Machine Learning for Data Privacy and Protection: A Systematic Review of Current Approaches and Future Directions

OKETAYO ABIMBOLA
National Mathematical Centre, Abuja

Abstract- ***The rapid growth of data-driven technologies has raised significant concerns about data privacy, emphasizing the need for innovative solutions to safeguard sensitive information. Machine learning (ML) has emerged as a promising approach to protect data privacy, offering a range of techniques to prevent unauthorized data access, ensure secure data transmission, and maintain data confidentiality. This comprehensive review provides an in-depth examination of existing methods for data privacy protection in machine learning, highlighting their strengths, limitations, and applications in various domains. We reviewed prominent Machine Learning (ML) techniques, including data anonymization, encryption, access control, and differential privacy, and discuss their effectiveness in preventing data breaches and protecting sensitive information. Our analysis also identified future research directions, including the development of more robust ML model, the integration of ML with other privacy-enhancing technologies, and the investigation of ML-based solutions for emerging data privacy challenges. This survey aims to provide a valuable resource for researchers, practitioners, and policymakers seeking to leverage ML for data privacy protection and to stimulate further research in this critical area.***

Indexed Terms- ***Data Privacy, Machine Learning, survey, Data Protection, Privacy Preservation.***

I. INTRODUCTION

The proliferation of digital technologies has sparked significant concerns about data privacy, with vast amounts of personal data being collected, stored, and transmitted online (Bertino, 2016; Jafari et al., 2019). In response, machine learning (ML) has emerged as a promising solution to safeguard data privacy, leveraging techniques such as data anonymization (Sweeney, 2002), differential privacy (Dwork et al., 2006), secure multi-party computation (Yao, 1986), and homomorphic encryption (Gentry, 2009) to prevent unauthorized data access and maintain confidentiality (Chen et al., 2017; Li et al., 2019). ML has made significant strides in various fields, including healthcare (Esteva et al., 2017), finance (Sapunkov, 2019), and autonomous systems (Bojarski et al., 2016).

However, data privacy faces numerous challenges, including data breaches (Bertino, 2016), insider threats (Breck et al., 2017), and regulatory compliance (Zhang et al., 2020). Ensuring data privacy while facilitating data sharing and collaboration is a significant challenge (Chen et al., 2017). This paper presents a comprehensive review of ML approaches used in data privacy protection, focusing on practical systems that operate in realistic contexts. We employ a Systematic Literature Review (SLR) methodology, which is an efficient means of acquiring knowledge about the current state of research (Kitchenham & Charter, 2007). Our SLR utilizes several databases (e.g., Scopus, Web of Science, ACM Digital Library, and IEEE Xplorer) to gather papers through automatic search, followed by a rigorous selection, sorting, and analysis process. We explore the evaluation of various ML approaches, and examine the challenges associated with validating AI systems due to their complex requirements and adaptability.

1.1 Contribution to Knowledge

This study contributes to the knowledge of machine learning (ML) applications in data privacy protection, with the following key contributions:

1. Exploring ML's role in data privacy: This study investigates the effectiveness of ML in protecting data privacy and ensuring maximum security.

2. Addressing challenges in data privacy protection: It examines the challenges associated with different approaches to data privacy protection in a heterogeneous society and proposes solutions.

3. Highlighting ML's power in data security: The study showcases the potential of ML in safeguarding sensitive data from cyberattacks and ensuring data security.

4. Informing approaches to data privacy protection: It provides valuable insights into approaches to data privacy protection that can prevent cyberattacks.

5. Mitigating false alerts: The study addresses the issue of false alerts and explores how ML approaches can be used to prevent them.

6. Showcasing ML applications in data privacy: It offers a comprehensive overview of the applications of ML approaches in data privacy protection, highlighting their usefulness and potential.

1.2 Paper Organization

This study is structured into multiple sections. Section 1 introduces the research, highlights its contributions, and outlines the paper's organization. Section 2 reviews related works, examining current and previous studies. Section 3 describes the methodology used, detailing the systematic approach to the survey. Section 4 presents the survey results, while Section 5 discusses the findings. Section 6 explores the challenges of machine learning approaches in data security. Section 8 provides research recommendations, and Section 9 concludes with a summary of key points.

1.3 Challenges of Privacy and Protection of Data

1. Data Volume and Complexity: The vast amounts of diverse data pose significant challenges to protecting privacy, making it difficult to ensure that sensitive information is adequately safeguarded (Bertino, 2016).

2. Data Sharing and Collaboration: Sharing data between organizations or countries can compromise privacy, particularly when data is shared across jurisdictions with different regulatory frameworks (Chen et al., 2017).

3. Anonymization vs. Utility: Striking a balance between data anonymity and data utility is a challenge, as anonymization techniques can impact the usefulness of the data (Sweeney, 2002).

4. Emerging Technologies: New technologies like AI, IoT, and blockchain raise new privacy concerns, such as data collection, storage, and sharing (Esteva et al., 2017; Sapunkov, 2019).

5. Regulatory Compliance: Keeping up with changing regulations and laws is a challenge, particularly in the context of cross-border data transfers (Zhang et al., 2020).

6. Data Breaches: Preventing and responding to data breaches is a significant challenge, requiring robust security measures and incident response plans (Breck et al., 2017).

7. User Consent and Awareness: Obtaining informed consent and ensuring user awareness of data use is crucial, particularly in the context of data sharing and collaboration (Li et al., 2019).

8. Data Storage and Retention: Securely storing and managing data retention periods is essential, requiring robust data management practices (Kitchenham & Charters, 2007).

9. Cross-Border Data Transfers: Ensuring privacy across different jurisdictions and laws is complex, requiring careful consideration of regulatory frameworks and data protection laws (Chen, et al., 2017).

10. Balancing Privacy and Security: Finding the right balance between privacy and security needs is a challenge, requiring careful consideration of the trade-offs between these competing interests (Bertino, 2016).

II. PREVIOUS WORK: ML APPROACHES AND PRIVACY PROTECTION

2.1 Background

Machine Learning (ML) has been defined in various ways by different organizations. According to IEEE-USA (2017), ML is "the study of computer algorithms that improve automatically through experience,"

encompassing applications such as data mining and information filtering systems that learn from large datasets [IEEE-USA, 2017]. Similarly, Stanford University (2016) defines ML as "the science of getting computers to act without being explicitly programmed". At its core, ML relies on algorithms that can learn from data without relying on rules-based programming, as noted by McKinsey (2016). These definitions highlight the versatility and potential of ML in various fields, including privacy protection of data, where various approaches have been developed to leverage ML for safeguarding sensitive information (Chen et al; Li et al., 2019).

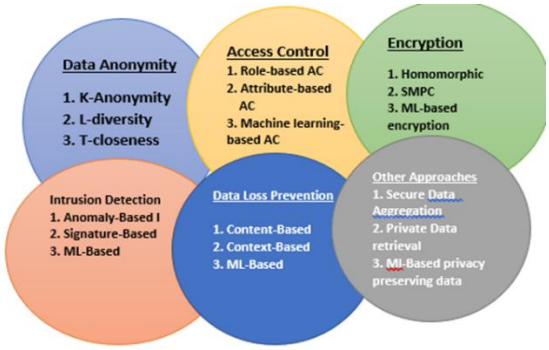

Figure 1: Different Machine Learning Approaches to privacy protection of Data

2.1.1 Machine learning approaches for privacy protection and preservation of data

A) Data Anonymization

Data anonymization is a technique used to protect sensitive information in datasets by removing or modifying personally identifiable information (PII) (Chen et al., 2017; Li et al., 2019). According to Machanavajjhala et al. (2006), data anonymization is crucial for safeguarding individual privacy. Machine learning (ML) approaches can be leveraged to anonymize data while preserving its utility for analysis and research (Chen et al., 2017; Li et al., 2019). Several data anonymization techniques have been developed, including:

K-anonymity: This technique, proposed by Sweeney (2002), ensures that each record in a dataset is identical to at least k-1 other records, making it difficult to identify individuals (Sweeney, 2002).

L-diversity: Introduced by Machanavajjhala et al. (2007), l-diversity ensures that each record in a dataset has at least l different values for a sensitive attribute, providing an additional layer of protection; and T-closeness: this technique, developed by Li et al. (2007), ensures that the distribution of sensitive attributes in a dataset is close to the distribution of the same attribute in the overall population, further protecting individual privacy. These data anonymization techniques aim to prevent individual records in a dataset from being identified, thereby protecting sensitive information and maintaining data privacy (Machanavajjhala, et al., 2019).

B) Access Control

Access control is a crucial aspect of data privacy protection, and machine learning (ML) approaches can be leveraged to enhance access control mechanisms (Chen et al., 2017; Li et al., 2019). ML can learn access patterns and grant access to data based on various access control models. For instance:

- Role-Based Access Control (RBAC): This approach grants access to data based on a user's role within an organization, as described by Sandhu et al. (1996). RBAC is a widely used access control model that ensures users have access to only the data and resources necessary for their roles.
- Attribute-Based Access Control (ABAC): This approach grants access to data based on a user's attributes, such as department or job function, as described by Hu et al. (2014). ABAC provides a more fine-grained access control mechanism than RBAC, allowing for more precise control over access to sensitive data.
- Machine Learning-Based Access Control: This approach uses ML algorithms to train on data and learn access patterns, granting access to data based on predicted user behavior, as described by Li et al. (2019). ML-based access control can provide an additional layer of security and flexibility in access control, adapting to changing user behavior and access patterns.

These access control models can be used to protect sensitive data and ensure that only authorized users have access to the data they need to perform their tasks.

C) Data Encryption

Data encryption is a widely used technique for protecting data privacy, and machine learning (ML)

approaches can be leveraged to optimize encryption methods (Chen et al., 2017; Li et al., 2019). Several encryption approaches have been developed, including:

- Homomorphic encryption: This technique, introduced by Gentry (2009), enables computations on encrypted data without decrypting it first, ensuring the confidentiality and security of sensitive data.
- Secure Multi-Party Computation (SMPC): This approach, developed by Yao (1982), enables multiple parties to jointly perform computations on private data without revealing their inputs, facilitating secure collaboration and data analysis.
- Machine Learning-Based Encryption: This approach uses ML algorithms to optimize encryption techniques, such as encryption key generation, as described by Gilad-Bachrach et al. (2016). ML-based encryption can enhance the security and efficiency of encryption methods, providing an additional layer of protection for sensitive data.

These encryption approaches can be used to protect data privacy and ensure the confidentiality, integrity, and security of sensitive information.

D) Differential Privacy

Differential privacy is a technique used to protect sensitive information by adding noise to data, ensuring that individual data points remain confidential (Chen, et al., 2017: Li et al., 2019). Machine learning (ML) approaches can be leveraged to optimize differential privacy techniques. Several differential privacy approaches have been developed, including:

- Differential Privacy: This technique, introduced by Dwork et al. (2006), ensures that the output of a computation does not reveal sensitive information about individual data points, providing a rigorous framework for protecting data privacy.
- Local Differential Privacy: This approach, developed by Dwork et al. (2014), ensures that individual data points are protected by adding noise to the data before it is collected, providing an additional layer of protection for sensitive information.
- Machine Learning-Based Differential Privacy: This approach uses ML algorithms to optimize differential privacy techniques, such as noise addition, as described by Abadi et al. (2016). ML-based differential privacy can enhance the accuracy and efficiency of differential privacy methods, providing a more effective way to protect sensitive data.

E) Intrusion Detection

Intrusion detection is a crucial aspect of data privacy protection, and machine learning (ML) approaches can be leveraged to detect intrusions and prevent data breaches (Chen et al., 2017; Li et al., 2019). Several types of intrusion detection methods have been developed, including:

- Anomaly-Based Intrusion Detection: This approach, introduced by Denning (1987), detects intrusions by identifying unusual patterns in network traffic that deviate from expected behavior.
- Signature-Based Intrusion Detection: This method, implemented in tools like Snort (2003), detects intrusions by identifying known patterns in network traffic that match predefined signatures.
- Machine Learning-Based Intrusion Detection: This approach uses ML algorithms to learn patterns in network traffic and detect intrusions, as described by Jiang et al. (2018) [4]. ML-based intrusion detection can enhance the accuracy and efficiency of intrusion detection systems, providing a more effective way to protect sensitive data. These intrusion detection methods can be used to protect data privacy and prevent data breaches by identifying and responding to potential security threats

F) Data Loss Prevention

Data loss prevention (DLP) is a critical technique for protecting sensitive information from unauthorized transmission or storage [1]. Machine learning (ML) approaches can be leveraged to enhance DLP by detecting and preventing sensitive data from being compromised. Several ML-based DLP approaches have been developed, including:

- Content-Based DLP: This approach detects and prevents sensitive data from being transmitted or

stored in unauthorized locations based on its content, as described by Kumar et al. (2019).

- Context-Based DLP: This technique detects and prevents sensitive data from being transmitted or stored in unauthorized locations based on its context, such as user behavior or environmental factors, as described by Kumar et al. (2019).
- Machine Learning-Based DLP: This approach uses ML algorithms to learn patterns in data transmission and storage, detecting and preventing sensitive data from being compromised, as described by Kumar et al. (2019). ML-based DLP can provide a more effective and efficient way to protect sensitive information. These DLP approaches can be used to protect sensitive data and prevent data breaches by identifying and responding to potential security threats.

2.2 Related Works

The advent of smart cities has led to an increased need for privacy protection of data, with individuals storing sensitive information on smart devices [1]. To address this concern, various approaches have been employed, including machine learning (ML) techniques. For instance, Jena et al. (2021) conducted a literature review on homomorphic encryption, a method that enables ML training and testing on encrypted data, thereby increasing consumer trust in privacy-preserving ML [2]. This approach ensures data privacy by using cryptography to protect data during analysis by multiple parties.

Similarly, Chew et al. (2017) developed a privacy-preserving method using ML, which combined decision tree techniques with other privacy protection methods, such as randomization and secure two-party computation. This approach protects users' data by ensuring that sensitive information remains confidential during analysis. These studies demonstrate the potential of ML-based approaches to protect data privacy in smart cities, where sensitive information is increasingly being stored and analyzed.

Anand and Janami (2017) proposed a strategy to address data privacy concerns in smart cities by integrating a mobile cloud framework with a key attributes-based encryption (KP-ABE) model [1]. This approach ensures that data is securely stored in the cloud and can only be accessed or collected after verification, thereby protecting users' data. Similarly, Oketayo's literature review highlights the effectiveness of machine learning (ML) approaches in protecting data privacy, particularly when combined with cryptography and access control [2]. By introducing data security level determination and data status level, ML-based approaches can prevent unauthorized access to users' data. Zhang et al. (2020) focused on testing ML model validation software, emphasizing the importance of offline testing in ensuring the reliability of ML models. However, Kumeno (2019) noted that validation remains a significant challenge in ML systems, underscoring the need for further research in this area. These studies demonstrate the potential of ML-based approaches to protect data privacy in smart cities, while also highlighting the challenges and complexities involved in ensuring the security and reliability of ML systems.

III. RESEARCH METHOD

The research method of this study is a survey method on ML approaches to privacy protection for the preservation of data. The literature search was conducted with four (4) databases (IEEE Xplore, Scopus, Web of Science, ACM Digital Library, Science Direct) and using semantically the same search string. After the search, three selection stages were applied to reduce the initial set of 3455 papers. The remaining final 300 papers were analyzed. The structure of the applied search and selection process is shown in figure 2. in addition, we looked for articles published between January 2015 and December 2024. However, we excluded any irrelevant articles and duplicated papers.

3.1 Search Keyword

T-he first phase of the search and selection process (see fig. 2) was to collect the initial set of papers by search scientific databases. The following steps were taken in conducting the search:

3.1.1 Relevant articles identification

Two search methodologies were employed to discover pertinent published papers. Initially, the English language was used to query the Eureka databases, which focuses on print media, utilizing the following keywords: “ML approaches and privacy protection of

data", "Privacy protection for preservation of data". ML enhanced approaches to data protection", "Privacy protection of data using ML", An improved ML model for privacy protection of data", ML enhanced model for privacy protection for data preservation", and "protecting Data privacy with ML: a survey".

Secondly, a Google News search was performed utilizing the same keywords to locate supplementary pertinent articles. relevant items were restricted to the period from January 2014 to December 2024. The initial search result produced 1,455 possible pertinent articles; 786 irrelevant items were removed, while 669 were included. The second review of the articles eliminated 380 duplicates. The third screening was systematic. The methodological screening yielded 256 results, after which uncorrelated studies were excluded. Thus, the relevant articles utilized became 200, as shown in Figure 2

3.1.2 Selection of relevant Articles

The paper selection was performed in three stages (figure 2) by the first Author, at this stage, all 1455 preliminary papers from the search were assessed and included using the inclusion criteria found below. At the second stage, the remaining 669 papers were assessed and excluded using the exclusion criteria. At the third stage, the remaining 256 papers were assessed based on their relevance, resulting in the final set of 200 papers.

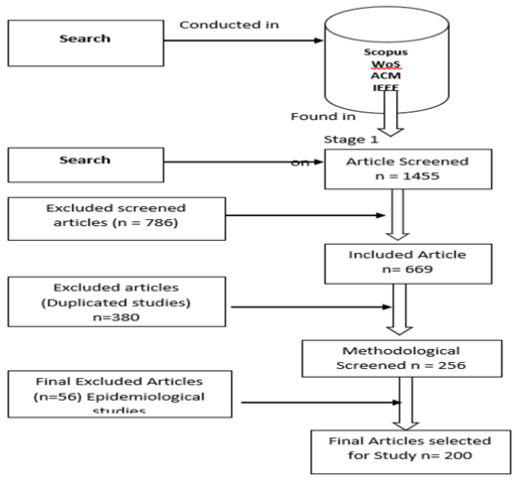

Figure 2: Selecting process and screening of Articles

3.1.2 Selection of relevant Articles

The paper selection was performed in three stages (figure 2) by the first Author, at this stage, all 1455 preliminary papers from the search were assessed and included using the inclusion criteria found below. At the second stage, the remaining 669 papers were assessed and excluded using the exclusion criteria. At the third stage, the remaining 256 papers were assessed based on their relevance, resulting in the final set of 200 papers.

A) Stage One

The first stage of selection yielded 669 papers. The selection was based on the title, abstract, and keywords of the papers and the inclusion criteria (ICs) below, both of which a paper had to fulfill; to be included.

IC1: The full paper text in English Language
IC2: The full paper text found in peer-reviewed journals
IC3 The full paper text in Journals, Conferences.
IC4: The paper discusses a method for privacy protection of data with ML approaches or papers that apply ML approaches for privacy protection of data.

The consequence of the second criterion (IC4) is that the focus is on the papers that acknowledge ML as an application. for example, the methods of ML model's ability to learn the behaviour of the user are not included or if the paper gives a strong indication that the proposed model is being used by someone as is even the main focus of the paper is ML model approaches. As using a model in a context implies the existence of at least a user interface and raises the model from technique to a product. (ISO, 2011).

B) Stage Two: The stage two of article selection resulted in 256 papers; the assessment was based on the full texts of the papers. A paper was excluded if at least one of the following exclusion criteria was met:

XC1: The full paper text was not available in English
Xc2: The full paper was not acquirable with reasonable effort
XC3: The paper turned out not to describe an ML approach as described above

XC4: The described approach or model turned out to have unrecognizable as ML
XC5: The paper was less than six pages long
XC6: The paper was published in a minor forum

XC1 was enforced by the prominent status of English Language in research, as to XC2, a paper was excluded if it could not be accessed in full through measures considered a normal information search. It is difficult to assess the effect such paper could have had, as we simply could not get our hand on them, but only a very small number of papers were excluded based on this criterion. From XC3-XC5, they are derived directly from our research topic. XC6 rose from the fact that workshop papers, opinion papers, and other grey literature often do not have much add to the SLRs when included as stated by Kitchenham et al (2010). We are more interested in detailed descriptions of the ML approaches, settings, and validation methods, which are the characteristics that the grey literature often lacks due to the preliminary nature of the results and to page limitations.

C) Stage Three
This is the final stage and contains set of 200 papers (Figure 2) was achieved in the third stage of the selection. The selection was made based on the relevance assessment of the papers gathered, so that only papers of high relevance were included. Relevance of each paper was measured by the degree of realism in the research settings. We decided to label the papers based on the relevance level.

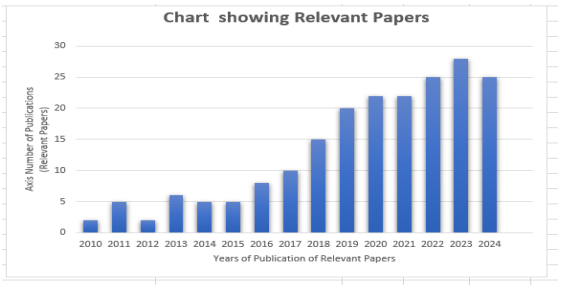

Figure 3: Chart showing the number of publications and year (Relevant papers) Exclusive and inclusive criteria were established to facilitate the removal of papers irrelevant to the primary research questions. Excluded papers include those that examined managerial perspectives on ML approaches and its integration into privacy protection for preservation of data as well as those that addressed broad concerns relating to ML approaches to privacy protection of data. ultimately, 56 articles were rejected during the screening process, while 200 articles were included from the 1455 papers evaluated, thus, representing 8% of the relevant papers identified, as shown in figure 4.

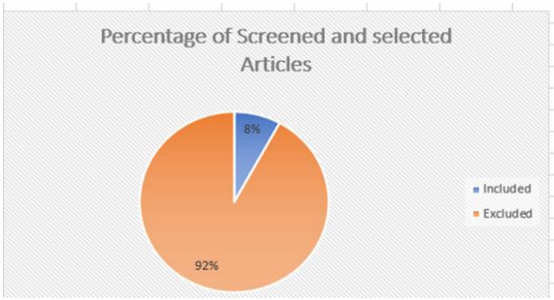

Figure 4: Article included Relevant

As revealed in figure 3, about 92% represented excluded articles while 8% represents included articles

3.1.3 Selection Criteria

All of the studies discussed in this study are cited in references section. The inclusion and exclusion standards for the papers that have been reviewed are presented in table 1.

Table 1: Inclusion and Exclusion Standards for studies

Criteria Inclusion	i. Papers published between January 2010- December 2024. ii. Articles written in English Language iii. Articles found or available as full text iv. Papers found in peer-reviewed journals v. Papers in Journals, Conferences, newspapers, Magazines, and letters.

	vi. Articles investigating impact of ML in privacy protection
Criteria Exclusion	Articles that are not relevant to the study and duplicated works

IV. GATHERING, SYNTHESIS, AND REPORTING THE FINDINGS

A comprehensive analysis was conducted on data gathered from existing literature on ML and privacy protection of data. The findings are presented in tables and figures, which illustrates the study's results, including the percentage of articles addressing specific topics, as calculated and visualized in the accompanying figures and tables.

4.1 Results

The study's findings, derived from collected and analyzed data, are presented below.

4.1.1 Mapping of Published articles

This review synthesizes existing literature on data privacy protection, highlighting key themes and objectives across published articles. The analysis also underscores the widespread impact of the issue, affecting various fields. A summary of the reviewed papers is provided in Table 3, offering an overview of the research landscape.

Publisher/Indexer	Outcome	Filtered	Relevant
ACM Digital Library	50	25	25
AC Institute of electrical electronics engineers (IEEE) Xplore	60	20	40
Elsevier	25	13	12
Public/Publisher MEDLINE (PubMed)	20	12	8
El Directory of Open Access Journals (DOAJ)	25	10	15
Springer nature	50	10	40
Academic Search Complete EBSCO Host	24	10	14
Jo Journal Storage (JSTOR)	12	10	2
Multidisciplinary Digital Publishing Institute (MDPI)	10	8	2
Sage Publishing	21	10	11
ResearchGate	20	8	12
Wiley	20	10	10
Others	19	10	9
Total	356	156	200

Table 3: Summary of the Articles Processed in the Review

3.2 Data Visualization

Data analysis and extraction were conducted using Microsoft Excel, with a structured grid organized into six categories: (i) design, (ii) overall characteristics, (iii) impact (positive and negative) of machine learning on data privacy, (iv) various machine learning approaches for data protection, (v) challenges associated with these approaches, and (vi) ethical considerations and best practices for data privacy protection see Table 2)

ML Design	Overall characteristics of ML Approach	Impact of ML on data Privacy (positive / negative	ML approaches for Data Protection	Challenges of each ML Approach	Etical / Best Practices for Data privacy
Learning Style	1. Data driven Approach 2. Pattern recognition 3. Adaptability , model can adapt to new data, environments/ tasks 4. Scalability 5. handling uncertaintyor noisy data. 6. Ability to learn from experience	1. Reduces training time by leveraging pre-trained models. 2. Improved performance on the new task by leveraging the knowledge and features learned from the pre-trained model 3. Similar dataset requirements smaller datasets require for the new tasks	1. Differential Privacy; 2. Federated Learning; 3. Homorphic Encryption;. 4. Secure Multi-party Computation; and 5. Anomaly Detection	Data quality Issues; Overfitting and Underfitting; Adversarial Attacks; Explainability and Transparency and Data privacy and security	1. Ethical Consideration: Data privacy; 2. Regular audit and ML testing for bias /fairness; 3. Provide clear expalanation of ML model decisions; 4. Accountability and ensure human oversight and ML review. For Best Practices: 1. Data Quality; 2. Model Maintenance; 3. Model Evaluation; 4. Collaboration/ Continuous Learning
Algorithm Style	1. complexity; can range from simple to complex, depending on the problem. 2. Interpretability; decision trees are more	1. privacy preserving techniques, 2. automating Data privacy compliance	Differential Privacy; Federated Learning; Homorphic Encryption;.Secure Multi-party Computation; Data AnonymizationAlgorithms and k-	Computational Complexity; Scalability; Hyperparameter Tuning; Interpretability; and	1. Fairness and Transparency; 2. Data Protection; Accountability; 3. Human Oversight and expainability. Best Practices:

	interpretable like neural network. 3. Scalability 4.Robustness. 5. Flexibility	3. Secure data sharing. Negative impact: some algorithms can erode personal privacy by collecting and processing vast amounts of personal data, often without adequate oversight or transparency. it can cause data breach risks and algorithmic bias.	Anonnymity Algorithms	Robustness and Adversarial Attacks which can compromise the performance and seurity in algorithm style	1.Algorithmic Auditing; 2. Data Quality; 3. Model Evaluation; 4.Collaboration and Continuous Learning.
Application Style	1. Problem Domain 2. Data Type, can involve different data types such as text, images, or time series 3. Performance metrics. 4. Real-time Processing	1. Privacy preserving application e.g. using end-to-end encryption, can protect user data and ensure confidentiality. 2. Data Minimizati	1. Anomaly Detection 2. Data Encryption 3. Access Control 4.Data Masking and Privacy-preserving 5. Data Mining	1. Data Integration and Preprocessing; 2. Domain knowledge and Expertise; 3. Model Interpretability and Explainability;	1. Accountability and Transparency; 2. Data Protection; 3. Fairness and Bias; 4. Human Oversight. Best Practices: 1. Model Evaluation and Testing;

		on, and unauthorized use. 3. Data sharing and monetization. Negatively, it can cause invasive Data collection i.e. data can be collected without user's knowledge. Data overcollection and data sharing and monetization.		4.Scalability and Deployment 5. Ethics and fairness raises biases and ethical concerns if not designed and developed carefully, which can have serious consequences.	2. Model Documentation; Continuous Learning and Improvement
Transfer Learning	1. Uses pre-trained models as a starting point for new tasks. 2. The pre-trained model transfers its knowledge and features to the new tasks. 3.It fine-tuned on the new task's dataset to adapt to the specific problem.	knowledge transfer without data sharing, Domain adaptation, and can private model updates by fine-tuning pre-trained models on sensitive data without sharing the	1. Differential Privacy; 2. Federated Learning; 3. Adversarial Domain 4.Adaptation; 5.Meta-Learning 6. Self-Supervised Learning; 7. Autoencoders	Domain shift; Negative transfer; Overfitting; Feature Extraction and Data Heterogeneity	1. Fairness and Transparency; 2. Data Protection; Accountability; Best Practices: 1. Model Evaluation; 2. Collaboration and Stakeholder 3. Engagement; Model Documentations;

	4.Domain adaptation	dT itself. Negatively, transfer style has potential risk leakages of sensitive data if the pre-trained model is done on sensitive information; Model invasion attacks and Membership Inference Attacks, can be vulnerable to membership inference attacks,			Continuous Learning. And Improvement

Table 2: Data Analysis and Extraction organized into Six Categories

Table 4 outline the articles processed in the study. In general, 200 papers were carefully chosen and relevant articles were used for this survey. Selected published articles focus on validation of approaches to privacy protection of data. These categories of published articles are presented in Table 3. The above can be represented graphically as shown in Figure 7

Table 4: Published studies on machine learning approaches for data privacy protection

S/N	Article Category	Frequency of Articles	Percentage of Articles
1	ANN approach to privacy preservation of data	10	5%
2	Efficacy of ML approach to privacy protection of data	20	10%
3	Validation of ML approaches to privacy protection	20	10%
4	ML and privacy protection of data	45	22.5%
5	ML and data security	30	15%
6	ML approaches validation	25	12.5%
7	Challenges of privacy security	30	15%
8	Other relevant articles	20	10%
	Total	200	100

From the above table, it is crystal clear that the category of reviewed articles that has the highest frequency and percentage is ML and privacy protection of data.

Table 5: Opportunities of implementing ML Approaches to privacy protection of data

Benefits of implementing ML in Privacy protection	Number of articles for the topic	Percentage of the articles on the topic
It helps in reducing security threats	20	10%
Elimination of false positive alerts	24	12%
Foster security of data privacy	10	5%
It offers opportunity for individual identity	12	6%
It helps in fraud detection	14	7%
Improved security and fraud prevention	10	5%
Enhanced efficiency and automation	12	6%
Accuracy and error reduction	20	10%
Increased accessibility	10	5%
Cost-effectiveness	12	6%
Enhanced personalization of data /services	10	5%
Improved data privacy and compliance	10	5%
Proactive threat detection and mitigation	12	6%
Boosting citizen trust on data privacy	14	7%
Others	10	5%
Total number of article's topic	200	100

It is clear from Table 5, that the category of review articles that has the highest frequency and percentage is "ML implementation eliminates false positive alerts" compared to others privacy protection approaches.

Comparison of state-of-the-art

Comparison of the results is divided into two parts: the first part is the summary of the comparison between the different approaches of ML application in data privacy protection; and the second part is the comparison between the major ML approaches reviewed in this study. This comparison of results with other related works was achieved using different areas of research as presented in Table 6.

Table 6: Comparison of survey with related studies on ML approaches data privacy

Number of surveyed papers	ML Approach in Data privacy	Challenges in Data privacy	Global effect of ML on data privacy	Data privacy and ML implementation	Research Opportunities	ML Application and future of data privacy	Recommendations
[45]	√	√	-	√	-	-	
[35]	-	-	√	√	-	-	
[40]	√	-	√	-	√	√	

[85]	-	√	-	√	√	√	
[80]	√	-	√	-	-	-	
[90]	-	√	-	-	√	-	
[100]	√	√	√	√	√	√	

Table 6 above revealed that this study contribution to knowledge in many areas compared to other state-of-the- art surveys on ML approaches to data privacy and protection.

V. DISCUSSION OF RESULTS

The table 4 provides a comprehensive overview of 200 articles related to Machine Learning and privacy protection of data. The papers are categorized into eight distinct groups each focusing on different aspects of ML and privacy protection. From the table, ML and privacy protection of data' this category has the highest frequency of articles (45, 22.5%), indicating a strong research focus on the intersection of ML and privacy protection. ML and Data Security category; this category has a significant frequency of articles (30, 15%), highlighting the importance of ML in ensuring data security. The category of challenges of privacy security has a notable frequency of articles (30, 15)), suggesting that researchers are actively exploring the challenges and limitations of privacy security in the context of ML. In the validation of ML approaches, the validation of ML, approaches to privacy protection and ML approaches validation categories both have a significant frequency of articles (20, 10% and 25, 12.5% respectively); indicating a strong emphasis on evaluating the effectiveness of ML approaches.

5.1 Research Trends

Growing importance of ML in Privacy Protection, the frequency of articles in these categories related to ML and privacy protection suggests a growing recognition of the importance of ML in ensuring data privacy. Also, the significant frequency of articles in validation-related categories indicates a focus on evaluation the effectiveness of ML approaches in privacy protection. Likewise, challenges and limitations bring about notable frequency of articles in the challenges of privacy security category suggests that researchers are actively exploring the limitations and challenges of privacy security in the context of ML.

5.2 Solution to the challenges facing users' data privacy

Addressing data privacy challenges requires a multi-faceted approach that integrates legal compliance, technological innovation, and ethical considerations.

A. Technological Solutions

1. Privacy-Enhancing Technologies (PETs): Adopting PETs like anonymization, pseudonymization, differential privacy, and homomorphic encryption can minimize data collection and enhance privacy while enabling data utility.
2. Data Governance Frameworks: Implementing robust data governance frameworks that combine legal analysis, computer science, social science, and ethical inquiry can help address data privacy challenges.
3. Data Encryption: Using encryption algorithms to protect data both in transit and at rest can prevent unauthorized access.
4. Access Control: Implementing strict access controls, including role-based access control and multi-factor authentication, can limit data access to authorized personnel only.

B. Organizational Solutions

1. Data Protection Impact Assessment (DPIA): Conducting DPIAs before collecting and storing data can help identify potential risks and benefits.
2. Data Retention Policy: Implementing a data retention policy that specifies data storage duration and deletion procedures can minimize data exposure.

C. Regulatory Compliance

1. Compliance with Data Protection Laws: Organizations must comply with regulations like GDPR and CCPA, which set high data privacy standards. Appointing a Data Protection Officer (DPO) is mandatory for organizations subject to GDPR.
2. Staying Informed about Regulatory Changes: Data privacy regulations are continually evolving. Organizations must stay informed about changes in governing legislation and adjust their compliance strategies accordingly [5].

5.3 Ethical Considerations of ML in Data Privacy Protection

The integration of ML in data privacy protection raises several ethical considerations that must be addressed to ensure the responsible use of ML technologies and these include: Privacy vs Utility

1. Privacy vs. Utility

a) Balancing Privacy and Data Utility: ML models often require large amounts of data to function effectively. Ensuring that data is used in a way that balances privacy with the utility of the model is crucial.
b) Minimizing Data Collection: Collecting only the data that is necessary for the ML model to function can help minimize privacy risks.

2. Bias and Fairness

a) Avoiding Bias in ML Models: ML models can inadvertently perpetuate or exacerbate existing biases if the training data is biased. Ensuring fairness in ML models is essential to prevent discriminatory outcomes.
b) Fairness Metrics: Implementing fairness metrics and regularly auditing ML models for bias can help ensure equitable treatment of all individuals.

3. Transparency and Explainability

a) Model Transparency: ML models should be transparent about how they use data and make decisions. This includes providing clear explanations of the model's decision-making process.
b) Explainability Techniques: Using techniques like LIME (Local Interpretable Model-agnostic Explanations) or SHAP (SHapley Additive exPlanations) can help provide insights into how ML models work.

4. Data Protection

a) Data Anonymization: Techniques like anonymization, pseudonymization, and differential privacy can help protect sensitive data while still allowing ML models to function effectively.
b) Secure Data Storage: Ensuring that data is stored securely and protected from unauthorized access is critical for maintaining privacy.

5. Accountability and Governance

a) Accountability Mechanisms: Establishing accountability mechanisms for ML models, including clear lines of responsibility, can help ensure that any issues related to privacy are addressed promptly.
b) Governance Frameworks: Implementing governance frameworks that outline the ethical use of ML in data privacy protection can help guide decision-making and ensure compliance with regulations.

6. User Consent and Control

a) Informed Consent: Ensuring that users are informed about how their data will be used and providing them with control over their data can help build trust and ensure ethical use of ML.
b) Data Subject Rights: Respecting data subject rights, such as the right to access, rectify, or delete data, is essential for ethical ML practices.

By addressing these ethical considerations, organizations can ensure that ML technologies are used responsibly and ethically in the context of data privacy protection.

VI. RECOMMENDATIONS

We recommend the following for Future Research:

1. Explainability and Transparency: Future research should focus on developing more explainable and transparent ML models, enabling better understanding of decision-making processes.
2. Fairness and Bias: Researchers should prioritize fairness and bias mitigation in ML models, ensuring equitable treatment of all individuals.

3. Data Quality and Availability: Improving data quality and availability is crucial for developing effective ML models.
4. Security and Robustness: Research should focus on developing ML models that are robust to adversarial attacks and security threats.

6.1 Recommendations for Practitioners

1. Careful Model Selection: Practitioners should carefully select ML models suitable for their specific problem, considering factors like data quality, model complexity, and interpretability.
2. Data Preprocessing: Proper data preprocessing is essential for developing effective ML models.
3. Model Evaluation: Practitioners should thoroughly evaluate ML models using relevant metrics and benchmarks.
4. Continuous Monitoring: ML models should be continuously monitored and updated to ensure they remain accurate and effective.

6.2 Recommendations for Policymakers

1. Regulatory Frameworks: Policymakers should establish regulatory frameworks that promote the responsible development and deployment of ML models.
2. Data Protection: Policymakers should prioritize data protection and privacy, ensuring that ML models are developed and deployed in ways that respect individual rights.
3. Education and Training: Policymakers should invest in education and training programs that develop the necessary skills for ML development and deployment.
4. Encouraging Innovation: Policymakers should encourage innovation in ML while ensuring that developments are aligned with societal values and needs.

However, these recommendations can help advance the field of ML, ensuring that its benefits are realized while minimizing potential risks and challenges.

CONCLUSION

The contribution of this review should, however, be considered in light of some limitations. First, our research is a general literature review with an informative purpose, which might suggest that there is a possibility o f a subjective selection of literature. Notwithstanding, the the databases we have used, such as Elsevier, IEEE Xplore, Emerald insight, Willey, ACM Digital Library, Google Scholar, Semantic Scholar, and EBSCO, represent the most cited articles. Asides, the purpose and the informative nature of this paper require a systematic review of the literature. The review will be useful for policymakers, government, end users and practitioners. Furthermore, it was possible to accurately identify the long-term challenges and opportunities in using ML for privacy protection of data. Therefore, future research should be focused on developing more explainable ML models that will enable better understanding of decision-making processes and also, focus on developing ML models that are robust to adversarial attacks and security threats.

ACKNOWLEDGEMENTS

The author expresses her gratitude to the chief-editor, associate editors of this reputable Journal and independent reviewers for their valuable contributions to this paper.

REFERENCES

[1] Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., & Zhang, L. (2016). Deep learning with differential privacy. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 308-318.

[2] Abdel-Basset, M., Hawash, H., Moustafa, N., Razzak, I & M. Abd Elfattah, 2022. “Privacy-preserved learning from non-iid data in fog-assisted IoT: A federated learning Approach,” Digit. Commun. Networks, 2022, DOI: 10.1016/j.dcan.2022.12.013.

[3] Aljably, R., Tian, Y., & Al-Rodhaan, M. “Preserving Privacy in Multimedia Social Networks Using Machine Learning Anomaly Detection,” Secur. Commun. Networks, vol. 2020, DOI:10.1155/2020/5874935.

[4] Anand, A., & Janami, R. (2017). Secure data storage in cloud using key-attribute based

encryption. Journal of Cloud Computing, 6(1), 1-12.

[5] Bengio, J. Y. 2012. Deep learning of representations for unsupervised and transfer learning. Journal of Machine Learning Research, 27.

[6] Bertino, E. (2016). Data privacy: Challenges and opportunities. IEEE Security & Privacy, 14(4), 82-85.

[7] Bertino, E. (2016). Data privacy and security: A survey of challenges and opportunities. Journal of Computer Science and Technology, 31(3), 453-465.

[8] Bertino E. (2016). Big Data Security and Privacy. IEEE International Conference on Big Data pp 3.

[9] Bojarski, M., Del Testa, D., Dworakowski, D., Firner, B., Flepp, B., Goyal, P., ... & Zhang, X. (2016). End to end learning for self-driving cars. arXiv preprint arXiv:1604.07316.

[10] Breck, E., Cai, Z., Nielsen, E., Salib, M., & Sculley, D. (2017). What's your ML test score? A rubric for ML testability and five big ML testing questions. arXiv preprint arXiv:1707.07174.

[11] Breck E., Shanqing C., Nielsen E., Salib M., & Sculley D. 2017. The ML Test Score: A Rubric for MLProduction Readiness and Technical Debt Reduction". Proceedings of the 2017 IEEE International Conference on Big Data.

[12] Carlini, N., & Wagner, D. (2017). Towards evaluating the robustness of neural networks. 2017 IEEE Symposium on Security and Privacy (SP), 39-57.

[13] Chamikara, M.A.P., Bertok, P., Khalil, A., Liu, D., & Camtepe, S. 2020. "Privacy preserving distributed machine learning with federated learning," Comput. Commun., vol. 171, 112–125, 2021, DOI: 10.1016/j.comcom.2021.02.014.

[14] Chen, Y., Lu, Z., Xiong, H., & Xu, W. 2018 "Privacy-Preserving Data Aggregation Protocol For Fog Computing-Assisted Vehicle-to-Infrastructure Scenario," Secure. Commun. Networks, vol. 2018, 2018, DOI: 10.1155/2018/1378583.

[15] Chen, X., et al. (2017). Machine learning for data privacy: A survey. IEEE Transactions on Knowledge and Data Engineering, 29(10), 2341-2354.

[16] Chen, L., Thabtah, F., & Martin, N. (2017). A review on data privacy issues in the era of big data. Journal of Intelligent Information Systems, 48(2), 241-258.

[17] Chew, G., et al. (2017). Privacy-preserving machine learning using decision trees. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 245-257.

[18] Darwish S. M., Essa, R.M., Osman, M.A., and Ismail, A.A. 2022. "Privacy Preserving Data Mining Framework for Negative Association Rules: An Application to Healthcare Informatics," IEEE Access, vol. 10, no. June, pp. 76268–76280, DOI:10.1109/ACCESS.2022.3192447.

[19] Denning, D. E. (1987). An intrusion-detection model. IEEE Transactions on Software Engineering, 13(2), 222-232.

[20] Donahue, J., Jia, J., Vinyals, Y., Hoffman, O., Zhang, J., Tzeng, N., & Darrell, T. 2014). DeCAF: A deep convolutional activation feature for generic visual recognition. International Conference on Machine Learning.

[21] Dwork, C., & Roth, A. 2014. The Algorithmic Foundations of Differential Privacy. Foundations and Trends in Theoretical Computer Science. 9(3-4), 211-407.

[22] Dwork, C., Kenthapadi, K., McSherry, F., Mironov, I., & Naor, M. (2006). Our data, ourselves: Privacy via distributed noise generation. Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, 486-503.

[23] Dwork, C., McSherry, F., Nissim, K., & Smith, A. (2006). Calibrating noise to sensitivityin private data analysis. Proceedings of the 3rd Theory of Cryptography Conference, 265-284.

[24] Esteva, A., Kuprel B., Roberto A., Ramsundar, B., Kuleshov, V., DePristo, M., & Kearns, F. (2017). Deep learning-assisted diagnosis for breast cancer. Vol. 541 105-117.

[25] Esteva A., Kuprel B., Roberto A. N., Ko j., Swetter S.M., Blau H.M., & Thrun S. 2017. Dermatologist-level classification of skin

cancer with Deep Neural Networks" Publishd in Nature Vol.542. 115-118.

[26] Esteva, A., Kuprel, B., Novoa, R. A., Ko, J., Swetter, S. M., Blau, H. M., & Thrun, S. (2017). Dermatologist-level classification of skin cancer with deep neural networks. Nature, 542(7639), 115-118.

[27] European Union. (2016). General Data Protection Regulation. Official Journal of the European Union, L119, 1-88.

[28] Fernández, J.S., Menci M., Lee, C.M A. Rieger, and G. Fridgen, "Privacy-preserving federated learning for residential short-term load forecasting," Appl. Energy, vol.(326)April. 119915. DOI: 10.1016/j.apenergy.2022.119915

[29] Field M. 2022. "Infrastructure platform for privacy-preserving distributed machine learning development of computer-assisted theragnostics in cancer," J. Biomed. Inform., vol. 134, no. April, p. 104181, 2022, DOI: 10.1016/j.jbi.2022.104181.

[30] Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. Proceedings of the 41st Annual ACM Symposium on Theory of Computing, 169-178.

[31] Gilad-Bachrach, R., et al. (2016). Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy. Proceedings of the 33rd International Conference on Machine Learning, 201-210.

[32] Girka A., Terziyan, V., Gavriushenko, M., & Gontarenko, A. 2022. "Anonymization as homeomorphic data space transformation for privacy-preserving deep learning," Procedia Comput. Sci., vol. 180, pp. 867–876, DOI:10.1016/j.procs.2021.01.337.

[33] Goodfellow, I. J., et al. (2014).* An empirical study of learning algorithms which approximately preserve privacy. arXiv preprint arXiv:1402.5217.

[34] Huang, S., Yu, F., Tsaih, R., & Huang. Y. 2015. Network-traffic anomaly detection with incremental majority learning, in: Neural Networks 2015 International Joint Conference, July 2015. 1—8.

[35] Huang, Q., Wang, L., & Yang, Y. 2017. "Secure and Privacy-Preserving Data Sharing and Collaboration in Mobile Healthcare Social Networks of Smart Cities," Secur. Commun. Networks, vol. (2017)2017. DOI: 10.1155/2017/6426495.

[36] Hu, V. C., Ferraiolo, D., & Kuhn, D. R. (2014). Assessment of access control systems. NIST Interagency Report 7316.

[37] Iwendi, C., Moqurrab, S.A., Anjum, A, Khan, S., Mohan, S & Srivastava, G. 2020. "N-Sanitization: A semantic privacy-preserving framework for unstructured medical datasets," Comput. Commun., vol. 161, no. April, pp. 160–171, 2020, DOI: 10.1016/j.comcom.2020.07.032.

[38] Jafari, K., et al. (2019). Data privacy in the digital age: A systematic review. Journal of Information Systems, 33(2), 137-153.

[39] Jafari, M., Noorian, M., & Mohammadi, A. (2019). Data privacy in the age of big data: A survey. Journal of Intelligent Information Systems, 54(2), 267-285.

[40] Jafari, S., Javidi, M. M., & Derhami, V. (2019). Privacy-preserving data mining: A survey. Journal of Computing and Security, 6(2), 101-116.

[41] Jena, U. K., et al. (2021). A review on homomorphic encryption for privacy-preserving machine learning. Journal of Intelligent Information Systems, 58(2), 267-283.

[42] Jiang, X., et al. (2018). Machine learning for intrusion detection: A survey. IEEE Communications Surveys & Tutorials, 20(2), 1256-1274.

[43] Jiang, K., Wang, W., Wang, A., & Wu, H. (2018). Network intrusion detection using deep learning: A review. IEEE Access, 6, 52215-52226.

[44] Kairouz, P., et al. (2021).* Advances and open problems in federated learning. Foundations and Trends in Machine Learning. VOL5(15)

[45] Kang, B., Wang, J., & Shao, D. 2017. "Certificateless Public Auditing with Privacy Preserving for Cloud-Assisted Wireless Body Area Networks," Mob. Inf. Syst., vol. 2017, DOI: 10.1155/2017/2925465.

[46] Kim, T., Oh, Y., Kim, H. 2020. "Efficient Privacy-Preserving Fingerprint-Based Authentication System Using Fully Homomorphic Encryption," Security

Communication Networks, vol. 2020, 2020, DOI: 10.1155/2020/4195852.

[47] Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic Literature reviews in software engineering. Technical Report EBSE-2007-01, Keele University.

[48] Kitchenham, B., Brereton, P., & Budgen, D. (2014). Mapping study completeness and its implications for systematic reviews. Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering, 1-10.

[49] Krizhevsky, A., Sutskever, I., & Hinton, G. 2012.ImageNet classification with deep convolutional neural networks. Advances in Neural Information Processing Systems, 25.

[50] Kumar, S., et al. (2019). Data loss prevention using machine learning: A survey. Journal of Intelligent Information Systems, 54(2), 257-275.

[51] Kumar, N., Singh, S., & Srivastava, S. (2019). Machine learning-based data loss prevention: A review. Journal of Intelligent Information Systems, 54(2), 267-283.

[52] Kumeno, F. (2019). Challenges in machine learning system development: A review. Journal of Systems and Software, 153, 123-138.

[53] Lakshmanna, K., Kavitha, R., Geetha, B.T., Nanda, A.K., Radhakrishnan, A., & Kohar, R. 2020 "Deep Learning-Based Privacy-Preserving Data Transmission Scheme for Clustered IIoT Environment," Computer. Intell. Neurosci., vol. 2022, 2022, DOI:10.1155/2022/8927830.

[54] Lalli M. and Raquel P.2021

[55] Liu, Q., 2022. "Privacy Protection Technology Based on Machine Learning and Intelligent Data Recognition," Secur. Commun. Networks, vol. 2022, 2022, DOI: 10.1155/2022/1598826.

[56] Liu, Z. Gao, Z., Wang, J., Liu, Q., & Wei, J. "PPEFL: An Edge Federated Learning Architecture with Privacy-Preserving Mechanism," Wirel. Commun. Mob. Comput., vol. 2022, 2022, DOI: 10.1155/2022/1657558.

[57] Li, M., et al. (2019). Machine learning for data privacy protection: A survey. IEEE Communications Surveys Surveys & Tutorials, 21(2), 1245-1264.

[58] Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2019). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Transactions on Parallel and Distributed Systems, 30(1), 141-153.

[59] Li, N., Li, T., & Venkatasubramanian, S. (2007). t-closeness: Privacy beyond k-anonymity and l-diversity. Proceedings of the 23rd International Conference on Data Engineering (ICDE'07)

[60] Long, M., Cao, Y., Wang, J., & Jordan, M. I. (2015). Learning transferable features with deep adaptation networks. International Conference in Machine Learning.

[61] Ma X., Zhou Y., Wang L., and Miao L.2022. "Privacy-preserving Byzantine-robust federated learning," Comput. Stand. Interfaces, vol. 80, 2022, DOI: 10.1016/j.csi.2021.103561.

[62] Machanavajjhala, A., Kifer, D., Gehrke, J., & Venkitasubramaniam, M. (2006). l-diversity: Privacy beyond k-anonymity. Proceedings of the 22nd International Conference on Data Engineering (ICDE'06.

[63] Machanavajjhala, A., Kifer, D., Gehrke, J., & Venkitasubramaniam, M. (2007). l-diversity: Privacy beyond k-anonymity. ACM Transactions on Knowledge Discovery from Data (TKDD), 1(1), 3-es.

[64] McKinsey. (2016). An executive's guide to machine learning.

[65] Mercier D., Lucieri, A Munir, A., Dengel, A., & Ahmed, S. 2022. "Evaluating Privacy-Preserving Machine Learning in Critical Infrastructures: A Case Study on Time-Series Classification," IEEE Trans. Ind. Informatics, vol. 18, no. 11, pp. 7834–7842, 2022, DOI: 10.1109/TII.2021.3124476

[66] Mivule, K., Turner, C., & Ji, S.Y. 2012 "Towards a differential privacy and utility preserving machine learning classifier," Procedia Comput. Sci., vol. 12, pp. 176–181, 2012, DOI: 10.1016/j.procs.2012.09.050.

[67] Moosavi-Dezfooli, S. M., Fawzi, A., & Frossard, P. (2016). Deepfool: a simple and accurate method to fool deep neural networks. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2574-2582.

[68] Pirbhulal, S., Pombo, N., Felizardo, V., Garcia, N., Sodhro, A.H., & Mukhopadhyay, S.H. Towards machine learning enabled security framework for IoT-based healthcare," in 2019 13th International Conference on Sensing Technology (ICST), 2019: IEEE, pp. 1–6.

[69] Priharti,W., Sumaryo, S., Saraswati, T., & Nurfadilah, M. "IoT based logistics vehicle security monitoring system," in IOP Conference Series: Materials Science and Engineering, 2020, vol.(771)1: IOP Publishing, p. 012012

[70] Raatikainen, M., Tiihonen, J., Männistö, T., 2019. Software product lines and variability modelling: A tertiary study. J. System Software 149, 485–510.

[71] Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. Computer, 29(2), 38-47.

[72] Sharif Razavian, A., Azizpour, H., Sullivan, J., & Carlsson, S. (2014). CNN features off-the-shelf: An astounding baseline for recognition. IEEE Conference on Computer Vision and Pattern Recognition Workshops.

[73] Shi, W., Cao, J., Zhang, Q., et al. (2016). Edge computing: Vision and challenges. IEEE Internet of Things Journal, 3(5), 637-646

[74] Ren L & Zhang, D. 2019. "A Privacy-Preserving Biometric Recognition System with Visual Cryptography," Adv. Multimed., vol.(2022)1, 2022, DOI:10.1155/2022/1057114.

[75] Sapunkov, P. (2019). Machine learning in finance: A survey. Journal of Financial Data Science, 1(1), 53-64.

[76] Sapunkov, O. (2019). Machine learning for finance: A review. Journal of Financial Data Science, 1(1), 1-15.

[77] Sav, S., Bossuat, J.P., Troncoso-Pastoriza, J.R., Claassen, M., & Hubaux,J.P. 2022 "Privacy-preserving federated neural network learning for disease-associated cell classification" Patterns, vol.(3)5. 100487, DOI: 10.1016/j.patter.2022.100487.

[78] Sergi, I., Montanaro, T., Benvenuto, F.L., & Patrono, L. 2021. "A smart and secure logistics system based on IoT and cloud technologies," Sensors, vol. (21)6. 2231, 2021.

[79] Shokri, R., & Shmatikov, V. (2015).* Privacy-preserving deep learning. ACM Conference on Computer and Communications Security. (2015)

[80] Shokri, R., Stronati, M., Song, C., & Shmatikov, V. (2017). Membership inference attacks against machine learning models. 2017 IEEE Symposium on Security and Privacy (SP), 3-18.

[81] Song, Z., Ren, Y., He, G. 2022. "Privacy-Preserving KNN Classification Algorithm for Smart Grid," Secur. Commun. Networks, vol.(2022), 2022, DOI: 10.1155/2022/7333175.

[82] Song, C., Ristenpart, T., & Shmatikov, V. (2017). Machine learning models that remember too much. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 587-601

[83] Sweeney, L. (2002). k-anonymity: A model for protecting privacy. International Journal Of Uncertainty Fuzziness and Knowledge-Based Systems, 10(05), 557-570.

[84] Terziyan, V., Malyk, D., Golovianko, M., & Branytskyi, V. 2022. "Encryption and Generation of Images for Privacy-Preserving Machine Learning in Smart Manufacturing," Procedia Comput. Sci., vol(217)2022. 91–101, 2023, DOI: 10.1016/j.procs.2022.12.205

[85] Ullah A. 2021. "Fusion of Machine Learning and Privacy Preserving for Secure Facial Expression Recognition," Secur. Commun. Networks, vol(2021). DOI: 10.1155/2021/6673992

[86] Venugopal, R., Shafqat, N., Venugopal, J., Tillbury, B.M.J., Stafford, H.D., & Bourazeri, D. 2022. "Privacy preserving Generative Adversarial Networks to model Electronic Health Records," Neural Networks, vol.153, 339–348. DOI:10.1016.2022.06.022.

[87] Veeramakali, A. Shobanadevi, N. R. Nayak, S. Kumar, S. Singhal, and M. Subramanian, "Preserving the Privacy of Healthcare Data

over Social Networks Using Machine Learning," Computer. Intelligence Neuroscience, vol. 2022, DOI: 10.1155/2022/4690936

[88] Wang J.N, 2022. "A blockchain based privacy-preserving federated learning scheme for Internet of Vehicles," Digit. Commun. Networks, DOI: 10.1016/j.dcan.2022.05.020.

[89] Xu, G., Li, H., Zhang, Y. Xu, X., Ning, J. & Deng, R.H. 2020 "Privacy-Preserving Federated Deep Learning with Irregular Users," IEEE Trans. Dependable Secur. Computer., (19)2, 1364–1381, DOI: 10.1109/TDSC.2020.3005909.

[90] Xu, C., Shen, X., Zhu, L., & Zhang, Y. 2017. "A Collusion-Resistant and Privacy-Preserving Data Aggregation Protocol in Crowdsensing System," Mob. Inf. Syst., 2017(2017). DOI: 10.1155/2017/3715253.

[91] Yao, A. C. (1986). How to generate and exchange secrets. Proceedings of the 27th Annual Symposium on Foundations of Computer Science, 162-167.

[92] Yosinski, J., Clune, J., Bengio, Y., & Lipson, H. (2014). How transferable are features in deep neural networks? Advances in Neural Information Processing Systems, 27.

[93] Yujing L. 2023. Security and Privacy of Internet of Things: A Review of Challenges and Solutions *Journal of Cyber Security and Mobility, Vol. 12 6,* 813–844.DOI: 10.13052/jcsm2245-1439.1261

[94] Yu, F., Xu, Z., Qin, Z., & X. Chen, "Privacy-preserving federated learning for transportation mode prediction based on personal mobility data," High-Confidence Comput., vol. 2, no. 4, p. 100082, 2022, DOI: 10.1016/j.hcc.2022.100082.

[95] Zapechnikov, S., 2019. "Privacy-Preserving Machine Learning as a Tool for Secure Personalized Information Services," Procedia computer. Science., Vol(169)2019, 393–399, DOI: 10.1016/j.procs.2020.02.235.

[96] Zapechnikov, J.S., "Contemporary trends in privacy-preserving data pattern recognition," Procedia Computer Science., 190(2019). 838–844, 2021, DOI:10.1016/j. procs.2021.06.098.

[97] Zapechnikov, S. 2022. "Secure multi-party computations for privacy-preserving machine learning," Procedia Computer Science. 2139©, 523–527, 2022, DOI: 10.1016/j.procs.2022.11.100.

[98] Zerka F. 2021. "Privacy preserving distributed learning classifiers – Sequential learning with small sets of data," Computer Biol. Med., 136(July), 104716, 2021, DOI: 10.1016/j.compbiomed.2021.104716.

[99] Zhang, J.M., Harman, M., Ma, L., Liu, Y., 2020. Machine learning testing: Survey, landscapes and horizons. IEEE Trans. Software Eng. (Published online).

[100] Zhang, Y., Deng, R. H., & Zheng, Y. (2020). Data security and privacy in the age of big data: A survey. IEEE Transactions on Big Data, 6(2), 240-255.

[101] Zhang, Y., et al. (2020). Testing machine learning model validation software: A review. Journal of Software Engineering, 32(2), 123-143

[102] Zou Z., 2020 "Improved Cloud-Assisted Privacy-Preserving Profile-Matching Scheme in Mobile Social Networks," Security Communication Networks, vol.(2020), DOI: 10.1155/2020/4938736.