International Journal of Computers and Informatics

Journal Homepage: https://www.ijci.zu.edu.eg

Int. j. Comp. Info. Vol. 8 (2025) 23–43

Paper Type: Original Article

Privacy-Preserving Federated Learning in Network Intrusion Detection: A Systematic Literature Review

Eman Shalabi [1], **Walid Khedr** [2, 1], **Ehab Rushdy** [1] and **Ahmad Salah** [3, 1, *]

[1] Department of Information Technology, Faculty of Computers and Informatics, Zagazig University, Zagazig, 44519, Egypt; Emails: emanselem@zu.edu.eg; wkhedr@zu.edu.eg; ehab.rushdy@zu.edu.eg; ahmad@zu.edu.eg

[2] College of Computer Science and Engineering, Taibah University, Yanbu 966144, Saudi Arabia; wkhedr@taibahu.edu.sa.

[3] College of Computing and Information Sciences, University of Technology and Applied Sciences, Ibri, 516, Oman; ahmad.salah@utas.edu.om.

Received: 01 Feb 2025 **Revised**: 10 Apr 2025 **Accepted**: 04 Jul 2025 **Published**: 06 Jul 2025

Abstract

Machine learning privacy preservation is essential because it defends against misuse and illegal access to sensitive personal data including financial information, medical records, and behavioral patterns. Centralizing data in one place is necessary for traditional machine learning techniques, which poses serious privacy problems. Federated learning becomes an innovative approach in this situation. With federated learning, the model comes to the data rather than the other way around, radically altering the training process for machine learning systems. Individual devices or organizations where the data is naturally located are used for the training process rather than a central server. Each participant trains the model using local data, and only model updates are returned to the global model for updating. Raw data never leaves its original place, hence there is a far lower chance of data breaches during transfer. This article proposes a systematic review of federated learning with privacy preservation for intrusion detection. The three chosen online libraries of IEEE Xplorer, Scopus, and Web of Science are searched. Each database has its corresponding search query. The search is conducted to include all papers published since 2016 on computer science research area. The search results contain 220 papers from the different search engines. After removing duplicated papers, the search results are reduced to 131. Inclusion and exclusion criteria are then used to filter the search results. After applying the criteria of inclusion and exclusion, only 32 papers are approved.

Keywords: Privacy Preservation, Machine Learning, Federated Learning, Intrusion Detection.

1 | Introduction

Data privacy is a discipline intended to protect data against improper or unauthorized access and theft [1]. It focuses on how to properly store, access, retain, and secure sensitive data. It also protects data from any alteration, so it maintains data stability and immutability. It is not only limited to the proper handling of personal data such as names, addresses, credit card numbers, and social security numbers but also other valuable data such as financial data, personal health information, and intellectual property. It can be applied to the data of individuals and organizations [2, 3].

Machine learning (ML) plays an important role for increasing productivity [4-6]. ML is increasingly used in many domains, such as healthcare [7], bioinformatics [8], agriculture [7], finance [9], manufacturing [9], natural language processing [10], and computer vision [11]. For ML to achieve effective results, the quality

Corresponding Author: ahmad@zu.edu.eg

of training data should be excellent, which depends on data size and data correctness. Large-scale datasets and perfect data has vastly improved and achieved excellent ML performance [12]. In order to obtain such excellent-quality data, many organizations work cooperatively, so privacy must be preserved.

Although ML achieves a great success rate, it can not be used in all domains due to its challenges [13, 14]. In such domains, the participants are more worried about the privacy of data as the data is stored and analyzed on the centralized server [15]. Federated learning (FL) represents the recent development in artificial intelligence. FL overcomes the ML challenges by applying the concept of decentralized data which in turn achieving and preserving the privacy of data.

In 2016, FL was initially presented by Google [16, 17]. FL is a decentralized method of ML. It works by enabling different devices or machines to train and learn a collaborative model without disclosing data with the centralized server [18]. It can be used in many areas including cybersecurity, healthcare, vehicle communications, and mobile and wireless networking [19]. It allows continual learning on client devices and ensuring that client data does not leave their devices.

FL provides important benefits over traditional ML methods. Unlike classical ML, FL provides data privacy and security by remaining data localized and performing training process on the client machines, not the centralized server [20]. FL ensures privacy as the data is stored and trained locally on end user devices such as mobile device or edge computing [21]. It achieves hardware efficiency by utilizing less complex hardware, as it does not require one central server to train and analyze data [22]. It also offers data diversity by granting access to heterogeneous datasets and enables real-time continual learning as client data is used to constantly enhance FL models without requiring the combination of data for continual ML [23].

FL can address privacy issues, improve scalability, lower latency, and enhance reliability [24]. In this work, we provide a systematic review to address privacy-preserving approaches and its importance to maintain and protect the data of users and organizations. We also identify FL concept along with its techniques that can be used to ensure data privacy. We systematically determine existing studies addressing privacy-preserving FL methods for malicious behavior detection. The contributions can be summarized as:

1. Identify the concept of privacy-preserving along with its importance, and applications.
2. Point out the privacy-preserving ML approaches.
3. Identify the foundations of FL and its motivations.
4. Identify the role of FL in preserving privacy.
5. Identify the applications of FL especially for preserving privacy.
6. Determine the most relevant techniques of FL used for achieving data privacy.

The rest of this study is organized as follows. Background of privacy preservation and FL are presented in Section 2. Section 3 contains related wok. Section 4 includes research methodology. Section 5 presents results. Conclusion is discussed in Section 6.

2 | Background

2.1 | Privacy Preservation

Due to the internet-centric world, the data privacy plays an important role in our life than ever before. It is critical to protect data such as users' accounts and assets from attackers. ML has a crucial role to our day-to-day existence. It is increasingly used in many applications from various domains starting from the detection of malware to new movies recommendation [25]. Some of these applications require sensitive personals' or organizations' data.

In traditional ML, the data is stored and trained on a centralized server. Centralized ML models require the data of individuals or organizations including sensitive data to be uploaded to the server in plaintext or clear format to extract patterns and build ML models, increasing the privacy and security risks [26, 27]. The performance of ML depends on two requirements. Such requirements are the training data volume and the computational resources [28-30].

In order to achieve excellent and acceptable results of ML, a significant amount of training data and powerful computer capabilities must be used for producing high privacy issues due to the possible threats, risks and dangers of private data leaks. ML models are also threatened by adversarial attacks including attacks that can infer properties, attributes, or membership [31]. Many ML applications require data from multiple input parties. The data is stored on the central server for being trained and tested.

There is a growing need for utilizing privacy preservation methods for ML data to achieve the privacy of data. Figure 1 shows different privacy-preserving approaches. Cryptographic approaches and perturbation techniques or differentiallyprivate data release represent the main privacy-preserving ML techniques [25].

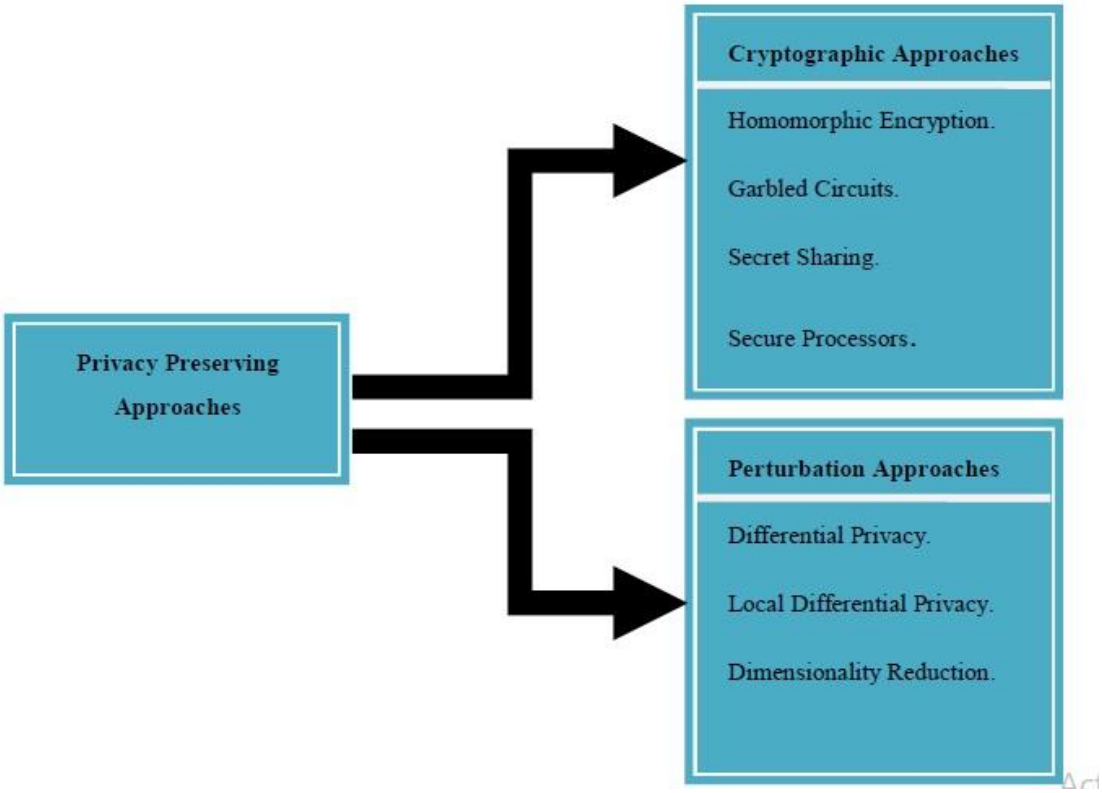

Figure 1. Privacy-preserving ML approaches.

Cryptographic approaches concentrate on performing ML training and testing on encrypted data. By utilizing these approaches, the data is stored on the central server in an encrypted form for being trained and tested. The Input parties don't have to stay online. The most popular privacy-preserving cryptographic methods include secure processors, secret sharing, garbled circuits, and homomorphic encryption (HE). [25].

HE is an approach in which the computations can be carried out on encrypted data [32]. It allows any third party to operate on the ciphertext data without needing to decrypt it in advance [33]. The encrypted result when decrypted to its original form matches the computation result carried on the clear or plaintext data [34-36]. The public key encryption technique (RSA) developed by Rivest, Shamir, and Adleman [37] is the first public-key encryption scheme applying HE property. RSA supports only multiplication operations. Goldwasser-Macali(GM) [38, 39] and Paillier [40] represent other types of of HE.

The three main types of HE are fully HE (FHE), somewhat HE (SHE), and Partially HE (PHE) [33]. PHE can support either multiplication or addition, SHE permits both operations of addition and multiplication but for a limited number, and FHE is the most flexible type of encryption since it permits infinite operations on encrypted data [33, 41-43]. There are many studies addressing privacy preservation using HE such as [44-47].

In the 1980s, Yao developed the garbled circuit [48]. This generic method is employed to protect two-party computation for participants who are not entirely dishonest. [49]. It can be combined with HE by some ML privacy-preserving approaches such as [50]. There are multiple studies utilizing garbled circuit such as [51-53].

Secret Sharing is one of cryptographic approaches used for achieving privacy preservation. This technique is used to distribute a secret between multiple parties. Every participating party holds a "share" of the distributing secret. When the shares are merged, the secret can be rebuilt, but individual shares are useless on their own[25]. In case of using secret sharing with threshold, there is no need for all the "shares" to reconstruct the secret [54, 55]. There are various studies utilizing secret sharing such as [56-58].

Secure processor is another type of cryptographic method used to achieve data privacy. The main idea behind this method is to collaborate multiple data owners to perform ML tasks using SGX-enabled data center. An adversary cannot control The computation-related SGX-processors [25]. [59, 60] utilize secure processor.

Perturbation Approaches include differential privacy (DP), local differential privacy (LDP) and dimensionality reduction (DP) techniques. DP is an important technique for data privacy. It was first proposed by [61]. It is useful and can be applied in many applications due to several properties such as composability, the ability to deal with large datasets, group privacy, and the Robustness of side information.

In order to safeguard data with no significant alteration, DP involves adding random noise to collected data. Laplace and Gaussian are common noise distributions that have varying effects on data utility and privacy [62]. The attacker cannot benefit from the acquired personal data because it is useless and does not include the person's record from the dataset. [63-65] address privacy preservation using DP.

LDP is considered as strong tool for privacy. In recent years, it has been widely adopted and applied in the real world by several organizations, including Google, Apple and Microsoft [66]. It provides much stronger data privacy protection by enabling users to locally perturb their own data without the need for the third trusted party. [67, 68] utilize LDP.

DR is a technique used for privacy preservation. It was proposed by [69]. In order to achieve data privacy, the data is perturbed by transferring it to a hyperplane of lesser dimensions. It applies lossy transformation. In such transformations, it is impossible to retrieve the exact original data from the reduced dimension data version, so it enhances privacy [25]. [70-72] utilize DR.

Privacy-preserving ML is increasingly being used in many areas. It can be used for cloud computing, Internet of Things (IoT), healthcare, and intrusion detection. [73-77] address privacy-preserving ML in cloud computing. [78-82] discuss privacy-preserving ML in IoT. [83-85] address privacy preservation in healthcare. [86] address privacy-preserving ML in electric vehicles. [87-89] address privacy-preserving ML for intrusion detection.

2.2| Federated Learning

Google proposed the concept of FL for the first time in 2016 [16, 17, 90]. The main idea is to build decentralized models of ML. Instead of storing data on a single large server, a dataset is distributed across different devices, which in turn prevents data leakage and maintains data privacy [91, 92]. The FL process is iterative, and with each iteration, the global model on the server—the basic machine learning model—is

enhanced. Figure 2 depicts FL diagram. In general, FL is composed of three major general steps, model selection, local training, and local models aggregation [93].

In model selection step, global model which represents centralized ML model is distributed to every client. To enhance efficiency, the global model can be pretrained with initial parameters on the central server before sharing with clients [94, 95]. In local training step, the global model is then trained locally at each client participating on FL process using its own individual data [96]. In local models aggregation step, the model updates are transmitted to the server to perform aggregation after local training step [97]. The global model is then updated by using the updated parameters and distributed to all the clients for starting a new iteration.

One of the essential properties of FL is privacy. Secure Multiparty Computation (SMC), DP, and HE are the privacy techniques used for FL [98]. SMC includes multiple parties; only its input and output are known to each party. With SMC, several parties can calculate a function using their inputs while preserving the privacy of those inputs [99]. In order to guarantee complete zero knowledge, it provides security proof by using well-defined simulation. [100, 101] adopt SMC with FL.

DP is the most used method because of its robust information theoretic guarantees, ease of usage in algorithms, and comparatively little system overhead [102]. DP is a nature approach used to prevent the data leakage using the addition of artificial noises. The challenge is how to choose the appropriate level of noise which will influence the FL process convergence rate and the privacy guarantee of clients [103]. [104-107] adopt DP along with FL.

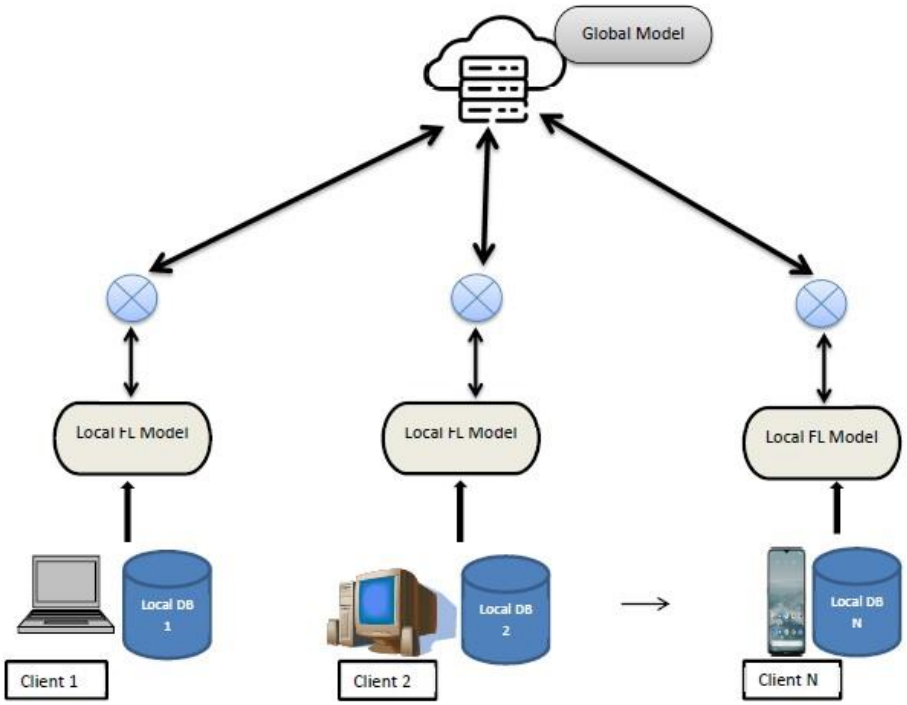

Figure 2. FL diagram.

The concept of HE is proposed by [108] for bank applications. Applying ML while exchanging parameters under the encryption method can help preserve the privacy of user data. There is little possibility of the data leakage as both the model and the data are not sent. [109-112] adopt HE along with FL.

There are three types of FL: federated transfer learning, vertical FL, and horizontal FL [98]. In horizontal FL, the data may have comparable feature spaces but differ greatly in sample spaces. The feature dimension of the data is the same. One illustration of horizontal FL is the federated model for Android smartphones [16].

If the data is divided vertically based on feature dimensions, vertical FL is appropriate. The data differs in feature space. The SecureBoost framework [113] is an illustration of vertical FL. The data in federated transfer learning does not share feature space or sample space. Thus, the major challenge in this scenario is the data labels lack with poor data quality. In this architecture, the knowledge can be moved from one domain to another domain to produce better learning results [114]. [18, 98, 115, 116] address the categorization of FL.

FL is used in many applications. It can be used in industry engineering or computer science applications [115]. Mobile devices applications, Wireless communication, healthcare applications, and industrial engineering applications are some of FL applications. FL can also be used for querying multiparty database without exposing the data. [98, 115] address the applications of FL. [117, 118] represent mobile devices FL applications. [119, 120] represent FL applications in wireless communication. [121, 122] are examples of FL applications in industrial engineering. [123, 124] are examples of FL applications in healthcare.

3 | Related Work

This section addresses the most related studies to privacy-preserving FL for intrusion detection. Table 1 lists the related studies along with their publication year, type, and source. The related studies include journals' and conferences' reviews, systematics, and surveys since 2016 in computer science research area. The search process is done in June 2022. The search is performed on three digital libraries; IEEE Xplorer, Web of Science, and Scopus. Each library has its own search query. Table 2 shows search term strings per database.

According to Table 1, there are ten studies talking about privacy-preserving FL in general, nine studies concentrate on IoT domain, two studies on the communication domain, and two other studies on the medicine domain.

3.1 | Generic Domain

The first ten studies in Table 1 are on general domain. The authors of [125] proposed a survey on DP mechanisms designed to ensure the privacy of users in the field of deep learning and FL. Their analysis is based on three factors; accuracy, communication cost, and computational complexity. The analysis demonstrated the gap in DP between accuracy, robustness, theory, and implementation. The analysis also resulted in many future directions to track privacy leaks while achieving a high accuracy.

Table 1. Related work studies.

Paper	Year	Type	Publisher
[126]	2022	C	IEEE
[127]	2021	C	IEEE
[128]	2022	J	IEEE
[129]	2022	J	IEEE
[130]	2021	J	IEEE
[131]	2022	J	IEEE
[132]	2021	J	IEEE
[133]	2020	J	IEEE
[125]	2022	J	IEEE
[134]	2021	J	IEEE
[135]	2017	C	IEEE
[136]	2021	C	IEEE
[137]	2021	J	IEEE
[138]	2021	J	IEEE

[139]	2020	J	IEEE
[140]	2022	J	IEEE
[141]	2019	J	IEEE
[142]	2020	J	IEEE
[143]	2022	J	Elsevier
[144]	2021	J	IEEE
[145]	2020	J	IEEE
[146]	2022	J	Wiley Online Library
[147]	2022	J	IEEE

Table 2. Related work search query per database.

Database	Query
IEEE Xplorer	(("Abstract":Privacy preserving) OR ("Abstract":Data Privacy)) AND (("Full Text Only":Malware Detection) OR ("Full Text Only":Intrusion Detection) OR ("Full Text Only":Malicious Behavior Detection)) AND (("Abstract":Distributed ML) OR ("Abstract":Distributed Learning) OR ("Abstract":Federated Learning)) AND (("Document Title":review) OR ("Document Title":systematic) OR ("Document Title":"survey"))
WoS	((AB=(Privacy preserving) OR AB=(Data Privacy)) AND (AB=(Detection) OR AB=(Malware Detection) OR AB=(Intrusion Detection) OR AB=(Malicious Behavior Detection)) AND (AB=(Distributed ML) OR AB=(Distributed Learning) OR AB=(Federated Learning) OR AB=(Federated Machine Learning))) AND (TI=(review) OR TI=(systematic) OR TI=(survey))
Scopus	((ABS(Privacy preserving) OR ABS(Data Privacy)) AND (ABS(Detection) OR ABS(Malware Detection) OR ABS(Intrusion Detection) OR ABS(Malicious Behavior Detection)) AND (ABS(Distributed ML) OR ABS(Distributed Learning) OR ABS(Federated Learning) OR ABS(Federated Machine Learning))) AND (TITLE(review) OR TITLE(systematic) OR TITLE(survey))

The authors of [134] presented a survey on applications, challenges, and main design factors of FL technology. According to this survey, FL has four design aspects, four core challenges, and four application areas. FL architectures, aggregation, personalization strategies, and data partitioning are examples of design elements. Communication cost, privacy and heterogeneity of systems, and statistical are the challenges of FL. Healthcare, Industrial engineering, mobile devices, IoT, and edge devices are the areas of FL application.

3.2 | Internet of Things Domain

[135-143] concentrated on IoT domain. In [135], the authors investigated the challenges of privacy and security in IoT. The privacy and security concerns in IoT systems include IoT devise storage, IoT web interfaces, IoT network services, IoT cloud connectivity, IoT software updates, and Industrial IoT. For example, cross website scripting and SQL injection are the most important security threats in IoT systems that may affect web interfaces. The privacy concerns of IoT cloud connectivity includes two issues; secure communications and access rights for IoT-Cloud. They also presented existing approaches to preserve security privacy in IoT environment such as rigorous testing, disabling universal plug and play, and learning automata based solution, and distributed denial of service DDOS alert mechanisms.

The authors of [138] presented a comprehensive analysis on FL's application in IoT domain. They also illustrated the role of FL in many critical IoT services , including mobile crowdsensing, attack detection, localization, data offloading and caching, IoT privacy and security, and IoT data sharing. They also discussed the potential of FL in various IoT applications like smart transportation, smart healthcare, smart

cities, smart industry, and unmanned aerial vehicles. They also illustrated several challenges include FL security and privacy concerns, FL-IoT communication and learning convergence issues, FL resource management, FL deployment of AI functions on IoT sensors, and FLIoT standard specifications.

3.3 | Communication Domain

[144, 145] concentrated on communication domain. The authors of [145] proposed a review of the use of blockchain in 5G networks and beyond networks. They discussed the benefits of integrating blockchain into the 5G networks. They introduced the classification of blockchain applications for 5G networks. The taxonomy includes communication management, network management, computing management, and services. For example, the taxonomy for network management includes NFV , SDN, and network slicing. The taxonomy for computing management includes MEC, content caching, distributed computing, data storage, and cloud computing.

D2D, resource allocation, spectrum sharing, infrastructure sharing, and infrastructure management are all included in the communication management taxonomy. The taxonomy for privacy and security includes authentication, fraud management, identity as a service, data privacy, and access control. The taxonomy for services includes billing & payment, roaming, content distribution, and digital rights. They applied layered approach in order to categorize the applications of blockchain in 5G ecosystems. They gave an overview of the proof of concept and field tests for the use of blockchain in 5G network.

3.4 | Medicine Domain

[146, 147] concentrated on medicine domain. The authors of [104] proposed a comprehensive review for the role of FL in the detection of COVID-19. They used chest X-ray (CXR) data sets for image. They presented a simple model using FL for identifying COVID-19. In order to demonstrate FL applicability in tackling the research issues of healthcare domain, they also reviewed previously published FL applications for COVID-19 research area.

The authors of [147] provided guidance for implementing ML based medical systems and applications. They proposed a survey of practical and technical challenges for implementing ML based medical systems. They discussed existing regulations facing ML in medical domain. These regulations include safety, reliability, robustness, security, privacy, explainability, transparency, and nondiscrimination. they also provided solutions to overcome medical ML challenges. FL along with large and representative datasets is one of the solution approaches. The other solutions involve domain knowledge careful exploitation, algorithmic impact evaluations, and the use of models for comprehensive out-of-distribution testing and verification.

4 | Research Methodology

4.1| Objectives

Using centralized machine learning in extremely sensitive systems, like healthcare systems, financial systems, and industrial systems, threatens individuals' and organizations' data and makes it vulnerable to attacks. This study aims to identify the needs for data privacy and its importance by identifying the problems and threats targeting centralized/classical ML systems. Moreover, the study also identifies privacy-preserving techniques used to protect individuals or organizations' data from any unauthorized or illegal action.

To sum up, the following is a formulation of the study's goals:

- O1: Identify the problems and threats targeting individuals and organizations implementing centralized ML. (Identify the need for privacy preservation or data privacy)
- O2: Identify privacy-preserving techniques used to assure ML systems' security.
- O3: Identify privacy-preserving ML domains.

- O4: Identify the importance of FL for the privacy of data.
- O5: Identify FL techniques used for data privacy.
- O6: Identify privacy-preserving FL applications.

Table 3. Research questions, motivations, and relevant objectives.

N	Research Question	Main Motivation	Objectives
RQ1	What are problems and threats of classical ML?	This research question identifies the importance and the need for privacy preservation or data privacy.	O1
RQ2	What are existing approaches used for privacy preservation?	This research question gives an overview of current privacy-preserving methods.	O2
RQ3	What are privacy-preserving ML domains?	This research question gives an overview of current privacy-preserving domains.	O3
RQ4	What is the role of FL in preserving privacy?	This research question addresses the importance of FL for improving the privacy of data.	O4
RQ5	What are FL techniques used for preserving privacy?	This research question presents an overview of existing FL techniques used for data privacy.	O5
RQ6	What are privacy-preserving FL applications?	This research question addresses an overview of FL based applications used for privacy preservation.	O6

4.2 | Research Questions

The purpose of this work is to address and explain privacy-preserving techniques and how they can be adopted with FL for malicious behavior detection. Based on this purpose, research questions are formulated following the guidelines of [148]. There are six main research questions for this study. Research questions are provided in Table 3, along with the motivation behind them and any associated goals. The search term is intended to be simple and generic as possible. It is created using search terms categorized into three groups; privacy preserving, intrusion detection, and distributed learning. For retrieving relevant papers, the guidelines of [148] are followed. Search queries are performed on the following three adopted online databases:

- IEEE Xplorer.
- Scopus.
- Web of Science.

The search is conducted to include all papers published since 2016 on computer science research area. Table 4 represents search query for each database.

Table 4. Search term strings per database.

Database	Keyword Searches
IEEE Xplorer	(("Abstract":"Privacy preserving" OR "Abstract":"Data Privacy") AND ("Abstract":"Detection" OR "Abstract":"Malware Detection" OR "Abstract":"Intrusion Detection" OR "Abstract":"Malicious Behavior Detection") AND ("Abstract":"Distributed ML" OR "Abstract":"Distributed Learning" OR "Abstract":"Federated Learning" OR "Abstract":"Federated ML")) NOT ("Abstract":"review" OR "Abstract":"systematic" OR "Abstract":"survey")
Scopus	((ABS(Privacy preserving) OR ABS(Data Privacy)) AND (ABS(Detection) OR ABS(Malware Detection) OR ABS(Intrusion Detection) OR ABS(Malicious Behavior Detection)) AND (ABS(Distributed ML) OR ABS(Distributed Learning) OR ABS(Federated Learning) OR ABS(Federated ML))) AND NOT (ABS(review) OR ABS(systematic) OR ABS(survey))
Web of Science	((AB=(Privacy preserving) OR AB=(Data Privacy)) AND (AB=(Detection) OR AB=(Malware Detection) OR AB=(Intrusion Detection) OR AB=(Malicious Behavior Detection)) AND (AB=(Distributed ML) OR AB=(Distributed Learning) OR AB=(Federated Learning) OR AB=(Federated ML))) NOT (AB=(review) OR AB=(systematic) OR AB=(survey))

4.3 | Study Selection

In this study, two screening stages were applied to generate the set of retrieved papers using search queries on the three selected databases of Scopus, IEEE Xplorer, and Web of Science. First stage represents the screening of titles and abstracts. In this stage, the papers' titles and abstracts are examined to determine relevance. Second stage represents full text screening. In this stage, the papers' full text is checked to determine if they achieve the inclusion criteria specified in Table 5. The authors screen the list of all papers separately. Their decisions are exchanged. The conflicts are also addressed and solved.

Table 5. Inclusion criteria.

ID	Criteria
I1	Papers published since 2016.
I2	Journals and early access papers.
I3	Full-length and complete published papers.
I4	Papers written in english.
I5	Papers aimed at privacy-preserving ML methods for malicious behavior detection.
I6	Papers applying federated ML.
I7	Papers applying technology to enhance and improve privacy.
I8	Experimental results ensure privacy.

Table 6. Exclusion criteria.

ID	Criteria
E1	Papers applying only federated ML without editing or enhancing privacy.
E2	Papers with experimental results do not test privacy.
E3	Proceeding papers.
E4	Review papers.
E5	Survey papers.
E6	Systematic review papers.
E7	Tutorial papers and editorials.
E8	Books or book chapters.
E9	Conferences.
E10	Magazines.
E11	Incomplete published papers (papers without full text available).
E12	Non-english studies.

4.4 | Inclusion and Exclusion Criteria

The amount of papers produces by searches using specified search queries for the three selected databases; IEEE Xplore, Scopus, and Web of Science, is decreased by specifying and applying a set of criteria for both inclusion and exclusion. Only journals and early access papers are included in this study. All papers published since 2016 are included in the search. The starting year 2016 is adopted since FL is first introduced by google in 2016 [16, 17]. Only English written papers addressing privacy preservation and FL for malicious behavior detection are included. Table 5 lists all of the adopted inclusion criteria, whereas Table 6 lists all of the exclusion criteria.

4.5 | Data Extraction Process

In this study, the data extraction process is performed by following the guidelines of [116]. Table 7 represents the designed data extraction form. Each paper is formed by using its corresponding metadata like publication source and publication year. A set of necessary information is also extracted for analysis.

Table 7. Data extraction form.

ID	Data Extraction Item	Description	RQ
D1	Paper ID	First author name + year	
D2	Year	The publication year	
D3	Source	The publication source	
D4	Threads	ML threats and the importance of privacy preservation	RQ1
D5	Approaches	Privacy-preserving approaches	RQ2
D6	Domains	Privacy-preserving domains	RQ3
D7	Role	FL role in preserving privacy	RQ4
D8	Techniques	FL techniques	RQ5
D9	Applications	Privacy-preserving FL applications	RQ6

Table 8. Number of studies that each database returned.

Database	Search Results
IEEE Xplorer	34
Scopus	117
Web of Science	69
Total	220

4.6 | Data Synthesis

Table 7 illustrates the mapping of research questions to data extraction. RQ1 is mapped to data item D4 which represents ML threats. RQ2 is mapped to data item D5 which represents privacy-preserving approaches. RQ3 is mapped to data item D6 which represents privacy-preserving domains. RQ4 is mapped to data item D7 which represents the role of FL in preserving privacy. RQ5 is mapped to data item D8 which represents FL techniques. RQ6 is mapped to data item D9 which represents privacy-preserving FL applications.

5 | Results

5.1 | Overview of Selected Studies

The search process is carried out in June 2022. The process yields 32 unique publications that have been published since 2016. The set of chosen digital libraries—IEEE Xplorer, Scopus, and Web of Science—are subjected to the created search query. Table 8 shows the amount of retrived papers from every library after applying conditions.

The search process includes three conditions. The first condition represents published papers since 2016. The second condition represents published papers in computer science research area. The final condition represents only journals and early accesses. The mentioned conditions are used to eliminate the number of papers that the search engines have retrieved. The set of 220 returned publications from various search engines are collected. The duplicate publications are then eliminated. This brings the total number of papers down to 131. Only 32 papers are approved after checking the criteria of inclusion and exclusion. Figure 3 depicts the entire overall selection process.

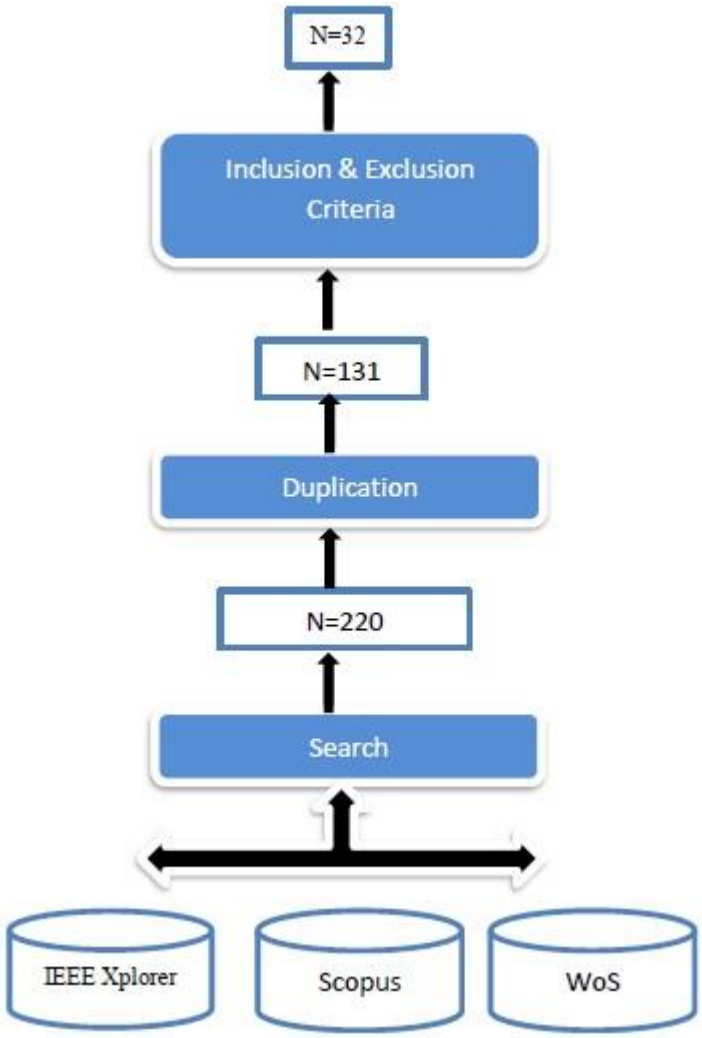

Figure 3. Selection process.

The distribution of chosen papers by source and year of publication is shown in Figure 4. As shown, the year of 2016, 2017, and 2019 has no publications matching the inclusion criteria. The interest into privacy-preserving FL starts getting more attentions since 2020. Scopus has the maximum number of publications matching the criteria of inclusion.

Table 9 displays the full list of chosen papers matching the inclusion criteria along with their corresponding year and publisher.

Table 9. List of selected studies

ID	Cite	Year	Publisher
P1	[149]	2022	Hindawi
P2	[150]	2022	Wiley Online Library
P3	[151]	2021	Elsevier
P4	[152]	2018	IEEE
P5	[153]	2020	IEEE
P6	[154]	2021	Hindawi
P7	[155]	2021	Wiley Online Library
P8	[156]	2022	Elsevier
P9	[157]	2021	IEEE
P10	[158]	2021	Elsevier
P11	[159]	2021	IEEE

P12	[160]	2020	IEEE
P13	[161]	2022	Elsevier
P14	[162]	2021	IEEE
P15	[51]	2020	IEEE
P16	[163]	2022	Elsevier
P17	[164]	2021	IEEE
P18	[165]	2021	Hindawi
P19	[166]	2020	IEEE
P20	[167]	2022	IEEE
P21	[168]	2022	IEEE
P22	[169]	2022	IEEE
P23	[109]	2021	IEEE
P24	[170]	2021	IEEE
P25	[171]	2022	IEEE
P26	[172]	2022	IEEE
P27	[173]	2021	IEEE
P28	[174]	2021	IEEE
P29	[111]	2021	IEEE
P30	[175]	2020	Taiwan Academic Network Management Committee
P31	[176]	2022	Multidisciplinary Digital Publishing Institute
P32	[177]	2021	IEEE

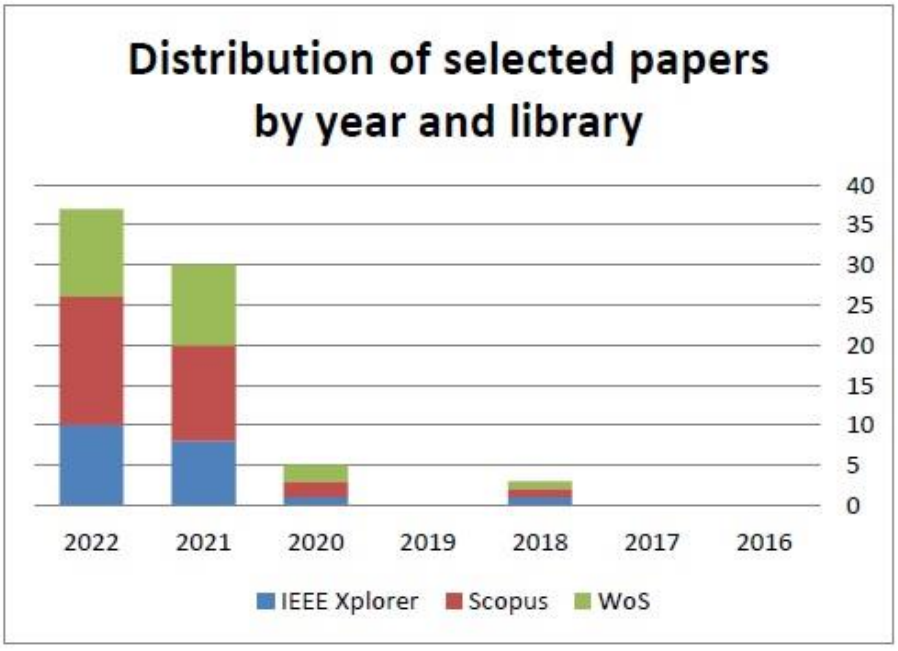

Figure 4. Distribution of selected papers by library and year.

5.2 | Importance of Privacy Preservation (RQ1)

For training model, Conventional ML techniques require the gathering and centralization of raw user data on servers, presenting serious privacy problems. Sensitive information is susceptible to misuse, data breaches, and illegal access as it must be uploaded to central servers. Furthermore, conventional ML systems

have the ability to inadvertently memorize and expose private information from their training data, which could reveal sensitive information about specific users. The demand for sophisticated privacy-preserving methods that can safeguard user data while facilitating efficient ML has been motivated by these privacy issues. Consequently, techniques like FL have been developed that enable training of models without requiring raw data to leave user devices.

5.3 | Privacy-Preserving Approaches (RQ2)

Privacy-preserving ML approaches have two main categories: cryptographic approaches and perturbation approaches. HE, secret sharing, garbled circuits, and secure processors represent cryptographic approaches while DP, LDP, and DR techniques represent perturbation approaches.

5.4 | Privacy-Preserving Domains (RQ3)

Privacy-preserving ML is increasingly being used in many areas. It can be used for cloud computing, IoT, healthcare, and intrusion detection.

5.5 | FL Role in Privacy Preservation (RQ4)

Classical ML depends on storing the users' or organizations' data on a centralized server for the purpose of model training and updating so its vulnerable to attacks not only by the server owners but also by any cyber attacks. FL is a new trend of ML which can overcome the problems of traditional ML and achieve the privacy of data. It implements traditional ML models with privacy features. Its a distributed ML models. Rather than traditional ML, FL doesn't require the data and ML model to be stored on a centralized server. The data will remain on its local users, and the model will be sent to the data. The core concept of FL is to deliver the model to the data rather than the other way around. so FL preserves privacy.

5.6 | FL Techniques for Privacy Preservation (RQ5)

SMC, DP, and HE are the most used FL privacy-preserving techniques. From our point of view, DP is the most used privacy-preserving FL technique for intrusion detection.

5.7 | Privacy-Preserving FL Applications (RQ6)

There are many applications for privacy-preserving FL, which are used in general domains, IoT domain, communication domain, medicine domain, mobile domain, and financial domain.

6 | Conclusion

This study provides a systematic review of privacy-preserving distributed ML for malicious behavior detection. search queries are performed on the three selected online databases of IEEE Xplorer, Scopus, and Web of Science. Each database has its corresponding search query. The search is performed to include all papers published since 2016 on computer science research area. The set of 220 returned papers from the various search engines are collected. After removing duplicated papers, the number of papers are reduced to 131. Only 32 papers are approved after checking the criteria of inclusion and exclusion. The interest into privacy-preserving FL starts getting more attentions since 2020 as there is no publications matching the inclusion criteria in 2016, 2017, and 2019.

Author Contribution

Conceptualization, E.S, W.K., E.R. and A.S.; Methodology, E.S, W.K., E.R. and A.S.; Software, E.S, W.K., E.R. and A.S.; Validation, E.S, W.K., E.R. and A.S.; formal analysis, E.S, W.K., E.R. and A.S.; investigation, E.S, W.K., E.R. and A.S.; resources, E.S, W.K., E.R. and A.S.; data maintenance, E.S, W.K., E.R. and A.S.; writing-creating the initial design, E.S, W.K., E.R. and A.S.; writing-reviewing and editing, E.S, W.K., E.R. and A.S.; visualization, E.S, W.K., E.R. and A.S.; monitoring, E.S, W.K., E.R. and A.S.; project

management, E.S, W.K., E.R. and A.S.; funding procurement, E.S, W.K., E.R. and A.S. Every author has read and approved the manuscript's published form.

Funding

This study has no funding source.

Data Availability

There is no data used in this study.

Conflicts of Interest

No conflicts of interest are disclosed by the authors.

References

[1] De Capitani Di Vimercati, S., S. Foresti, G. Livraga, and P. Samarati, Data privacy: definitions and techniques. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2012. **20**(06): p. 793-817.
[2] Martin, K.D. and P.E. Murphy, The role of data privacy in marketing. Journal of the Academy of Marketing Science, 2017. **45**(2): p. 135-155.
[3] Browne, P.S., Data privacy and integrity: an overview, in Proceedings of the 1971 ACM SIGFIDET (now SIGMOD) Workshop on Data Description, Access and Control. 1971. p. 237-240.
[4] Wardhani, R.S., K. Kant, A. Sreeram, M. Gupta, E. Erwandy, and P.K. Bora, Impact of Machine Learning on the Productivity of Employees in Workplace. 2022. p. 930-934.
[5] Negrei, B. and V.-F. Duma, Correlating machine vision and learning with robot handling in increasing productivity of airbags manufacturing. 2024.
[6] Umrao, S., S. Kumar, H. Gupta, and K. Saxena, Comparison of Machine Learning Techniques to Estimate Increase in Crop Productivity. 2023.
[7] Ghosh, S. and R. Dasgupta, Machine Learning and Life Sciences, in Machine Learning in Biological Sciences: Updates and Future Prospects. 2022, Springer. p. 89-102.
[8] Cannataro, M., P.H. Guzzi, G. Agapito, C. Zucco, and M. Milano, Machine learning. 2022, Elsevier BV. p. 11-27.
[9] Joshi, P.K., R. Prakash, and A.K. Rai, A Comprehensive Review of Machine Learning Application Across Different Domains. 2024. p. 1266-1270.
[10] Marella, S.T. and G.Y. Hong, An Application-Oriented Survey on the Adaptability of Artificial Intelligence for Natural Language Processing: A Survey, in 5G Internet of Things and Changing Standards for Computing and Electronic Systems. 2022, IGI Global. p. 172-181.
[11] Ranjana, R., B. Narendra Kumar Rao, J. Raja, N. Panini Challa, and K.R. Madhavi, Machine learning and computer vision-beyond modeling, training, and algorithms. 2023, IET.
[12] Flach, P., Performance evaluation in machine learning: the good, the bad, the ugly, and the way forward, in Proceedings of the AAAI Conference on Artificial Intelligence. 2019. p. 9808-9814.
[13] Baier, L., F. Jöhren, and S. Seebacher, Challenges in the Deployment and Operation of Machine Learning in Practice, in ECIS. 2019.
[14] Injadat, M., A. Moubayed, A.B. Nassif, and A. Shami, Machine learning towards intelligent systems: applications, challenges, and opportunities. Artificial Intelligence Review, 2021. **54**(5): p. 3299-3348.
[15] De Cristofaro, E., An overview of privacy in machine learning. arXiv preprint arXiv:2005. 08679, 2020.
[16] McMahan, B., E. Moore, D. Ramage, S. Hampson, and B.A. y Arcas, Communication-efficient learning of deep networks from decentralized data, in Artificial intelligence and statistics. 2017. p. 1273-1282.
[17] Konečn\`y, J., H.B. McMahan, D. Ramage, and P. Richtárik, Federated optimization: Distributed machine learning for on-device intelligence. arXiv preprint arXiv:1610. 02527, 2016.
[18] Zhang, C., Y. Xie, H. Bai, B. Yu, W. Li, and Y. Gao, A survey on federated learning. Knowledge-Based Systems, 2021. **216**: p. 106775.
[19] Shaheen, M., M.S. Farooq, T. Umer, and B.-S. Kim, Applications of federated learning; Taxonomy, challenges, and research trends. Electronics, 2022. **11**(4): p. 670.
[20] Garst, S., J. Dekker, and M. Reinders, A comprehensive experimental comparison between federated and centralized learning. bioRxiv, 2023: p. 2023-2007.
[21] Aminifar, A., M. Shokri, and A. Aminifar, Privacy-Preserving Edge Federated Learning for Intelligent Mobile-Health Systems. 2024.
[22] Bektemyssova, G. and G. Bakirova, Comparative analysis of federated machine learning algorithms. Scientific journal of Astana IT University, 2024.
[23] Sharma, S., Z. Hasan, and V. Paranjape, Optimizing Federated Learning Techniques for Advanced Decentralized AI Systems. International Journal of Innovative Research in Computer and Communication Engineering, 2023. **10**(08): p. 7721-7729.
[24] Schwanck, F.M., M.T. Leipnitz, J. Carbonera, and J. Wickboldt, A Framework for testing Federated Learning algorithms using an edge-like environment. arXiv. org, 2024. **abs/2407.12980**.
[25] Al-Rubaie, M. and J.M. Chang, Privacy-preserving machine learning: Threats and solutions. IEEE Security & Privacy, 2019. **17**(2): p. 49-58.

[26] Peng, S., Y. Yang, M. Mao, and D.-S. Park, Centralized Machine Learning Versus Federated Averaging: A Comparison using MNIST Dataset. Ksii Transactions on Internet and Information Systems, 2022. **16**(2): p. 742-756.
[27] Xu, Y., J. Zhang, and Y. Gu, Privacy-Preserving Heterogeneous Federated Learning for Sensitive Healthcare Data. 2024.
[28] Jain, A., G. Swaminathan, P. Favaro, H.-P. Yang, A. Ravichandran, H. Harutyunyan, A. Achille, O. Dabeer, B. Schiele, A. Swaminathan, and S. Soatto, A Meta-Learning Approach to Predicting Performance and Data Requirements. arXiv. org, 2023. **abs/2303.01598**.
[29] Selvan, R.A., J. Schön, and E.B. Dam, Operating critical machine learning models in resource constrained regimes. arXiv. org, 2023. **abs/2303.10181**.
[30] Faheem, S.M., M.I. Babar, R.A. Khalil, and N.A. Saeed, Performance Analysis of Selected Machine Learning Techniques for Estimating Resource Requirements of Virtual Network Functions (VNFs) in Software Defined Networks. Applied Sciences, 2022. **12**(9): p. 4576-4576.
[31] Xu, R., N. Baracaldo, and J. Joshi, Privacy-preserving machine learning: Methods, challenges and directions. arXiv preprint arXiv:2108. 04417, 2021.
[32] Yi, X., R. Paulet, and E. Bertino, Homomorphic encryption, in Homomorphic encryption and applications. 2014, Springer. p. 27-46.
[33] Singh, V.K., A.S. Chauhan, A. Singh, and R. Thakur, Homomorphic Encryption: Hands Inside the Gloves. 2023. p. 248-253.
[34] Knight, E., I. Yolou, J. Li, C. Koçkan, M.R. Jensen, and M. Gerstein, Homomorphic Encryption: An Application to Polygenic Risk Scores. 2024.
[35] Wang, W., C. Li, and S. Li, Multi-key Homomorphic Encryption Algorithm Based on Fuzzy Clustering. 2023. p. 436-440.
[36] Rajashree, S., B. Vineetha, A.B. Mehta, and P.B. Honnavalli, Homomorphic Encryption Approach for String Concatenation. 2022. p. 267-272.
[37] Rivest, R.L., A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978. **21**(2): p. 120-126.
[38] Goldwasser, S. and S. Micali, Probabilistic encryption & how to play mental poker keeping secret all partial information, in Providing sound foundations for cryptography: on the work of Shafi Goldwasser and Silvio Micali. 2019. p. 173-201.
[39] ElGamal, T., A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE transactions on information theory, 1985. **31**(4): p. 469-472.
[40] Paillier, P., Public-key cryptosystems based on composite degree residuosity classes, in International conference on the theory and applications of cryptographic techniques. 1999. p. 223-238.
[41] Jain, N. and A.K. Cherukuri, Revisiting Fully Homomorphic Encryption Schemes. arXiv preprint arXiv:2305.05904, 2023.
[42] Zhang, J., X. Cheng, L. Yang, J. Hu, X. Liu, and K. Chen, SoK: Fully Homomorphic Encryption Accelerators. ACM Computing Surveys, 2024.
[43] Kamble, A., M.M. Jiet, and C. Puri, Homomorphic Encryption and its Applications in Multi-Cloud Security. 2024.
[44] Lee, J.-W., H. Kang, Y. Lee, W. Choi, J. Eom, M. Deryabin, E. Lee, J. Lee, D. Yoo, Y.-S. Kim, and Others, Privacy-preserving machine learning with fully homomorphic encryption for deep neural network. IEEE Access, 2022. **10**: p. 30039-30054.
[45] Giacomelli, I., S. Jha, M. Joye, C.D. Page, and K. Yoon, Privacy-preserving ridge regression with only linearly-homomorphic encryption, in International conference on applied cryptography and network security. 2018. p. 243-261.
[46] Aono, Y., T. Hayashi, L. Wang, S. Moriai, and Others, Privacy-preserving deep learning via additively homomorphic encryption. IEEE Transactions on Information Forensics and Security, 2017. **13**(5): p. 1333-1345.
[47] Yousif, H.M. and S.M. Hameed, Preserving Genotype Privacy Using AES and Partially Homomorphic Encryption. Iraqi journal of science, 2024: p. 1663-1678.
[48] Bellare, M., V.T. Hoang, and P. Rogaway, Foundations of garbled circuits, in Proceedings of the 2012 ACM conference on Computer and communications security. 2012. p. 784-796.
[49] Huang, Y., D. Evans, J. Katz, and L. Malka, Faster Secure ${$Two-Party$}$ Computation Using Garbled Circuits, in 20th USENIX Security Symposium (USENIX Security 11). 2011.
[50] Li, L., A. Liu, Q. Li, G. Liu, and Z. Li, Privacy-preserving collaborative Web services QoS prediction via YAO's garbled circuits and homomorphic encryption. Journal of Web Engineering, 2016: p. 203-225.
[51] Raja, G., S. Anbalagan, G. Vijayaraghavan, S. Theerthagiri, S.V. Suryanarayan, and X.-W. Wu, SP-CIDS: Secure and private collaborative IDS for VANETs. IEEE Transactions on Intelligent Transportation Systems, 2020. **22**(7): p. 4385-4393.
[52] Hussain, S.U., B. Li, F. Koushanfar, and R. Cammarota, TinyGarble2: Smart, Efficient, and Scalable Yao's Garble Circuit. 2020, ACM. p. 65-67.
[53] Hashemi, M., S. Roy, F. Ganji, and D. Forte, Garbled EDA: Privacy Preserving Electronic Design Automation. 2022. p. 1-9.
[54] Silva, D., L. Harmon, and G. Delavignette, Threshold secret sharing with geometric algebras. Mathematical Methods in the Applied Sciences, 2024. **47**(3): p. 1318-1330.
[55] Hueca, A., S. Mudd, and T. Shimeall, Introduction to the Special Issue on Information Sharing. 2024. **4**: p. 1-2.
[56] Huo, X. and M.-X. Liu, A Secret-Sharing Based Privacy-Preserving Distributed Energy Resource Control Framework. 2022. p. 963-966.
[57] Liang, J., H. Peng, and L. Li. A Privacy-Preserving Scheme by Combining Compressed Sensing and Secret Sharing in Cloud Environment. Springer.
[58] Zhang, Y., Z. Duo, J. Cai, and X.W. Zhao, Threshold Secret Sharing and Symmetric Encryption Algorithm-Based Hybrid Protection Framework for Enterprise Privacy. 2022. p. 357-364.
[59] Jie, Y., Y. Ren, Q. Wang, Y. Xie, C. Zhang, L. Wei, and J. Liu, Multi-Party Secure Computation with Intel SGX for Graph Neural Networks. 2022: p. 528-533.
[60] Widanage, C., W. Liu, J. Li, H. Chen, X. Wang, H. Tang, and J. Fox, HySec-Flow: Privacy-Preserving Genomic Computing with SGX-based Big-Data Analytics Framework. 2021, IEEE Computer Society. p. 733-743.
[61] Dwork, C., Differential privacy: A survey of results, in International conference on theory and applications of models of computation. 2008. p. 1-19.
[62] Yogi, M.K. and A.S.N. Chakravarthy, Impact of noise customization in differential privacy for cyber physical systems. 2024. p. 68-77.

[63] Owusu-Agyemeng, K., Z. Qin, H. Xiong, Y. Liu, T. Zhuang, and Z. Qin, MSDP: multi-scheme privacy-preserving deep learning via differential privacy. Personal and Ubiquitous Computing, 2021: p. 1-13.
[64] Phan, N., X. Wu, H. Hu, and D. Dou, Adaptive laplace mechanism: Differential privacy preservation in deep learning, in 2017 IEEE international conference on data mining (ICDM). 2017. p. 385-394.
[65] Abadi, M., A. Chu, I. Goodfellow, H.B. McMahan, I. Mironov, K. Talwar, and L. Zhang, Deep learning with differential privacy, in Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. 2016. p. 308-318.
[66] Cormode, G., S. Jha, T. Kulkarni, N. Li, D. Srivastava, and T. Wang, Privacy at scale: Local differential privacy in practice, in Proceedings of the 2018 International Conference on Management of Data. 2018. p. 1655-1658.
[67] Arachchige, P.C.M., P. Bertok, I. Khalil, D. Liu, S. Camtepe, and M. Atiquzzaman, Local differential privacy for deep learning. IEEE Internet of Things Journal, 2019. **7**(7): p. 5827-5842.
[68] Yang, M., L. Lyu, J. Zhao, T. Zhu, and K.-Y. Lam, Local differential privacy and its applications: A comprehensive survey. arXiv preprint arXiv:2008. 03686, 2020.
[69] Liu, K., H. Kargupta, and J. Ryan, Random projection-based multiplicative data perturbation for privacy preserving distributed data mining. IEEE Transactions on knowledge and Data Engineering, 2005. **18**(1): p. 92-106.
[70] Chen, Z. and K. Omote, A Privacy Preserving Scheme with Dimensionality Reduction for Distributed Machine Learning. 2021, IEEE. p. 45-50.
[71] Dervishi, L., W. Li, A. Halimi, X. Jiang, J. Vaidya, and E. Ayday, Privacy preserving identification of population stratification for collaborative genomic research. Bioinformatics, 2023. **39**(Supplement_1): p. i168-i176.
[72] El Ouadrhiri, A., A. Abdelhadi, and P.H. Phung. Hensel's Compression-Based Dimensionality Reduction Approach for Privacy Protection in Federated Learning. IEEE.
[73] Hesamifard, E., H. Takabi, M. Ghasemi, and C. Jones, Privacy-preserving machine learning in cloud, in Proceedings of the 2017 on cloud computing security workshop. 2017. p. 39-43.
[74] Gupta, R. and A.K. Singh, A Differential Approach for Data and Classification Service-Based Privacy-Preserving Machine Learning Model in Cloud Environment. New Generation Computing, 2022: p. 1-28.
[75] Li, P., J. Li, Z. Huang, T. Li, C.-Z. Gao, S.-M. Yiu, and K. Chen, Multi-key privacy-preserving deep learning in cloud computing. Future Generation Computer Systems, 2017. **74**: p. 76-85.
[76] Liu, L., R. Chen, X. Liu, J. Su, and L. Qiao, Towards practical privacy-preserving decision tree training and evaluation in the cloud. IEEE Transactions on Information Forensics and Security, 2020. **15**: p. 2914-2929.
[77] Jiang, Y., K. Zhang, Y. Qian, and R.Q. Hu, Efficient and Privacy-preserving Distributed Learning in Cloud-Edge Computing Systems, in Proceedings of the 3rd ACM Workshop on Wireless Security and Machine Learning. 2021. p. 25-30.
[78] Zhu, L., X. Tang, M. Shen, F. Gao, J. Zhang, and X. Du, Privacy-preserving machine learning training in IoT aggregation scenarios. IEEE Internet of Things Journal, 2021. **8**(15): p. 12106-12118.
[79] Singh, S., S. Rathore, O. Alfarraj, A. Tolba, and B. Yoon, A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. Future Generation Computer Systems, 2022. **129**: p. 380-388.
[80] Zheng, M., D. Xu, L. Jiang, C. Gu, R. Tan, and P. Cheng, Challenges of privacy-preserving machine learning in IoT, in Proceedings of the First International Workshop on Challenges in Artificial Intelligence and Machine Learning for Internet of Things. 2019. p. 1-7.
[81] Arachchige, P.C.M., P. Bertok, I. Khalil, D. Liu, S. Camtepe, and M. Atiquzzaman, A trustworthy privacy preserving framework for machine learning in industrial IoT systems. IEEE Transactions on Industrial Informatics, 2020. **16**(9): p. 6092-6102.
[82] Briggs, C., Z. Fan, and P. Andras, A review of privacy-preserving federated learning for the Internet-of-Things. Federated Learning Systems, 2021: p. 21-50.
[83] Aminifar, A., M. Shokri, F. Rabbi, V.K.I. Pun, and Y. Lamo, Extremely Randomized Trees With Privacy Preservation for Distributed Structured Health Data. IEEE Access, 2022. **10**: p. 6010-6027.
[84] Aminifar, A., Privacy-Preserving Machine Learning and Data Sharing in Healthcare Applications. 2022.
[85] Kaissis, G.A., M.R. Makowski, D. Rückert, and R.F. Braren, Secure, privacy-preserving and federated machine learning in medical imaging. Nature Machine Intelligence, 2020. **2**(6): p. 305-311.
[86] Sani, A.R., M.U. Hassan, and J. Chen, Privacy Preserving Machine Learning for Electric Vehicles: A Survey. arXiv preprint arXiv:2205. 08462, 2022.
[87] Ravikanth, R. and T.P. Jacob, Implementation of Robust Privacy-Preserving Machine Learning with Intrusion Detection and Cybersecurity Protection Mechanism, in A Fusion of Artificial Intelligence and Internet of Things for Emerging Cyber Systems. 2022, Springer. p. 183-201.
[88] Novikova, E., E. Doynikova, and S. Golubev, Federated Learning for Intrusion Detection in the Critical Infrastructures: Vertically Partitioned Data Use Case. Algorithms, 2022. **15**(4): p. 104.
[89] Vanathi, D., S. Prabhadevi, P. Sabarishamalathi, P.G. Scholar, and I.M. Kp, Machine Learning Based Collaborative Privacy-Preserving Intrusion Detection System for VANETs.
[90] Konečn\`y, J., H.B. McMahan, F.X. Yu, P. Richtárik, A.T. Suresh, and D. Bacon, Federated learning: Strategies for improving communication efficiency. arXiv preprint arXiv:1610. 05492, 2016.
[91] Ma, J., L. Chen, J. Xu, and Y. Yuan, FedCrow: Federated-Learning-Based Data Privacy Preservation in Crowd Sensing. Applied Sciences, 2024. **14**(11): p. 4788-4788.
[92] Akter, M. and N. Moustafa, Federated Learning-Based Privacy Protection Methods for Internet of Things Systems. 2024.
[93] Alazab, M., S.P. Rm, M. Parimala, P.K.R. Maddikunta, T.R. Gadekallu, and Q.-V. Pham, Federated Learning for Cybersecurity: Concepts, Challenges, and Future Directions. IEEE Transactions on Industrial Informatics, 2021. **18**(5): p. 3501-3509.
[94] Ge, B., Y. Zhou, L. Xie, and L.T. Kou, Pre-Training Model and Client Selection Optimization for Improving Federated Learning Efficiency. 2024.
[95] Wang, Z., Y. Zhou, Y. Shi, and K.B. Letaief, Federated Fine-Tuning for Pre-Trained Foundation Models Over Wireless Networks. 2024.
[96] Kim, D.S., S. Ahmad, and T.K. Whangbo, Federated regressive learning: Adaptive weight updates through statistical information of clients. Applied Soft Computing, 2024: p. 112043-112043.

[97] Pękala, B., A. Wilbik, J. Szkoła, K. Dyczkowski, and P. Żywica, Federated Learning with the Choquet Integral as Aggregation Method. 2024: p. 1-8.
[98] Yang, Q., Y. Liu, T. Chen, and Y. Tong, Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology (TIST), 2019. **10**(2): p. 1-19.
[99] Seo, M., Fair and secure multi-party computation with cheater detection. Cryptography, 2021. **5**(3): p. 19.
[100] Hernandez, R., O.G. Bautista, M.H. Manshaei, A. Sahin, and K. Akkaya, Outsourcing Privacy-Preserving Federated Learning on Malicious Networks through MPC. 2023.
[101] Piotrowski, T. and Z. Nochta, Towards a Secure Peer-to-Peer Federated Learning Framework. 2022. p. 19-31.
[102] Li, T., A.K. Sahu, A. Talwalkar, and V. Smith, Federated learning: Challenges, methods, and future directions. IEEE Signal Processing Magazine, 2020. **37**(3): p. 50-60.
[103] Wei, K., J. Li, M. Ding, C. Ma, H.H. Yang, F. Farokhi, S. Jin, T.Q.S. Quek, and H.V. Poor, Federated learning with differential privacy: Algorithms and performance analysis. IEEE Transactions on Information Forensics and Security, 2020. **15**: p. 3454-3469.
[104] Truex, S., L. Liu, K.-H. Chow, M.E. Gursoy, and W. Wei, LDP-Fed: Federated learning with local differential privacy, in Proceedings of the Third ACM International Workshop on Edge Systems, Analytics and Networking. 2020. p. 61-66.
[105] Wu, X., Y. Zhang, M. Shi, P. Li, R. Li, and N.N. Xiong, An adaptive federated learning scheme with differential privacy preserving. Future Generation Computer Systems, 2022. **127**: p. 362-372.
[106] Choudhury, O., A. Gkoulalas-Divanis, T. Salonidis, I. Sylla, Y. Park, G. Hsu, and A. Das, Differential privacy-enabled federated learning for sensitive health data. arXiv preprint arXiv:1910. 02578, 2019.
[107] Adnan, M., S. Kalra, J.C. Cresswell, G.W. Taylor, and H.R. Tizhoosh, Federated learning and differential privacy for medical image analysis. Scientific reports, 2022. **12**(1): p. 1-10.
[108] Rivest, R.L., L. Adleman, M.L. Dertouzos, and Others, On data banks and privacy homomorphisms. Foundations of secure computation, 1978. **4**(11): p. 169-180.
[109] Wen, M., R. Xie, K. Lu, L. Wang, and K. Zhang, Feddetect: A novel privacy-preserving federated learning framework for energy theft detection in smart grid. IEEE Internet of Things Journal, 2021. **9**(8): p. 6069-6080.
[110] Ou, W., J. Zeng, Z. Guo, W. Yan, D. Liu, and S. Fuentes, A homomorphic-encryption-based vertical federated learning scheme for rick management. Computer Science and Information Systems, 2020. **17**(3): p. 819-834.
[111] Hou, J., M. Su, A. Fu, and Y. Yu, Verifiable privacy-preserving scheme based on vertical federated random forest. IEEE Internet of Things Journal, 2021.
[112] Zhang, L., J. Xu, P. Vijayakumar, P.K. Sharma, and U. Ghosh, Homomorphic Encryption-based Privacy-preserving Federated Learning in IoT-enabled Healthcare System. IEEE Transactions on Network Science and Engineering, 2022.
[113] Cheng, K., T. Fan, Y. Jin, Y. Liu, T. Chen, D. Papadopoulos, and Q. Yang, Secureboost: A lossless federated learning framework. IEEE Intelligent Systems, 2021. **36**(6): p. 87-98.
[114] Pan, S.J., X. Ni, J.-T. Sun, Q. Yang, and Z. Chen, Cross-domain sentiment classification via spectral feature alignment, in Proceedings of the 19th international conference on World wide web. 2010. p. 751-760.
[115] Li, L., Y. Fan, M. Tse, and K.-Y. Lin, A review of applications in federated learning. Computers & Industrial Engineering, 2020. **149**: p. 106854.
[116] Aledhari, M., R. Razzak, R.M. Parizi, and F. Saeed, Federated learning: A survey on enabling technologies, protocols, and applications. IEEE Access, 2020. **8**: p. 140699-140725.
[117] Qian, Y., L. Hu, J. Chen, X. Guan, M.M. Hassan, and A. Alelaiwi, Privacy-aware service placement for mobile edge computing via federated learning. Information Sciences, 2019. **505**: p. 562-570.
[118] Feng, J., C. Rong, F. Sun, D. Guo, and Y. Li, PMF: A privacy-preserving human mobility prediction framework via federated learning. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2020. **4**(1): p. 1-21.
[119] Tran, H.-V., G. Kaddoum, H. Elgala, C. Abou-Rjeily, and H. Kaushal, Lightwave power transfer for federated learning-based wireless networks. IEEE Communications Letters, 2020. **24**(7): p. 1472-1476.
[120] Ang, F., L. Chen, N. Zhao, Y. Chen, W. Wang, and F.R. Yu, Robust federated learning with noisy communication. IEEE Transactions on Communications, 2020. **68**(6): p. 3452-3464.
[121] Saputra, Y.M., D.T. Hoang, D.N. Nguyen, E. Dutkiewicz, M.D. Mueck, and S. Srikanteswara, Energy demand prediction with federated learning for electric vehicle networks, in 2019 IEEE Global Communications Conference (GLOBECOM). 2019. p. 1-6.
[122] Yang, W., Y. Zhang, K. Ye, L. Li, and C.-Z. Xu, Ffd: A federated learning based method for credit card fraud detection, in International conference on big data. 2019. p. 18-32.
[123] Lee, J., J. Sun, F. Wang, S. Wang, C.-H. Jun, X. Jiang, and Others, Privacy-preserving patient similarity learning in a federated environment: development and analysis. JMIR medical informatics, 2018. **6**(2): p. e7744.
[124] Huang, L., A.L. Shea, H. Qian, A. Masurkar, H. Deng, and D. Liu, Patient clustering improves efficiency of federated machine learning to predict mortality and hospital stay time using distributed electronic medical records. Journal of biomedical informatics, 2019. **99**: p. 103291.
[125] El Ouadrhiri, A. and A. Abdelhadi, Differential privacy for deep and federated learning: A survey. IEEE Access, 2022. **10**: p. 22359-22380.
[126] Sah, M.P. and A. Singh, Aggregation Techniques in Federated Learning: Comprehensive Survey, Challenges and Opportunities, in 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE). 2022. p. 1962-1967.
[127] Zhang, J., M. Li, S. Zeng, B. Xie, and D. Zhao, A survey on security and privacy threats to federated learning, in 2021 International Conference on Networking and Network Applications (NaNA). 2021. p. 319-326.
[128] Jiang, Z., W. Wang, B. Li, and Q. Yang, Towards Efficient Synchronous Federated Training: A Survey on System Optimization Strategies. IEEE Transactions on Big Data, 2022.
[129] Liu, Z., J. Guo, W. Yang, J. Fan, K.-Y. Lam, and J. Zhao, Privacy-Preserving Aggregation in Federated Learning: A Survey. arXiv preprint arXiv:2203. 17005, 2022.
[130] Nassif, A.B., M.A. Talib, Q. Nasir, H. Albadani, and F.M. Dakalbab, Machine learning for cloud security: a systematic review. IEEE Access, 2021. **9**: p. 20717-20735.

[131]Zhan, Y., J. Zhang, Z. Hong, L. Wu, P. Li, and S. Guo, A survey of incentive mechanism design for federated learning. IEEE Transactions on Emerging Topics in Computing, 2021.
[132]Zhang, Q., C. Xin, and H. Wu, Privacy-Preserving Deep Learning Based on Multiparty Secure Computation: A Survey. IEEE Internet of Things Journal, 2021. **8**(13): p. 10412-10429.
[133]AbdulRahman, S., H. Tout, H. Ould-Slimane, A. Mourad, C. Talhi, and M. Guizani, A survey on federated learning: The journey from centralized to distributed on-site learning and beyond. IEEE Internet of Things Journal, 2020. **8**(7): p. 5476-5497.
[134]Rahman, K.M.J., F. Ahmed, N. Akhter, M. Hasan, R. Amin, K.E. Aziz, A.M. Islam, M.S.H. Mukta, and A.N. Islam, Challenges, applications and design aspects of federated learning: A survey. IEEE Access, 2021. **9**: p. 124682-124700.
[135]Kumar, N., J. Madhuri, and M. ChanneGowda, Review on security and privacy concerns in Internet of Things, in 2017 International Conference on IoT and Application (ICIOT). 2017. p. 1-5.
[136]Chen, B., Y. Liu, S. Zhang, J. Chen, and Z. Han, A Survey on Smart Home Privacy Data Protection Technology, in 2021 IEEE Sixth International Conference on Data Science in Cyberspace (DSC). 2021. p. 583-590.
[137]Imteaj, A., U. Thakker, S. Wang, J. Li, and M.H. Amini, A survey on federated learning for resource-constrained iot devices. IEEE Internet of Things Journal, 2021. **9**(1): p. 1-24.
[138]Nguyen, D.C., M. Ding, P.N. Pathirana, A. Seneviratne, J. Li, and H.V. Poor, Federated learning for internet of things: A comprehensive survey. IEEE Communications Surveys & Tutorials, 2021. **23**(3): p. 1622-1658.
[139]Lim, W.Y.B., N.C. Luong, D.T. Hoang, Y. Jiao, Y.-C. Liang, Q. Yang, D. Niyato, and C. Miao, Federated learning in mobile edge networks: A comprehensive survey. IEEE Communications Surveys & Tutorials, 2020. **22**(3): p. 2031-2063.
[140]Ali, M., F. Naeem, M. Tariq, and G. Kaddoum, Federated Learning for Privacy Preservation in Smart Healthcare Systems: A Comprehensive Survey. IEEE Journal of Biomedical and Health Informatics, 2022: p. 1-14.
[141]Chen, J. and X. Ran, Deep learning with edge computing: A review. Proceedings of the IEEE, 2019. **107**(8): p. 1655-1674.
[142]Rafique, W., L. Qi, I. Yaqoob, M. Imran, R.U. Rasool, and W. Dou, Complementing IoT services through software defined networking and edge computing: A comprehensive survey. IEEE Communications Surveys & Tutorials, 2020. **22**(3): p. 1761-1804.
[143]Campos, E.M., P.F. Saura, A. González-Vidal, J.L. Hernández-Ramos, J.B. Bernabe, G. Baldini, and A. Skarmeta, Evaluating Federated Learning for intrusion detection in Internet of Things: Review and challenges. Computer Networks, 2022: p. 108661.
[144]Nguyen, V.-L., P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, Security and privacy for 6G: A survey on prospective technologies and challenges. IEEE Communications Surveys & Tutorials, 2021. **23**(4): p. 2384-2428.
[145]Tahir, M., M.H. Habaebi, M. Dabbagh, A. Mughees, A. Ahad, and K.I. Ahmed, A review on application of blockchain in 5G and beyond networks: Taxonomy, field-trials, challenges and opportunities. IEEE Access, 2020. **8**: p. 115876-115904.
[146]Naz, S., K.T. Phan, and Y.-P.P. Chen, A comprehensive review of federated learning for COVID-19 detection. International Journal of Intelligent Systems, 2022. **37**(3): p. 2371-2392.
[147]Petersen, E., Y. Potdevin, E. Mohammadi, S. Zidowitz, S. Breyer, D. Nowotka, S. Henn, L. Pechmann, M. Leucker, P. Rostalski, and Others, Responsible and Regulatory Conform Machine Learning for Medicine: A Survey of Challenges and Solutions. IEEE Access, 2022.
[148]Kuhrmann, M., D.M. Fernández, and M. Daneva, On the pragmatic design of literature studies in software engineering: an experience-based guideline. Empirical software engineering, 2017. **22**(6): p. 2852-2891.
[149]Alazzam, M.B., F. Alassery, and A. Almulihi, Federated Deep Learning Approaches for the Privacy and Security of IoT Systems. Wireless Communications and Mobile Computing, 2022. **2022**.
[150]Xia, Z., Y. Chen, B. Yin, H. Liang, H. Zhou, K. Gu, and F. Yu, Fed_ADBN: An efficient intrusion detection framework based on client selection in AMI network. Expert Systems, 2022.
[151]Yuan, Y., Y. Yuan, T. Baker, L.M. Kolbe, and D. Hogrefe, FedRD: Privacy-preserving adaptive Federated learning framework for intelligent hazardous Road Damage detection and warning. Future Generation Computer Systems, 2021. **125**: p. 385-398.
[152]Zhang, T. and Q. Zhu, Distributed privacy-preserving collaborative intrusion detection systems for VANETs. IEEE Transactions on Signal and Information Processing over Networks, 2018. **4**(1): p. 148-161.
[153]Zhao, L., S. Hu, Q. Wang, J. Jiang, C. Shen, X. Luo, and P. Hu, Shielding collaborative learning: Mitigating poisoning attacks through client-side detection. IEEE Transactions on Dependable and Secure Computing, 2020. **18**(5): p. 2029-2041.
[154]Cheng, X., Q. Luo, Y. Pan, Z. Li, J. Zhang, and B. Chen, Predicting the APT for Cyber Situation Comprehension in 5G-Enabled IoT Scenarios Based on Differentially Private Federated Learning. Security and Communication Networks, 2021. **2021**.
[155]Fontenla-Romero, O., B. Pérez-Sánchez, and B. Guijarro-Berdiñas, DSVD-autoencoder: a scalable distributed privacy-preserving method for one-class classification. International Journal of Intelligent Systems, 2021. **36**(1): p. 177-199.
[156]Ibitoye, O., M.O. Shafiq, and A. Matrawy, Differentially private self-normalizing neural networks for adversarial robustness in federated learning. Computers & Security, 2022. **116**: p. 102631.
[157]Kong, Q., F. Yin, R. Lu, B. Li, X. Wang, S. Cui, and P. Zhang, Privacy-preserving aggregation for federated learning-based navigation in vehicular fog. IEEE Transactions on Industrial Informatics, 2021. **17**(12): p. 8453-8463.
[158]Kumar, K.P.S., S.A.H. Nair, D.G. Roy, B. Rajalingam, and R.S. Kumar, Security and privacy-aware artificial intrusion detection system using federated machine learning. Computers & Electrical Engineering, 2021. **96**: p. 107440.
[159]Kumar, P., G.P. Gupta, and R. Tripathi, PEFL: Deep Privacy-Encoding-Based Federated Learning Framework for Smart Agriculture. IEEE Micro, 2021. **42**(1): p. 33-40.
[160]Lu, Y., X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, Federated learning for data privacy preservation in vehicular cyber-physical systems. IEEE Network, 2020. **34**(3): p. 50-56.
[161]Nasser, N., Z.M. Fadlullah, M.M. Fouda, A. Ali, and M. Imran, A lightweight federated learning based privacy preserving B5G pandemic response network using unmanned aerial vehicles: A proof-of-concept. Computer Networks, 2022. **205**: p. 108672.
[162]Popoola, S.I., R. Ande, B. Adebisi, G. Gui, M. Hammoudeh, and O. Jogunola, Federated deep learning for zero-day botnet attack detection in IoT-edge devices. IEEE Internet of Things Journal, 2021. **9**(5): p. 3930-3944.

[163]Raza, A., K.P. Tran, L. Koehl, and S. Li, Designing ecg monitoring healthcare system with federated transfer learning and explainable ai. Knowledge-Based Systems, 2022. **236**: p. 107763.
[164]Ruzafa-Alcazar, P., P. Fernandez-Saura, E. Marmol-Campos, A. Gonzalez-Vidal, J.L.H. Ramos, J. Bernal, and A.F. Skarmeta, Intrusion Detection based on Privacy-preserving Federated Learning for the Industrial IoT. IEEE Transactions on Industrial Informatics, 2021.
[165]Shi, J., L. Qi, K. Li, and Y. Lin, Signal Modulation Recognition Method Based on Differential Privacy Federated Learning. Wireless Communications and Mobile Computing, 2021. **2021**.
[166]So, J., B. Güler, and A.S. Avestimehr, Byzantine-resilient secure federated learning. IEEE Journal on Selected Areas in Communications, 2020. **39**(7): p. 2168-2181.
[167]Zhou, J., N. Wu, Y. Wang, S. Gu, Z. Cao, X. Dong, and K.-K.R. Choo, A Differentially Private Federated Learning Model against Poisoning Attacks in Edge Computing. IEEE Transactions on Dependable and Secure Computing, 2022.
[168]Zhang, Z., N. He, Q. Li, K. Wang, H. Gao, and T. Gao, DetectPMFL: Privacy-Preserving Momentum Federated Learning Considering Unreliable Industrial Agents. IEEE Transactions on Industrial Informatics, 2022.
[169]Chen, B., H. Zeng, T. Xiang, S. Guo, T. Zhang, and Y. Liu, ESB-FL: Efficient and Secure Blockchain-Based Federated Learning with Fair Payment. IEEE Transactions on Big Data, 2022.
[170]Nguyen, D.C., M. Ding, P.N. Pathirana, A. Seneviratne, and A.Y. Zomaya, Federated learning for COVID-19 detection with generative adversarial networks in edge cloud computing. IEEE Internet of Things Journal, 2021.
[171]Rehman, A., I. Razzak, and G. Xu, Federated Learning for Privacy Preservation of Healthcare Data from Smartphone-based Side-Channel Attacks. IEEE Journal of Biomedical and Health Informatics, 2022.
[172]Ma, S., J. Nie, J. Kang, L. Lyu, R.W. Liu, R. Zhao, Z. Liu, and D. Niyato, Privacy-preserving Anomaly Detection in Cloud Manufacturing via Federated Transformer. IEEE Transactions on Industrial Informatics, 2022.
[173]Bugshan, N., I. Khalil, N. Moustafa, and M.S. Rahman, Privacy-Preserving Microservices in Industrial Internet of Things Driven Smart Applications. IEEE Internet of Things Journal, 2021.
[174]Cui, L., Y. Qu, G. Xie, D. Zeng, R. Li, S. Shen, and S. Yu, Security and privacy-enhanced federated learning for anomaly detection in iot infrastructures. IEEE Transactions on Industrial Informatics, 2021. **18**(5): p. 3492-3500.
[175]Li, Y., Z. Zhang, Z. Zhang, and Y.-C. Kao, Secure federated learning with efficient communication in vehicle network. Journal of Internet Technology, 2020. **21**(7): p. 2075-2084.
[176]Ho, T.-T., K.-D. Tran, and Y. Huang, FedSGDCOVID: Federated SGD COVID-19 Detection under Local Differential Privacy Using Chest X-ray Images and Symptom Information. Sensors, 2022. **22**(10): p. 3728.
[177]Li, J., Y. Meng, L. Ma, S. Du, H. Zhu, Q. Pei, and X. Shen, A federated learning based privacy-preserving smart healthcare system. IEEE Transactions on Industrial Informatics, 2021. **18**(3).