Systematic Review of Available Models That Function as Solutions to Data Privacy in Deep Learning for Electronic Healthcare Systems

Laureen Akumu Ndeda, Dr. Samuel Oonge, Dr. Calvins Otieno

Maseno University

DOI: https://doi.org/10.51584/IJRIAS.2026.11080037

Received: 16 August 2026; Accepted: 21 August 2026; Published: 02 September 2026

ABSTRACT

Healthcare delivery requires the handling of sensitive personal health information (PHI); protecting this data is essential to maintain patient confidentiality and prevent unauthorized access. Despite the transformative potential of cloud-based deep learning in healthcare, the integration of sensitive Personal Health Information (PHI) into these systems is hindered by a critical trade-off between data utility and computational privacy. Current industry-standard techniques, such as anonymization and obfuscation, fail to provide robust protection against modern re-identification attacks. There remains a significant gap in creating a framework that provides formal data privacy guarantees without sacrificing the discriminative feature learning necessary for clinical diagnostics. This systematic review examines the application of differential privacy (DP) and the SPDZ protocol in electronic healthcare systems. The review addressed three sub-questions: the current research status of differential privacy in healthcare, approaches used to identify privacy challenges, and solutions proposed to mitigate risks across different subject domains. A comprehensive search yielded 4,970 studies, of which 316 were screened in full. After exclusions, 58 studies were analyzed. Results highlight increasing global interest in integrating SPDZ with differential privacy to strengthen data protection while enabling secure computation. Limitations included potential keyword bias, restricted temporal scope, and language constraints. Overall, the findings underscored the growing role of differential privacy in healthcare data for secure, privacy-preserving computation.

Keywords: Differential Privacy, SPDZ Protocol, Data Protection methods, Electronic Health Records, Privacy-Preserving Computation, Systematic Review, Healthcare Data Governance, Secure Multi-Party Computation, Patient Data Confidentiality, Digital Health Standards.

BACKGROUND

While this research is focused on the field of data privacy, a systematic evaluation was conducted to further investigate the topic of using differential privacy for data privacy in healthcare. The systematic review presented in this study explored the landscape of differential privacy use in enhancing data privacy for healthcare systems. The review analyzed four core research sources. The overarching research question focused on identifying data privacy measures using differential privacy and SPDZ. The review delved into three key sub-questions: the research status of data privacy using differential privacy, what research approaches have been used by researchers to identify data privacy issues in electronic healthcare systems, what proposed solutions have been implemented to address data privacy in electronic healthcare systems and the subject matter domains adopted in the studies.

The search process identified 4,970 potential studies, with six selected journals contributing significantly. After excluding duplicates and applying inclusion criteria, 316 articles were eligible for full-text screening. Subsequent exclusions yielded 70 articles, leading to a final set of 58 studies for analysis. This systematic review had certain limitations, such as potential bias in keywords, a limited temporal scope, and language restrictions. These limitations affected the comprehensiveness and diversity of the studies included. However, the findings emphasize the global focus on using SPDZ and differential privacy for data protection.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VIII August 2026

The study's systematic review explored the use of differential privacy to enhance data privacy for healthcare systems.

Conducting a systematic literature review on data privacy issues using differential privacy identified the research gaps and trends in data privacy and differential privacy, thus providing insights into areas that need further exploration and helped to understand the current state of research. This review can also help in evaluating different methodologies and techniques used in differential privacy research. By synthesizing existing literature, our study identified the strengths and weaknesses of the different approaches. This review will also aid in benchmarking and performance evaluation of the available different differential privacy mechanisms. By analyzing existing research, this study will also be able to determine techniques that offer better data privacy guarantees with minimal impact on data utility.

Data Sources

Critical analysis of data sources plays a critical role in shaping the reliability of the results in a systematic review. In this study, the study adopted a meticulous approach of using Google Scholar's five-year h-index and h-median indicators to pinpoint and select appropriate sources for the review. These metrics offered a quantitative assessment of a journal's significance and reach, determined by the number of times the articles are referenced within a specific time window.

With these metrics, the study was able to guarantee that the sources chosen were not only recent but also held substantial recognition and influence within the field of Differential Privacy and Data Privacy.

Table 1: Title of the Journals Included in this Search for the Literature

SNo	Journal Name	h5-Index	h5-median
1	International Conference on Financial Cryptography and Data Security	46	95
2	ACM Conference on Data and Application Security and Privacy	25	39
3	Data Privacy Management, Cryptocurrencies, and Blockchain Technology	17	23
4	International Conference on Data and Applications Security and Privacy	15	29

The data sources for the systematic review comprised the top six ranked journals, from which four were chosen and summarized for further analysis. These selected journals include the International Conference on Financial Cryptography and Data Security, the ACM Conference on Data and Application Security and Privacy, Data Privacy Management, Cryptocurrencies, and the Blockchain Technology International Conference on Data and Applications Security. The choice of these journals was justified by their high-impact factors and recognition as leading-edge publications. For instance, the International Conference on Financial Cryptography and Data Security has an h5-index of 46, thus signifying that it has published 46 or more articles with corresponding citations over the past five years. Another search was conducted on IEEE (Institute of Electrical and Electronics Engineers). Conducting a systematic review specifically within IEEE publications provides several advantages: high-quality research, relevancy aiding the systematic review to remain current, comprehensive coverage for topics under review, international perspectives, and access to full-text articles, making it easier to access the articles to include in a systematic review. Overall, conducting the systematic review within IEEE publications ensured that the review was based on high-quality, up-to-date research from a reputable source.

This selection criterion ensured that the chosen sources are significant and authoritative and, therefore, contribute significantly to the scholarly discourse on the subject matter. Employing these metrics and then selecting prominent journals for summarization is consistent with my aim to offer a thorough and insightful overview of the research landscape.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VIII August 2026

Search Strategy

The search strategy utilized in this systematic review was crafted to ensure the retrieval of pertinent and high-quality research articles. These articles contributed to the exploration of methods to enhance data privacy through the implementation of differential privacy.

The search process identified 4,970 potential studies, with six selected journals contributing significantly. After excluding duplicates and applying inclusion criteria, 316 articles were eligible for full-text screening. Subsequent exclusions yielded 70 articles, leading to a final set of 58 studies for analysis. This systematic review had certain limitations, such as potential bias in keywords, a limited temporal scope, and language restrictions. These limitations may thus affect the comprehensiveness and diversity of the studies included. However, the findings emphasized the global focus on using SPDZ for data privacy.

The systematic review presented in this study explored the landscape of differential privacy use in enhancing data privacy for healthcare systems.

Conducting a systematic literature review on data privacy issues using differential privacy identified the research gaps and trends in the field of data privacy and differential privacy, thus providing insights into areas that need further exploration and helping in understanding the current state of research. This review will also help in evaluating different methodologies and techniques used in differential privacy research. By synthesizing existing literature, our study can identify the strengths and weaknesses of the different approaches. This review will also aid in benchmarking and performance evaluation of the different differential privacy mechanisms. By analyzing existing research, the study will be able to determine techniques that offer better privacy guarantees with minimal impact on data utility.

The chosen keywords were data privacy and differential privacy. These were strategically selected to encompass the core focus of the study. These selected keywords were considered comprehensive and an accurate representation of the subject matter under investigation. Employing these keywords streamlined the search process, ensuring that the retrieved articles were directly relevant to the research purpose.

In line with the review's research questions, the search was limited to the last five years to obtain more current research. Moreover, for inclusion in the review, each article had to satisfy all the inclusion criteria and none of the exclusion criteria outlined in Table 2. This review primarily focused on peer-reviewed journal articles.

While peer-reviewed conference proceedings could have offered valuable insights into ongoing works not yet published in journals, they were excluded because the study aimed to examine research articles published in top-ranked technology and security journals. Likewise, dissertations, government publications, and organizational reports were excluded from the review, as these types of articles are typically not published in academic journals. Furthermore, books and book chapters, which often focus on theory or cite empirical findings from other studies, were also excluded from this review.

The inclusion and exclusion criteria were carefully delineated to narrow down the study's scope and guarantee the selection of articles that closely aligned with the research objectives. Inclusion criteria comprised articles published within the last five years, articles written in English, and articles explicitly addressing differential privacy. Exclusion criteria included non-peer-reviewed articles, articles that did not focus solely on how data privacy can be enhanced with differential privacy, and articles exploring contexts other than data privacy.

A summary of these criteria is presented in Table 2 below:

Table 2: Inclusion and Exclusion Criteria

Criteria	Inclusion Criteria	Exclusion Criteria
Source Type	Peer-reviewed journals	Not peer-reviewed

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VIII August 2026

Publication Date	Published within the last five years	Older than five years
Language	Written in English	Non-English literature
Relevance	Specifically addresses data privacy and differential privacy and how to enhance data privacy	Explores other contexts
Relevance	Must be involved in healthcare systems	Any study outside the healthcare systems context

Search Process and Search Results

The search process for relevant articles within the selected journals followed a comprehensive and systematic approach, employing a combination of databases and keywords. The databases used included Google Scholar and IEEE databases. Within each of the journals' databases, electronic searches were conducted using the following search terms: "differential privacy," "SPDZ," and "data privacy." This diligent approach identified many potential studies, with 4,970 articles initially identified. A 'title search' was conducted using the term "differential privacy." "Differential privacy," "healthcare differential privacy," "SPDZ" and "data privacy."

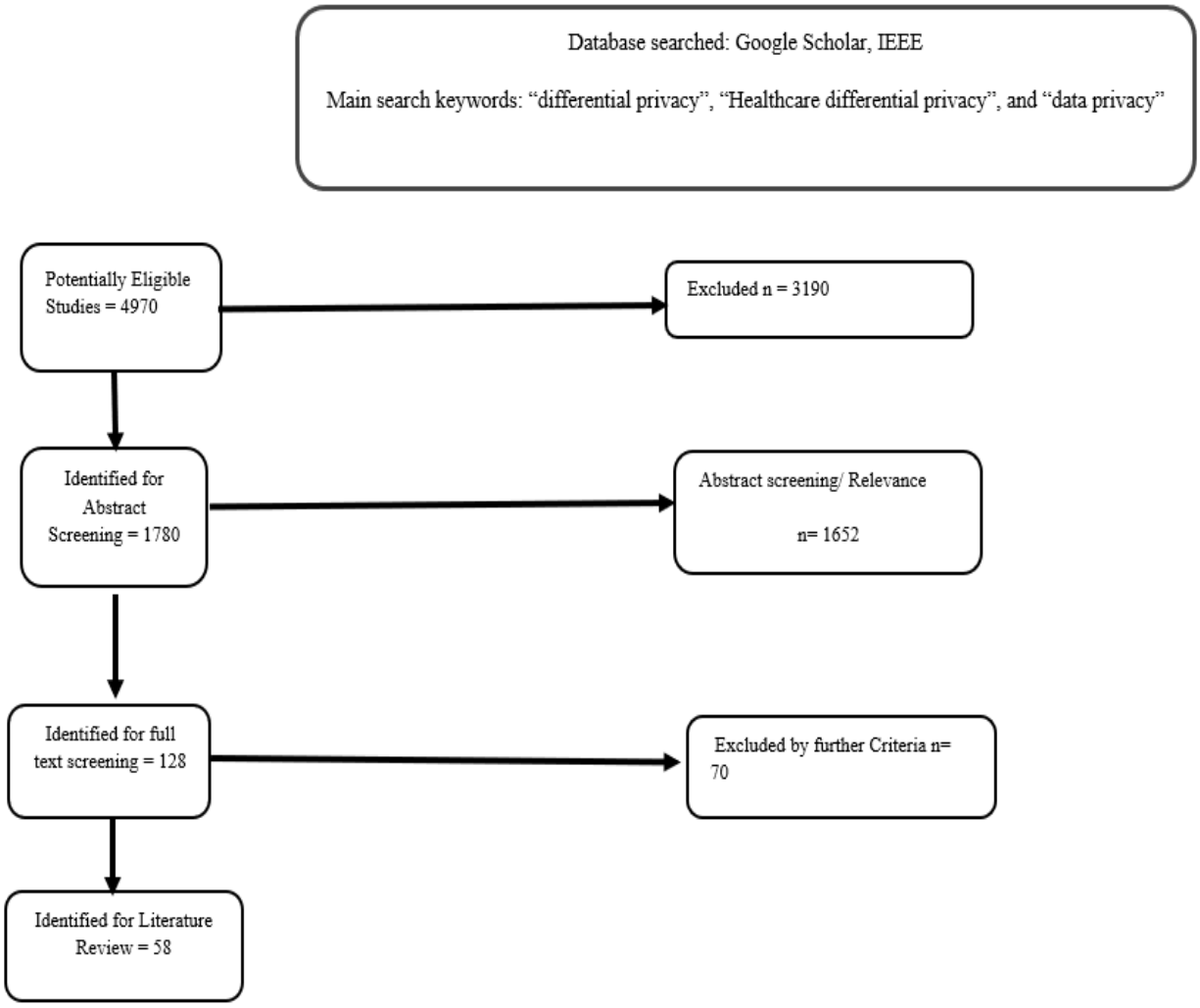

Figure 1: PRISMA framework for inclusion and exclusion criteria

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VIII August 2026

Review of Available Differential Privacy Models

i) *Local Differential Privacy (LDP) Model*: By altering data before it is even gathered, this type of model strategy is to safeguard personal privacy. Before uploading their data to the central server, each user modifies it locally (Wang et al., 2022). Randomized response is a crucial component of Local Differential Privacy (LDP). A method called randomized response was first used to allow the survey participants to answer delicate topics honestly and privately. In order to maintain the confidentiality of the true response while yet enabling the derivation of accurate aggregate statistics, it works by having participants randomly modify their answers depending on a predetermined probability distribution (Hidano & Murakami, 2022). Significant noise introduction is a drawback of several LDP models, as data analysis may become less useful as a result of the model trainings (Wang et al., 2022).

ii) *Gaussian Mechanism Model*: The Gaussian Mechanism Model, proposed by Dwork and Roth in 2014, is a foundational method for achieving differential privacy by adding carefully calibrated Gaussian noise to query responses. This model adds noise from a Gaussian distribution to query responses to ensure differential privacy. It is widely used in scenarios with differentially private mean and logistic regression (Malek et al., 2021). While it offers strong privacy guarantees, repeated application of the Gaussian Mechanism Model to answer multiple queries or perform multiple analyses can lead to cumulative privacy loss. Over time, the accumulation of noise may compromise the overall privacy protection the mechanism provides, especially in settings with correlated queries or data. It is also prone to data reconstruction attacks, and the model might not be suitable for non-Gaussian data distributions or when query sensitivity is difficult to compute (Erlingsson et al., 2019).

iii) *Objective Perturbation Model:* By altering a learning algorithm's goal function, Abadi et al. (2016) introduced the goal Perturbation Model (OPM), a technique for privacy-preserving machine learning. OPM has its own set of drawbacks, especially when it comes to security and privacy, even while it has some benefits in terms of protecting privacy. It is frequently used to train deep learning models by introducing noise into gradients or the loss function. Since the model perturbs the objective function, there is the occurrence of the hindrance of convergence, thus affecting the model's optimal performance (Nasr et al., 2020). While OPM aims to provide privacy guarantees, the level of privacy protection it offers may not always satisfy the rigorous standards of differential privacy. Adversaries with access to auxiliary information or background knowledge may still be able to breach privacy protections provided by OPM (Abadi et al., 2016).

iv) *Federated Learning Models*: This method enables model training across decentralized devices without sharing raw data (McMahan et al., 2017). Differential privacy can be incorporated into federated learning to ensure privacy-preserving model updates (Wang et al., 2022). However, this method may face challenges with communication overhead and convergence (Konečnỳ et al., 2016). Federated learning relies on the premise that sensitive data remains on the devices, and only model updates are shared. However, ensuring data privacy and security remains a significant challenge. There may be concerns about data leakage during the model aggregation process or potential attacks aimed at compromising the privacy of individual user data (Konečnỳ et al., 2016).

PrivMets Model

PrivMets (Xu, C., Cheng, X., Hu, Y., Li, Y., & Li, X., 2017) is a local differential privacy (LDP) model that has been used in healthcare research to protect patients' privacy while allowing for meaningful data analysis. It is designed for healthcare data analysis and can be used for tasks like clustering, classification, and regression. The algorithm is based on a tree-based data structure and achieves differential privacy by adding noise to the data before releasing it. It uses a tree-based data structure to achieve differential privacy, and it is effective in protecting patients' privacy while still providing accurate results (Kairouz et al., 2021).

Privacy goal: PrivMets uses local differential privacy (LDP) to protect patients' privacy. LDP ensures that individual data points cannot be linked to specific individuals in the dataset, even by an attacker who has access

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VIII August 2026

to other information. PrivMets achieves this by adding noise to the data before releasing it, which makes it difficult to identify specific individuals or sensitive information.

Data Structure: The PrivMets model represents the data using a tree-based data structure. The data is partitioned into smaller subsets at each level of the tree, which reduces the amount of noise that needs to be added to the data to achieve differential privacy. This makes PrivMets more efficient than other LDP algorithms that use a flat data structure.

Accuracy: PrivMets have been shown to achieve high accuracy in healthcare data analysis tasks. This is important for healthcare researchers who need to obtain meaningful insights from the data they are analyzing. The PrivMets model achieves this by carefully tuning the parameters of the algorithm and using a tree-based data structure to reduce the amount of noise that is added to the data.

Table 2.1: Summary of the research gaps for the PrivMets model (Xu et al. 2017)

	Major Focus	**Research Focus Gaps**
1	*High accuracy* PrivMets has been shown to achieve high accuracy in data analysis while still providing strong privacy guarantees. This means that researchers can obtain useful insights from healthcare data without compromising patients' privacy.	*Limited protection against membership inference attacks:* PrivMets does not provide strong protection against membership inference attacks, which are attacks that attempt to identify whether a specific individual is included in the dataset. This means that there is an emerging risk of re-identification in some of these cases.
2	*Flexibility:* PrivMets is a flexible LDP model that can be applied to a variety of healthcare data analysis tasks, including clustering, classification, and regression. This makes it a versatile tool for healthcare researchers.	*Computationally expensive:* PrivMets can be computationally expensive, particularly when used with large datasets. This means that it may not be feasible to use PrivMets in all healthcare research contexts.
3	*Scalability:* PrivMets is scalable and can be used to analyze large datasets. This is important in healthcare research, where large datasets are common.	*Requires careful parameter tuning:* PrivMets require careful parameter tuning to achieve optimal performance. This can be time-consuming and may require significant expertise.

The PrivMets algorithm by Xu et al. (2017) protects healthcare data privacy during analysis. However, researchers should treat it as supplementary guidance. The performance of the algorithm should be assessed: In a healthcare research project, PrivMets should be evaluated on the performance of the task at hand before being used (Xiao, X., and Tao, Y., 2015). This may be done by evaluating the algorithm on sample data or benchmark datasets and comparing its performance to alternative LDP strategies or non-private strategies. One should also learn about the weaknesses of LDP (Shokri, R., & Shmatikov, V., 2015). LDP is a strong privacy-preserving method, but it has some limitations and is susceptible to some kinds of attacks, including the membership inference attacks. In this study, data preprocessing methods have to be taken into consideration (Zhang et al., 2016). PrivMets uses a tree-based data structure to model the data, and this can be optimized with the help of data preprocessing methods. The methods that researchers can use to enhance the efficiency and the accuracy of PrivMets are dimensionality reduction or feature selection. Finally, the effect of noise on downstream analysis should be evaluated: Adding noise to the data is a major part of LDP, but downstream analysis activities, including clustering or classification, can also be affected. The researchers should pay much attention to the effects of the additional noise on the particular analysis task and adjust the parameters of PrivMets to optimize its functioning (Dwork and Roth, 2014).

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VIII August 2026

Geo-indistinguishability model

Andrade et al. (2016) proposed a framework for privacy-preserving spatial data analysis using the geo-indistinguishability model. Geo-indistinguishability is a privacy model that aims to protect the location privacy of individuals in spatial data analysis. The research proposed a scalable and efficient algorithm for geo-indistinguishable spatial data publication. Their approach uses a quadtree-based partitioning scheme to divide the space into smaller cells and then adds noise to the coordinates of the cells in a way that preserves geo-indistinguishability. This study also proposed a method for optimizing the privacy budget, which controls the amount of noise added to the data. Their approach uses a cost-benefit analysis to balance the privacy and utility of the released data and adjusts the privacy budget accordingly.

Overall, the contributions of Andrade et al. (2016) have helped to advance the field of privacy-preserving spatial data analysis. Their proposed algorithm and privacy budget optimization method have made it easier to apply the geo-indistinguishability model in practice, and their framework provides a useful guide for researchers and practitioners interested in privacy-preserving spatial data analysis.

Table 2.2: Summary of the research gaps for the geo-indistinguishability model

	Major Focus	**Research Focus Gaps**
1	*Strong privacy protection*—The privacy-preserving geo-indistinguishability model proposed by Andrade et al. (2016) provides strong privacy protection by adding noise to the location data, making it difficult for an attacker to infer the exact location of an individual. This has been highlighted in several studies, including Chen et al. (2019) and Jiao et al. (2020).	*Assumption of static locations* - The model assumes that the locations of individuals are static and don't change over time. This is not true in real-world scenarios, making it difficult to protect the privacy of individuals. This limitation has been noted in several studies, including Zou et al. (2018) and Wang et al. (2020).
2	*Preservation of data utility* The algorithm proposed by Andrade et al. (2016) adds noise to the location data in a way that preserves the statistical properties of the data, allowing for meaningful spatial analysis to be performed. This has been noted in several studies, including Zou et al. (2018) and Xu et al. (2021).	*Budgetary Concerns* The privacy budget controls the amount of noise introduced to the data by determining the degree of privacy protection offered by the model. Depending on the particular use case, the privacy budget must be carefully selected to strike a compromise between privacy and utility. Numerous investigations, such as Chen et al. (2019) and Xu et al. (2021), have identified this restriction.
3	*Scalability and efficiency* The quadtree-based partitioning scheme used by the algorithm allows for the data to be partitioned into smaller cells, making it scalable and efficient for use with large datasets. This has been highlighted in several studies, including Wang et al. (2020) and Vatsalan et al. (2019).	*Euclidean distance limitation* The model only considers Euclidean distance between locations, which may not be appropriate for all applications. For example, it may not be suitable for measuring distances on a network or road network. This limitation has been noted in several studies, including Zou et al. (2018) and Wang et al. (2020).

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VIII August 2026

DP-SGD (Differentially Private Stochastic Gradient Descent) Model

In 2016, Abadi et al. introduced a machine learning technique that protects privacy. Differential privacy is incorporated into this model, which is an extension of the well-known stochastic gradient descent process, to safeguard the training data's privacy. Without jeopardizing the privacy of those who provided the data, DP-SGD provides a way to train machine learning models on sensitive data (Abadi et al., 2016). At each stage of the stochastic gradient descent method, the DP-SGD model adds random noise to the objective function's gradient. To guarantee that the method satisfies a predetermined degree of differential privacy, this noise is meticulously tuned. By varying the amount of noise supplied to the gradient, one can change the algorithm's privacy guarantee. DP-SGD is intended to achieve a balance between privacy and accuracy, allowing machine learning models to be trained with reasonable accuracy while protecting the privacy of the training data (Abadi et al., 2016).

Table 2.3: Summary of the research gaps identified in the DP-SGD model.

	Major Focus	**Research Focus Gaps**
1	*Privacy Preservation* provides a rigorous guarantee of privacy preservation. The algorithm ensures that the training process does not leak any sensitive information from the training data, even when the data is highly sensitive.	*Increased Computational Complexity* *DP-SGD* has additional computations that ensure privacy preservation, which can increase the computational complexity of the training process. This makes training times slower than non-private approaches.
2	*Flexibility* DP-SGD can be applied to a wide range of machine-learning problems, including classification, regression, and clustering. It can also be used with a variety of different types of neural networks, including deep neural networks and convolutional neural networks.	*Reduced Model Utility* The privacy guarantees provided by DP-SGD come at the cost of reduced model utility. This means that the accuracy of the trained model may be lower than that of a model trained without privacy guarantees.
3	*High Accuracy:* DP-SGD can achieve high accuracy even when the training data is noisy or incomplete. This is because the algorithm is designed to work with noisy data and can adapt to the noise in the data.	*Hyperparameter Tuning:* DP-SGD requires the tuning of hyperparameters, like the privacy budget and learning rate, to achieve the desired level of privacy and accuracy. This can be a time-consuming and challenging process.

Private Aggregation of Teacher Ensembles Model.

This machine-learning architecture protects privacy (Papernot et al., 2018). The Pate framework is made to make it possible to train reliable and accurate models on confidential data. Several "teacher" models, each with its own parameters and biases, are trained on various subsets of the data in order for this system to function. A smaller set of "student" models trained on non-sensitive data are then labeled using the teacher models. While the teachers' individual predictions are kept confidential, the student models are trained to provide a consensus prediction based on the teacher models' projections. Predictions on sensitive data are then made using this consensus forecast.

Differential privacy and federated learning are two important privacy strategies used by Pate. To prevent any specific training example from being deduced from the output, differential privacy adds noise to the teaching models' output. Federated learning maintains privacy by allowing student models to be trained on a central server without necessitating the transfer of sensitive data to that server (Papernot et al., 2018).

Table 2.4: Summary of the research gaps identified for the PATE model.

	Major Focus	**Research Focus Gaps**
1	*Privacy preservation—This* model allows for the training of accurate machine learning models while preserving the privacy of individual data points. Since the individual data points are never directly exposed to the model, there is no risk of sensitive information being revealed.	*Elevated levels of computation* Since the PATE model uses multiple teacher models, it requires more computational power than traditional models, which increases the time and cost required for training.
2	*Improved data protection—The* model enables a higher level of data protection than traditional models because the model does not have direct access to the data. Instead, it only receives the aggregate results of multiple teacher models, which makes it much more difficult to extract specific data points from the model.	*Limited data sharing*—The model requires data to be divided into subsets for each teacher model, which can limit the amount of data that can be shared between different organizations or parties.
3	*Improvement in accuracy*—Since the model uses multiple teacher models, it achieves higher accuracy than traditional models that only use one model. This is because the teacher models can each learn various aspects of the data, and the student model can then combine their knowledge.	*The trade-off between privacy and accuracy—in* some cases, the model sacrifices accuracy to preserve privacy. For example, if the number of teacher models is limited, the model cannot learn as much from the data as it would with more models.

Machine Learning Models that Utilize Differential Privacy.

The SPDZ protocol is a cryptographic protocol designed for secure computation among parties. It is particularly relevant in privacy-preserving machine learning (PPML) and deep learning applications.

Sensitive data from various sources, such as actual healthcare data, can frequently be trained into machine learning models. Research has shown that the SPDZ protocol will make it possible to securely aggregate data from several sources and train the model on encrypted data without disclosing raw values. Deep learning models need a lot of processing power, and SPDZ allows models to be trained on encrypted data. Among other things, it facilitates training on encrypted pictures for facial recognition and medical diagnosis, privacy-preserving backpropagation in gradient-based learning, and secure matrix multiplications that are crucial for deep learning layers (Mishra et al., 2020).

Using federated learning, differential privacy (DP), and secure multi-party computation (SMPC), a number of recent research have investigated privacy-preserving deep learning in healthcare. A framework combining secure aggregation, DP, and federated learning for medical imaging categorization was presented by Fares and Emam Saad (2024). Their work highlighted the viability in privacy-sensitive healthcare settings by showing that hospitals can cooperatively train models without disclosing raw patient data while maintaining accuracy similar to centralized training.

Jarin and Eshete (2021) introduced the PRICURE system, which combines SMPC with DP for collaborative neural network inference on medical datasets. The study showed that privacy guarantees could be maintained without significantly compromising model utility, making it suitable for multi-institutional healthcare applications. Similarly, Choquette-Choo et al. (2021) developed CaPC Learning, a framework ensuring confidentiality of data and intermediate computations through SMPC and privacy-preserving techniques, emphasizing the relevance of hybrid privacy methods in healthcare collaborations.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VIII August 2026

Das et al. (2024) focused on improving the efficiency of secure multi-party deep learning by integrating DP with communication-optimized cryptographic protocols. Their approach reduces computation and communication overhead while maintaining strong privacy, which is particularly useful for collaborative healthcare modeling across institutions. Sharma et al. (2025) demonstrated an SPDZ-based SMPC framework for training deep learning models on encrypted clinical datasets, highlighting both privacy protection and practical deployment challenges, including computational and communication costs.

Zhang et al. (2025) proposed an optimized MPC protocol for deep learning that reduces communication rounds and computational load while preserving privacy, supporting scalable applications in distributed healthcare settings. Studies focusing on differential privacy include Enhance DP for Clinical Data Analysis (2025), which applied DP mechanisms to CNN and reinforcement learning models for clinical decision-making. By carefully calibrating noise, the framework protected individual patient data while retaining predictive utility, illustrating the privacy-accuracy trade-offs.

Privacy-aware Hierarchical Federated Learning (2025) integrated DP and SMPC in a hierarchical federated learning system, enabling large-scale collaborative training across hospitals. The study demonstrated that combining these techniques provides formal privacy guarantees while supporting scalable and practical AI applications in healthcare.

Table 3: Summary of reviewed literature

Author(s) & Year	**Techniques Used**	**Summary / Focus**	**Pros of the secure hybrid deep learning model**
Fares & Emam Saad (2024)	Federated Learning + Differential Privacy + Secure Aggregation	Privacy-preserving medical imaging using ResNet; hospitals collaborate without sharing raw images; maintains near-centralized accuracy	SPDZ + DP can perform secure computation on raw data before aggregation, protecting inputs even more strongly while still allowing DP to preserve output privacy
Jarin & Eshete (2021)	SMPC + Differential Privacy	PRICURE: Multi-party neural network inference with DP; protects sensitive patient data without sharing raw data	Hybrid model enhances protection by securing computations with SPDZ, reducing reliance on trust in other parties and strengthening privacy against internal leakage
Choquette-Choo et al. (2021)	SMPC + Privacy Techniques	CaPC Learning: Confidential and private collaborative learning; data and intermediate computations kept confidential	SPDZ + DP adds formal statistical privacy guarantees (DP) on outputs, complementing SMPC's cryptographic privacy to mitigate inference attacks
Das et al. (2024)	DP + SMPC	Communication-efficient secure multi-party deep learning; reduces overhead while maintaining privacy	SPDZ and DP can further optimize computation by selectively applying DP to sensitive outputs while computing gradients securely, thus achieving higher privacy with maintained accuracy.
Sharma et al. (2025)	SPDZ-based SMPC	Multi-party neural network training on encrypted clinical datasets	By integrating DP, the hybrid model also protects model outputs, preventing re-identification or membership inference attacks beyond what SPDZ alone achieves.
Zhang et al. (2025)	Optimized SMPC Protocol	Efficient and scalable MPC for deep learning; reduces	SPDZ + DP provides both efficiency and output-level privacy, surpassing SMPC-

		communication and computation costs	only approaches in threat coverage and regulatory alignment
Enhance DP for Clinical Data Analysis (2025)	Differential Privacy (DP) in CNN & RL	Protects individual patient contributions while performing predictive modeling in clinical datasets; balances privacy-accuracy trade-off	The hybrid model reduces DP-induced accuracy loss by computing most operations securely under SPDZ and applying DP selectively to outputs, improving model utility.
Privacy-aware Hierarchical Federated Learning (2025)	DP + SMPC	Large-scale hierarchical federated learning for healthcare preserves patient privacy across hospitals.	SPDZ + DP strengthens both input-level protection and output-level DP guarantees, improving threat resilience and enabling cross-hospital collaboration with minimal privacy risk.

The SPDZ protocol is a cryptographic protocol designed for secure computation among parties. It is particularly relevant in privacy-preserving machine learning (PPML) and deep learning applications.

Sensitive data from various sources, such as actual healthcare data, can frequently be trained into machine learning models. The SPDZ protocol will make it possible to securely aggregate data from several sources and train the model on encrypted data without disclosing raw values. Deep learning models need a lot of processing power, and SPDZ allows models to be trained on encrypted data. Among other things, it facilitates training on encrypted pictures for facial recognition and medical diagnosis, privacy-preserving backpropagation in gradient-based learning, and secure matrix multiplications that are crucial for deep learning layers (Mishra et al., 2020).

Using federated learning, differential privacy (DP), and secure multi-party computation (SMPC), a number of recent research have investigated privacy-preserving deep learning in healthcare. A framework combining secure aggregation, DP, and federated learning for medical imaging categorization was presented by Fares and Emam Saad (2024). Their work highlighted the viability in privacy-sensitive healthcare settings by showing that hospitals can cooperatively train models without disclosing raw patient data while maintaining accuracy similar to centralized training.

Jarin and Eshete (2021) introduced the PRICURE system, which combines SMPC with DP for collaborative neural network inference on medical datasets. The study showed that privacy guarantees could be maintained without significantly compromising model utility, making it suitable for multi-institutional healthcare applications. Similarly, Choquette-Choo et al. (2021) developed CaPC Learning, a framework ensuring confidentiality of data and intermediate computations through SMPC and privacy-preserving techniques, emphasizing the relevance of hybrid privacy methods in healthcare collaborations.

Das et al. (2024) focused on improving the efficiency of secure multi-party deep learning by integrating DP with communication-optimized cryptographic protocols. Their approach reduces computation and communication overhead while maintaining strong privacy, which is particularly useful for collaborative healthcare modeling across institutions. Sharma et al. (2025) demonstrated an SPDZ-based SMPC framework for training deep learning models on encrypted clinical datasets, highlighting both privacy protection and practical deployment challenges, including computational and communication costs.

Zhang et al. (2025) proposed an optimized MPC protocol for deep learning that reduces communication rounds and computational load while preserving privacy, supporting scalable applications in distributed healthcare settings. Studies focusing on differential privacy include Enhance DP for Clinical Data Analysis (2025), which applied DP mechanisms to CNN and reinforcement learning models for clinical decision-making. By carefully calibrating noise, the framework protected individual patient data while retaining predictive utility, illustrating the privacy-accuracy trade-offs.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VIII August 2026

Privacy-aware Hierarchical Federated Learning (2025) integrated DP and SMPC in a hierarchical federated learning system, enabling large-scale collaborative training across hospitals. The study demonstrated that combining these techniques provides formal privacy guarantees while supporting scalable and practical AI applications in healthcare.

Table 4: Summary of privacy-preserving deep learning studies in healthcare, techniques used, and how the hybrid SPDZ + Differential Privacy (DP) model enhances privacy, accuracy, and scalability compared to previous approaches.

Author(s) & Year	Techniques Used	Summary/Focus	Pros of the Secure Hybrid Deep Learning Model
Fares & Emam Saad (2024)	Federated Learning + DP + Secure Aggregation	Privacy-preserving medical imaging; collaborative model training without sharing raw images	SPDZ + DP secures computations on raw data and adds output-level DP guarantees, preserving accuracy and privacy.
Jarin & Eshete (2021)	SMPC + DP	PRICURE: Multi-party neural network inference; protects patient data	The hybrid model strengthens privacy via SPDZ, thus reducing reliance on trust and mitigating internal leakage.
Choquette-Choo et al. (2021)	SMPC + Privacy Techniques	CaPC Learning: Confidential collaborative learning; protects intermediate computations	SPDZ + DP adds formal statistical privacy to outputs, mitigating inference attacks.
Das et al. (2024)	DP + SMPC	Communication-efficient SMPC with DP reduces overhead.	SPDZ + DP enables secure gradient computation and selective DP, enhancing privacy without reducing utility.
Sharma et al. (2025)	SPDZ-based SMPC	Training on encrypted clinical datasets	Integrating DP protects outputs against inference attacks, while SPDZ secures inputs.
Zhang et al. (2025)	Optimized SMPC Protocol	Efficient and scalable MPC for deep learning	SPDZ + DP enhances efficiency while providing output-level privacy.
Journal of Big Data (2025)	DP in CNN & RL	Protects individual contributions in clinical datasets	The hybrid model reduces DP-induced accuracy loss by secure SPDZ computation.
Privacy-aware HFL (2025)	DP + SMPC	Large-scale hierarchical federated learning across hospitals	SPDZ + DP strengthens input and output-level privacy, enabling scalable cross-hospital collaboration.

Solution for Data Privacy in Healthcare

The sensitive nature of medical information and the expanding use of data-driven diagnoses have made protecting patient privacy in the healthcare industry more important than ever. When it comes to facilitating collaborative analysis or deep learning on distributed datasets, traditional data protection techniques frequently fall short. In this regard, developments in Multi-Party Computation (MPC) protocols, like SPDZ and its variations, present viable options for carrying out safe, private computations across various healthcare data sources.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VIII August 2026

Recurrent neural networks (RNNs) process sequential data, such as time series and natural language. Here, the SPDZ protocol helps secure text classification and speech recognition by processing encrypted sequences, privacy-preserving sentiment analysis, avoiding direct access to sensitive user text, and financial forecasting on encrypted stock market data (Riazi et al., 2019). Convolutional neural networks (CNNs) process images and videos, often containing private information. In this case, the SPDZ protocol will enable secure image classification, thus ensuring privacy in medical imaging, privacy-preserving facial recognition by securing biometric data, and encrypted training of CNNs for sensitive surveillance applications (Rouhani et al., 2018).

Recurrent Neural Networks (RNNs) are widely used to process sequential data, including time series, natural language, and speech (Riazi et al., 2019). In privacy-sensitive applications, the SPDZ protocol enables secure computation on encrypted sequences. This allows for privacy-preserving text classification, sentiment analysis, speech recognition, and even financial forecasting on encrypted stock market data. The combination of RNNs with SPDZ ensures that sensitive user information or proprietary sequences are never exposed during model training or inference.

Convolutional Neural Networks (CNNs) are designed for image and video processing, which often contain private or sensitive information. Integrating CNNs with the SPDZ protocol allows for secure image classification, privacy-preserving facial recognition, and encrypted training for surveillance or medical imaging applications (Rouhani et al., 2018). By operating on encrypted data, SPDZ protects individual privacy while enabling accurate feature extraction and classification, making CNNs suitable for sensitive real-world applications.

Table 5: Applications of RNNs and CNNs with SPDZ for Privacy-Preserving Machine Learning

Neural Network	Data Type	Privacy-Preserving Application	Reference
RNN	Sequential (text, speech, time series)	Secure text classification, sentiment analysis, speech recognition, financial forecasting on encrypted data	Riazi et al., 2019
CNN	Images and videos	Secure image classification, privacy-preserving facial recognition, encrypted training for medical imaging and surveillance	Rouhani et al., 2018

With the above literature, SPDZ could allow privacy-preserving analysis of CBIS-DDSM mammograms and associated metadata. For example, RNNs can be adapted for sequential or metadata-based tasks, and CNNs can be used for secure image classification and tumor detection on encrypted mammographic images, all while ensuring that sensitive patient data remains confidential during training and inference. This approach would support privacy-aware deep learning on CBIS-DDSM without exposing raw data, combining advances in secure computation with established medical imaging benchmarks.

Emerging Multi-Party Computation (MPC) protocols, such as SPDZ and its derivatives, are coming up and have improved efficiency and scalability for deep learning tasks. These protocols enable the secure computation of

gradients and other operations essential for training neural networks across distributed datasets. The challenges, however, remain, including optimizing the MPC protocols for large-scale datasets and improving their computational efficiency without compromising security. Nevertheless, ongoing research efforts are needed to refine MPC techniques for broader adoption in privacy-sensitive applications, such as healthcare diagnostics (Goswami, 2024).

Research has shown that the SPDZ protocol provides secure frameworks for computing gradients and aggregating model updates across distributed datasets. These protocols ensure that individual data remains encrypted and confidential throughout the training process, mitigating risks associated with data breaches and privacy violations (Goswami, 2024).

Training with secure multi-party computation uses data encryption that addresses security problems during data training. Likewise, the network can also be rendered safe by the use of an encrypted model that solves the security issue of model owners. This ensures that the privacy needs of customer data are well catered for and thus delivers a more satisfying experience to address security concerns in this untrusted environment testing (Sayyad, 2020).

REFERENCES

1. Choquette-Choo, C. A., Dullerud, N., Dziedzic, A., Zhang, Y., Jha, S., Papernot, N., & Wang, X. (2021). Capc learning: Confidential and private collaborative learning. arXiv preprint arXiv:2102.05188.
2. Das, S., Chowdhury, S. R., Chandran, N., Gupta, D., Lokam, S., & Sharma, R. (2025). Communication-efficient, secure, and private multi-party deep learning. Proceedings on Privacy Enhancing Technologies.
3. Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. Foundations and Trends® in Theoretical Computer Science, 9(3–4), 211-407.
4. Fares, M. H., & Emam Saad, A. M. S. (2024). Towards privacy-preserving medical imaging: Federated learning with differential privacy and secure aggregation using a modified ResNet architecture.
5. Hassan, M. U., Rehmani, M. H., & Chen, J. (2019). Differential privacy techniques for cyber-physical systems: A survey. IEEE Communications Surveys Tutorials, 1-1. [Advance online publication]. https://doi.org/10.1109/COMST.2019.2906131
6. International Organization for Standardization. ISO 9000:2015, Quality Management Systems—Fundamentals and Vocabulary, 5th ed.; International Organization for Standardization: Geneva, Switzerland, 2015.
7. Jarin, I., & Eshete, B. (2021). PRICURE: Privacy-preserving collaborative inference in a multi-party setting.
8. Joshi, R., Negi, S., & Sachdeva, S. (2021). Cloud-Based Interoperability in Healthcare. In Computational methods and data engineering (pp. 599-611). Springer, Singapore.
9. Kaissis, G., Ziller, A., Ryffel, T., Usynin, D., Trask, A., Lima, I., Mancuso, J., Jungmann, F., Steinborn, M., Saleh, A., Makowski, M., Rueckert, D., & Braren, R. (2021). End-to-end privacy-preserving deep learning on multi-institutional medical imaging. Nature Machine Intelligence, 3(6), 473-484. https://doi.org/10.1038/s42256-021-00337-8
10. Kasyap, H., & Tripathy, S. (2021). Privacy-preserving decentralized learning framework for the healthcare system. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 17(2s), 1-24.
11. Knott, B., Venkataraman, S., Hannun, A., Sengupta, S., Ibrahim, M., & van der Maaten, L. (2021). Crypten: Secure multi-party computation meets machine learning. Advances in Neural Information Processing Systems, 34, 4961-4973.
12. Konečný, J., McMahan, H. B., Ramage, D., & Richtárik, P. (2016). Federated optimization: Distributed machine learning for on-device intelligence. arXiv preprint arXiv:1610.02527.
13. Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security techniques for the electronic health records. Journal of Medical Systems, 41(8), 127. https://doi.org/10.1007/s10916-017-0778-4
14. Kuhn, M., & Johnson, K. (2013). Applied predictive modeling (Vol. 26, p. 13). New York: Springer.
15. Kumar, N., Rathee, M., Chandran, N., Gupta, D., Rastogi, A., & Sharma, R. (2020, May). Cryptflow: Secure tensorflow inference. In 2020 IEEE Symposium on Security and Privacy (SP) (pp. 336-353). IEEE.

16. Kuo, T. T., & Ohno-Machado, L. (2018). Modelchain: A decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks. arXiv preprint arXiv:1802.01746.
17. Kussel, T., Brenner, T., Tremper, G., Schepers, J., Lablans, M., & Hamacher, K. (2022). Record linkage-based patient intersection cardinality for rare disease studies using Mainzelliste and secure multi-party computation. Journal of translational medicine, 20(1), 458.
18. Lee, R. S., Gimenez, F., Hoogi, A., Miyake, K. K., Gorovoy, M., & Rubin, D. L. (2017). A curated mammography data set for use in computer-aided detection and diagnosis research. Scientific data, 4(1), 1-9.
19. Lee S, Kim J, Kwon Y, Kim T, Cho S Privacy Preservation in Patient Information Exchange Systems Based on Blockchain: System Design Study J Med Internet Res 2022;24(3):e29108 URL: https://www.jmir.org/2022/3/e29108 DOI: 10.2196/29108
20. Li, Q., Wen, Z., Wu, Z., Hu, S., Wang, N., Li, Y., ... & He, B. (2021). A survey on federated learning systems: Vision, hype and reality for data privacy and protection. IEEE Transactions on Knowledge and Data Engineering, 35(4), 3347-3366.
21. M. Li, X. Yue, W. Jiang, H. Wang, Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. PMID: 27565509. https://doi.org/10.1007/ s10916-016-0574-6
22. Y. Li, Z. Zhang, M. Winslett, and Y. Yang. Compressive Mechanism: Utilizing Sparse Representation in Differential Privacy. WPES, 2011.
23. Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2017, October). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In 2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC) (pp. 1-5). IEEE.
24. Liu, J., Tian, Y., Zhou, Y., Xiao, Y., & Ansari, N. (2020). Privacy-preserving distributed data mining based on secure multi-party computation. Computer Communications, 153, 208-216.
25. 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.
26. Luo, E., Bhuiyan, M. Z. A., Wang, G., Rahman, M. A., Wu, J., & Atiquzzaman, M. (2018). Privacy protector: Privacy-protected patient data collection in IoT-based healthcare systems. IEEE Communications Magazine, 56(2), 163-168.
27. Malek, M., Mironov, I., Prasad, K., Shilov, I., & Tramèr, F. (2021). Antipodes of label differential privacy: PATE and ALIBI. arXiv preprint arXiv:2106.03408.
28. Manogaran, G., Thota, C., Lopez, D., & Sundarasekar, R. (2017). Big data security intelligence for healthcare industry 4.0. In Cybersecurity for Industry 4.0 (pp. 103-126). Springer, Cham.
29. Marinič, M. (2015). The importance of health records. Health, 7(5), 617-624.
30. McLeod, A., & Dolezel, D. (2018). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology in Society, 54, 1–10. https://doi.org/10.1016/j.techsoc.2018.01.009
31. McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017, April). Communication-efficient learning of deep networks from decentralized data. In Artificial Intelligence and Statistics (pp. 1273-1282). PMLR.
32. Michael, O. R., & Rabin, M. O. (1981). How to exchange secrets by oblivious transfer. Technical report, Aiken Computation Laboratory. Harvard University.
33. Mittal, M., Sangani, R., & Srivastava, K. (2015). Testing data integrity in distributed systems. Procedia Computer Science, 45, 446-452.
34. Y.-A. De Montjoye, L. Radaelli, V. K. Singh et al., "Unique in the shopping mall: On the reidentifiability of credit card metadata," Science, vol. 347, no. 6221, pp. 536–539, 2015.
35. Moody DL, Shanks GG. Improving the quality of data models: Empirical validation of a quality management framework. Inf Syst. 2003;28:619–650.
36. Nasr, M., Shokri, R., & Houmansadr, A. (2018, October). Machine learning with membership privacy using adversarial regularization. In Proceedings of the 2018 ACM SIGSAC conference on computer and communications security (pp. 634-646).
37. Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2019). Blockchain for secure EHRs sharing of mobile cloud-based e-health systems. IEEE Access, 7, 66792-66806.
38. Niu, S., Chen, L., Wang, J., & Yu, F. (2019). Electronic health record sharing scheme with searchable attribute-based encryption on blockchain. IEEE Access, 8, 7195-7204.

39. Nogueira, E., Moreira, A., Lucrédio, D., Garcia, V., & Fortes, R. (2016). Issues on developing interoperable cloud applications: definitions, concepts, approaches, requirements, characteristics and evaluation models. Journal of Software Engineering Research and Development, 4(1), 1-23.
40. Nyaga, B. N. (2016). Information Security And Service Delivery In Health Sector: Case Study of Chogoria Hospital (Doctoral dissertation, School Of Business, University of Nairobi).
41. Olaronke, I., & Oluwaseun, O. (2016, December). Big data in healthcare: Prospects, challenges and resolutions. In 2016 Future Technologies Conference (FTC) (pp. 1152-1157). IEEE.
42. Oluoha, O. M., Odeshina, A. B. I. S. O. L. A., Reis, O. L. U. W. A. T. O. S. I. N., Okpeke, F. R. I. D. A. Y., Attipoe, V. E. R. L. I. N. D. A., & Orieno, O. (2023). A privacy-first framework for data protection and compliance assurance in digital ecosystems. Iconic Research and Engineering Journals, 7(4), 620-646.
43. Owusu-Agyemang, K., Qin, Z., Benjamin, A., Xiong, H., & Qin, Z. (2021). Guaranteed distributed machine learning: Privacy-preserving empirical risk minimization. Mathematical Biosciences and Engineering, 18(4), 4772-4796.
44. Papernot, N., Song, S., Mironov, I., Raghunathan, A., Talwar, K., & Erlingsson, Ú. (2018). Scalable private learning with pate. arXiv preprint arXiv:1802.08908.
45. Park, Y. S., Konge, L., & Artino Jr, A. R. (2020). The positivism paradigm of research. Academic medicine, 95(5), 690-694.
46. Park KJ, Alvarado-Cabrero I, Duggan MA, Kiyokawa T, Mills AM, Ordi J, Otis CN, Plante M, Stolnicu S, Talia KL, Wiredu EK, Lax SF, McCluggage WG (2021). Carcinoma of the Cervix Histopathology Reporting Guide. 5th edition. International Collaboration on Cancer Reporting; Sydney, Australia. ISBN: 978-1-922324-43-6.
47. K. Peterson, R. Deeduvanu, P. Kanjamala, K. Boles, A blockchain-based approach to health information exchange networks (2016).
48. Phan, T. C., & Tran, H. C. (2023). Consideration of data security and privacy using machine learning techniques. International Journal of Data Informatics and Intelligent Computing, 2(4), 20-32.
49. Pierrelouis, N. (2025). Optimizing Differential Privacy Parameters in Machine Learning Healthcare Models: Implementation and Pre-Deployment for Medical Device Data (Doctoral dissertation, Marymount University).
50. Piligrimiene Z, Buciuuiene I. Exploring managerial and professional view to healthcare service quality. Journal of Economics and Management. 2011; 16: 1304-1317.
51. Rahman, M., Gupta, P., & Singh, R. (2019). Schema Matching and Data Integration: Challenges and Opportunities. International Journal of Data Management, 6(3), 88-102.
52. Riazi, M. S., Rouani, B. D., & Koushanfar, F. (2019). Deep learning on private data. IEEE Security & Privacy, 17(06), 54-63.
53. Rogaway, P., & Shrimpton, T. (2004). Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In Fast Software Encryption: 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004. Revised Papers 11 (pp. 371-388). Springer Berlin Heidelberg.
54. Roh, Y., Heo, G., & Whang, S. E. (2019). A Survey on Data Collection for Machine Learning. IEEE, 1-20.
55. Rumbold, J. M., & Pierscionek, B. K. (2018). What are data? A categorization of the data sensitivity spectrum. Big data research, 12, 49-59.
56. Sabater, C. (2022). Efficient and robust protocols for privacy-preserving semi-decentralized machine learning (Doctoral dissertation, Université de Lille).
57. Sajid, A., & Abbas, H. (2016). Data privacy in cloud-assisted healthcare systems: state of the art and future challenges. Journal of Medical Systems, 40(6), 1-16.
58. Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. Journal of Information System Security, 10(3).
59. Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications and research directions. SN computer science, 2(3), 160.
60. Sawyer-Lee, R., Gimenez, F., Hoogi, A., & Rubin, D. (2016). Curated breast imaging subset of digital database for screening mammography (CBIS-DDSM).

61. Sayyad, S. (2020, July). Privacy preserving deep learning using secure multiparty computation. In 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 139-142). IEEE.
62. Schneble, C. O., Elger, B. S., & Shaw, D. M. (2018). The impact of Big Data on the doctor-patient relationship. Bioethics, 32(4), 237–244. https://doi.org/10.1111/bioe.12430
63. Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare Data Breaches: Insights and Implications. Healthcare (Basel, Switzerland), 8(2), 133. https://doi.org/10.3390/healthcare8020133
64. Shamir, A. (1979). How to share a secret. Communications of the ACM, 22(11), 612-613.
65. Sharma, S., Xing, C., & Liu, Y. (2019). Privacy-preserving deep learning with SPDZ. In The AAAI Workshop on Privacy-Preserving Artificial Intelligence (Vol. 4).
66. Shen, N., Bernier, T., Sequeira, L., Strauss, J., Silver, M. P., Carter-Langford, A., & Wiljer, D. (2019). Understanding the patient privacy perspective on health information exchange: a systematic review. International Journal of Medical Informatics, 125, 1-12.
67. Shenoy, A., & Appel, J. M. (2017). Safeguarding confidentiality in electronic health records. Cambridge Q. Healthcare Ethics, 26(2), 337-343.
68. Shepherd, D. (2017, 11 29). Cloud interoperability and portability – necessary or nice-to-have? Retrieved 6 12, 2022, from https://insightaas.com.
69. Shokri, R., & Shmatikov, V. (2015). Privacy-preserving deep learning. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (pp. 1310-1321).
70. Simsion GC, Witt GC. Data Modeling Essentials. 3rd ed. Amsterdam; Boston: Morgan Kaufmann Publishers; 2005.
71. Singh, J. P., Aqsa, A., Ghani, I., Sonani, R., & Govindarajan, V. (2025). Privacy-aware hierarchical federated learning in healthcare: integrating differential privacy and secure multi-party computation. Future Internet, 17(8), 345.
72. Sittig DF, Singh H. A new socio-technical model for studying health information technology in complex adaptive healthcare systems. In: Cognitive Informatics for Biomedicine. Cham: Springer; 2015. p. 59–80
73. Smith, S. W., & Koppel, R. (2014). Healthcare information technology's relativity problems: a typology of how patients' physical reality, clinicians' mental models, and healthcare information technology differ. Journal of the American Medical Informatics Association, 21(1), 117–131.
74. Sun, J., Zhu, X., Zhang, C., & Fang, Y. (2011, June). HCPP: Cryptography-based secure EHR system for patient privacy and emergency healthcare. In 2011 31st International Conference on Distributed Computing Systems (pp. 373-382). IEEE.
75. Supriya, M., & Deepa, A. J. (2020). Machine learning approach on healthcare big data: a review. Big Data and Information Analytics, 5(1), 58-75.
76. Tayyab, M., Marjani, M., Jhanjhi, N. Z., Hashem, I. A. T., Usmani, R. S. A., & Qamar, F. (2023). A comprehensive review on deep learning algorithms: Security and privacy issues. Computers & Security, 131, 103297.
77. Theodouli, A., Arakliotis, S., Moschou, K., Votis, K., & Tzovaras, D. (2018, August). On the design of a blockchain-based system to facilitate healthcare data sharing. In 2018 17th IEEE International Conference on Trust, Security, And Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE) (pp. 1374-1379). IEEE.
78. Tolk, A., Diallo, S., & Turnitsa, C. D. (2007). Applying the levels of conceptual interoperability model in support of integratability, interoperability, and composability for system-of-systems engineering. Journal of Systemics, Cybernetics, and Informatics, 5(5), 65-74.
79. Vimalachandran, P., Wang, H., Zhang, Y., Heyward, B., & Zhao, Y. (2017, December). Preserving patient-centered controls in electronic health record systems: A reliance-based model implication. In 2017 International Conference on Orange Technologies (ICOT) (pp. 37-44). IEEE.
80. Vora, J., Nayyar, A., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M. S., & Rodrigues, J. J. (2018, December). BHEEM: A blockchain-based framework for securing electronic health records. In 2018 IEEE Globecom Workshops (GC Wkshps) (pp. 1-6). IEEE.
81. Wang, D., Ye, M., & Xu, J. (2017). Differentially private empirical risk minimization revisited: Faster and more general. Advances in Neural Information Processing Systems, 30.

82. Wang, T., Blocki, J., Li, N., & Jha, S. (2017). Locally differentially private protocols for frequency estimation. In 26th USENIX Security Symposium (USENIX Security 17) (pp. 729-745).
83. Wang, T., & Li, S. (2022). Automating Data Integration: AI-driven Approaches in Large-Scale Systems. Journal of Intelligent Information Systems, 15(1), 45-60.
84. Warner, S. L. "Randomized Response: A Survey Technique for Eliminating Evasive Answer Bias." Journal of the American Statistical Association 60.309 (1965): 63-69.
85. Wei, J., Lin, Y., Yao, X., Zhang, J., & Liu, X. (2020). Differential privacy-based genetic matching in personalized medicine. IEEE Transactions on Emerging Topics in Computing, 9(3), 1109-1125.
86. Wei, K., Li, J., Ding, M., Ma, C., Yang, H. H., Farokhi, F., & Poor, H. V. (2020). Federated learning with differential privacy: Algorithms and performance analysis. IEEE transactions on information forensics and security, 15, 3454-3469.
87. Woods, A., Kramer, S. T., Xu, D., & Jiang, W. (2023). Secure Comparisons of Single Nucleotide Polymorphisms Using Secure Multiparty Computation: Method Development. JMIR Bioinformatics and Biotechnology, 4, e44700.
88. Xia, Q. I., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trustless medical data sharing among cloud service providers via blockchain. IEEE Access, 5, 14757-14767.
89. Xiao, X., & Tao, Y. (2015). Output perturbation techniques and privacy in data publishing. Foundations and Trends® in Databases, 7(1-2), 1-167.
90. Xie, L., Lin, K., Wang, S., Wang, F., & Zhou, J. (2018). Differentially private generative adversarial network. arXiv preprint arXiv:1802.06739.
91. Xu, C., Cheng, X., Hu, Y., Li, Y., & Li, X. (2017). PrivMets: A Secure and Efficient Framework for Privacy-Preserving Data Sharing. IEEE Transactions on Dependable and Secure Computing, 15(5), 794-807. doi: 10.1109/TDSC.2016.2531406
92. Yadav, N., Pandey, S., Gupta, A., Dudani, P., Gupta, S., & Rangarajan, K. (2023). Data privacy in healthcare: In the era of artificial intelligence. Indian Dermatology Online Journal, 14(6), 788-792.
93. Yao, A. C. (1982, November). Protocols for secure computations. In 23rd annual symposium on foundations of computer science (sfcs 1982) (pp. 160-164). IEEE.
94. Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: applying blockchain to securely and scalably share clinical data. Computational and structural biotechnology journal, 16, 267-278.
95. Zhang, S., Qu, G., Zhang, Z., Huang, M., Jin, H., & Yang, L. (2025). Efficient and secure multi-party computation protocol supporting deep learning. Cybersecurity, 8(1), 46.
96. Zhao, B. Z. H., Kaafar, M. A., & Kourtellis, N. (2020, November). Not one but many tradeoffs: Privacy vs. utility in differentially private machine learning. In Proceedings of the 2020 ACM SIGSAC Conference on Cloud Computing Security Workshop (pp. 15-26).