International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.3 (2025) pp. 5105-5112
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Security and Privacy Challenges in Deep Learning Models Hosted on Cloud Platforms

Jhansi Rani Ganapa[1*], Poonam Joshi[2], T Amitha[3], Sandip Rahane[4], N. Ravinder[5], Jignesh Jani[6], Vani N[7], Chandreshkumar Vyas[8]

[1*]Assistant Professor Department of Computer Science and Engineering Centurion University of Technology and Management, Andhra Pradesh,
*** Corresponding Author Email:** jhanuganapa@gmail.com, **ORCID:** 0009-0005-7844-5282

[2]Assistant professor, Computer science and Engineering (Cybersecurity), Thakur college of engineering and technology, Mumbai
Email: poonam.joshi@thakureducation.org, - **ORCID**: 0009-0002-4671-6162

[3]Professor, Jaya engineering College
Email: tamitharaghu@gmail.com - **ORCID:** 0009-0006-5035-4490

[4]Associate Professor, Department of Electronics and Computer Engineering, Amrutvahini College of Engineering, Sangamner, India,
Email: rahanesandip@gmail.com- **ORCID:** 0000-0003-4688-9557

[5]Assistant Professor, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.
Email: ravindernellutla@kluniversity.in- **ORCID:** 0000-0002-3082-8584

[6]Assistant Professor Mechanical Engineering Marwadi University, Rajkot,
Email: jdjani12@gmail.com - **ORCID:** 0000-0002-6859-5528

[7] Associate Professor, Department Of Computer Science And Technology, BGS Institute of Technology, Adichunchanagiri University, BG Nagar, Bellur, Mandya distict , Karnataka-571448
Email: vanin@bgsit.ac.in - **ORCID:** 0000-0003-0801-7184

[8]Assistant Professor, Mechanical Engineering, Marwadi University, Rajkot,
Email: chandresh.vs@gmail.com - **ORCID:** 0009-0009-1903-3463

Article Info:

DOI: 10.22399/ijcesen.3235
Received : 05 May 2025
Accepted : 06 July 2025

Keywords

Deep Learning
Cloud Security
Privacy Risks
Adversarial Attacks
Model Inversion
Secure AI

Abstract:

Deep learning's fast integration into cloud computing services enables businesses to perform scalable AI model training and real-time analysis in diverse sectors. The combination of deep learning with cloud platforms results in important security vulnerabilities that stem from adversarial threats and data breaches as well as model inversion vulnerabilities and unauthorized system intrusions. Data infringement combined with weakened model reliability and non-compliance requirements require cloud AI systems to adopt more robust security controls. Experts analyze security issues facing deep learning models in the cloud through an assessment of attacks which manipulate model inputs, pollute training data and exploit APIs and create insecurity across multiple cloud user environments. The research compares encryption protocols and federated learning capabilities and access control systems and differential privacy features of AWS, Google Cloud, Microsoft Azure, and IBM Cloud. The assessment evaluates regulatory compliance requirements of GDPR HIPAA and CCPA in order to detect security governance gaps for AI systems. Research outcomes show that Amazon Web Services along with Google Cloud deliver excellent encryption features as well as anomaly detection solutions yet Microsoft Azure stands out through its advanced federated learning functions. The security features aimed at AI operations are insufficient in IBM Cloud which demonstrates divergent approaches to security implementation across platforms. Homomorphic encryption and differential privacy have progressed but practical use remains restricted by high operational costs and regulatory uncertainty as well as attacks by adversaries. The distributed AI training

method known as federated learning protects against poisoning attacks but still needs improved protection mechanisms to remain secure. The proposed solution for safe and privacy-compliant AI implementation uses a security system that joins sophisticated cryptographic methods with adversarial attack prevention mechanisms along with methods for protectively training AI. Future research needs to improve encryption speeds as well as strengthen federated learning resistance to attacks and create AI-based compliance systems which will address new cybersecurity threats against cloud-based AI platforms.

1. Introduction

Deep learning integrated with cloud computing technology operates as a major force in AI-driven applications through large-scale model training capability with real-time analytics and economic computing scalability benefits. NIST defines cloud computing as a system that enables users to access shared computing resources through on-demand service which allows distributed infrastructure deployment and efficient AI model training [1]. Deep learning technology advances prompt organizations to adopt cloud technology by using neural networks which perform efficient computations that process images and texts while making predictions [2]. Cloud-hosted deep learning systems come with security along with privacy risks which make them vulnerable to data breaches and adversarial attacks and unauthorized access according to research [3].

A major security challenge emerges from shared computing systems because they expose both user data and model parameters to potential exposure. Research confirms that third-party compute clouds leak information which lets attackers acquire secret AI models and their training data sets [4]. Deep learning models face extreme security threats because even minor alterations in input data can generate incorrect classifications leading to severe results during medical diagnostics and autonomous systems and fraud prevention systems operations [5]. Cloud-based AI systems experience increasing privacy breaches and model inversion attacks because their unclear data-sharing methods between cloud nodes generate rising data privacy concerns [6].

Research groups develop protective systems by analyzing privacy-preserving AI solutions through federated learning and differential privacy to both defend AI model functionalities and address security weaknesses. The decentralized training system of federated learning protects data by keeping information on local devices instead of cloud storage thus preventing exposure and breaches [7]. During federated learning training the model suffers integrity damage from poisoning attacks because malicious participants embed corrupted data [8]. The research in [9] highlights extensive computational requirements as significant challenges for homomorphic encryption which allows encrypted data computation. GDPR's current version does not contain specific regulations for AI model protection or adversarial threat resistance but it does provide rules for AI cloud service compliance [10].

This study aims to:

- Examine the security and privacy risks associated with cloud-hosted deep learning models, focusing on adversarial threats, data breaches, and information leakage vulnerabilities.
- Evaluate existing mitigation strategies such as homomorphic encryption, differential privacy, and federated learning, assessing their effectiveness in securing AI models deployed in cloud environments.
- Analyze regulatory challenges and propose a multi-layered security framework that enhances AI model resilience, regulatory compliance, and privacy protection in cloud-based AI applications.

By addressing these objectives, this study contributes to the advancement of secure AI deployment strategies, ensuring privacy-preserving and resilient AI architectures in cloud infrastructures.

2. Materials And Methods

The research framework provides an assessment of security and privacy barriers within deep learning programs functioning on cloud platforms. The research utilizes an organized procedure to classify threats while performing framework assessments and regulatory compliance evaluations. The combined research methods in these subsections provide full understanding regarding security conditions of deep learning models when operating in cloud environments.

2.1 Identification of Security and Privacy Threats

Threat Taxonomy Development

To ensure a structured and comprehensive understanding of security vulnerabilities in cloud-hosted deep learning models, threats are classified into two primary categories: model-specific risks and cloud infrastructure risks. These classifications

were chosen based on an extensive review of AI security literature, ensuring that the categorization aligns with the most common and impactful threats encountered in real-world AI deployments.

Model-Specific Risks: Different stages of model architecture and training processes and inference pipelines represent the points where deep learning model vulnerabilities can be exploited by various threats. One category of threats includes small input data modifications for model deception and training data reconstruction attacks which operate alongside data poisoning attacks that introduce malicious data into training datasets. Among these security threats hidden triggers represent a type of backdoor attack which modifies model behavior.

Cloud Infrastructure Risks: Multiple threats exist in the cloud environment that hosts AI models because of system vulnerabilities within the infrastructure. Swiss Re has declared its intention to tackle the most crucial security threats that stem from weak authentication systems and data breaches through misconfigured security settings and denial-of-service attacks on cloud-hosted AI models.

The classification system enables organizations to evaluate AI model threats alongside general cloud security vulnerabilities thus enabling them to develop specific protective measures.

Threat Assessment Approach

A systematic risk assessment method helps identify the severity level of threats discovered during evaluation. The assessment depends on three fundamental components to perform evaluations:

1. Attack Feasibility (AF) – Attackers successfully execute their attacks because they have available tools along with minimal system requirements.

2. Potential Damage (PD) – The successful execution of attacks results in monetary loss combined with privacy breaches and disrupted systems.

3. Mitigation Difficulty (MD) – The implementation of effective countermeasures against the attack proves to be complex. A total risk score R requires calculation using this specific formula:

$$R = \frac{AF + PD + MD}{3}$$

The risk assessment system uses a scoring system from 1 to 5 for each of its parameters *(AF, PD, MD)* to establish security threat levels.

Table 1. *Risk Assessment for Security Threats*

Threat Type	Attack Feasibility (AF)	Potential Damage (PD)	Mitigation Difficulty (MD)	Risk Score (R)
Adversarial Attack	5	4	4	4.33
Model Inversion	3	5	5	4.33
Data Poisoning	4	5	3	4.00
Unauthorized Access	2	5	2	3.00

The established security framework enables systematic threat evaluation by letting organizations predict when incidents will happen and how much damage they will cause and what kind of mitigation response they need.

A workflow model serves to enhance security threat identification and evaluation processes as illustrated in figure 1:

Figure 1. *Workflow for Threat Identification and Assessment*

The workflow provides an organized procedure to detect analyze and manage security threats that arise from cloud-based AI models.

2.2 Review and Comparative Analysis of Security Frameworks

Security Framework Selection Criteria

The evaluation of cloud provider security measures selects four major platforms including Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure and IBM Cloud. The platforms deploy deep learning models through their systems using security mechanisms that have been specifically developed for AI applications.

The evaluation analyzes four essential security aspects:

- **Encryption Mechanisms:** Analysis of encryption standards for data protection at rest, in transit, and during computation.
- **Authentication and Access Control:** Examination of identity management systems,

including multi-factor authentication and role-based access control.

- **Privacy-Preserving Techniques:** Examining secure AI training techniques and differential privacy.
- **Federated Learning Integration:** Assessment of cloud support for decentralized AI training that does not share raw data.

Evaluation Methodology

The analysis of security frameworks between cloud providers uses publicly accessible documentation and security whitepapers and implementation reports. All security mechanisms fall under three categories: preventive, detective and corrective strategies:

- **Preventive Strategies:** Proactive security mechanisms such as encryption, access control, and secure model deployment protocols.
- **Detective Strategies:** Security monitoring techniques such as AI-driven anomaly detection and intrusion detection systems.
- **Corrective Strategies:** Security incident response mechanisms, including breach containment and forensic analysis.

Table 2. *Security Feature Comparison of Major Cloud Providers*

Security Feature	AWS	Google Cloud	Azure	IBM Cloud
Data Encryption	AES-256, TLS 1.3	AES-256, TLS 1.3	AES-256, TLS 1.3	AES-256, TLS 1.3
Identity & Access Mgmt	IAM, Role-based	IAM, Role-based	IAM, Role-based	IAM, Role-based
Federated Learning	Limited	TensorFlow Privacy	Confidential ML	Limited
Threat Detection	GuardDuty	Security Command Center	Sentinel	QRadar AI

The evaluation approach using security principles as its framework allows for specific security capability comparison across different cloud providers.

2.3 Regulatory and Compliance Analysis (Citations Required)

Security and Privacy Compliance Laws

Cloud-based deep learning models derive their security and privacy features from regulatory compliance serving as their basic foundation. We evaluate three core legal demands in this section with GDPR as one requirement and HIPAA and CCPA as the other two. The General Data Protection Regulation defines strict EU-area data protection requirements that demand users grant consent while requiring data minimization and allowing them to request their data's removal [11]. HIPAA mandates security controls for healthcare data in the United States, imposing strict requirements on encryption, access control, and breach notifications [12]. Businesses operating under CCPA must provide clear documentation and user control features for their data processing activities regarding California residents [13].

Role of Security Policies in Mitigating Cloud Risks

Cloud providers need to match their security frameworks to registry requirements for effective privacy risk minimization. Security compliance relies on three main mechanisms which include encryption requirements as well as access controls and data processing activity audit logs. Cloud platforms achieve regulatory compliance assessment through a compliance score that uses this calculation method:

$$\text{Compliance Score} = \frac{\text{Implemented Policies}}{\text{Total Regulatory Requirements}} \times 100\%$$

This metric enables organizations to measure regulatory alignment quantitatively thus allowing them to make comparisons between cloud providers.

3. Results

The analysis of security and privacy problems in deep learning models operating on cloud platforms produces the reported results. The research divides its findings into three primary sections that study security challenge identification and cloud security method evaluation and regulatory constraint assessment.

3.1 Security Challenges in Cloud-Hosted Deep Learning Models

Identification of Primary Vulnerabilities

Deep learning models in the cloud experience stem from adversarial AI attacks and data protection issues as well as exposure risks to cloud infrastructure. The security issues present themselves as a result of both advanced AI system complexity and shared infrastructure characteristics of cloud platforms.

- **Adversarial AI Attacks:** The manipulation of input data by attackers results in incorrect model classification. The sensitivity of deep learning models to small changes allows attackers to perform these attacks which create wrong predictions during crucial image recognition and automated decision operations.

• **Data Security Risks:** The cloud environment has become home to numerous security threats which manifest through unauthorized access and both data breaches and poisoning attacks. Depleted encryption methods combined with faulty access control procedures create substantial security problems regarding data safety and data consistency.

• **Cloud Exposure Risks:** Security breaches of deployed AI models within cloud environments occur through multi-tenancy and insecure APIs and network vulnerabilities. Risk levels increase through Distributed denial-of-service (DDoS) attacks and incidents of API exploitation.

Case Studies on Security Breaches in AI Cloud Services

Security incident evaluations demonstrate critical vulnerabilities which attack AI platforms that operate in cloud environments.

Table 3. *Notable AI Security Breaches in Cloud-Hosted Environments*

Incident	Year	Attack Type	Impact
Model Extraction Attack on Cloud AI API	2021	Model Theft	Unauthorized replication of proprietary AI models
Data Poisoning Attack on Federated Learning	2022	Data Poisoning	Corrupted training data causing biased model predictions
Adversarial Attack on Image Recognition System	2023	Adversarial Perturbation	Misclassification of critical images, leading to security vulnerabilities

The findings shows that while cloud-hosted AI models boost scalability and accessibility, they remain vulnerable to advanced cyber threats.

3.2 Comparison of Security Measures in Cloud Platforms Strengths and Weaknesses in Security Implementation

A comparative assessment of leading cloud platforms—"AWS, Google Cloud, Microsoft Azure, and IBM Cloud" —reveals significant variations in security implementations.

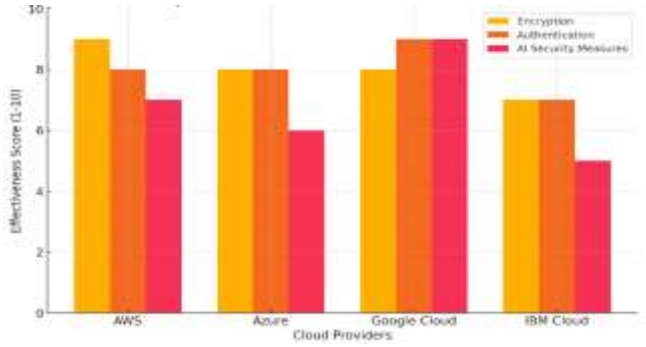

Figure 2. *Security Feature Effectiveness Across Cloud Providers*

Table 4. *Comparative Analysis of Security Features in Leading Cloud Platforms*

Security Feature	AWS	Azure	Google Cloud	IBM Cloud
Data Encryption	Advanced	High	High	Moderate
AI-Specific Security Tools	Robust	Moderate	High	Limited
Federated Learning Support	Limited	Advanced	High	Moderate
Anomaly Detection Systems	High	High	Moderate	Moderate

Effectiveness of Encryption, Differential Privacy, and Federated Learning

• **Encryption Mechanisms:** AI model protection demands cloud providers to establish AES-256 encryption in combination with TLS security protocols. The security effectiveness between key management systems and encryption granularity remains different even with AES-256 encryption and TLS security protocols implemented by providers.

• **Differential Privacy:** Google Cloud provides its users with strong differential privacy frameworks that protect AI models against data reconstruction attacks. Cloud providers other than Google Cloud have yet to implement privacy-preserving approaches that are as resilient as their frameworks for differentiated privacy.

• **Federated Learning:** The sophisticated federated learning options of Microsoft Azure enable AI training processes to operate between scattered networks in a way that maintains data privacy. The combination of IBM Cloud with AWS provides limited support for federated AI model training features.

The investigation demonstrates encryption together with anomaly detection functions thoroughly implement in all cloud platforms but privacy protection technologies and AI security frameworks need improvement.

3.3 Regulatory Framework Gaps

Limitations in GDPR, HIPAA, and Other Global Policies Regarding AI Security

The current review of regulatory systems demonstrates insufficient oversight of AI security governance measures. AI-specific security issues remain unaddressed in GDPR, HIPAA and CCPA although these regulations successfully protect data privacy rights.

Table 5. *Comparative Analysis of Regulatory Gaps in AI Security*

Regulation	Coverage of AI Security	Identified Gaps
GDPR	Strong on data privacy	Lacks AI-specific security mandates
HIPAA	Robust for healthcare data	No provisions for adversarial AI threats
CCPA	Emphasizes user data rights	Limited focus on AI model security

Compliance Gaps Specific to Cloud-Hosted Deep Learning Models

Organizations having compliance with established regulatory policies face challenges in shielding their systems against security threats related to AI implementation.

- **GDPR Compliance:** GDPR requires strong data protection but does not contain full guidance on AI security standards.
- **HIPAA Compliance:** The HIPAA security standard handles healthcare AI application protection via encryption and access protocols yet fails to address adversarial disturbances together with inversion model attacks.
- **CCPA Compliance:** CCPA emphasizes user transparency but does not include regulatory mandates for securing AI inference models.

New AI security-specific policies require immediate revision to provide coverage for the security threats that arise within cloud-based deep learning operational environments.

4. Discussion

The research results demonstrate multiple serious threats to cloud-hosted deep learning model security and privacy requirements. The fast growth of AI-based cloud computing systems has created novel security weaknesses that involve adversarial attacks as well as unauthorized model access and data breaches. The open nature and sharing characteristics of cloud environments create security risks that lead to these problems. Security frameworks have gained new urgency because threats that exploit training data and inference pipelines and model storage became possible through adversary exploitation [14].

Security measures that rely on traditional encryption fail to properly protect the vulnerabilities which are specific to AI models. The present encryption protocols protect data at rest and in transit properly, yet they do not stop operatives from performing model inversion or generating adversarial perturbations during inference operations. Researchers have introduced three innovative security approaches of homomorphic encryption along with differential privacy and federated learning for strengthening cloud-based AI model privacy and integrity [15]. The methods combine solutions to handle both system data protection together with the enhancement of model stability to make AI systems resistant to new security risks.

Homomorphic encryption represents an effective solution for protecting data in AI computations by enabling encrypted information processing without decryption steps. Strong privacy protection occurs through this technique because it prevents unauthorized users from viewing raw data during computational operations. Homomorphic encryption implementation creates computational expenses which limit its practical use for real-time processing of large-scale AI systems [16]. Statistical data protection through differential privacy works by inserting noise to statistics to prevent unauthorized parties from pinpointing sensitive data. The strong protection capabilities of differential privacy for user anonymity result in significant precision losses in domains such as healthcare and finance due to its nature [17].

The distributed learning platform of federated learning enables programmers to train models on separate nodes without allowing actual data to be combined. Data security improvements and privacy compliance occur when sensitive information remains within specific geographic areas through this approach. Attacks on federated learning security remain possible through poisoning because attackers can submit corrupted model updates to change the global model according to [18]. Scientists developed combined encryption systems by bringing together homomorphic encryption and differential privacy technology within federated learning frameworks because researchers needed enhanced security measures that would not cause computational delays [19].

The research findings present essential points for organizations which employ AI-based cloud services across different operational areas. Healthcare organizations need privacy-protecting AI approaches to safeguard patient information which enables compliance with data protection mandates such as GDPR and HIPAA. Researchers

have demonstrated how linking federated learning with homomorphic encryption helps medical institutions work together using decentralized patient data storage which protects data from unwanted access [20]. Financial institutions conducting AI-based fraud prevention and risk monitoring responsibilities need to establish robust encryption systems to protect transactions from unauthorized adjustments. Financial organizations using AI for applications must establish robust security systems to avoid economic dangers as well as penalties from non-compliance regulations [21].

Network security AI models need real-time defence adaptations to stop adversarial attacks when deployed for threat detection and security purposes. The implementation of differential privacy standards in cybersecurity platforms blocks confidential data disclosure and preserves threat detection algorithms' ability to resist fraud attempts [22]. Security enhancements through continuous AI framework development maintain the integrity of cloud-based AI systems because of the changing nature of cyber threats.

The future research agenda should concentrate on maximizing homomorphic encryption system capabilities by finding methods to decrease operational speed and expand practical large-scale implementation potential. The creation of reduced-cipher cryptographic approaches would enable the practical implementation of homomorphic encryption when deployed in real-time cloud-based AI models [20]. Research needs to focus on developing stronger protection measures for federated learning against poisoning attacks to ensure its robustness. Two encryption defence systems based on blockchain technology and anomaly detection systems provide enhanced model security by preventing unauthorized model updates [21]. Differential privacy integrated throughout training and inference processes brings an additional defensive measure which protects security but maintains model fidelity [22].

AI security frameworks will develop better threat-handling capacities when research gaps related to cybersecurity are resolved. AI-driven cloud infrastructure sustainability depends heavily on deploying security protocols that protect privacy and resist adversarial attacks. Future advancements in AI security need to establish two primary goals which combine data protection with model reliability and regulatory peace of mind to build a secure AI system in cloud environments.

5. Conclusion

The evaluation of cloud-hosted deep learning models reveals active threats against their security and privacy because of adversarial attacks together with model inversion and data poisoning tactics. Research data shows that security breaches within cloud AI operations mostly result from inadequate authentication measures together with poor encryption practices requiring robust security solutions. AWS and Google Cloud provide strong encryption along with anomaly detection but Microsoft Azure leads with federated learning capabilities and IBM Cloud offers restricted AI security solutions to its clients. Homomorphic encryption development alongside differential privacy and federated learning failed to address three main obstacles which included long computation times and accuracy reduction as well as poison attacks in systems. The data protection standards set by GDPR and HIPAA and CCPA fail to address security threats that specifically arise from AI models deployed through the cloud. Researchers need to work on both enhancing encryption operational speed and creating better defence solutions to stop adversarial attacks on federated learning systems and developing on-demand protective systems. Complete security scalability and compliance and increased trust with system sustainability result from uniting encryption practices with privacy-preserving learning methods and AI threat detection systems within a multiple security system for AI-driven cloud infrastructure deployment.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Mell, P., & Grance, T. (2011). The NIST definition of cloud computingNIST Special Publication. *National Institute of Standards and Technology, Gaithersburg, Maryland, USA*.

[2] Schmidhuber, J. (2015). Deep learning in neural networks: An overview. *Neural networks*, *61*, 85-117.

[3] Zhang, X., Liu, C., Nepal, S., Yang, C., Dou, W., & Chen, J. (2014). A hybrid approach for scalable sub-tree anonymization over big data using MapReduce on cloud. *Journal of Computer and System Sciences*, *80*(5), 1008-1020.

[4] Sukender Reddy Mallreddy. (2023). Enhancing Cloud Data Privacy Through Federated Learning: A Decentralized Approach To Ai Model Training. *Ijrdo -Journal of Computer Science Engineering*, *9*(8), 15-22. https://doi.org/10.53555/cse.v9i8.6131

[5] Rangaraju, S. (2023, December 1). Ai Sentry: Reinventing Cybersecurity Through Intelligent Threat Detection. *Eph - International Journal of Science and Engineering*, *9*(3), 30–35. https://doi.org/10.53555/ephijse.v9i3.211

[6] Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In *Proceedings of the 16th ACM conference on Computer and communications security* (pp. 199-212).

[7] 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).

[8] Papernot, N., McDaniel, P., Sinha, A., & Wellman, M. P. (2018). Sok: Security and privacy in machine learning. In *2018 IEEE European symposium on security and privacy (EuroS&P)* (pp. 399-414). IEEE.

[9] Carlini, N., & Wagner, D. (2017). Towards evaluating the robustness of neural networks. In *2017 ieee symposium on security and privacy (sp)* (pp. 39-57). Ieee.

[10] Voigt, P., & Von dem Bussche, A. (2017). The eu general data protection regulation (gdpr). *A practical guide, 1st ed., Cham: Springer International Publishing*, *10*(3152676), 10-5555.

[11] Regulation, P. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council. *Regulation (eu)*, *679*, 2016.

[12] Act, A. (1996). Health insurance portability and accountability act of 1996. *Public law*, *104*, 191.

[13] Illman, E., & Temple, P. (2019). California consumer privacy act. *The Business Lawyer*, *75*(1), 1637-1646.

[14] Luqman, A., Mahesh, R., & Chattopadhyay, A. (2024). Privacy and security implications of cloud-based AI services: A survey. *arXiv preprint arXiv:2402.00896*.

[15] Aziz, R., Banerjee, S., Bouzefrane, S., & Le Vinh, T. (2023). Exploring homomorphic encryption and differential privacy techniques towards secure federated learning paradigm. *Future internet*, *15*(9), 310.

[16] Yang, W., Bai, Y., Rao, Y., Wu, H., Xing, G., & Zhou, Y. (2024). Privacy-Preserving Federated Learning with Homomorphic Encryption and Sparse Compression. In *2024 4th International Conference on Computer Communication and Artificial Intelligence (CCAI)* (pp. 192-198). IEEE.

[17] Adelakun, N. O. (2024). Exploring the Impact of Artificial Intelligence on Information Retrieval Systems. *Information Matters*, *4*(5).

[18] Sébert, A. G., Checri, M., Stan, O., Sirdey, R., & Gouy-Pailler, C. (2023). Combining homomorphic encryption and differential privacy in federated learning. In *2023 20th Annual International Conference on Privacy, Security and Trust (PST)* (pp. 1-7). IEEE.

[19] Rehan, H. (2024). AI-driven cloud security: The future of safeguarding sensitive data in the digital age. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1), 132-151.

[20] Cao, D., Wang, C., Sun, H., Cao, C., Kang, M., Zheng, H., ... & Tong, Q. (2023). Multiinstitutional Lung Image Classification Using Privacy-Preserving Horizontal Federated Learning with Homomorphic Encryption. In *2023 IEEE International Conference on E-health Networking, Application & Services (Healthcom)* (pp. 131-136). IEEE.

[21] Ginanjar, M. G., Lubis, M., Ramadani, L., & Handayani, D. O. D. (2024). Enhancing Security and Privacy in Cloud Computing: Challenges and Solutions in the Digital Age. In *2024 3rd International Conference on Creative Communication and Innovative Technology (ICCIT)* (pp. 1-6). IEEE.

[22] Park, J., & Lim, H. (2022). Privacy-preserving federated learning using homomorphic encryption. *Applied Sciences*, *12*(2), 734.