NIPES

Journal of Science and Technology Research

Journal homepage: www.nipesjournals.org.ng

A Systematic Review of Centralized and Decentralized Machine Learning Models: Security Concerns, Defenses and Future Directions

Glory Nosawaru Edegbe & Samuel Acheme
Department of Computer Science, Edo State University Uzairue, Edo State Nigeria
Email: edegbe.glory@edouniversity.edu.ng, acheme20.samuel@edouniversity.edu.ng

Article Info

Keywords: *Machine learning model, Centralized Machine learning, Decentralized Machine Learning.*

Received 19 August 2024
Revised 15 December 2024
Accepted 21 December 2024
Available online 17 January 2025

https://doi.org/10.5281/zenodo.14681449

Abstract

Models are the heart of machine learning as they represent the end product of the learning process and help in making predictions. With the widespread adoption of machine learning and the ever-increasing security concerns especially when dealing with sensitive data like healthcare and financial data, the security of machine learning models has become expedient to guarantee the privacy of training data and ensure the continuous acceptance and adoption of machine learning in fields involving sensitive data. This study presents a systematic review of centralized and decentralized machine learning models; security challenges, common application areas and defence mechanisms implemented to curb the security threats in centralized and decentralized machine learning models. Also, we propose future directions and avenues for research and development to improve the security, performance and resilience of centralized and decentralized machine learning models.

1.0. Introduction

Machine learning (ML) has revolutionized various sectors by enabling systems to learn and improve from experience without being explicitly programmed [1, 2]. At the core of ML are models, which are mathematical representations learned from data to make predictions on new, unseen data [3, 4]. Traditionally, ML models are trained in centralized environments where large datasets are gathered and processed [5, 6]. While this approach has yielded results, it raises great concerns about security, privacy and scalability [7, 8]. To address these challenges, decentralized ML has emerged as an alternative to enhance privacy in the learning process [5, 9]. Centralized models, though effective possess inherent vulnerabilities to various security threats [10, 11]. The centralized storage and processing of sensitive data make them attractive for attacks such as data breaches, poisoning, intellectual property theft and byzantine failures [12, 13, 14]. Furthermore, centralized models hinder collaboration and knowledge sharing among organizations [15, 16]. Decentralized ML models distribute data and computation across multiple nodes, enhancing privacy, security, and resilience [17, 18]. By dividing silos and enabling collaborative learning, decentralized models unlock the potential of massive datasets while preserving data control and ownership [19, 20, 21]. However, decentralized systems introduce new challenges like byzantine failures and communications security challenges [22, 23, 24].

1.1 Machine Learning Model

The ML model is the mathematical representation of the real-world process learned from the data [25, 26]. A dataset of examples is fed into the model, the model learns from these examples to distinguish between the objects presented by identifying underlying patterns [27, 28, 29].

Supervised and unsupervised learning are the two common types of machine learning [30, 31]. In supervised learning, the model is trained with the use of labelled data, in labelled data the desired output is given for each input [32, 33, 34]. The goal of the model in supervised learning is to learn a mapping function that will accurately predict the label for unseen data [35, 36, 37]. Classification and regression are common tasks in supervised learning. Classification predicts the category using discrete labels while regression predicts continuous numerical values [30, 38]. Unsupervised learning deals with unlabeled data, the task of the model is to find hidden patterns within the data to make predictions [39]. Clustering and dimensionality reduction are examples of unsupervised learning techniques. In clustering, similar data points are grouped together, in dimensionality reduction, complex data is simplified by reducing the number of features [1].

When a model is trained, it can be used for predictions on new data. This is where the true value of the model lies [40]. The accuracy of prediction is dependent on many factors like algorithm, complexity of model, quality and quantity of the data etc. [41].

ML models are not infallible, they can make mistakes and also expose sensitive training data used to train them to adversaries [42, 43, 44]. Privacy-preserving machine learning (PPML) techniques are privacy guarantees put in place to ensure the privacy of training data and preserve model integrity [45, 46].

1.2 Security of Machine Learning Model

ML has been tremendously useful. However, it has also introduced a new frontier of security challenges [47]. It is expected that machine learning models should learn from data and make accurate predictions while protecting the privacy of training data [48]. These models rely on vast amounts of data to learn, improve and make predictions and this has made them targets for data breaches [4, 49]. Malicious actors can take advantage of model vulnerabilities in data collection, storage, and processing to manipulate, steal or misuse data [50, 51].

Machine learning models are vulnerable to adversarial attacks, where attackers can inject malicious inputs to deceive the model [52]. These attacks can manipulate the output of the model leading to incorrect decisions with devastating consequences [52, 53]. Different techniques like adversarial training, input validation, robust optimization etc. can help to mitigate these risks [50].

Besides adversarial model attacks, machine learning models can also leak sensitive information about training data. A common privacy-preserving technique to curb this is differential privacy, a technique that adds noise to data to protect privacy [54, 55]. Furthermore, model stealing attacks are also a possibility, where attackers attempt to replicate the functionality of a model without access to the original training data, necessitating robust model protection mechanisms [44, 56].

2.0 Related Works

[3], presented a comparative analysis of centralized versus federated averaging. They compared federated averaging with centralized learning models. Their results showed that centralized models perform better than federated averaging in terms of accuracy, however, they noted that security risks is much higher in centralized models as a result of storing data in a central location.

[5], performed a convergence performance between classical and federated machine learning using two datasets that are available publicly. Logistic regression using the MNIST dataset and image classification using the CIFAR-10 dataset were used. Their results showed that federated learning has higher convergence in a limited communication round while maintaining the anonymity of the participants.

[7], carried out a survey analyzing the journey and transition from centralized to distributed learning. They examined and compared different machine learning deployment architectures, and they provided a new classification of federated learning research fields and topics based on a thorough

analysis of technical challenges. They elaborated on taxonomies that cover different challenging aspects, trends and contributions in literature including system designs, models, application areas, security and resource management.

[8], examined and compared different machine learning deployment architectures considering centralized and federated machine learning. They provided a new classification of federated learning topics and research directions based on an analysis of technical challenges and recent related work. They elaborated comprehensive taxonomies that cover different challenging aspects in centralized learning as well as federated learning. Also, they discussed important open research directions.

[9], surveyed distributed learning and federated learning. Firstly, they proposed an architecture for federated learning systems and related techniques. Secondly, they explained federated learning systems from four aspects namely aggregation algorithms, types of parallelism, security and data communication. Thirdly, they presented four federated systems that are widely used based on functional architecture. Finally, they summarized their limitations and presented suggested research directions.

[19], presented an analysis of federated learning, introduced the development process, architecture, definition and classification of federated learning and explained the concept of federated learning by comparing it with centralized machine learning. Also, they described peculiar challenges of federated learning that need to be addressed. Finally, they discussed future research directions in federated learning systems based on deep learning.

[31], carried out a comparative analysis of centralized and federated machine learning. They discussed the different factors affecting federated learning and the differences between federated learning and centralized learning. They empirically demonstrated the effect the number of samples per device has on the distribution of the output labels of federated systems. They showed that federated learning has a cost advantage when the size of the model to be trained is not large. Finally, they presented the need for careful design to enhance cost and performance.

[37], studied the changing landscape in machine learning, they analyzed the evolution of machine learning from centralized to distributed and then to federated learning. Also, they addressed each type of machine learning as well as their different limitations and strengths.

[59], carried out a study on centralized and decentralized federated approaches using the transformer architecture to estimate remaining useful life. They noted the advantage of using decentralized federated learning over centralized learning and compared the performance of decentralized federated learning with centralized methods. They compared the performance of decentralized federated learning with centralized learning using two federated algorithms to predict the useful life of an asset remaining.

[63], carried out a study on the applications of distributed learning for the Internet of things. They provided a background of machine learning and presented a preliminary to typical distributed learning approaches. Then they carried out an extensive review of distributed learning for IoT services. From the literature they reviewed, they present challenges of distributed learning for IoT and propose promising research directions and solutions.

3.0 Methodology

This study employed a systematic review approach, building on previous studies [36, 57, 58]. We developed specific research questions to direct our search, selection, and analysis of existing literature. This strategy was essential to accomplish the objectives of this study. The objectives of this study are to; examine the vulnerabilities associated with centralized and decentralized machine learning models, identify existing defense mechanisms and propose future research directions to strengthen the security of centralized and decentralized machine learning models. The inclusion criteria are research papers written in English language that; contain valuable content on centralized

and decentralized machine learning models and papers containing relevant content on the security challenges in machine learning models written over the last decade i.e. from 2015 to 2024. Papers not meeting these criteria were not collected. Research papers were sourced by a desk search on the Scopus database with keywords like "machine learning models", "centralized machine learning models", "decentralized machine learning models" and "security of machine learning models". Table 1 shows the statistics of the papers obtained through the desk search per year.

Table 1: Distribution of sourced papers

S/N	Year	Number of Articles
1	2015	15
2	2016	11
3	2017	13
4	2018	15
5	2019	15
6	2020	13
7	2021	21
8	2022	12
9	2023	13
10	2024	17

Also, for analysis, we employed judgmental sampling to select a paper from each year based on the suitability and relevance of the publication to the context of this review. It has been noted that Judgmental sampling is very effective in scenarios where a direct and particular target is desired and a population that exhibits pertinent qualities that meet the set target specification is necessary [57]. Going forward, our assertions, descriptions, analyses, arguments and conclusions about the topic at hand were based on the chosen papers.

4.0 Discussion

4.1 Centralized Machine Learning Models

A centralized machine learning model is one where all data is collected and processed in a central location, this location is usually a powerful server or a cluster of servers residing either in a data centre or a cloud environment [59]. By collecting data from different sources, centralized machine learning empowers algorithms to reveal patterns and make predictions [60]. However, centralized machine learning models are faced with security and privacy concerns [15], this is because, when sensitive data is collected from different sources and amalgamated in a single location, it becomes a potential target for attackers [47]. A data breach can have devastating consequences, exposing personal, medical or financial records [18]. Beyond exposure to sensitive information, compromised trust in handling data can erode public confidence in machine learning and its adoption in certain fields [18].

Another critical security challenge is that a centralized system is a single point of failure. If the central repository is compromised, the entire infrastructure will be at risk. This vulnerability can lead to losses, reputational damage and loss of confidence in the infrastructure [5, 15].

The security challenges posed by centralized learning models demand a proactive and comprehensive approach to safeguard sensitive data, preventing sensitive data and protecting the integrity of machine learning models [18].

4.2 Decentralized Machine Learning Models

Decentralized machine learning models are distributed models that distribute the computational load across multiple devices. This distributed framework presents many advantages chiefly because it eliminates the vulnerability of having a single point of failure [17].

Also, decentralized models enhance privacy by keeping data in localized devices thereby reducing the risk of data breaches. Unlike centralized systems where large amount of data is aggregated in a central repository, decentralized systems minimize the exposure of sensitive information [61]. Decentralized machine learning like federated learning has offered good security and has gained acceptance in many fields involving sensitive user data [19].

Besides security, decentralized machine learning models also enhance scalability. As data volume continues to increase, centralized systems face processing challenges. Decentralized models address this challenge by harnessing the collective computational power of numerous devices. This distributed approach enables the handling of massive datasets without overwhelming a single entity [19, 59].

Moreover, decentralization improves system resilience. In traditional centralized systems, a single point of failure can cripple the entire system. Decentralized architectures, on the other hand, distribute the workload, making them more robust to failures. If one node malfunctions, the system can continue operating with minimal disruption [19, 62].

However, decentralized machine learning models also have unique security challenges. As a result of the distributed nature of the system, a larger attack surface is presented making it susceptible to various threats [22]. A major concern is data poisoning, where attackers can introduce misleading or corrupted data into the training process, thereby compromising model integrity. For instance, poisoning patient data in a decentralized healthcare system can lead to incorrect treatment recommendations or diagnoses [63, 9].

Model theft is another critical issue. As a resulted of the distributed nature of the learning model, intellectual property protection is complex. Malicious actors can steal the parameters of the model or replicate the behaviour of the model by accessing and analysing the data from different nodes. This presents a significant risk to the development of proprietary machine learning models [19].

Communication vulnerabilities are also another challenge in decentralized machine learning models. The exchange of model updates and the intermediate results between the different devices can be intercepted and tampered with. This can compromise the integrity and privacy of the learning process. Attackers can also exploit this vulnerability to inject malicious code or manipulate the model's behaviour [5, 8].

4.3 Comparative Analysis of Centralized and Decentralized Machine Learning Models.

In this section, we present a comparative analysis of centralized and decentralized machine learning models considering efficiency, scalability, and security. The efficiency of a machine learning model refers to the speed, resource allocation and overall performance of the model [46]. A more efficient model can process data faster with less computational power, and achieve similar or better results compared to a less efficient one [49]. Scalability is the ability of the model to handle increasing amounts of data or computational complexity without a significant impact on performance [37, 38]. A scalable model can efficiently process larger datasets and handle more complex tasks, making it suitable for applications with growing demands [38]. Security refers to the protection of the model, data, and infrastructure from unauthorized access, manipulation, or misuse. It involves safeguarding the confidentiality, integrity, and availability of machine learning data and components to ensure that the system operates as intended and remains reliable [11, 64].

4.3.1 Efficiency in Centralized and Decentralized Machine Learning Models

Figure 1 shows a comparative analysis of the efficiency of centralized and decentralized machine learning models.

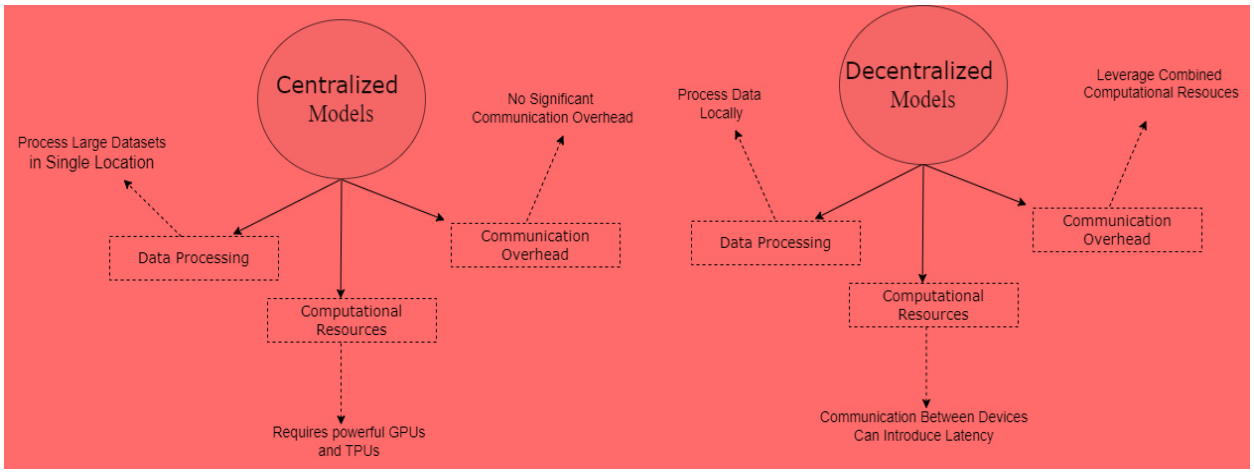

Figure 1: Efficiency of centralized and decentralized machine learning models

Centralized servers can process large datasets efficiently due to the centralized location of powerful servers, data processing in decentralized models is done locally by participating devices thereby leading to slower processing for large datasets [8].

Decentralized models leverage the computational resources of individual devices thus improving efficiency. Centralized models require powerful hardware (GPUs, and TPUs) for training and inference [28].

Centralized models present no significant communication overhead as all data and processing occur on a single server. However, communication between individual devices and the server in decentralized models can introduce latency and overhead [5].

4.3.2 Scalability in Centralized and Decentralized Machine Learning Models

Figure 2 shows a comparative analysis of the scalability in centralized and decentralized machine learning models.

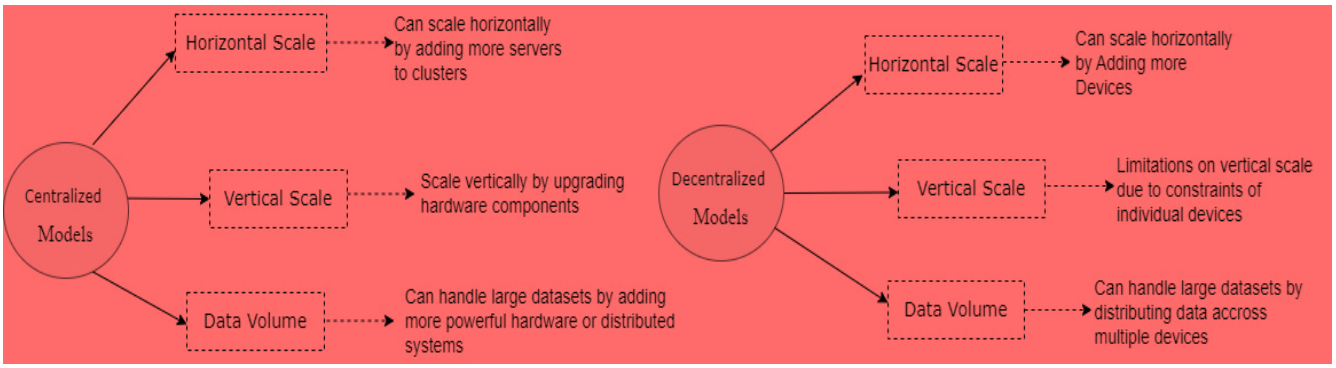

Figure 2: Scalability in centralized and decentralized machine learning models.

Horizontal scaling is the process of increasing the computational power of a system by adding more machines or nodes to a cluster [65]. This allows the system to handle larger workloads and improve performance without modifying the existing software or hardware. In centralized models, horizontal

scaling can be done by adding more servers to the cluster while horizontal scaling can be implemented in decentralized models by adding more devices to the network [66].
Vertical scaling involves increasing the computational power of a single machine or node by upgrading its hardware components [66]. This involves adding more memory, storage, or processing power to the existing machine. Centralized models can scale vertically by upgrading hardware components while decentralized models may have limitations to vertical scalability due to constraints of individual devices [65, 66].
Centralized models can handle large datasets by adding more powerful hardware while decentralized models can handle large datasets by distributing data across multiple devices thereby reducing the computational burden on individual machines [6].

4.3.3 Security Analysis of Centralized and Decentralized Machine Learning Models

Table 2 shows the security analysis of centralized and decentralized machine learning models.

Table 2: Security Analysis of Centralized and Decentralized Machine Learning Models

Vulnerability	Centralized Models	Decentralized Models
Single point of failure	High risk	Not Applicable
Model poisoning	High risk	Potential risk at individual nodes
Data privacy	High risk	Lower risk
Intellectual property theft	High risk	Lower risk
DDoS attacks	Low risk	High risk
Byzantine failure	Low risk	High risk
Communication security	Less critical	Critical

Centralized machine learning has a high risk of a single point of failure as a result of the central collection of data, if the central server experiences failure, the entire infrastructure will be compromised. On the other hand, decentralized learning addressed the challenge of a single point of failure by distributing data and processing across multiple devices. Therefore, failure of devices will be localized [31].
Model poisoning involves the manipulation of the training data by an adversary to degrade the performance of the model. The risk and mode of propagation of model poisoning differ significantly in centralized and decentralized machine learning models. Model poisoning in centralized machine learning models involve data poisoning which is injecting malicious data into the training set thereby making the model make misleading predictions [45]. Model poisoning in decentralized models can be carried out by either manipulating model updates sent to the central server, this can be gradient poisoning (modifying gradients to shift the model in a particular direction) or data poisoning as in the case of centralized model poisoning [31]. Inference poisoning is also another mode of propagation of model poisoning in a decentralized system, inference poisoning occurs at the inference phase and involves manipulating input data or the model itself to make incorrect predictions [45]. The risk of model poisoning in centralized models is high because data is located in a single location and malicious data can be injected easily. However, the risk of model poisoning in decentralized models also does exist but this risk is resident in the individual nodes [7, 45].
Privacy attacks in machine learning models lead to exposure of sensitive training data [64]. Centralized learning presents a high risk to privacy because of the centralized location of training data [20]. Centralized models are highly vulnerable to data breach as they offer a single point of failure, centralized models are also highly vulnerable to data misuse because the centralized entity has complete control over the data [8, 24]. Transparency issues are also a major privacy concern in

centralized machine learning as users often have limited visibility into how their data is used. Decentralized learning reduces privacy risk because data is not localized, guarantees data sovereignty because data remains under user control, reduces exposure of sensitive data because only necessary data is shared, and it also enhances transparency because data owners have more control over data usage [28].

Intellectual property theft in machine learning models occurs when someone uses another person's proprietary machine learning model, its data or components illegally [52, 54]. For theft of intellectual property in machine learning systems, attackers usually employ reverse engineering which involves analyzing the parameters and structures of the model to recreate a similar model, potentially stealing the intellectual property embedded in the model [67]. Centralized models are more vulnerable to intellectual property theft because the centralized repository is a potential target for attackers and also, reverse engineering is also easier in centralized models as attackers can easily analyze model output. [37]. Decentralized models have far less risk of intellectual property theft because reverse engineering is difficult in decentralized machine learning as a result of the distributed nature of data and computation [25].

While the possibility of denial of service cannot be denied in centralized machine learning, the risk is generally lower because of the centralized nature of data and computation [5]. However, in decentralized models, the risk of DDOS is higher because of its distributed nature as attackers can target individual nodes to deny training or inference, overwhelm individual nodes and slow down the distributed network thus impacting overall system performance [32].

Byzantine fault tolerance is the ability of machine learning models to continue operation correctly even when some of its components fail arbitrarily [61]. A byzantine failure occurs when a component misbehaves in a certain way, where one or more nodes behave maliciously or unpredictably including sending contradictory information to different parts of the system [61, 67]. The risk of byzantine failure exists in a centralized learning model but this risk is low because data is localized. However, the risk of byzantine failure is high in decentralized models where coordination is essential. In decentralized models, nodes can deviate from agreed-upon protocol, send misleading or incorrect information or even attempt to sabotage the training process [8, 48].

Communication security is a critical aspect of decentralized machine learning, the risk of communication security in centralized machine learning models is less critical as compared to that of decentralized machine learning models [19]. Communication security concerns in centralized models exist in data transmission (where data from different sources are transferred to the central server) and model transmission (when the model is distributed to different clients) [6]. Communication security breaches have a high risk in decentralized machine learning models and this is because of the coordination of learning between the different devices and the central server making it easier for adversaries to poison model updates [63].

4.4 Defense Mechanisms

Table 3 shows the different defense mechanisms put in place to protect centralized and decentralized machine learning models.

Table 3: Defense mechanisms in centralized and decentralized machine learning models

Vulnerability	Centralized Models	Decentralized Models
Single Point of Failure	Disaster recovery and backups	Not Applicable
Model Poisoning	Model monitoring, data validation and adversarial training	Outlier detection and federated learning

Privacy	Differential privacy, encryption and access control	Homomorphic encryption, differential privacy and federated learning
Intellectual Property Theft	Model obfuscation, access control and watermarking	Model obfuscation and federated learning
DDoS Attacks	Load balancing, intrusion detection, rate limitation	Load balancing, rate limiting, intrusion detection.
Byzantine Failure	Not applicable	Reputation systems, outlier detection and consensus algorithms
Communication security	Encryption, authentication and integrity checks	Encryption, authentication and integrity checks

4.5 Application Areas of Centralized Machine Learning Models

Centralized models are suitable in scenarios where; Large datasets are available as they can efficiently handle massive amounts of data [59]. Also, centralized models are suitable where data privacy is not a major concern; When data can be shared freely without compromising sensitive information, centralized models offer a straightforward and efficient solution [23]. Centralized models are also suitable when real-time predictions are required. Centralized models can be optimized for low latency, making them suitable for applications that demand immediate results [11]. Real-world applications of centralized machine learning models include; recommendation systems because centralized models can analyze vast amounts of data to provide personalized recommendations for content, products or services. Centralized models are also suitable for image recognition; centralized models can be trained on large datasets of images to achieve high accuracy in tasks like object detection and facial recognition [22]. Also, centralized models are suitable for natural language processing tasks; this is because centralized models can leverage large language models to understand and generate human language [31]. Fraud detection is also another area where centralized models are highly desirable as these models analyze patterns in large financial data to identify fraudulent transactions and protect against financial losses [68].

4.6 Application Areas of Decentralized Machine Learning Models

Decentralized models are suitable in scenarios where; Data privacy is a major concern because decentralized models can protect sensitive data by keeping it local and only sharing model updates [30, 22]. Decentralized models are also suitable when data is distributed across multiple devices because they can leverage data from a wide range of sources thus improving model accuracy and generalizability [68]. Also, decentralized models are desirable in scenarios where scalability is required, this is because they can be easily scaled to handle large numbers of devices and data points [52]. Real world applications of decentralized machine learning models include; federated ML models, they are used to train ML models on individual devices and share model updates without sharing their data thus ensuring privacy [24]. Internet of Things is another application of decentralized models; decentralized models have been deployed on IoT devices to analyze local data and make autonomous decisions thereby reducing the need for centralized cloud processing [54]. Also, decentralized models find applications in edge computing as they can be used to process data at the edge of the network, thus, reducing latency and improving responsiveness [54]. Decentralized models can also be integrated into blockchain technology to ensure data privacy and security [10].

4.7 Common Security Challenges and Solutions in Centralized and Decentralized Machine Learning Models

In this section, we discussed common security challenges and solutions in centralized and decentralized machine learning models. We considered data privacy, model poisoning and model interoperability which are common security challenges in centralized and decentralized machine learning models.

Data privacy in machine learning models refers to the protection of sensitive information used to train and deploy these models [55]. This involves ensuring that data is collected, stored, and processed without exposure [10]. Protecting privacy in decentralized models involves encryption to make it difficult for unauthorized parties to access, implementing strong access controls and data anonymization; transforming data to remove personally identifiable information making it harder to link an individual to his personal data [6]. Protecting privacy in decentralized models involves privacy-preserving techniques like homomorphic encryption; carrying out computation on encrypted data without decryption, secure multi-party computation; where multiple parties can collaborate on a task without revealing individual inputs, differential privacy; adding noise to data to protect individual privacy while preserving statistical accuracy, and the use of blockchain; a distributed ledger that can be used to securely record and track data transactions ensuring transparency and immutability [33, 42, 51].

Model poisoning is a malicious attack where adversaries inject malicious inputs into the training data of a machine learning model. These malicious inputs can be designed to mislead the model, causing it to produce incorrect or biased outputs [34]. By poisoning the model, attackers can compromise its accuracy, reliability, and security. In centralized models, anomaly detection can be used to mitigate model poisoning as statistical techniques can identify unusual or suspicious data points that may be indicative of poisoning attacks [11]. Input validation, adversarial training and ensemble methods are other techniques to address model poisoning in centralized models. Input validation can prevent malicious inputs from being processed. Adversarial training involves training the model with adversarial examples and this can make it more resilient to poisoning attacks. Ensemble methods involve combining multiple models and this can reduce the impact of poisoning attacks in centralized models [34, 69]. Preventing model poisoning in decentralized models involves techniques like secure aggregation to aggregate data from multiple nodes securely without revealing individual inputs. Reputation systems a technique to track the behaviour of nodes can help identify malicious nodes and thus prevent decentralized models from poisoning attacks by identifying and isolating malicious actors [33, 51, 70]. Also, adversarial distributed training which involves training the model across multiple nodes can make it more resistant to poisoning attacks [47].

Model interpretability is the ability to understand how a model arrives at its predictions. It involves explaining the decision-making process behind a model's outputs [67]. This is crucial for building trust in models, especially in high-stakes applications like healthcare or finance [43]. In centralized models, Local Interpretable Model-Agnostic Explanations LIME, a technique that approximates a complex model with a simpler and more interpretable model can be used to enhance model interpretability [43]. Shapley Additive exPlanations SHAP promotes interpretability by assigning to each feature a value that represents its contribution to the prediction, providing a global explanation of the model. Also, rule-based models that explicitly represent rules can be used in centralized models to enhance model interpretability [67]. In decentralized models, consensus mechanisms are highly beneficial to ensuring model interpretability [52]. Decentralized models can use consensus algorithms to agree on a common interpretation even if the individual nodes have different explanations [56]. Federated interpretability is another technique in decentralized models to ensure interpretability. Federated interpretability is a technique that applies interpretability

methods locally on individual nodes in a decentralized machine learning system to provide insights into how the model arrives at its predictions without sharing the raw data [37, 11].

5.0 Future Directions

Figure 3 is a pictorial representation of the research progress and proposed future directions.

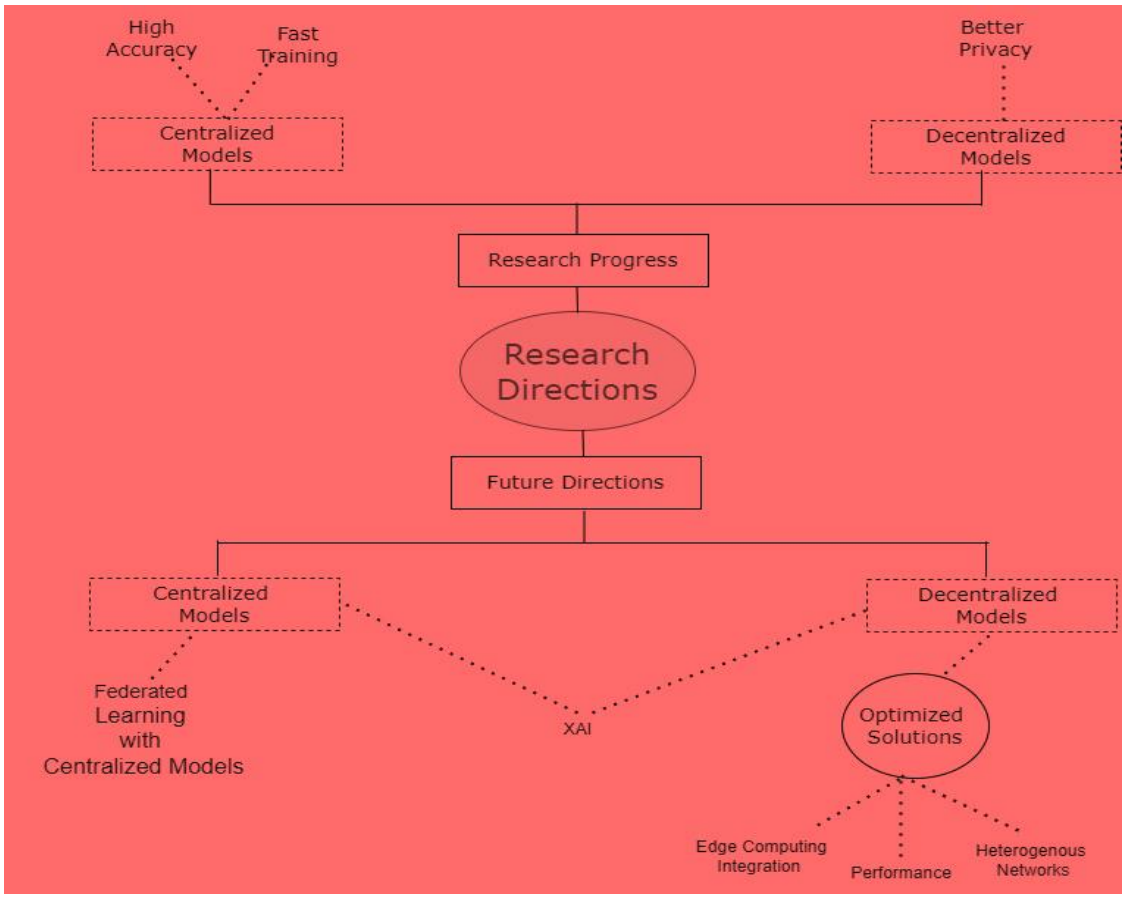

Figure 3: Research progress and future directions

The adoption of machine learning in certain fields is heavily reliant on addressing the challenges posed by both centralized and decentralized models [50]. While high accuracy and faster training time is a unique advantage of centralized learning over decentralized learning [68, 71]. Decentralized learning offers better privacy guarantee compared to centralized learning [60, 72]. Moving forward, research should focus on optimizing techniques for integrating federated learning into centralized systems. This can help leverage distributed data for training models while maintaining central location of data. This approach will enhance privacy, explainability and ethical considerations. Also, decentralized systems require optimized solutions for security, heterogeneous networks, efficient integration of edge computing and improved model performance. Researchers should focus on the integration of explainable A.I (XAI) into centralized and decentralized models. Understanding collaboration and revealing model contributions can help identify risk in decentralized systems, XAI can help ensure this in decentralized systems [67, 73]. In centralized systems, XAI can be used as a critical tool to understand model decisions and identify biases. XAI will a valuable tool to enhance reliability, accountability and transparency in both centralized and decentralized systems [67].

Finally, future research can focus on bridging the gap between centralized and decentralized machine learning approaches to bolster security, privacy, scalability, ethical concerns, model accuracy as well as model interpretability.

6.0 Conclusion

To harness the full potential of machine learning, it is expedient to address the unique security concerns posed by machine learning models. Maintaining public trust and acceptability is dependent on the performance of machine learning systems and the security of user data used in training. In this study, we explored the various security risks associated with centralized and decentralized machine learning models as well as the different defence mechanisms put in place to curb these threats. Furthermore, we suggest future research directions to improve the security, performance, and resilience of centralized and decentralized machine learning systems.

References

[1] Singh, A., Thakur, N., & Sharma, A. (2016). A review of supervised machine learning algorithms. In 2016 3rd international conference on computing for sustainable global development (INDIACom) (pp. 1310-1315). Ieee.

[2] Zhu, M., Wang, J., Yang, X., Zhang, Y., Zhang, L., Ren, H., ... & Ye, L. (2022). A review of the application of machine learning in water quality evaluation. Eco-Environment & Health, 1(2), 107-11

[3] Alloghani, M., Al-Jumeily, D., Mustafina, J., Hussain, A., & Aljaaf, A. J. (2020). A systematic review on supervised and unsupervised machine learning algorithms for data science. Supervised and unsupervised learning for data science, 3-21.

[4] Dhall, D., Kaur, R., & Juneja, M. (2020). Machine learning: a review of the algorithms and its applications. Proceedings of ICRIC 2019: Recent innovations in computing, 47-63.

[5] Asad, M., Moustafa, A., & Ito, T. (2021). Federated learning versus classical machine learning: A convergence comparison. arXiv preprint arXiv:2107.10976.

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

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

[8] Alsagheer, D., Xu, L., & Shi, W. (2023). Decentralized machine learning governance: Overview, opportunities, and challenges. IEEE Access.

[9] Liu, J., Huang, J., Zhou, Y., Li, X., Ji, S., Xiong, H., & Dou, D. (2022). From distributed machine learning to federated learning: A survey. Knowledge and Information Systems, 64(4), 885-917.

[10] Chen, X., Ji, J., Luo, C., Liao, W., & Li, P. (2018). When machine learning meets blockchain: A decentralized, privacy-preserving and secure design. In 2018 IEEE international conference on big data (big data) (pp. 1178-1187). IEEE.

[11] Peng, S., Yang, Y., Mao, M., & Park, D. S. (2022). Centralized machine learning versus federated averaging: A comparison using mnist dataset. KSII Transactions on Internet and Information Systems (TIIS), 16(2), 742-756.

[12] Elgabli, A., Park, J., Bedi, A. S., Bennis, M., & Aggarwal, V. (2020, March). Communication efficient framework for decentralized machine learning. In 2020 54th Annual Conference on Information Sciences and Systems (CISS) (pp. 1-5). IEEE.

[13] Schelter, S., Biessmann, F., Januschowski, T., Salinas, D., Seufert, S., & Szarvas, G. (2015). On challenges in machine learning model management.

[14] Hu, Y., Niu, D., Yang, J., & Zhou, S. (2019). FDML: A collaborative machine learning framework for distributed features. In Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (pp. 2232-2240).

[15] Hussain, G. J., & Manoj, G. (2022). Federated learning: A survey of a new approach to machine learning. In 2022 First International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT) (pp. 1-8). IEEE.

[16] Sharifani, K., & Amini, M. (2023). Machine learning and deep learning: A review of methods and applications. World Information Technology and Engineering Journal, 10(07), 3897-3904.

[17] Hoque, M. M., Tahir, M., Sainio, P., & Ahmad, I. (2024). Resource Consumption Analysis of Distributed Machine Learning Models for 6G Security.

[18] Sharma, V. (2022). A study on data scaling methods for machine learning. International Journal for Global Academic & Scientific Research, 1(1), 31-42.
[19] Hu, K., Li, Y., Xia, M., Wu, J., Lu, M., Zhang, S., & Weng, L. (2021). Federated learning: a distributed shared machine learning method. Complexity, 2021(1), 8261663.
[20] Tufail, S., Riggs, H., Tariq, M., & Sarwat, A. I. (2023). Advancements and challenges in machine learning: A comprehensive review of models, libraries, applications, and algorithms. Electronics, 12(8), 1789.
[21] Verbraeken, J., Wolting, M., Katzy, J., Kloppenburg, J., Verbelen, T., & Rellermeyer, J. S. (2020). A survey on distributed machine learning. Acm computing surveys (csur), 53(2), 1-33.
[22] Korkmaz, C., Kocas, H. E., Uysal, A., Masry, A., Ozkasap, O., & Akgun, B. (2020, November). Chain fl: Decentralized federated machine learning via blockchain. In 2020 Second international conference on blockchain computing and applications (BCCA) (pp. 140-146). IEEE.
[23] Vikström, J. (2021). Comparing decentralized learning to federated learning when training deep neural networks under churn.
[24] Wang, M., Fu, W., He, X., Hao, S., & Wu, X. (2020). A survey on large-scale machine learning. IEEE Transactions on Knowledge and Data Engineering, 34(6), 2574-2594.
[25] Angra, S., & Ahuja, S. (2017, March). Machine learning and its applications: A review. In 2017 international conference on big data analytics and computational intelligence (ICBDAC) (pp. 57-60). IEEE.
[26] Zhou, P., Lin, Q., Loghin, D., Ooi, B. C., Wu, Y., & Yu, H. (2021, April). Communication-efficient decentralized machine learning over heterogeneous networks. In 2021 IEEE 37th International Conference on Data Engineering (ICDE) (pp. 384-395). IEEE.
[27] Al-Jarrah, O. Y., Yoo, P. D., Muhaidat, S., Karagiannidis, G. K., & Taha, K. (2015). Efficient machine learning for big data: A review. Big Data Research, 2(3), 87-93.
[28] Alzubi, J., Nayyar, A., & Kumar, A. (2018, November). Machine learning from theory to algorithms: an overview. In Journal of physics: conference series (Vol. 1142, p. 012012). IOP Publishing.
[29] Jo, T. (2021). Machine learning foundations. Machine Learning Foundations. Springer Nature Switzerland AG. https://doi. org/10.1007/978-3-030-65900-4.
[30] Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. Science, 349(6245), 255-260.
[31] Majeed, I. A., Kaushik, S., Bardhan, A., Tadi, V. S. K., Min, H. K., Kumaraguru, K., & Muni, R. D. (2022). Comparative assessment of federated and centralized machine learning. arXiv preprint arXiv:2202.01529.
[32] Bi, Q., Goodman, K. E., Kaminsky, J., & Lessler, J. (2019). What is machine learning? A primer for the epidemiologist. American journal of epidemiology, 188(12), 2222-2239.
[33] Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H. B., Patel, S., ... & Seth, K. (2017, October). Practical secure aggregation for privacy-preserving machine learning. In proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (pp. 1175-1191).
[34] Wang, Z., Ma, J., Wang, X., Hu, J., Qin, Z., & Ren, K. (2022). Threats to training: A survey of poisoning attacks and defences on machine learning systems. ACM Computing Surveys, 55(7), 1-36.
[35] Li, W., Wang, C. H., Cheng, G., & Song, Q. (2023). International conference on machine learning. Transactions on machine learning research.
[36] Mosavi, A., Ozturk, P., & Chau, K. W. (2018). Flood prediction using machine learning models: Literature review. Water, 10(11), 1536.
[37] Naik, D., & Naik, N. (2023). The changing landscape of machine learning: A comparative analysis of centralized machine learning, distributed machine learning and federated machine learning. In UK Workshop on Computational Intelligence (pp. 18-28). Cham: Springer Nature Switzerland.
[38] Panayiotou, T., Savvas, G., Tomkos, I., & Ellinas, G. (2019, December). Centralized and distributed machine learning-based QoT estimation for sliceable optical networks. In 2019 IEEE Global Communications Conference (GLOBECOM) (pp. 1-7). IEEE.
[39] Rajoub, B. (2020). Supervised and unsupervised learning. In Biomedical signal processing and artificial intelligence in healthcare (pp. 51-89). Academic Press.
[40] Sindhu Meena, K., & Suriya, S. (2020). A survey on supervised and unsupervised learning techniques. In Proceedings of international conference on artificial intelligence, smart grid and smart city applications: AISGSC 2019 (pp. 627-644). Springer International Publishing.
[41] Talaei Khoei, T., Ould Slimane, H., & Kaabouch, N. (2023). Deep learning: Systematic review, models, challenges, and research directions. Neural Computing and Applications, 35(31), 23103-23124.
[42] David, B., Dowsley, R., Katti, R., & Nascimento, A. C. (2015, November). Efficient unconditionally secure comparison and privacy preserving machine learning classification protocols. In International Conference on Provable Security (pp. 354-367). Cham: Springer International Publishing.

[43] Došilović, F. K., Brčić, M., & Hlupić, N. (2018). Explainable artificial intelligence: A survey. In 2018 41st International convention on information and communication technology, electronics and microelectronics (MIPRO) (pp. 0210-0215). IEEE.
[44] Liu, B., Ding, M., Shaham, S., Rahayu, W., Farokhi, F., & Lin, Z. (2021). When machine learning meets privacy: A survey and outlook. ACM Computing Surveys (CSUR), 54(2), 1-36.
[45] Ahmad, A., Harjula, E., Ylianttila, M., & Ahmad, I. (2020). Evaluation of machine learning techniques for security in SDN. In 2020 IEEE Globecom Workshops (GC Wkshps (pp. 1-6). IEEE.
[46] Brito, C., Ferreira, P., Portela, B., Oliveira, R., & Paulo, J. (2023, March). Soteria: Preserving privacy in distributed machine learning. In Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing (pp. 135-142).
[47] Wahab, O. A., Mourad, A., Otrok, H., & Taleb, T. (2021). Federated machine learning: Survey, multi-level classification, desirable criteria and future directions in communication and networking systems. IEEE Communications Surveys & Tutorials, 23(2), 1342-1397.
[48] Yu, Y., Li, H., Chen, R., Zhao, Y., Yang, H., & Du, X. (2019). Enabling secure intelligent network with cloud-assisted privacy-preserving machine learning. IEEE Network, 33(3), 82-87.
[49] El Naqa, I., & Murphy, M. J. (2015). What is machine learning? (pp. 3-11). Springer International Publishing.
[50] Zapechnikov, S. (2020). Privacy-preserving machine learning as a tool for secure personalized information services. Procedia Computer Science, 169, 393-399.
[51] Zapechnikov, S. (2022). Secure multi-party computations for privacy-preserving machine learning. Procedia Computer Science, 213, 523-527.
[52] Zhang, Y., Bai, G., Li, X., Curtis, C., Chen, C., & Ko, R. K. (2020). Privcoll: Practical privacy-preserving collaborative machine learning. In European Symposium on Research in Computer Security (pp. 399-418). Cham: Springer International Publishing.
[53] Zhang, Q., Xiang, T., Cai, Y., Zhao, Z., Wang, N., & Wu, H. (2022). Privacy-Preserving Machine Learning as a Service: Challenges and Opportunities. IEEE Network.
[54] Zhou, X., Xu, K., Wang, N., Jiao, J., Dong, N., Han, M., & Xu, H. (2021). A secure and privacy-preserving machine learning model sharing scheme for edge-enabled IoT. IEEE Access, 9, 17256-17265.
[55] Zhu, H., Liu, X., Lu, R., & Li, H. (2016). Efficient and privacy-preserving online medical prediagnosis framework using nonlinear SVM. IEEE journal of biomedical and health informatics, 21(3), 838-85.
[56] Tan, A. Z., Yu, H., Cui, L., & Yang, Q. (2022). Towards personalized federated learning. IEEE transactions on neural networks and learning systems, 34(12), 9587-9603.
[57] W. Nwankwo, A. S. Olayinka & K. E. Ukhurebor. "The Urban Traffic Congestion Problem in Benin City and the Search for an ICT-improved Solution". International Journal of Science and Technology, vol. 8, iss. 12, pp. 65- 72, 2019.
[58] W. Nwankwo, C. Adetunji, K. E. Ukhurebor, S. Makinde & B. Ubi. "The Precursory Machinery of Internet of Things (IoT) in the Platform for Harmonizing Bio-Mined Data. Nigerian." Research Journal of Engineering and Environmental Sciences, vol. 5, iss. 2, pp. 786-796, 2020.
[59] Kamei, S., & Taghipour, S. (2023). A comparison study of centralized and decentralized federated learning approaches utilizing the transformer architecture for estimating remaining useful life. Reliability Engineering & System Safety, 233, 109130.
[60] Lyu, X., Xiao, Y., Daley, B., & Amato, C. (2021). Contrasting centralized and decentralized critics in multi-agent reinforcement learning. arXiv preprint arXiv:2102.04402.
[61] Bouhata, D., Moumen, H., Mazari, J. A., & Bounceur, A. (2022). Byzantine fault tolerance in distributed machine learning: a survey. arXiv preprint arXiv:2205.02572.
[62] Kar, B., Yahya, W., Lin, Y. D., & Ali, A. (2022). A survey on offloading in federated cloud-edge-fog systems with traditional optimization and machine learning. arXiv preprint arXiv:2202.10628.
[63] Le, M., Huynh-The, T., Do-Duy, T., Vu, T. H., Hwang, W. J., & Pham, Q. V. (2024). Applications of Distributed Machine Learning for the Internet-of-Things: A Comprehensive Survey. IEEE Communications Surveys & Tutorials.
[64] Zerka, F., Barakat, S., Walsh, S., Bogowicz, M., Leijenaar, R. T., Jochems, A., ... & Lambin, P. (2020). Systematic review of privacy-preserving distributed machine learning from federated databases in health care. JCO clinical cancer informatics, 4, 184-200.
[65] Biletskyy, B. O. (2019). Horizontal and Vertical Scalability of Machine Learning Methods. *PROBLEMS IN PROGRAMMING*, (2), 69-80.
[66] Geng, J., Li, D., & Wang, S. (2019, June). Horizontal or vertical? a hybrid approach to large-scale distributed machine learning. In *Proceedings of the 10th Workshop on Scientific Cloud Computing* (pp. 1-4).
[67] Angelov, P. P., Soares, E. A., Jiang, R., Arnold, N. I., & Atkinson, P. M. (2021). Explainable artificial intelligence: an analytical review. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 11(5), e1424.
[68] Khan, A. A., & Adve, R. S. (2020). Centralized and distributed deep reinforcement learning methods for downlink sum-rate optimization. IEEE Transactions on Wireless Communications, 19(12), 8410-8426.

[69] Alfaro-Navarro, J. L., Cano, E. L., Alfaro-Cortés, E., García, N., Gámez, M., & Larraz, B. (2020). A fully automated adjustment of ensemble methods in machine learning for modeling complex real estate systems. *Complexity*, *2020*(1), 5287263.
[70] Gyawali, S., Qian, Y., & Hu, R. Q. (2020). Machine learning and reputation-based misbehavior detection in vehicular communication networks. *IEEE Transactions on Vehicular Technology*, *69*(8), 8871-8885.
[71] Koloskova, A., Lin, T., & Stich, S. U. (2021). An improved analysis of gradient tracking for decentralized machine learning. Advances in Neural Information Processing Systems, 34, 11422-11435.
[72] Kong, L., Lin, T., Koloskova, A., Jaggi, M., & Stich, S. (2021, July). Consensus control for decentralized deep learning. In International Conference on Machine Learning (pp. 5686-5696). PMLR.
[73] Minh, D., Wang, H. X., Li, Y. F., & Nguyen, T. N. (2022). Explainable artificial intelligence: a comprehensive review. Artificial Intelligence Review, 1-66.