EUROPEAN ACADEMIC RESEARCH
Vol. XIII, Issue 11/ February 2026

Impact Factor: 3.4546 (UIF)
DRJI Value: 5.9 (B+)

ISSN 2286-4822
www.euacademic.org

Federated Learning Approaches for Edge Computing and IoT Cybersecurity: An Investigation

SHAHAD SHARAF ALDEEN YAHYA
DR. ESSA IBRAHIM ESSA
Kirkuk University
College of Computer Science and Information Technology
Kirkuk, Iraq
Corresponding authors:
Email: stcm24004@uokirkuk.edu.iq.
Email: dr.essa@uokirkuk.edu.iq

Abstract

Federated learning with edge computing and the internet of things (IoT) is considered for energy-efficient privacy-enhancing cybersecurity. The upshot of the review is that federated learning allows training of shared models without exchanging any raw data with the cloud and reduces risk of leaks and improves privacy (in particular in multi-device settings where device capabilities and network connectivity vary). The paper investigates how edge computing can support the placement of intelligence near sensors and IoT objects to reduce response times and enable real-time security responses (e.g., threats detection, anomaly identification). It differentiates between centralized and decentralized/diffused learning methodologies, and improves understanding of the merits of decentralized approaches for eradicating centralized single points of failure and enhancing attack resilience, and the challenges of coordinating and harmonizing models. In conclusion, the paper identifies promising research directions for future work in terms of the more pervasive use of decentralized learning-based approaches for enhancing edge security for IoT systems.

Keywords: Federation learning, Edge Computing, Internet of Thing, Cybersecurity, Cross Device, Decentralized Learning.

1. INTRODUCTION:

Cisco predicts that the connected IoT devices is anticipated to be around 75 billion by 2025 representing about 2.5 times the data generated in 2020, which was around 31 billion. Furthermore, IoT devices are increasingly equipped with advanced sensors for various mass data sensing applications, such as smart industry [1], healthcare [2], and UAV applications [3]. The current demand for time- and quality-sensitive IoT applications is substantial, necessitating highly available and flexible infrastructure. However, managing large, diverse, and decentralized IoT datasets while delivering services at a fixed performance level using cloud infrastructure seems impractical. Edge computing (EC) is an advanced architecture that brings cloud computing (CC) services closer to data sources, reducing latency and bandwidth costs while enhancing network flexibility and availability[4].Because of bandwidth constraints and privacy issues, transferring local data to the cloud for centralized training is not viable. This has spurred the development of so-called edge intelligence [5-6]. AI is expected to shift from the central cloud to the network edge to utilize the computing capabilities of the devices for

training models. To make sure edge data are kept secret and connectivity cost is minimized, special ML techniques need to be adopted to perform learning at edge nodes while protecting user data, i.e. This may be realized by a popular approach called unit learning (FL). This scheme can be considered as a rigorous algorithm as well as a core-edge computing design. Federated learning is characterized as a ML approach that learns an algorithm from locally distributed data holds on numerous edge devices or servers without data sharing [7-9]. Figure 1 illustrates the structure of the review article:

Fig 1. A Structure of Review Paper

2. FEDERATED LEARNING (FL):

First introduced by Google researchers in 2016, it emerged as a compromise between connectivity costs, learning modeling power, and data privacy protection [7], [9-13]. It is a distributed machine learning technology that trains models on the devices of users, companies, or individuals under centralized supervision, without the need to exchange local datasets. This ensures data privacy during the training process [14]. Its operation consists of four steps: (1) The central server collects model gradients from clients, (2) it compiles and updates the global model, (3) it sends the updated global model to clients, and (4) clients continue training locally using their own data [14].

2.1. Structure

The structure of the federated learning consists of four layers refer to Figure 2. each with a different function in the distributed learning mechanism [15].

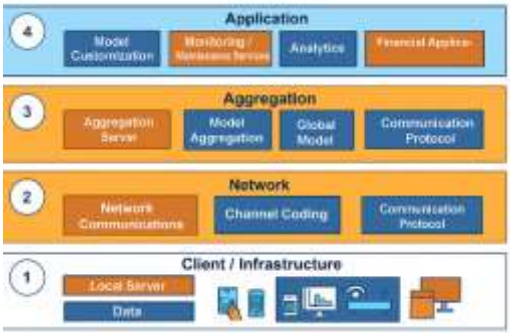

Fig 2. structure of the federated learning

a) *Client/Infrastructure layer*: This layer consist of the local devices and servers that actively participate in the ML process. The devices provide their local data and learning models to the central one [15]. A subdivision termed the Data Layer controls the local data and learning models at this layer, whilst the data is being processed and security stored on the single devices [16-17].
b) *Network Layer*: This is the layer responsible for the interaction of the devices, nodes, local servers and assembly servers among the ML system [15]. And it applies advanced channel coding to adjust a given data to the delay, to the congested channels and to a number of communication protocols among which: 6G, 5G, Z-Wave, ZigBee, Wi-Fi for an inter-exchange of data [16-18].
c) *Aggregation Layer*: Is the heart of the distributed system architecture that, integrates local model to global model. The model assembly process is controlled by the central assembly server. Different assembly methods define how the local models updates are aggregated into the global model [16-17].
d) *Application layer*: this can be considered as the top layer where the global model is adapted to the applications. It also comprises critical services including monitoring and maintenance to guarantee the continual and dependable functioning of FL system [15-17].

2.2. FL Taxonomy

Figure 3. illustrates the classification of unified learning and identifies its key components as follows: data segmentation methodologies, degree of integration (across isolated systems or across devices), and communication framework (centralized or decentralized). When these components are integrated, a framework is created for implementing unified learning across diverse applications, while considering data protection and efficiency [15].

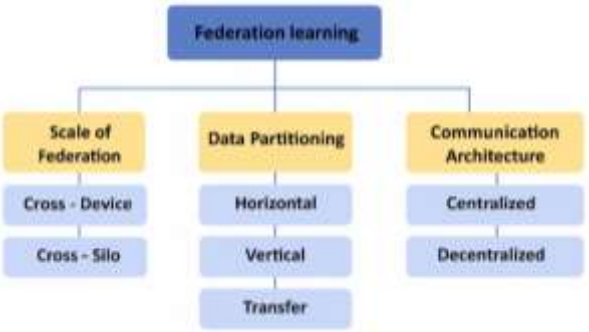

Fig 3. Federal Taxonomy

2.2.1. Coordination and Architectures: which are the participant nodes in the learning. It consists of four basic entities: the learner, the employee, and the computing and communication framework [19]. The learning process, which may be a high-level computing unit, is carried out by the overall learning model and its components. It handles customer interactions [20]. This may lead to a rejection of errors in the model [21]. In unified learning, the customers are the devices or locations that contain the data. Each customer selects a model based on its data, and then this model is sent to the

customer accordingly. Researchers then combine these research results to obtain a new global model [22]. There is a basic operating style: centralized and decentralized [23].

a) Centralized architecture: This approach relies on a central server that collects model parameters from all clients and builds a single global model by integrating these updates [24].

b) Decentralized architecture: In this method, process management is not centralized. Instead, multiple machines collaborate in a distributed manner to train the model. Each machine/server must communicate with the other machines and perform model integration locally [24].

2.2.2 Scale of Federation Learning

Federal learning schemes are categorized with respect to the number of users. According to this, are divided into two:

a) Cross-Device Federations: These consortia utilize multiple small devices with limited computing power. They comprise a larger number of devices (such as mobile phones or IoT devices) that have limitations in processing and data storage capacity. All participating devices contribute to training the global model [25].

b) Cross-Silo Federations: These consortia are used in large organizations that possess vast amounts of data. This approach requires customers, and potentially organizations, to have sufficient resources in terms of computing power and data. This approach allows these organizations to collaboratively improve a global model while maintaining the confidentiality of their original data, thus protecting privacy and facilitating the use of aggregated data [26].

2.2.3. Data segmentation in federative learning is divided into three types [27]:

a) Horizontal Federated learning: This type is applied when datasets have identical feature spaces but different sample spaces [28].

b) Vertical Federated learning: This type is applied when datasets have different feature spaces but share the same sample space [28].

c) Transitional Federated learning: This type is applied when datasets have different feature spaces and different sample spaces [28].

2.3. Federated Learning Applications:

a) Federated Learning in Healthcare: It is used for its ability to securely handle sensitive patient information across decentralized platforms. It has enabled the development of personalized diagnostics, medical image analysis, and real-time patient monitoring [29].

b) Federated Learning in Finance and Banking: It has facilitated the creation of collaborative models for fraud detection and the provision of personalized financial services, reducing the risk of data breaches while improving service quality [16].

c) Federated Learning in Smart Cities: Its use has led to increased operational efficiency, improved the standard of living for residents, and facilitated the provision of intelligent information to citizens about traffic systems, transportation, public safety, smart parking, smart agriculture, and more [30].

2.4. Attacks of Federation learning:

There are several types of attacks that affect the collaborative learning process in edge-fed federated learning, the most important of which are Byzantine attacks and poisoning attacks. A Byzantine attack occurs when a fully trusted node becomes malicious after all authentication and verification procedures have been successfully completed [14]. If some nodes are compromised, attacked, or disrupted, the entire federated learning system collapses [16]. A poisoning attack, which is an injection attack during the federated

learning training process, falls into two categories: data poisoning and model poisoning. [31].

Table 1. Summary of attacks in federation learning

References	Attack types	Description	Attackers
G. Shirvani, S. Ghasemshirazi, and B. Beigzadeh [27]	Backdoor Attacks	The attacker incorporates a "backdoor" or concealed trigger within the model. The model operates effectively with certain data sets but has failures with others.	Malicious agents (who manipulate local data/updates).
T. Li, A. K. Sahu, A. Talwalkar, and V. Smith [13]	Privacy/Data Inference Attacks	This type seeks to obtain more sensitive or confidential information regarding raw customer training data.	Central server, other clients, or external monitors intercepting traffic.
G. Shirvani, S. Ghasemshirazi, and B. Beigzadeh [27]	Model Sabotage Attacks	Disseminating harmful or deceptive local updates. The objective is to markedly diminish the model's accuracy.	Malicious agents (unauthorized participants) .
Albshaier, L., Almarri, S., & Albuali, A.[30]	Communication bottlenecks	Overcrowded wireless communications results in the loss of model parameters or heightened latency. This may be exploited or merely impede convergence, so dramatically undermining system reliability and security.	Environmental factors (such as unstable networks) or malicious clients (such as network overload) can contribute to this issue.

2.5. Defenses of Federation learning:

The client may sometimes, intentionally or unintentionally, make a mistake in the training system designed for federation learning, leading to atypical behaviors. These atypical behaviors must be mitigated to avoid negative consequences. Several solutions have been proposed, primarily related to the secure training process for federation learning. Researchers have developed attack detection strategies using a pre-trained model, anomaly detection, and a pre-trained server-level autoencoder to identify anomalous model weight updates and their sources [14].

Table 2. Summary of defenses in federation learning

Targeted	Attack Defense/Proposed	Solution Description	Research Source
Model Poisoning and Backdoor Attacks	Efficient Assembly Methods	Algorithms (such as median or truncated average) are used to calculate the average of the model to detect any malicious or unwanted updates sent by clients, thus preventing model corruption	Albshaier, L., Almarri, S., & Albuali, A. (2025).
privacy/Data Inference Attacks	Secure Multiparty Computing (SMPC)	An encryption protocol that allows a central server to compute the assembled model without decrypting or viewing model updates sent by clients.	Shirvani, G., Ghasemshirazi, S., & Beigzadeh, B. (2024, October).
Connection Bottlenecks/High Latency:	Model Compression:	Applying techniques such as quantization and others to reduce the size of the model and its updates significantly reduces communication costs and network latency.	Albshaier, L., Almarri, S., & Albuali, A. (2025).
Connection Bottlenecks/Transaction Loss	Dynamic Era Modulation	An adaptive scheme to dynamically set the number of local training epochs performed by each machine, reducing the total number of communication rounds required for model convergence.	Xiang, T., Bi, Y., Chen, X., Liu, Y., Wang, B., Shen, X., & Wang, X. (2023).
System Failures/Heterogeneity	Computational Encoder	Using algorithmic iteration to make blended learning resilient to (slow or idle) hardware, ensuring that overall training speed is not affected by the slowest participants.	Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020).

2.6 Challenges of Federation learning:

Figure 4. illustrates several issues that may arise in this domain, such as data imbalance and costly connections. The issues discussed in this section are enumerated below.

Fig 4. Challenges in Federation Learning

2.6.1 Imbalanced Data: We categorized these FL imbalances into three distinct groups for enhanced differentiation [13]:

- **a)** Size imbalance: when the dimensions of each edge node's data sample are inconsistent.
- **b)** Local imbalance: This is sometimes referred to as non-identical distribution or independent distribution, as not all nodes possess the same data distribution.
- **c)** Global imbalance: represents a dataset characterized by class imbalance throughout all nodes.

2.6.2 Expensive Communication: FL networks theoretically included an immense number of devices (such as millions of laptops and mobile devices), and network connectivity may be computationally intensive and slower by several orders of magnitude. In these networks, communication necessitates greater computational resources than conventional data center environments [13].

2.6.3 Systems Heterogeneity: The ferreted networks exhibit inherent heterogeneity stemming from variations in network connectivity (Wi-Fi, 3G, 4G, 5G), hardware (CPU, RAM), power (battery level), communication, storage, and computational capabilities of nodes[13].

2.6.4 Statistical Heterogeneity: The edges often gather and disseminate data in a non-independent and identically distributed manner throughout the network. Cellular phone users may employ an extensive vocabulary for predicting the subsequent word. Moreover, the data quantity across various edges may vary, and a foundational structure reflecting the interactions between devices and their corresponding distributions may be present. This data generation scenario contradicts the conventional Independent and Identically Distributed assumption of distributed optimization, increases the chance of straggler and makes analysis, modeling, and evaluation more complex [32–34].

2.6.5 Privacy: Because unified learning only takes model updates, such as gradient information, and not the entire dataset, it makes user data more secure. However, broadcasting local model updates at different stages of the training process may lead to information leakage to the main server or other malicious actors [32].

3. EDGE COMPUTING (EC):

EC is the processing of data near the data source rather than the traditional method of pulling the data into a central cloud data center [30],[35].

This approach reduces latency, improves response time, reduces the cost of data transmission and conserves network bandwidth through local data processing at the network edge [4], [36-37]. It is suitable for real-time data applications such as IoT devices, driverless cars, industrial automation [35],[38]. This method overcomes the limitations of traditional centralized computing paradigms such as cloud computing [39].

3.1. Architecture:

Figure 5. illustrates the basic architecture of edge computing. Edge computing servers are located closer to the user than cloud servers[40].

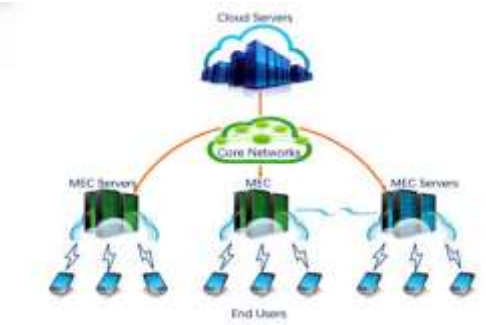

Fig 5. Edge computing architecture (a survey of edge computing for the Internet of Things).

The edge computing architecture is classified into three components: the front-end, the near-end, and the remote end:

- **a)** Front End: Peripheral devices, such as sensors and actuators, are located at the front end of the edge computing architecture. The front end environment improves user interaction, response speed, and provides real-time services for some applications thanks to the computing power offered by numerous nearby peripheral devices [40].
- **b)** Near End: The processing capacity for data traffic between gateways installed at the near end remains the highest in networks. The majority of data processing and storage activities are transferred to the near-end environment. As a result, users can benefit from significantly faster data computation and storage speeds, with only a slight increase in latency [40].
- **c)** Remote End: The placement of cloud computing servers at longer distances from peripherals results in significantly higher latencies over networks. Therefore, the cloud computing servers in the remote environment not only offer higher computing capability and larger data storage capacity but also enable large scale parallel data processing and knowledge extraction [41-42].

3.2. Characteristics of Edge Computing:

The notion of edge computing is summarized in three aspects, namely micro cloud computing, fog computing and mobile edge computing [43]. They're all the same idea: Bring computing power out of the cloud and on to the network edge[44].

3.3 Cloud Computing vs. Edge Computing:

Cloud computing has revolutionized how data is managed and used. It provides on-demand, self-service computing resources over the internet, without requiring users to own any physical infrastructure, on a pay-as-you-go basis. Instead of transferring all data to a central cloud data center, edge computing is a model where computation takes place at or near the data source. This at-source processing reduces latency and saves bandwidth [42].

Table 3. The difference between cloud computing and edge computing

Properties	Cloud computing	Edge computing
Component	Virtual resource	Edge node
Storage	Unlimited	Limited
Deployment	Centralized	Decentralized
Network access type	Mostly WAN	LAN(WLAN)
Number of computing resource location	Few	Many
Proximity to client device	Low	High
Response time	Slow	Fast
Connection to resource	Long	Short
Latency	High	Low

3.4. Edge Computing Applications:

a) Edge Computing in Smart Cities: Traffic, environmental, energy consumption and safety data can be managed by a large number of IoT devices generating big data [45]. It also helped to alleviate network congestion, speed up data processing, and preserve privacy [7].

b) Real-Time Applications: Edge computing plays a significant role in time-critical applications, such as self-driving cars or industrial control systems, that further need to make decisions in real-time [45-46].

c) Healthcare and Remote Monitoring: Real-time patient monitoring using edge computing has been applied especially in rural or home care. Wearable technology, connected health devices and portable medical devices can function at edge level by analyzing data and relaying data related to patient condition, such as vital signs, in real time and sending alerts if there is an emergency. This method enhances response time, which is critical for patients [45].

3.5. Challenges of Edge Computing: There are various challenges and issues would affect the performance of edge computing, such as:

a) Processing and storage capabilities are limited: The cloud data centers that are centralized have a much higher processing power and storage size than edge devices. Data-intensive processing or calculations can be difficult for edge devices because of their size and Power constraints[35].

b) Security and Schedule of Distributive Infrastructure: It's very hard to secure and enforce the same security posture across each of these individual node when you're distributed processing data on any number of machines, across various physical locations. Network security not only protects users, but it also defines an attack surface for every edge device, which must be provided with strong security defenses to protect the network from being exploited which could result in unauthorized access, malware, and data exfiltration [39].

c) Integration with Cloud Computing and Existing IT Systems: Integrating edge computing solutions with cloud computing and legacy IT systems can be challenging. Data flow between edge devices and central systems requires careful coordination,

leading to complex challenges in data synchronization and enterprise interoperability [30]. Managing legacy systems requires meticulous planning, often accompanied by customized solutions to ensure compatibility with both edge and cloud infrastructure [39].

3.6 Advantages of Edge Computing: Edge computing is suitable for real-time data processing application, resource efficient, and privacy rad: 16 considerations for 5G user IoT applications when deployed in the environment due to its decentralized processing close to the data source [30],[39]. The primary profitable advantages are:

- **a)** Lower latency and faster response time: As data is processed locally, there are limited delays introduced in moving the data to and from a local or remote server. The processing at the edge enables the low latency that is needed for applications requiring instant decisions such as autonomous driving, industrial automation and health care monitoring [35].
- **b)** Enhanced Bandwidth: This is achieved by processing and filtering at the source, rather than sending raw data to a central cloud for further analysis, thus eliminating irrelevant data. Optimal bandwidth utilization reduces transmission costs, which is highly desirable for many IoT devices that continuously generate data.[35, 39]
- **c)** Enhancing Privacy and Data Security: The Nature of this type of keeping data close to its source as owner, and does not require that hosts/sensitive data be transmitted over potentially insecure networks. Locally processed and stored data is less susceptible to external attacks resulting in increased privacy and security [47].

4. THE INTERNET OF THINGS (IoT):

This architectural design simply illustrates how embedded computing devices can be integrated with the existing internet, achieving autonomy in data collection and sharing. This technology leverages the capabilities of the internet and extends to non-traditional computing objects, such as physical objects embedded with sensors and software, enabling them to communicate and interact with each other or their environment [48]. This has led to the creation of an intelligent computing platform on top of billions of devices to solve real-world problems [49]. The components of an IoT system consist of three basic layers: the perception layer, the network layer, and the application layer, as illustrated in Figure 6 [50]:

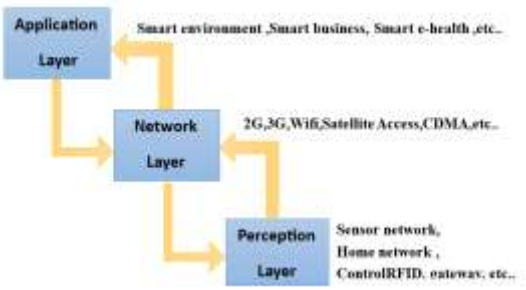

Fig 6. Architecture of IOT (Cyber Security: A Review of Internet of Thing (IOT) Security Issues, Challenges and Techniques).

4.1. Internet of Things (IoT) Infrastructure:

The operation of the Internet of Things relies on four components, as shown in Figure 7.:

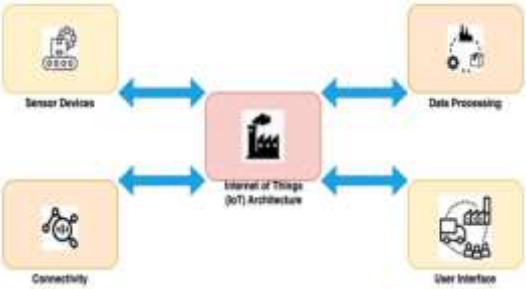

Fig 7. The four main components of the Internet of Things[51]

a) Sensors: These are small, microprocessors integrated into electronic devices that monitor or collect environmental data. Their function may be limited to reading temperature or collecting comprehensive data, such as video recordings [52].

b) Connectivity: The sensor requires a cloud connection to communicate, for example, a 5G network. Different strategies have been used depending on the types of devices the user configures. Connections may include mobile networks, Wi-Fi, GPS, satellites, local area networks (LANs), wide area networks (WANs), or other types [53].

c) Data Processing: The data is sent to the cloud and then processed, for example, monitoring temperatures within a specified range and assessing household activity using cameras [54].

d) User Interface: This is a basic interface used to manage IoT applications within a specific framework. For example, if the temperature exceeds a certain threshold, a notification is sent to the user, allowing them to monitor the temperature and adjust the environment accordingly [55].

4.2. IoT Attacks:

The use of diverse smart devices, applications, and services makes them more vulnerable to attack. We will examine some of the types of attacks these devices face as follows [56].

Table 4: Illustrating the attacks that Internet of Things (IoT) devices

References	Category	Types / Description	Thread models
Sfar et al., 2018; Roman et al., 2013	Device	High-end class, Low-end class	Stealing devices, modifying existing software, targeting individuals, and injecting malware.
Abomhara & Køien, 2015; Sicari et al., 2015	Location	Internal, External	Misuse of internal information, theft of internal data, external scanning, and remote code execution.
Zarpelão et al., 2017; Alaba et al., 2017	Access level	Active, Passive	Traffic analysis, eavesdropping, modification, injection attacks, jamming, replay attacks

References	Category	Types / Description	Thread models
Lin et al., 2017; Mosenia & Jha, 2017	Information damage level	Interruption, Eavesdropping, Modification, Fabrication, Replay, Man-in-the-middle	DoS, Jamming, Sniffing, Fake Data Injection
Conti et al., 2018; Sicari et al., 2015	Host promise	User, Hardware, Software	Credential Theft, Physical Tampering, Hardware Trojans, Vulnerability Exploits, Malware
Do et al., 2019; Zarpelão et al., 2017	Strategy	Physical, Logical	Jamming, Routing Attacks Software Exploits, Authentication Bypass
Mukherjee et al., 2017; Raza et al., 2013	Protocol – based	Disruption, Deviation	DoS/DDov , Packet Dropping, Routing Table Poisoning
Khan & Salah, 2018; Sicari et al., 2015	Layer – based	Perception, Network, Middleware, Application, Interface	Sensor Tampering , Wormhole, API Exploits, Malware, Weak Authentication

Attacks targeting devices, such as those targeting high-end and low-end devices, are categorized as follows: High-end attacks utilize powerful, fully equipped devices to target the Internet of Things (IoT) system, while low-end attacks utilize low-power devices for the same purpose. Site attacks represent both internal and external threats. Access-level attacks encompass both aggressive and passive attacks [57],[58]. Information corruption attacks include jamming, eavesdropping, modification, and replay. Host-based attacks target users, devices, and software. Strategic attacks include physical and cognitive attacks. Protocol-based attacks include jamming and spoofing. Layer-based attacks encompass cognitive, network, middleware, and application-based attacks [59].

4.3. IoT Challenges:

Due to the expansion of the Internet of Things (IoT), security vulnerabilities have emerged significantly. These vulnerabilities pose a threat to enhanced security. The following are some IoT security challenges that need to be addressed [29].

- **a)** Malware and Ransomware: The increasing number of IoT devices is now exploiting the surge in malware and ransomware targeting them. Encryption is also highly relied upon by ransomware to limit user access to devices, damage them, and capture user data [60].
- **b)** Cryptocurrency Botnets: The rise of cryptocurrencies has brought with it an increase in hacking attempts to steal their assets. Even with new technologies emerging such as blockchain to avoid the hacking risk [61].

c) Lack of Encryption: Encryption provides a good way to safeguard data from being accessed by the bad actors, however it is very challenging on IoT security. Such devices do not have any limitations and can do what an ordinary computer can do. The consequence of this is more security holes that give programmers the ability to easily beat the security protections they need to bypass [62].

d) Micro-Attacks in the IoT: Micro-attacks pose some of the most significant challenges in IoT security. They are harder and harder to discover, and they can be executed without being identified. Hackers can also breach routine operations, like printers and cameras [63].

e) Phishing Attacks: These are due to security flaws, ongoing technological evolution, and IoT devices is one of the recent means of attacks. Signals can apparently be sent from hackers to IoT devices to create a host of issues. It is considered as a most prevalent type of security breach due to the fact that most of the companies do not train their employees to keep up with the newest phishing threats [64].

f) Weak Default Passwords: Weak default passwords are prevalent among IoT devices. While it is good practice to change the password, some IT admins forget to do this vital step. A simple password also makes your IoT device more susceptible to a brute-force attack [65].

4.4. Internet of Things (IoT) Applications:

IoT is understood as a proximate cloud of objects (devices, sensors, actuators, etc.) equipped with a digital or analog interface capable of collecting and disseminating data that is influencing the efficiency, sustainability, and liveliness of cities [1]. In smart cities, IoT devices are embedded in the urban infrastructure such as transportation, power grids, and streets to form a pervasive network, in which data is constantly collected, transmitted, and processed. This fabric allows for more informed decision-making and streamlined processes for city officials, and better services for citizens [66]. The IoT enables the transformation of cities to not only high-tech but also more sustainable, resilient, and tailored to the need of their inhabitants through data-driven paradigm [28]. Application of IoT in smart city brings several advantages such as increase in efficiency. Several city processes can be monitored and controlled in real-time due to IoT devices that facilitate a quick reaction to environmental conditions. Intelligent transportation systems can take advantage of IoT data to enhance the management of traffic congestion [36].

5. CYBERSECURITY:

Security is the process of providing assurance that matter is protected against the risk of physical or non-physical destruction, unauthorized access, theft or loss via the maintenance of confidentiality, integrity and availability of information relevant to that matter [67], [68]. Due to higher risk of potential data loss or other types of cybercrime, many small business owners are anxious about their online presence or the take up of modern technology advancements. That said, there are measures you can take to shield your organization and your customers from these threats [67].

5.1. Challenges of cybersecurity

In discussions regarding cybersecurity, a pertinent question arises: "What are we striving to protect ourselves against?" There are three primary features we find burdensome in a resistor [19]:

- **a)** Unauthorized Access.
- **b)** Unauthorized Deletion.
- **c)** Unauthorized Modification.

An essential definition pertinent to cybersecurity is CIA. CIA represents Confidentiality, Integrity, and Availability. It is stipulated that secret content must be securely maintained and safeguarded against alterations by unauthorized individuals [23]. It must be accessible when required for authorized users. The CIA triad should be a fundamental component at the organizational level when formulating information security and cybersecurity policies [51],[68]:

a) Confidentiality: Confidentiality is the safeguarding of personal information. Confidentiality entails safeguarding a customer's information exclusively between the client and oneself, without influence from others, including coworkers, acquaintances, or relatives. Assaults are [19]:

1. Decrypting encrypted data.
2. Human, during the intermediate assaults on unencrypted text.
3. Data exfiltration / illicit duplication of confidential information.
4. Remediating spyware or malware on a server.

b) Integrity: In the context of computer systems, pertains to methods ensuring that data is accurate, reliable, and protected from unauthorized alterations. Assaults are [69]:

1. Web exploitation for malware deployment.
2. Illegitimately accessing servers and altering records.
3. Unauthorized database fraud.
4. Exerting remote control over Zombie systems.

c) Availability: In the context of a computer system, availability refers to the capacity of a user to access data or resources in a specified environment and in the correct format. Assaults are [19]:

1. DOS / DDOS attacks.
2. Ransomware assaults necessitated the encryption of critical data.
3. Intentionally sabotaging the power supply of a server room.
4. Overwhelming a server with an excessive number of requests

5.2. Attacks of Cybersecurity:

a) Malware: Malware encompasses a number of threats, including viruses and worms, described as malicious code that often steals data and degrades computer software [70].

b) Phishing: Phishing in the guise of a legitimate request for information from a trustworthy third party Phishing attacks are initiated via email, prompting individuals to click on a link and input personal information. Emails have become far more sophisticated in recent years, complicating the ability of certain individuals to distinguish between accurate information and falsehoods [70].

c) Password Attacks: The Middleman is attempting to get unauthorized access to our system by monitoring user passwords and personal information without our knowledge [70].

d) Distributed Denial-of-Service (DDoS) attacks: These attacks disrupt network services. Sniffers transmit large amounts of data, creating numerous connection requests to the network, causing it to become overloaded and eventually crash [70].

6. Summary of Previous Studies:

The table below presents a systematic collection of information on previous studies, categorized by publication year, main objective, methodology, data type, field, challenges, research problem, main findings, and research gap. This comparative analysis is a useful step in identifying shortcomings in the current literature and addressing incomplete aspects of previous studies.

Table 5: The summary of some review studies

Title Public	Public Year	Main Objective	Methodology	Data Type	Field	Challenges\ Problem	Main Findings	Research Gap
1.An Overview on Edge Computing Research	2020	To provide a comprehensive overview of Edge Computing (EC) research and its challenges.	Survey/Overview	Theoretical/Literature	Edge Computing (EC)	Bandwidth load, slow response, poor security, and privacy in traditional cloud computing.	Summarizes current techniques and identifies future research directions.	Need for practical, applied solutions to the identified challenges.
2.Cyber Security with IOT	2019	To discuss cybersecurity guidelines and threats in the context of the Internet of Things (IoT).	Review Paper	Theoretical/Literature	IoT Cybersecurity	The significant security anxiety introduced by IoT.	Identifies common threats (DoS, viruses) and basic protection methods.	Limited to the mentioned basic areas.
3.Cyber Security: A Review of Internet of Things (IoT) Security Issues, Challenges and Techniques	2019	To review IoT security issues, challenges, and techniques.	Review	Theoretical/Statistical (Crime Stats)	IoT Cybersecurity	Rising cybercrimes and the urgent need to secure cyberspace.	Comprehensive review of threats, vulnerabilities, and defensive techniques.	Necessity for developing sustainable and effective security solutions.
4.IoT from cyber security perspective Case study JYVSECTEC	2018	To focus on the cybersecurity perspective of IoT environment/appliances and apply a case study.	Master's Thesis: Conceptual + Practical (Case Study)	Operational Case Data (Risk assessment/Pen testing)	IoT Cybersecurity, Case Study	Increasing number of IoT devices and the need to secure them against vulnerabilities and attacks.	Identifies weaknesses and provides recommendations for basic protection and administrative security controls.	Results are limited to the single case study environment (JYVSECTEC) .
5.Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics	2018	A systematic review of IoT cybersecurity, including architecture, taxonomy, and key countermeasures.	Systematic Review	Theoretical/Literature	IoT Cybersecurity	The challenge of protecting and integrating heterogeneous smart devices.	Reviews key architecture, taxonomy, and countermeasures for IoT.	Need for effective solutions for integration and protection of heterogeneous devices.
6.Federated Learning: Attacks, Defenses, Opportunities, and Challenges	2024	To provide a comprehensive overview of security and privacy features in Federated Learning (FL).	Comprehensive Overview and Review	Theoretical/Literature	Federated Learning (FL)	The immaturity of FL and the controversy over its security and privacy implications.	Identifies the attack surface and reviews current and proposed defense measures.	Building a secure environment for FL to achieve widespread future adoption.
7.Edge Computing and IoT in Smart Cities - An Overview	2024	To study the synergy of Edge Computing and IoT as critical enablers for creating smart cities	Overview/Book Chapter	Theoretical/Conceptua l	Smart Cities, EC, IoT	Urban growth and high sustainability expectations.	Demonstrates the complementary role of the two technologies in building more efficient and resilient smart cities.	Need for in-depth analysis of specific applications and performance measurement.
8.Exploring the Synergy of Fog Computing, Blockchain, and Federated Learning for IoT Applications: A Systematic Literature Review	2024	To explore the synergy of Fog Computing, Blockchain, and FL for IoT applications.	Systematic Literature Review (SLR) of 40 papers.	Theoretical/Literature	IoT, Fog Computing, Blockchain, FL	Research gap in examining the interoperability of the technologies across IoT architectural layers.	Proposes a new framework that addresses the interoperability of the three technologies.	None (The study filled the gap it identified).
9.Applications of Federated Learning; Taxonomy, Challenges, and Research Trends	2022	A comprehensive review of FL applications, taxonomy, challenges, and research trends.	Survey/Literature Review	Theoretical/Literature	Federated Learning (FL)	Challenges related to FL (e.g., heterogeneity, privacy, communication costs).	Classifies applications, and identifies key challenges and future research directions.	Need for practical solutions for challenges like heterogeneity and privacy in FL environments.
10.Intelligent deep federated learning model	2025	To develop the IDFLM-ES model for deep FL to detect intrusion and	Model Development (IDFLM-ES based	Training/Testing Data (for intrusion detection)	IoT Security, Edge Computing, FL	Information leakage/privacy issues and the	Proposes the IDFLM-ES model which improves	Need for effective privacy-

Title Public	Public Year	Main Objective	Methodology	Data Type	Field	Challenges\ Problem	Main Findings	Research Gap
for enhancing security in internet of things enabled edge computing environment		enhance security in IoT-enabled EC environment.	on Federated Hybrid Deep Learning)			challenge of heterogeneity when implementing FL.	security, intrusion detection, and overcomes heterogeneity.	preserving intrusion detection models in both homogeneous and heterogeneous IoT environments.
11.Heterogeneity -Aware Federated Learning with Adaptive Local Epoch Size in Edge Computing	2023	To minimize the wall-clock convergence time of FL by adapting the Local Epoch Size, considering both resource and statistical heterogeneity.	Mathematical Modeling and Analysis (Deriving Convergence Upper Bound)	Mathematical/Experimental (for convergence analysis)	Federated Learning (FL) in Edge Computing.	Resource and statistical heterogeneity in EC environments causing long FL training time.	Proves the relationship between the number of training rounds and local epoch size under non-IID data distribution.	Need to solve the non-convex problem of minimizing FL training time while maintaining accuracy.
12.Cybersecurity Challenges and Solutions in Internet of Things (IoT) Networks	2018	To survey current IoT cybersecurity threats and explore emerging solutions (lightweight encryption, blockchain, AI-driven anomaly detection).	Survey	Theoretical/Literature	IoT Cybersecurity	Device resource constraints, network heterogeneity, and diverse attack surfaces in IoT.	Identifies threats (hardware vulnerabilities, network attacks, privacy issues) and discusses trade-offs between security, performance, and scalability.	Need for better trade-offs between security, performance, and scalability in IoT deployments.

7. CONCLUSION

Analysis of 70 studies has shown that integrating federal learning with edge computing is a promising approach to addressing the security and privacy challenges of IoT systems. The studies also demonstrated that decentralized training using edge computing significantly reduces the risk of data leaks compared to centralized models. This enhances the ability to detect threats and anomalies in real time due to the processing's proximity to the data source. Moreover, the results reveal that federated learning achieves a good accuracy under a wide range of non-IID degree in cross- device scenario, since it strikes a good balance between model accuracy and communication efficiency. Studies also validate that decentralized architecture mitigates single point of failures, hardens against attacks but it struggles with constrained computational resources of edge-based architecture, power fluctuations, and interruptions of connectivity. While there are some benefits to federal learning, it comes with a number of threats. Since it is more vulnerable to poisoning attacks, gradient manipulation, and even data recovery from updates, it is necessary to combine it with other security techniques such as differential encryption, secure clustering, and verification of update integrity. The studies find that the paths for good progress toward the future are to design and enhance hybrid architectures that leverage edge computing with the efficiency of the cloud, and to address the issue of clustering and its bias due to its distribution, also considering the need to enable FL to work in highly dynamic and large IoT environments, for maintaining cyber security and enhancing the trustworthiness of intelligent systems.

Acknowledgements
The authors would you like to thank the Computer Science and Information Technology department, Kirkuk University, Iraq, for support this work.

REFERENCES

[1] R. Basir *et al.*, "Fog computing enabling industrial internet of things: State-of-the-art and research challenges," *Sensors (Switzerland)*, vol. 19, no. 21, pp. 1–38, 2019, doi: 10.3390/s19214807.
[2] R. Pryss, M. Reichert, J. Herrmann, B. Langguth, and W. Schlee, "Mobile crowd sensing in clinical and psychological trials-a case study," *Proc. - IEEE Symp. Comput. Med. Syst.*, vol. 2015-July, pp. 23–24, 2015, doi: 10.1109/CBMS.2015.26.

[3] L. Liu, C. Chen, Q. Pei, S. Maharjan, and Y. Zhang, "Vehicular Edge Computing and Networking: A Survey," *Mob. Networks Appl.*, vol. 26, no. 3, pp. 1145–1168, 2021, doi: 10.1007/s11036-020-01624-1.
[4] H. G. Abreha, C. J. Bernardos, A. de la Oliva, L. Cominardi, and A. Azcorra, "Monitoring in fog computing: State-of-the-art and research challenges," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 36, no. 2, pp. 114–130, 2021, doi: 10.1504/ijahuc.2021.113384.
[5] G. Zhu *et al.*, "Pushing AI to wireless network edge: an overview on integrated sensing, communication, and computation towards 6G," *Sci. China Inf. Sci.*, vol. 66, no. 3, 2023, doi: 10.1007/s11432-022-3652-2.
[6] X. Wang, Y. Han, C. Wang, Q. Zhao, X. Chen, and M. Chen, "In-edge AI: Intelligentizing mobile edge computing, caching and communication by federated learning," *IEEE Netw.*, vol. 33, no. 5, pp. 156–165, 2019, doi: 10.1109/MNET.2019.1800286.
[7] H. Brendan McMahan, E. Moore, D. Ramage, S. Hampson, and B. Agüera y Arcas, "Communication-efficient learning of deep networks from decentralized data," *Proc. 20th Int. Conf. Artif. Intell. Stat. AISTATS 2017*, vol. 54, 2017.
[8] S. Ji *et al.*, "Emerging trends in federated learning: from model fusion to federated X learning," *Int. J. Mach. Learn. Cybern.*, vol. 15, no. 9, pp. 3769–3790, 2024, doi: 10.1007/s13042-024-02119-1.
[9] P. Kairouz, H. B. McMahan, B. Avent, A. Bellet, and ..., *Advances and open problems in federated learning*. 2019.
[10] D. Ropout, "E Fficient F Ederated L Earning," *Iclr*, vol. 1, no. 2018, pp. 1–12, 2021.
[11] J. Konečný, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, "Federated Learning: Strategies for Improving Communication Efficiency," pp. 1–10, 2017, [Online]. Available: http://arxiv.org/abs/1610.05492
[12] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, pp. 1–19, 2019, doi: 10.1145/3298981.
[13] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated Learning: Challenges, Methods, and Future Directions," *IEEE Signal Process. Mag.*, vol. 37, no. 3, pp. 50–60, 2020, doi: 10.1109/MSP.2020.2975749.
[14] S. Xu, Z. Yu, K. Fu, Q. Jia, and R. Xie, "Machine Learning Enabled Edge Computing: A Survey and Research Challenges," 2022. doi: 10.1007/978-981-16-8558-3_14.
[15] W. V. Solis, J. Marcelo Parra-Ullauri, and A. Kertesz, "Exploring the Synergy of Fog Computing, Blockchain, and Federated Learning for IoT Applications: A Systematic Literature Review," *IEEE Access*, vol. 12, no. April, pp. 68015–68060, 2024, doi: 10.1109/ACCESS.2024.3398034.
[16] L. U. Khan, W. Saad, Z. Han, E. Hossain, and C. S. Hong, "Federated learning for internet of things: Recent advances, taxonomy, and open challenges," *IEEE Commun. Surv. Tutorials*, vol. 23, no. 3, pp. 1759–1799, 2021, doi: 10.1109/COMST.2021.3090430.
[17] M. Moshawrab, M. Adda, A. Bouzouane, H. Ibrahim, and A. Raad, "Reviewing Federated Learning Aggregation Algorithms; Strategies, Contributions, Limitations and Future Perspectives," *Electron.*, vol. 12, no. 10, pp. 1–35, 2023, doi: 10.3390/electronics12102287.
[18] H. Zhang, J. Bosch, and H. H. Olsson, "Federated learning systems: Architecture alternatives," *Proc. - Asia-Pacific Softw. Eng. Conf. APSEC*, vol. 2020-Decem, pp. 385–394, 2020, doi: 10.1109/APSEC51365.2020.00047.
[19] P. D. Babu, C. Pavani, and C. E. Naidu, "Cyber Security with IOT," *5th Int. Conf. Sci. Technol. Eng. Math. ICONSTEM 2019*, vol. 1, pp. 109–113, 2019, doi: 10.1109/ICONSTEM.2019.8918782.
[20] A. Abdullah, R. Hamad, M. Abdulrahman, H. Moala, and S. Elkhediri, "CyberSecurity: A Review of Internet of Things (IoT) Security Issues, Challenges and Techniques," 2019. doi: 10.1109/CAIS.2019.8769560.
[21] J. Golosova and A. Romanovs, "The advantages and disadvantages of the blockchain technology," *2018 IEEE 6th Work. Adv. Information, Electron. Electr. Eng. AIEEE 2018 - Proc.*, 2018, doi: 10.1109/AIEEE.2018.8592253.
[22] A. Nilsson, S. Smith, G. Ulm, E. Gustavsson, and M. Jirstrand, "A performance evaluation of federated learning algorithms," *DIDL 2018 - Proc. 2nd Work. Distrib. Infrastructures Deep Learn. Part Middlew. 2018*, pp. 1–8, 2018, doi: 10.1145/3286490.3286559.
[23] V. Sulkamo, "IoT from cyber security perspective Case study JYVSECTEC School of Technology, Communication and Transport Information Technology Master's Degree Programme in Cyber Security," 2018.
[24] A. Brecko, E. Kajati, J. Koziorek, and I. Zolotova, "Federated Learning for Edge Computing: A Survey," *Appl. Sci.*, vol. 12, no. 18, pp. 1–36, 2022, doi: 10.3390/app12189124.
[25] W. Yang, N. Wang, Z. Guan, L. Wu, X. Du, and M. Guizani, "A Practical Cross-Device Federated Learning Framework over 5G Networks," *IEEE Wirel. Commun.*, vol. 29, no. 6, pp. 128–134, 2022, doi: 10.1109/MWC.005.2100435.
[26] W. Yao, T. Liu, Y. Cui, and Y. Zhu, "Heterogeneity-Aware Federated Learning with Adaptive Local Epoch Size in Edge Computing," *2023 19th Int. Conf. Mobility, Sens. Netw.*, pp. 167–174, 2023, doi: 10.1109/MSN60784.2023.00036.
[27] G. Shirvani, S. Ghasemshirazi, and B. Beigzadeh, "Federated Learning: Attacks, Defenses, Opportunities, and Challenges," pp. 1–14.
[28] M. Duan, D. Liu, X. Chen, R. Liu, Y. Tan, and L. Liang, "Self-Balancing Federated Learning with Global Imbalanced Data in Mobile Systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 1, pp. 59–71, 2021, doi: 10.1109/TPDS.2020.3009406.
[29] M. Babar, B. Qureshi, and A. Koubaa, *Investigating the impact of data heterogeneity on the performance of federated learning algorithm using medical imaging*, vol. 19, no. 5 May. 2024. doi: 10.1371/journal.pone.0302539.
[30] L. Albshaier, S. Almarri, and A. Albuali, "Federated Learning for Cloud and Edge Security: A Systematic Review of Challenges and AI Opportunities," *Electron.*, vol. 14, no. 5, 2025, doi: 10.3390/electronics14051019.
[31] Z. Yang, M. Chen, K. K. Wong, H. V. Poor, and S. Cui, "Federated Learning for 6G: Applications, Challenges, and Opportunities," *Engineering*, vol. 8, pp. 33–41, 2022, doi: 10.1016/j.eng.2021.12.002.

[32] W. Y. B. Lim *et al.*, "Federated Learning in Mobile Edge Networks: A Comprehensive Survey," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 3, pp. 2031–2063, 2020, doi: 10.1109/COMST.2020.2986024.
[33] Y. Zeng *et al.*, "Adaptive Federated Learning With Non-IID Data," *Comput. J.*, vol. 66, no. 11, pp. 2758–2772, 2023, doi: 10.1093/comjnl/bxac118.
[34] M. Luo, F. Chen, D. Hu, Y. Zhang, J. Liang, and J. Feng, "No Fear of Heterogeneity: Classifier Calibration for Federated Learning with Non-IID Data," *Adv. Neural Inf. Process. Syst.*, vol. 8, no. NeurIPS, pp. 5972–5984, 2021.
[35] N. A. Angel, D. Ravindran, P. M. D. R. Vincent, K. Srinivasan, and Y. C. Hu, "Recent advances in evolving computing paradigms: Cloud, edge, and fog technologies," *Sensors*, vol. 22, no. 1, 2022, doi: 10.3390/s22010196.
[36] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A Survey on Mobile Edge Computing: The Communication Perspective," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 4, pp. 2322–2358, 2017, doi: 10.1109/COMST.2017.2745201.
[37] P. Mach and Z. Becvar, "Mobile Edge Computing: A Survey on Architecture and Computation Offloading," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 3, pp. 1628–1656, 2017, doi: 10.1109/COMST.2017.2682318.
[38] Q. Wang, G. Jin, Q. Li, K. Wang, Z. Yang, and H. Wang, "Industrial Edge Computing: Vision and Challenges," *Inf. Control*, vol. 50, no. 3, pp. 257–274, 2021, doi: 10.13976/j.cnki.xk.2021.1030.
[39] B. Bajic, I. Cosic, B. Katalinic, S. Moraca, M. Lazarevic, and A. Rikalovic, "Edge computing vs. Cloud computing: Challenges and opportunities in industry 4.0," *Ann. DAAAM Proc. Int. DAAAM Symp.*, vol. 30, no. 1, pp. 864–871, 2019, doi: 10.2507/30th.daaam.proceedings.120.
[40] W. Yu *et al.*, "A Survey on the Edge Computing for the Internet of Things," *IEEE Access*, vol. 6, pp. 6900–6919, 2017, doi: 10.1109/ACCESS.2017.2778504.
[41] R. Chataut, A. Phoummalayvane, and R. Akl, "Unleashing the Power of IoT: A Comprehensive Review of IoT Applications and Future Prospects in Healthcare, Agriculture, Smart Homes, Smart Cities, and Industry 4.0," *Sensors*, vol. 23, no. 16, 2023, doi: 10.3390/s23167194.
[42] W. Yu, G. Xu, Z. Chen, and P. Moulema, "A cloud computing based architecture for cyber security situation awareness," *2013 IEEE Conf. Commun. Netw. Secur. CNS 2013*, pp. 488–492, 2013, doi: 10.1109/CNS.2013.6682765.
[43] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges," *Futur. Gener. Comput. Syst.*, vol. 78, pp. 680–698, 2018, doi: 10.1016/j.future.2016.11.009.
[44] K. Dolui and S. K. Datta, "Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing," *GIoTS 2017 - Glob. Internet Things Summit, Proc.*, 2017, doi: 10.1109/GIOTS.2017.8016213.
[45] R. Dave, N. Seliya, and N. Siddiqui, "The Benefits of Edge Computing in Healthcare, Smart Cities, and IoT," *J. Comput. Sci. Appl.*, vol. 9, no. 1, pp. 23–34, 2021, doi: 10.12691/jcsa-9-1-3.
[46] T. Zhang, Y. Li, and C. L. Philip Chen, "Edge computing and its role in Industrial Internet: Methodologies, applications, and future directions," *Inf. Sci. (Ny).*, vol. 557, pp. 34–65, 2021, doi: 10.1016/j.ins.2020.12.021.
[47] G. Carvalho, B. Cabral, V. Pereira, and J. Bernardino, "Edge computing: current trends, research challenges and future directions," *Computing*, vol. 103, no. 5, pp. 993–1023, 2021, doi: 10.1007/s00607-020-00896-5.
[48] D. Fawzy, S. M. Moussa, and N. L. Badr, "The Internet of Things and Architectures of Big Data Analytics: Challenges of Intersection at Different Domains," *IEEE Access*, vol. 10, pp. 4969–4992, 2022, doi: 10.1109/ACCESS.2022.3140409.
[49] I. Ud Din *et al.*, "The Internet of Things: A Review of Enabled Technologies and Future Challenges," *IEEE Access*, vol. 7, pp. 7606–7640, 2019, doi: 10.1109/ACCESS.2018.2886601.
[50] L. Da Xu, Y. Lu, and L. Li, "Embedding Blockchain Technology into IoT for Security: A Survey," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10452–10473, 2021, doi: 10.1109/JIOT.2021.3060508.
[51] A. D. Jurcut, P. Ranaweera, and L. Xu, "Introduction to IoT Security," *IoT Secur. Adv. Authentication*, pp. 27–64, 2020, doi: 10.1007/978-1-4842-6434-8_1.
[52] A. A. Khan *et al.*, "Secure Remote Sensing Data With Blockchain Distributed Ledger Technology: A Solution for Smart Cities," *IEEE Access*, vol. 12, no. March, pp. 69383–69396, 2024, doi: 10.1109/ACCESS.2024.3401591.
[53] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *J. Inf. Secur. Appl.*, vol. 38, pp. 8–27, 2018, doi: 10.1016/j.jisa.2017.11.002.
[54] G. Kesavan, P. Sanjeevi, and P. Viswanathan, "A 24 hour IoT framework for monitoring and managing home automation," *Proc. Int. Conf. Inven. Comput. Technol. ICICT 2016*, vol. 1, 2016, doi: 10.1109/INVENTIVE.2016.7823205.
[55] D. Navani, S. Jain, and M. S. Nehra, "The internet of things (IoT): A study of architectural elements," *Proc. - 13th Int. Conf. Signal-Image Technol. Internet-Based Syst. SITIS 2017*, vol. 2018-Janua, pp. 473–478, 2017, doi: 10.1109/SITIS.2017.83.
[56] Y. Lu and L. Da Xu, "Internet of things (IoT) cybersecurity research: A review of current research topics," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2103–2115, 2019, doi: 10.1109/JIOT.2018.2869847.
[57] M. Hossain, R. Hasan, and A. Skjellum, "Securing the Internet of Things: A Meta-Study of Challenges, Approaches, and Open Problems," *Proc. - IEEE 37th Int. Conf. Distrib. Comput. Syst. Work. ICDCSW 2017*, pp. 220–225, 2017, doi: 10.1109/ICDCSW.2017.78.
[58] A. Mayzaud, R. Badonnel, and I. Chrisment, "A taxonomy of attacks in RPL-based internet of things," *Int. J. Netw. Secur.*, vol. 18, no. 3, pp. 459–473, 2016.
[59] S. U. Rehman, K. W. Sowerby, and C. Coghill, "Analysis of impersonation attacks on systems using RF fingerprinting and low-end receivers," *J. Comput. Syst. Sci.*, vol. 80, no. 3, pp. 591–601, 2014, doi: 10.1016/j.jcss.2013.06.013.
[60] C. M. Zahra SR, "RansomWare and Internet of Things: A New Security Nightmare," in *9th international conference on cloud computing, data science & engineering*, 2019, pp. 1–9.

[61] Y. Lu, "Security and Privacy of Internet of Things: A Review of Challenges and Solutions," *J. Cyber Secur. Mobil.*, vol. 12, no. 6, pp. 813–844, 2023, doi: 10.13052/jcsm2245-1439.1261.
[62] J. King and A. I. Awad, "A distributed security mechanism for Resource-Constrained IoT Devices," *Inform.*, vol. 40, no. 1, pp. 133–143, 2016.
[63] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," *2015 10th Int. Conf. Internet Technol. Secur. Trans. ICITST 2015*, pp. 336–341, 2016, doi: 10.1109/ICITST.2015.7412116.
[64] B. Naqvi, K. Perova, A. Farooq, I. Makhdoom, S. Oyedeji, and J. Porras, "Mitigation strategies against the phishing attacks: A systematic literature review," *Comput. Secur.*, vol. 132, p. 103387, 2023, doi: 10.1016/j.cose.2023.103387.
[65] D. Yu, L. Zhang, Y. Chen, Y. Ma, and J. Chen, "Large-Scale IoT Devices Firmware Identification Based on Weak Password," *IEEE Access*, vol. 8, pp. 7981–7992, 2020, doi: 10.1109/ACCESS.2020.2964646.
[66] M. R. Kaur, "Edge Computing and IoT in Smart Cities-An Overview," *Holist. Res. Perspect.*, vol. 11, no. April, 2024.
[67] A. Stango, N. R. Prasad, and D. M. Kyriazanos, "A threat analysis methodology for security evaluation and enhancement planning," *Proc. - 2009 3rd Int. Conf. Emerg. Secur. Information, Syst. Technol. Secur. 2009*, pp. 262–267, 2009, doi: 10.1109/SECURWARE.2009.47.
[68] B. Schneier, "Secrets and Lies: DIGITAL SECURITY IN A NETWORKED WORLD," *Secrets Lies Digit. Secur. a Networked World*, pp. 1–414, 2015, doi: 10.1002/9781119183631.
[69] M. Kozik Rafałand Chorąś, "Current cyber security threats and challenges in critical infrastructures protection," *2013 2nd Int. Conf. Informatics Appl. ICIA 2013*, pp. 93–97, 2013, doi: 10.1109/ICoIA.2013.6650236.
[70] O. Galinina, S. Andreev, I. Conference, and D. Hutchison, *Internet of Things , Smart Spaces , and Next Generation*, vol. 1, no. 18. 2018. [Online]. Available: http://dx.doi.org/10.1007/978-3-030-01168-0_11