitigate Sybil and 51% Cyber Attacks. International Journal of Intelligent Engineering and Systems. 2024 Nov 1;17(6).

[88] Chen M, Chen Y. Eavesdropping Interference in Wireless Communication Networks Based on Physical Layer Security. International Journal of Advanced Computer Science and Applications. 2024 Sep 1;15(9).

[89] Hazra R, Chatterjee P, Singh Y, Podder G, Das T. Data Encryption and Secure Communication Protocols. InStrategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning 2024 (pp. 546-570). IGI Global.

[90] Jagannath RO, Jain AK. Browser-in-the-middle attacks: A comprehensive analysis and countermeasures. Security and Privacy. 2024 Sep;7(5):e410.

[91] Stanco G, Navarro A, Frattini F, Ventre G, Botta A. A comprehensive survey on the security of low power wide area networks for the Internet of Things. ICT Express. 2024 Mar 18.

[92] Nyangaresi VO, Morsy MA. Towards privacy preservation in internet of drones. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[93] Kumar A, Sharma I, Mittal S. Enhancing Security through a Machine Learning Approach to Mitigate Man-in-the-Middle Attacks. In2024 IEEE 9th International Conference for Convergence in Technology (I2CT) 2024 Apr 5 (pp. 1-6). IEEE.

[94] Qiao Y, Chen D, Sun QZ, Tian G, Wang W. Unveiling stealthy man-in-the-middle cyber-attacks on energy performance in grid-interactive smart buildings. Energy Conversion and Management. 2024 Nov 1;319:118949.

[95] Tyagi V, Saraswat A, Bansal S. An Analysis of Securing Internet of Things (IoT) Devices from Man-in-the-Middle (MIMA) and Denial of Service (DoS). InSmart Cities 2023 Nov 30 (pp. 337-357). CRC Press.

[96] Sharma A, Babbar H, Vats AK. A Supervised Machine Learning Framework for Early Detection of Man-in-the-middle Attacks. In2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM) 2024 Feb 21 (pp. 1-6). IEEE.

[97] Cecílio J, Souto A. Security Issues in Industrial Internet-of-Things: Threats, Attacks and Solutions. In2024 IEEE International Workshop on Metrology for Industry 4.0 and IoT (MetroInd4. 0 and IoT) 2024 May 29 (pp. 458-463). IEEE.

[98] Narang M, Jatain A, Punetha N. A Survey on Detection of Man-In-The-Middle Attack in IoMT Using Machine Learning Techniques. InInternational Conference on Computational Intelligence 2023 Nov 4 (pp. 117-132). Singapore: Springer Nature Singapore.

[99] Nyangaresi VO, Ghaib AA, Jasim HM, Abduljabbar ZA, Ma J, Al Sibahee MA, Aldarwish AJ, Ali AH, Neamah HA. Message Verification Protocol Based on Bilinear Pairings and Elliptic Curves for Enhanced Security in Vehicular Ad Hoc Networks. Computers, Materials and Continua. 2024 Oct 1;81(1):1029-57.

[100] Ogu EC, Ojesanmi OA, Awodele O, Kuyoro S. A botnets circumspection: The current threat landscape, and what we know so far. Information. 2019 Oct 30;10(11):337.

[101] Asadi M, Jamali MA, Heidari A, Navimipour NJ. Botnets Unveiled: A Comprehensive Survey on Evolving Threats and Defense Strategies. Transactions on Emerging Telecommunications Technologies. 2024 Nov;35(11):e5056.

[102] Yumlembam R, Issac B, Jacob SM, Yang L. Comprehensive botnet detection by mitigating adversarial attacks, navigating the subtleties of perturbation distances and fortifying predictions with conformal layers. Information Fusion. 2024 Jun 13:102529.

[103] Acton T, Datta PM. Endpoint cybersecurity: When smart devices turn stupid. Journal of Information Technology Teaching Cases. 2024 Mar 27:20438869241242142.

[104] Bulbul SS, Abduljabbar ZA, Mohammed RJ, Al Sibahee MA, Ma J, Nyangaresi VO, Abduljaleel IQ. A provably lightweight and secure DSSE scheme, with a constant storage cost for a smart device client. Plos one. 2024 Apr 25;19(4):e0301277.

[105] Huseinović A, Mrdović S, Bicakci K, Uludag S. A survey of denial-of-service attacks and solutions in the smart grid. IEEE Access. 2020 Sep 25;8:177447-70.

[106] Akinsanya MO, Ekechi CC, Okeke CD. Security paradigms for iot in telecom networks: conceptual challenges and solution pathways. Engineering Science and Technology Journal. 2024 Apr 26;5(4):1431-51.

[107] Ahmed SF, Alam MS, Afrin S, Rafa SJ, Taher SB, Kabir M, Muyeen SM, Gandomi AH. Towards a secure 5G-enabled Internet of Things: A survey on requirements, privacy, security, challenges, and opportunities. IEEE Access. 2024 Jan 10.

[108] Xia D, Jiang C, Wan J, Jin J, Leung VC, Martínez-García M. Heterogeneous network access and fusion in smart factory: A survey. ACM Computing Surveys. 2022 Dec 7;55(6):1-31.

[109] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[110] Sharma H, Sharma G, Kumar N. AI-assisted secure data transmission techniques for next-generation HetNets: A review. Computer Communications. 2023 Dec 18.

[111] Islam MS, Rahman MA, Bin Ameedeen MA, Ajra H, Ismail ZB, Zain JM. Blockchain-Enabled Cybersecurity Provision for Scalable Heterogeneous Network: A Comprehensive Survey. CMES-Computer Modeling in Engineering and Sciences. 2024 Jan 1;138(1).

[112] Sun Y, Cao J, Ma M, Li H, Niu B, Li F. Privacy-preserving device discovery and authentication scheme for D2D communication in 3GPP 5G HetNet. In2019 International Conference on Computing, Networking and Communications (ICNC) 2019 Feb 18 (pp. 425-431). IEEE.

[113] Ramezanpour K, Jagannath J, Jagannath A. Security and privacy vulnerabilities of 5G/6G and WiFi 6: Survey and research directions from a coexistence perspective. Computer Networks. 2023 Feb 1;221:109515.

[114] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA. Low complexity smart grid security protocol based on elliptic curve cryptography, biometrics and hamming distance. Plos one. 2024 Jan 23;19(1):e0296781.

[115] Liu J. Exploration of Factors Influencing Computer Network Information Security and Prevention Strategies in Colleges and Universities. In2024 5th International Conference on Education, Knowledge and Information Management (ICEKIM 2024) 2024 Aug 31 (pp. 595-606). Atlantis Press.

[116] Liu L, De Vel O, Han QL, Zhang J, Xiang Y. Detecting and preventing cyber insider threats: A survey. IEEE Communications Surveys and Tutorials. 2018 Feb 1;20(2):1397-417.

[117] Alzaabi FR, Mehmood A. A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods. IEEE Access. 2024 Feb 26;12:30907-27.

[118] Al-Mhiqani MN, Ahmad R, Zainal Abidin Z, Yassin W, Hassan A, Abdulkareem KH, Ali NS, Yunos Z. A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations. Applied Sciences. 2020 Jul 28;10(15):5208.

[119] Nyangaresi VO, Abduljabbar ZA, Mutlaq KA, Bulbul SS, Ma J, Aldarwish AJ, Honi DG, Al Sibahee MA, Neamah HA. Smart city energy efficient data privacy preservation protocol based on biometrics and fuzzy commitment scheme. Scientific Reports. 2024 Jul 13;14(1):16223.

[120] Cao Y, Zhao Y, Wang Q, Zhang J, Ng SX, Hanzo L. The evolution of quantum key distribution networks: On the road to the qinternet. IEEE Communications Surveys and Tutorials. 2022 Jan 18;24(2):839-94.

[121] Rao PM, Deebak BD. A comprehensive survey on authentication and secure key management in internet of things: Challenges, countermeasures, and future directions. Ad Hoc Networks. 2023 Jul 1;146:103159.

[122] Banoth R, Regar R. Asymmetric Key Cryptography. InClassical and Modern Cryptography for Beginners 2023 Jun 25 (pp. 109-165). Cham: Springer Nature Switzerland.

[123] El-Hajj M, Beune P. Lightweight public key infrastructure for the Internet of Things: A systematic literature review. Journal of Industrial Information Integration. 2024 Aug 10:100670.

[124] Wang C, Wang Y, Chen Y, Liu H, Liu J. User authentication on mobile devices: Approaches, threats and trends. Computer Networks. 2020 Apr 7;170:107118.

[125] Nandy T, Idris MY, Noor RM, Kiah LM, Lun LS, Juma'at NB, Ahmedy I, Ghani NA, Bhattacharyya S. Review on security of internet of things authentication mechanism. IEEE Access. 2019 Oct 16;7:151054-89.

[126] Nyangaresi VO. A Formally Verified Authentication Scheme for mmWave Heterogeneous Networks. Inthe 6th International Conference on Combinatorics, Cryptography, Computer Science and Computation (605-612) 2021.

[127] Ammar M, Russello G, Crispo B. Internet of Things: A survey on the security of IoT frameworks. Journal of Information Security and Applications. 2018 Feb 1;38:8-27.

[128] Omotunde H, Ahmed M. A comprehensive review of security measures in database systems: Assessing authentication, access control, and beyond. Mesopotamian Journal of CyberSecurity. 2023 Aug 7;2023:115-33.

[129] Singh AK, Garg A. Authentication protocols for securing IoMT: current state and technological advancements. Securing Next-Generation Connected Healthcare Systems. 2024 Jan 1:1-29.

[130] Wani AR, Gupta SK, Khanam Z, Rashid M, Alshamrani SS, Baz M. A novel approach for securing data against adversary attacks in UAV embedded HetNet using identity based authentication scheme. IET Intelligent Transport Systems. 2023 Nov;17(11):2171-89.

[131] Al Sibahee MA, Abduljabbar ZA, Luo C, Zhang J, Huang Y, Abduljaleel IQ, Ma J, Nyangaresi VO. Hiding scrambled text messages in speech signals using a lightweight hyperchaotic map and conditional LSB mechanism. Plos one. 2024 Jan 3;19(1):e0296469.

[132] Banafaa M, Pepeoğlu Ö, Shayea I, Alhammadi A, Shamsan Z, Razaz MA, Alsagabi M, Al-Sowayan S. A comprehensive survey on 5G-and-beyond networks with UAVs: Applications, emerging technologies, regulatory aspects, research trends and challenges. IEEE Access. 2024 Jan 2.

[133] Tariq U, Ahmed I, Bashir AK, Shaukat K. A critical cybersecurity analysis and future research directions for the internet of things: a comprehensive review. Sensors. 2023 Apr 19;23(8):4117.

[134] Pathak V, Singh K, Khan T, Shariq M, Chaudhry SA, Das AK. A secure and lightweight trust evaluation model for enhancing decision-making in resource-constrained industrial WSNs. Scientific Reports. 2024 Nov 15;14(1):28162.

[135] Aziz Al Kabir M, Elmedany W, Sharif MS. Securing IOT devices against emerging security threats: Challenges and mitigation techniques. Journal of Cyber Security Technology. 2023 Oct 2;7(4):199-223.

[136] Nyangaresi VO, Alsamhi SH. Towards secure traffic signaling in smart grids. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 196-201). IEEE.

[137] Aburbeian AM, Fernández-Veiga M. Secure Internet Financial Transactions: A Framework Integrating Multi-Factor Authentication and Machine Learning. AI. 2024 Jan 10;5(1):177-94.

[138] Ullah Y, Roslee MB, Mitani SM, Khan SA, Jusoh MH. A survey on handover and mobility management in 5G HetNets: current state, challenges, and future directions. Sensors. 2023 May 25;23(11):5081.

[139] Shabbir A, Rizvi S, Shirazi MF, Alam MM, Su'ud MM. Maximizing energy efficiency in HetNets through centralized and distributed sleep strategies under QoS constraint. Scientific Reports. 2024 Oct 28;14(1):25839.

[140] Israr A, Yang Q, Israr A. Cost-efficient microgeneration renewable energy provision dimensioning for sustainable 5G heterogeneous network. Sustainable Energy, Grids and Networks. 2024 Sep 1;39:101493.

[141] Umran SM, Lu S, Abduljabbar ZA, Nyangaresi VO. Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry. Internet of Things. 2023 Dec 1;24:100969.

[142] Darwish T, Kurt GK, Yanikomeroglu H, Senarath G, Zhu P. A vision of self-evolving network management for future intelligent vertical HetNet. IEEE Wireless Communications. 2021 Aug;28(4):96-105.

[143] Gures E, Shayea I, Alhammadi A, Ergen M, Mohamad H. A comprehensive survey on mobility management in 5G heterogeneous networks: Architectures, challenges and solutions. IEEE Access. 2020 Oct 13;8:195883-913.

[144] Al-Hawawreh M, Alazab M, Ferrag MA, Hossain MS. Securing the Industrial Internet of Things against ransomware attacks: A comprehensive analysis of the emerging threat landscape and detection mechanisms. Journal of Network and Computer Applications. 2023 Dec 4:103809.

[145] Aslan Ö, Aktuğ SS, Ozkan-Okay M, Yilmaz AA, Akin E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics. 2023 Mar 11;12(6):1333.

[146] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. InThe Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021 2022 Jun 12 (pp. 81-99). Cham: Springer International Publishing.

[147] Nagar G. The Evolution of Ransomware: Tactics, Techniques, and Mitigation Strategies. Valley International Journal Digital Library. 2024 Jun 30:1282-98.

[148] Bajpai P, Enbody R. Know thy ransomware response: a detailed framework for devising effective ransomware response strategies. Digital Threats: Research and Practice. 2023 Oct 20;4(4):1-9.

[149] Qureshi SU, He J, Tunio S, Zhu N, Nazir A, Wajahat A, Ullah F, Wadud A. Systematic review of deep learning solutions for malware detection and forensic analysis in IoT. Journal of King Saud University-Computer and Information Sciences. 2024 Aug 27:102164.

[150] Möller DP. Ransomware attacks and scenarios: Cost factors and loss of reputation. InGuide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices 2023 Apr 19 (pp. 273-303). Cham: Springer Nature Switzerland.

[151] Scanzio S, Wisniewski L, Gaj P. Heterogeneous and dependable networks in industry–A survey. Computers in Industry. 2021 Feb 1;125:103388.

[152] Al Sibahee MA, Nyangaresi VO, Abduljabbar ZA, Luo C, Zhang J, Ma J. Two-Factor Privacy Preserving Protocol for Efficient Authentication in Internet of Vehicles Networks. IEEE Internet of Things Journal. 2023 Dec 7.

[153] Hazra A, Adhikari M, Amgoth T, Srirama SN. A comprehensive survey on interoperability for IIoT: Taxonomy, standards, and future directions. ACM Computing Surveys (CSUR). 2021 Nov 23;55(1):1-35.

[154] Mall P, Amin R, Das AK, Leung MT, Choo KK. PUF-based authentication and key agreement protocols for IoT, WSNs, and smart grids: A comprehensive survey. IEEE Internet of Things Journal. 2022 Jan 11;9(11):8205-28.

[155] Roman R, Lopez J, Mambo M. Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. Future Generation Computer Systems. 2018 Jan 1;78:680-98.

[156] Ali B, Gregory MA, Li S. Multi-access edge computing architecture, data security and privacy: A review. IEEE Access. 2021 Jan 21;9:18706-21.

[157] Nyangaresi VO, Ma J. A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In2022 IEEE World Conference on Applied Intelligence and Computing (AIC) 2022 Jun 17 (pp. 416-422). IEEE.

[158] Jimmy FN. Cyber security Vulnerabilities and Remediation Through Cloud Security Tools. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023. 2024 Apr 12;2(1):129-71.

[159] Ahmed S, Khan M. Securing the Internet of Things (IoT): A comprehensive study on the intersection of cybersecurity, privacy, and connectivity in the IoT ecosystem. AI, IoT and the Fourth Industrial Revolution Review. 2023 Sep 16;13(9):1-7.

[160] Obi OC, Akagha OV, Dawodu SO, Anyanwu AC, Onwusinkwue S, Ahmad IA. Comprehensive review on cybersecurity: modern threats and advanced defense strategies. Computer Science and IT Research Journal. 2024 Feb 2;5(2):293-310.

[161] Beltrán ET, Gómez ÁL, Feng C, Sánchez PM, Bernal SL, Bovet G, Pérez MG, Pérez GM, Celdrán AH. Fedstellar: A platform for decentralized federated learning. Expert Systems with Applications. 2024 May 15;242:122861.

[162] Mohialdin SH, Abdulrahman LQ, Al-Yoonus MH, Abduljabbar ZA, Honi DG, Nyangaresi VO, Abduljaleel IQ, Neamah HA. Utilizing Machine Learning for the Early Detection of Coronary Heart Disease. Engineering, Technology and Applied Science Research. 2024 Oct 9;14(5):17363-75.

[163] Usama M, Qadir J, Raza A, Arif H, Yau KL, Elkhatib Y, Hussain A, Al-Fuqaha A. Unsupervised machine learning for networking: Techniques, applications and research challenges. IEEE access. 2019 May 14;7:65579-615.

[164] Drainakis G, Katsaros KV, Pantazopoulos P, Sourlas V, Amditis A. Federated vs. centralized machine learning under privacy-elastic users: A comparative analysis. In2020 IEEE 19th International Symposium on Network Computing and Applications (NCA) 2020 Nov 24 (pp. 1-8). IEEE.

[165] Sun D, Hu J, Wu H, Wu J, Yang J, Sheng QZ, Dustdar S. A comprehensive survey on collaborative data-access enablers in the IIoT. ACM Computing Surveys. 2023 Sep 15;56(2):1-37.

[166] Hosseini P, Taheri S, Akhavan J, Razban A. Privacy-preserving federated learning: Application to behind-the-meter solar photovoltaic generation forecasting. Energy Conversion and Management. 2023 May 1;283:116900.

[167] Nyangaresi VO. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In2022 International Conference on Inventive Computation Technologies (ICICT) 2022 Jul 20 (pp. 1-6). IEEE.

[168] El Ouadrhiri A, Abdelhadi A. Differential privacy for deep and federated learning: A survey. IEEE access. 2022 Feb 15;10:22359-80.

[169] Wu X, Zhang Y, Shi M, Li P, Li R, Xiong NN. An adaptive federated learning scheme with differential privacy preserving. Future Generation Computer Systems. 2022 Feb 1;127:362-72.

[170] Su G, Wang J, Xu X, Wang Y, Wang C. The Utilization of Homomorphic Encryption Technology Grounded on Artificial Intelligence for Privacy Preservation. International Journal of Computer Science and Information Technology. 2024 Mar 13;2(1):52-8.

[171] Reddi S, Rao PM, Saraswathi P, Jangirala S, Das AK, Jamal SS, Park Y. Privacy-preserving electronic medical record sharing for IoT-enabled healthcare system using fully homomorphic encryption, IOTA, and masked authenticated messaging. IEEE Transactions on Industrial Informatics. 2024 May 16.

[172] Mohammed MA, Hussain MA, Oraibi ZA, Abduljabbar ZA, Nyangaresi VO. Secure Content Based Image Retrieval System Using Deep Learning. J. Basrah Res.(Sci.). 2023 Dec 30;49(2):94-111.

[173] Bouacida N, Mohapatra P. Vulnerabilities in federated learning. IEEE Access. 2021 Apr 23;9:63229-49.

[174] Hossain MT, Islam S, Badsha S, Shen H. Desmp: Differential privacy-exploited stealthy model poisoning attacks in federated learning. In2021 17th International Conference on Mobility, Sensing and Networking (MSN) 2021 Dec 13 (pp. 167-174). IEEE.

[175] Luan Z, Li W, Liu M, Chen B. Robust Federated Learning: Maximum Correntropy Aggregation Against Byzantine Attacks. IEEE Transactions on Neural Networks and Learning Systems. 2024 Apr 23.

[176] Xu S, Xia H, Zhang R, Liu P, Fu Y. FedNor: A robust training framework for federated learning based on normal aggregation. Information Sciences. 2024 Dec 1;684:121274.

[177] Nyangaresi VO, El-Omari NK, Nyakina JN. Efficient Feature Selection and ML Algorithm for Accurate Diagnostics. Journal of Computer Science Research. 2022 Jan 25;4(1):10-9.

[178] Adelipour S, Haeri M. Private outsourced model predictive control via secure multi-party computation. Computers and Electrical Engineering. 2024 May 1;116:109208.

[179] Chouhan A, Purushothama BR. A Survey on Secure Aggregation for Privacy-Preserving Federated Learning. InInternational Conference on Advancements in Smart Computing and Information Security 2023 Dec 1 (pp. 13-26). Cham: Springer Nature Switzerland.

[180] Bao H, Yuan M, Deng H, Xu J, Zhao Y. Secure multiparty computation protocol based on homomorphic encryption and its application in blockchain. Heliyon. 2024 Jul 30;10(14).

[181] Fereidooni H, Marchal S, Miettinen M, Mirhoseini A, Möllering H, Nguyen TD, Rieger P, Sadeghi AR, Schneider T, Yalame H, Zeitouni S. SAFELearn: Secure aggregation for private federated learning. In2021 IEEE Security and Privacy Workshops (SPW) 2021 May 27 (pp. 56-62). IEEE.

[182] Al-Chaab W, Abduljabbar ZA, Abood EW, Nyangaresi VO, Mohammed HM, Ma J. Secure and Low-Complexity Medical Image Exchange Based on Compressive Sensing and LSB Audio Steganography. Informatica. 2023 May 31;47(6).

[183] Almutairi S, Barnawi A. Federated learning vulnerabilities, threats and defenses: A systematic review and future directions. Internet of Things. 2023 Sep 26:100947.

[184] Martínez Beltrán ET, Sánchez Sánchez PM, López Bernal S, Bovet G, Gil Pérez M, Martínez Pérez G, Huertas Celdrán A. Mitigating communications threats in decentralized federated learning through moving target defense. Wireless Networks. 2024 Jan 28:1-5.

[185] Zhang C, Yang S, Mao L, Ning H. Anomaly detection and defense techniques in federated learning: a comprehensive review. Artificial Intelligence Review. 2024 Jun;57(6):1-34.

[186] Akter S, Chellappan S, Chakraborty T, Khan TA, Rahman A, Al Islam AA. Man-in-the-middle attack on contactless payment over NFC communications: design, implementation, experiments and detection. IEEE Transactions on Dependable and Secure Computing. 2020 Oct 12;18(6):3012-23.

[187] Nyangaresi VO. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture. 2022 Dec 1;133:102763.

[188] Mishra A, Jabar TS, Alzoubi YI, Mishra KN. Enhancing privacy-preserving mechanisms in Cloud storage: A novel conceptual framework. Concurrency and Computation: Practice and Experience. 2023 Nov 30;35(26):e7831.

[189] Javadpour A, Ja'fari F, Taleb T, Zhao Y, Bin Y, Benzaïd C. Encryption as a service for IoT: opportunities, challenges and solutions. IEEE Internet of Things Journal. 2023 Dec 15.

[190] Ashrif FF, Sundararajan EA, Hasan MK, Ahmad R, Hashim AH, Talib AA. Provably secured and lightweight authenticated encryption protocol in machine-to-machine communication in industry 4.0. Computer Communications. 2024 Mar 15;218:263-75.

[191] Alauthman M, Aldweesh A, Al-Qerem A, Al Maqousi AY, Almomani A, Alkasassbeh M. Cryptographic Protocols for Internet of Things (IoT) Security Lightweight Schemes and Practical Deployment. Innovations in Modern Cryptography. 2024:431-48.

[192] Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA, Nyangaresi VO, Honi DG, Abdulsada AI, Jiao X. Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map. IEEE Access. 2022 Feb 11;10:26257-70.

[193] Wang N, Zhao Y, Qu Y, Cui L, Li B, Gao L. From Data Integrity to Global ModeI Integrity for Decentralized Federated Learning: A Blockchain-based Approach. In2024 International Joint Conference on Neural Networks (IJCNN) 2024 Jun 30 (pp. 1-8). IEEE.

[194] Issa W, Moustafa N, Turnbull B, Sohrabi N, Tari Z. Blockchain-based federated learning for securing internet of things: A comprehensive survey. ACM Computing Surveys. 2023 Jan 13;55(9):1-43.

[195] Hei X, Yin X, Wang Y, Ren J, Zhu L. A trusted feature aggregator federated learning for distributed malicious attack detection. Computers and Security. 2020 Dec 1;99:102033.

[196] Javed AR, Hassan MA, Shahzad F, Ahmed W, Singh S, Baker T, Gadekallu TR. Integration of blockchain technology and federated learning in vehicular (iot) networks: A comprehensive survey. Sensors. 2022 Jun 10;22(12):4394.

[197] Ahmad AY, Verma N, Sarhan N, Awwad EM, Arora A, Nyangaresi VO. An IoT and Blockchain-Based Secure and Transparent Supply Chain Management Framework in Smart Cities Using Optimal Queue Model. IEEE Access. 2024 Mar 18.

[198] Chen X, Qiu W, Chen L, Ma Y, Ma J. Fast and practical intrusion detection system based on federated learning for VANET. Computers and Security. 2024 Jul 1;142:103881.

[199] Khan R, Tariq N, Ashraf M, Khan FA, Shafi S, Ali A. FL-DSFA: Securing RPL-Based IoT Networks against Selective Forwarding Attacks Using Federated Learning. Sensors. 2024 Sep 8;24(17):5834.

[200] Alshammari ST, Al-Razgan M, Alfakih T, AlGhamdi KA. Building a Comprehensive Trust Evaluation Model to Secure Cloud Services from Reputation Attacks (February 2024). IEEE Access. 2024 Oct 1.

[201] Kumar B, Bhuyan B. Game Theoretic Defense Framework Against Sybil Attacks. SN Computer Science. 2024 Sep 3;5(7):857.

[202] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[203] Mothukuri V, Parizi RM, Pouriyeh S, Huang Y, Dehghantanha A, Srivastava G. A survey on security and privacy of federated learning. Future Generation Computer Systems. 2021 Feb 1;115:619-40.

[204] Kornaros G. Hardware-assisted machine learning in resource-constrained IoT environments for security: review and future prospective. IEEE Access. 2022 May 30;10:58603-22.

[205] Bukhari SM, Zafar MH, Abou Houran M, Moosavi SK, Mansoor M, Muaaz M, Sanfilippo F. Secure and privacy-preserving intrusion detection in wireless sensor networks: Federated learning with SCNN-Bi-LSTM for enhanced reliability. Ad Hoc Networks. 2024 Mar 15;155:103407.

[206] Rahman A, Hasan K, Kundu D, Islam MJ, Debnath T, Band SS, Kumar N. On the ICN-IoT with federated learning integration of communication: Concepts, security-privacy issues, applications, and future perspectives. Future Generation Computer Systems. 2023 Jan 1;138:61-88.

[207] Zaki Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Signal propagation parameters estimation through designed multi layer fibre with higher dominant modes using OptiFibre simulation. Journal of Optical Communications. 2022 Jun 23(0).

[208] Alhashimi HF, Hindia MN, Dimyati K, Hanafi EB, Safie N, Qamar F, Azrin K, Nguyen QN. A survey on resource management for 6G heterogeneous networks: current research, future trends, and challenges. Electronics. 2023 Jan 28;12(3):647.

[209] Torra V. A systematic construction of non-iid data sets from a single data set: non-identically distributed data. Knowledge and Information Systems. 2023 Mar;65(3):991-1003.

[210] Vahidian S, Morafah M, Chen C, Shah M, Lin B. Rethinking data heterogeneity in federated learning: Introducing a new notion and standard benchmarks. IEEE Transactions on Artificial Intelligence. 2023 Jul 6;5(3):1386-97.

[211] Wang C, Yang Y, Zhou P. Towards efficient scheduling of federated mobile devices under computational and statistical heterogeneity. IEEE Transactions on Parallel and Distributed Systems. 2020 Sep 14;32(2):394-410.

[212] Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Spatial single mode laser source interaction with measured pulse based parabolic index multimode fiber. Journal of Optical Communications. 2022 Jun 21.

[213] Hussain F, Hassan SA, Hussain R, Hossain E. Machine learning for resource management in cellular and IoT networks: Potentials, current solutions, and open challenges. IEEE communications surveys and tutorials. 2020 Jan 7;22(2):1251-75.

[214] Wu C, Fan H, Wang K, Zhang P. Enhancing federated learning in heterogeneous internet of vehicles: A collaborative training approach. Electronics. 2024 Oct 11;13(20):3999.

[215] Ye M, Fang X, Du B, Yuen PC, Tao D. Heterogeneous federated learning: State-of-the-art and research challenges. ACM Computing Surveys. 2023 Oct 21;56(3):1-44.

[216] Kumar KN, Mohan CK, Cenkeramaddi LR. The impact of adversarial attacks on federated learning: A survey. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2023 Oct 9;46(5):2672-91.

[217] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Sep 1;15:100210.

[218] Nabavirazavi S, Taheri R, Ghahremani M, Iyengar SS. Model poisoning attack against federated learning with adaptive aggregation. InAdversarial Multimedia Forensics 2023 Nov 15 (pp. 1-27). Cham: Springer Nature Switzerland.

[219] Zhang Z, Cao X, Jia J, Gong NZ. Fldetector: Defending federated learning against model poisoning attacks via detecting malicious clients. InProceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining 2022 Aug 14 (pp. 2545-2555).

[220] Song M, Wang Z, Zhang Z, Song Y, Wang Q, Ren J, Qi H. Analyzing user-level privacy attack against federated learning. IEEE Journal on Selected Areas in Communications. 2020 Jun 5;38(10):2430-44.

[221] Fang H, Qiu Y, Yu H, Yu W, Kong J, Chong B, Chen B, Wang X, Xia ST, Xu K. Privacy leakage on dnns: A survey of model inversion attacks and defenses. arXiv preprint arXiv:2402.04013. 2024 Feb 6.

[222] Yenurkar GK, Mal S, Nyangaresi VO, Hedau A, Hatwar P, Rajurkar S, Khobragade J. Multifactor data analysis to forecast an individual's severity over novel COVID-19 pandemic using extreme gradient boosting and random forest classifier algorithms. Engineering Reports. 2023:e12678.

[223] Lyu L, Yu H, Zhao J, Yang Q. Threats to federated learning. Federated Learning: Privacy and Incentive. 2020:3-16.

[224] Yin F, Lin Z, Kong Q, Xu Y, Li D, Theodoridis S, Cui SR. FedLoc: Federated learning framework for data-driven cooperative localization and location data processing. IEEE Open Journal of Signal Processing. 2020 Nov 6;1:187-215.

[225] Wei K, Li J, Ding M, Ma C, Yang HH, Farokhi F, Jin S, Quek TQ, Poor HV. Federated learning with differential privacy: Algorithms and performance analysis. IEEE transactions on information forensics and security. 2020 Apr 17;15:3454-69.

[226] Batool H, Anjum A, Khan A, Izzo S, Mazzocca C, Jeon G. A secure and privacy preserved infrastructure for VANETs based on federated learning with local differential privacy. Information Sciences. 2024 Jan 1;652:119717.

[227] Nyangaresi VO. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science. 2022 Jul 9;3(5):364.

[228] Kruthika B, Rajagopal SM, Kavitha CR. Homomorphic Encryption for Secure Data Analysis: A Hybrid Approach using PKCS1_OAEP Padding. In2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT) 2024 Jan 4 (pp. 481-485). IEEE.

[229] Gandhi BM, Vaghadia SB, Kumhar M, Gupta R, Jadav NK, Bhatia J, Tanwar S, Alabdulatif A. Homomorphic Encryption and Collaborative Machine Learning for Secure Healthcare Analytics. Security and Privacy. 2024:e460.

[230] Pandey S, Bhushan B. Recent Lightweight cryptography (LWC) based security advances for resource-constrained IoT networks. Wireless Networks. 2024 May;30(4):2987-3026.

[231] Hang CN, Yu PD, Morabito R, Tan CW. Large Language Models Meet Next-Generation Networking Technologies: A Review. Future Internet. 2024 Oct 7;16(10):365.

[232] Al Sibahee MA, Ma J, Nyangaresi VO, Abduljabbar ZA. Efficient Extreme Gradient Boosting Based Algorithm for QoS Optimization in Inter-Radio Access Technology Handoffs. In2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) 2022 Jun 9 (pp. 1-6). IEEE.

[233] Ahmad I, Rodriguez F, Kumar T, Suomalainen J, Jagatheesaperumal SK, Walter S, Asghar MZ, Li G, Papakonstantinou N, Ylianttila M, Huusko J. Communications security in Industry X: A survey. IEEE Open Journal of the Communications Society. 2024 Jan 19.

[234] Ashfaq M, Nur S. IoT Sensor Networks-Orchestrating Connectivity, Efficiency, and Intelligence Across Diverse Domains. International Journal of Innovative Research in Computer Science and Technology. 2024 May 1;12(3):154-61.

[235] Mousavi SK, Ghaffari A, Besharat S, Afshari H. Security of internet of things based on cryptographic algorithms: a survey. Wireless Networks. 2021 Feb;27(2):1515-55.

[236] Zhang J, Chen B, Zhao Y, Cheng X, Hu F. Data security and privacy-preserving in edge computing paradigm: Survey and open issues. IEEE access. 2018 Mar 28;6:18209-37.

[237] Nyangaresi VO, Yenurkar GK. Anonymity preserving lightweight authentication protocol for resource-limited wireless sensor networks. High-Confidence Computing. 2023 Nov 24:100178.

[238] Rahaman M, Arya V, Orozco SM, Pappachan P. Secure Multi-Party Computation (SMPC) Protocols and Privacy. InInnovations in Modern Cryptography 2024 (pp. 190-214). IGI Global.

[239] Muazu T, Mao Y, Muhammad AU, Ibrahim M, Kumshe UM, Samuel O. A federated learning system with data fusion for healthcare using multi-party computation and additive secret sharing. Computer Communications. 2024 Feb 15;216:168-82.

[240] Aldea CL, Bocu R, Solca RN. Real-time monitoring and management of hardware and software resources in heterogeneous computer networks through an integrated system architecture. Symmetry. 2023 May 23;15(6):1134.

[241] Aledhari M, Razzak R, Parizi RM, Saeed F. Federated learning: A survey on enabling technologies, protocols, and applications. IEEE Access. 2020 Jul 31;8:140699-725.

[242] Abood EW, Abdullah AM, Al Sibahe MA, Abduljabbar ZA, Nyangaresi VO, Kalafy SA, Ghrabta MJ. Audio steganography with enhanced LSB method for securing encrypted text with bit cycling. Bulletin of Electrical Engineering and Informatics. 2022 Feb 1;11(1):185-94.

[243] Wahab OA, Mourad A, Otrok H, Taleb T. Federated machine learning: Survey, multi-level classification, desirable criteria and future directions in communication and networking systems. IEEE Communications Surveys and Tutorials. 2021 Feb 10;23(2):1342-97.

[244] Khan LU, Saad W, Han Z, Hossain E, Hong CS. Federated learning for internet of things: Recent advances, taxonomy, and open challenges. IEEE Communications Surveys and Tutorials. 2021 Jun 18;23(3):1759-99.

[245] Imteaj A, Thakker U, Wang S, Li J, Amini MH. A survey on federated learning for resource-constrained IoT devices. IEEE Internet of Things Journal. 2021 Jul 6;9(1):1-24.

[246] Chen R, Li L, Xue K, Zhang C, Pan M, Fang Y. Energy efficient federated learning over heterogeneous mobile devices via joint design of weight quantization and wireless transmission. IEEE Transactions on Mobile Computing. 2022 Oct 11;22(12):7451-65.

[247] Nyangaresi VO, Mohammad Z. Privacy preservation protocol for smart grid networks. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[248] Liu Z, Guo J, Yang W, Fan J, Lam KY, Zhao J. Privacy-preserving aggregation in federated learning: A survey. IEEE Transactions on Big Data. 2022 Jul 15.

[249] Guembe B, Misra S, Azeta A. Privacy Issues, Attacks, Countermeasures and Open Problems in Federated Learning: A Survey. Applied Artificial Intelligence. 2024 Dec 31;38(1):2410504.

[250] Yaacoub JP, Noura HN, Salman O. Security of federated learning with IoT systems: Issues, limitations, challenges, and solutions. Internet of Things and Cyber-Physical Systems. 2023 Jan 1;3:155-79.

[251] Aouedi O, Sacco A, Khan LU, Nguyen DC, Guizani M. Federated Learning for Human Activity Recognition: Overview, Advances, and Challenges. IEEE Open Journal of the Communications Society. 2024.

[252] Chen H, Wang H, Long Q, Jin D, Li Y. Advancements in federated learning: Models, methods, and privacy. ACM Computing Surveys. 2024 Nov 7;57(2):1-39.

[253] Cao Y, Zhang J, Zhao Y, Su P, Huang H. SRFL: A Secure and Robust Federated Learning framework for IoT with trusted execution environments. Expert Systems with Applications. 2024 Apr 1;239:122410.