Journal of Science and Technology
ISSN: 2456-5660 Volume 10, Issue 07 (July -2025)
www.jst.org.in *DOI: https://doi.org/10.46243/jst.2025.v10.i07.pp29-36*

Privacy and Data Protection: Ensuring Compliance with Federated Learning in the Digital Age

Guman Singh Chauhan[1*], Venkata Surya Teja Gollapalli[2], Kannan Srinivasan[3], Rahul Jadon[4], Gamachis Ragasa Gutata[5]

[1]John Tesla Inc, Texas, USA. Email: gumansinghchauhan@ieee.org

[2]Centene Management Company LLC, Missouri, United States. Email: venkatasuryatejagollapalli@ieee.org

[3]Saiana Technologies Inc, New Jersey, USA. Email: kannansrinivasan@ieee.org

[4]CarGurus Inc, Massachusetts, USA. Email: rahuljadon@ieee.org

[5]College of Engineering and Technology, Dambi Dollo University, Dambi Dollo, Ethiopia. Email: gamachisragasa@dadu.edu.et

To Cite this Article

Guman Singh Chauhan, Venkata Surya Teja Gollapalli, Kannan Srinivasan, Rahul Jadon, Gamachis Ragasa Gutata. **Privacy and Data Protection: Ensuring Compliance with Federated Learning in the Digital Age**, *Journal of Science and Technology*, Vol. 10, Issue 07, July 2025, pp. 29-36.

Article Info

Received: 25-Apr-2025 Revised: 10-May-2025 Accepted: 04-June-2025 Published: 06-July-2025

Abstract

Today's digital age has made privacy and data protection a major concern-generally, with the kind of technologies that are turning things around and bringing everything to the cloud. FL will most likely provide a solution to the distance and make things clear in collaboration without exposing raw information from a consortium to boost its privacy. However, existing FL solutions include such challenges as increased overhead communication, risk in leaking data, and even the inefficiency of secure aggregation. To mitigate these constraints, this research proposes the Autoencoder-Based Federated Learning framework by integrating prevailing techniques such as differential privacy and homomorphic encryption that safeguard both the security and efficiency of the model. This method does not only steal model ideas for autoencoders to compress before sciences transmission but hugely reduces the transmission bandwidth and possibly minimizes gradient leakage. However, adaptive normalization is used to handle institutional heterogeneity to maintain better performance for the model. Conclusion of experimentation indicated that this framework could significantly reduce communication overhead while retaining high federated learning accuracy and even better security. Further, the trust-based client evaluation mechanism is presented to detect malicious behavior and improve reliability regarding federated aggregation. The experiment showed that Autoencoder Based Federated Learning was a scalable, secure, and privacy-efficient solution to applications tailored for healthcare, finance, and other sensitive data environments.

Keywords: *Federated Learning, Privacy Protection, Autoencoders, Secure Aggregation, Differential Privacy.*

1. Introduction

Security and data protection have become more important in the digital context where people rely on data-driven technologies. Organizations nowadays collect huge amounts of personal, financial, and confidential information that needs to be protected from breaches [1]. Data security ensures that unauthenticated access or theft or misuse of information is granted [2]. Regulations like these really impose tight handling for user data through rules that are within them, like that of GDPR and HIPAA [3]. Although all of that, cyber threats keep evolving, hence making privacy protection a challenge all through [4]. AI and machine learning have made data security really more complex because they usually demand large amounts of real data for training [5]. Traditional data-sharing methods leave raw data vulnerable to third parties [6]. Risks secure computation techniques and

encryption methods mitigate, but they usually come at the high price of computational overhead [7]. Companies should try never to breach this fine line of accessibility and security in their compliance with laws [8]. Indeed, privacy hygiene is required in such a world that is highly interconnected to trust in and protect sensitive data.

The data cannot have privacy and security without proper standards. Weak data security standards have brought in privacy and data breaches [9]. Hacking is another method that also brings about unauthorized access to sensitive data [10]: Most of its involvement is from weaknesses contained in the systems. As data are increasingly placed in the cloud or stored remotely, interception and hacking may become possible [11]. But, on the other side, it identifies the insider threat, which occurs when employees misuse or fake-to-leak the confidential information. Without proper encryption techniques, an attacker can break encryption and misuse data inappropriately [12]. Several organizations cannot adopt strong data governance policies, leading to unregulated access and numerous risks [13]. Phishing and social engineering attacks trick a number of users to reveal personal information [14]. The flood of data points emerges because of the massive growth of IoT with little or no security in their collection [15]. Most promise but holds little regarding data utility versus privacy, forcing companies to take compromises at times damaging the protection appointed. Regulatory non-compliance and obsolete security frameworks worsen the situation for data exposure and loss.

Methods for the protection of privacy in a traditional sense include encryption, access control mechanisms, and secure storage [16]. Homomorphic encryption makes it possible to run computations on encrypted data but introduces prohibitively high computational complexity[17]. SMPC, on the other hand, avoids revealing records while allowing their analysis, but uses a lot of communication overhead [18]**.** Differential privacy causes noise addition in data so that it cannot be leaked; however, a lot of noise can reduce the use of that data**.** FL allows training of the model without the actual raw data shared, which is good for privacy, but still, there are gradient leaks Blockchain-based solutions have an advantage in securing and transparent sharing of data but fail in terms of scalability and high energy consumption [19]. Firewalls and intrusion detection systems can help protect networks from cyberattacks, but neither can eliminate all security threats altogether [20]. Anonymization techniques try to eliminate personally identifiable information, though these techniques are subject to re-identification formation[21]. Secure enclaves may provide a trusted execution environments but usually require specialized hardware[22]. Even with all the advancements, the privacy methods existing today are still either inefficient or completely unable to protect all sensitive information from advanced threats.

Autoencoder-based federated learning in privacy provides more secured features than other frameworks by compressing model updates before uploading them to the server. Autoencoders allow removal of identifiable patterns while retaining important components of learning and keeping communication cost lower while increasing the model's scalability. Further strengthening data protection is achieved via differential privacy combined with homomorphic encryption. Such will reduce various adversarial attacks, for example, gradient leakage, and also increase the rate at which convergence is achieved within the model. Autoencoder-based federated learning enhances compliance with regulations by combining privacy-preserving techniques with efficient data compression, all while optimizing model performance, making it highly suitable for secure applications within healthcare, finance, and other data-sensitive industries.

Section 2 discusses the Literature Review. Section 3 gives the problem statement and Section 4 Privacy-Preserving Data Processing Framework Using Autoencoder-Based Federated Learning. Section 5 result and discussion, and Section 6 gives a conclusion with suggestions for future directions of research.

2. Literature Review

Methods that currently exist such as VGG-16, IrisConvNet, SVM, and residual networks have serious issues such as excessively higher computational costs and longer training times[23]. Furthermore, the suggested FRCNN outperforms all these methods by intercalating classification and regression layers that optimize these processes to enhance their efficiency and accuracy. RF-SVM has difficulties in the classification of IBD, owing to overfitting and class imbalance problems [24]. This EL model intended for research combines Logistic Regression, Random Forest, and Gaussian Naïve Bayes that make the model better in feature selection and accurate prediction.

One significant drawback of the conventional object detection approaches is that they could not effectively balance generating features across different scales [25]. This work presents an improvement on the detection accuracy by introducing a novel loss function in the CIoU-YOLO v5 method, whereas traditional such as DLM model failed to perform well on that domain semantic data transmission leading to performance drop. [26] suggested existing methods like CNNs, SVM, and Random Forest aid lung disease diagnosis but face issues like class imbalance, poor generalization, and high false positives, impacting accuracy.

 DOI: https://doi.org/10.46243/jst.2025.v10.i07.pp29-36

Existing methods of managing finance budgets employ traditional rule-based applications and manual tracking techniques [27]. Such approaches are, therefore, not adaptable or efficient. AI tricks such as machine learning and data mining allow automation of processes, although data privacy, computation costs, and the difficult integration with the existing legacy systems may act as counterforces. [28] suggested traditional supply chain security systems rely on centralized databases and encryption, which are less secure. Blockchain, IoT, and CP-ABE provide enhanced security, whereas confronting challenges of computational protocols and acceptance.

3. Problem Statement

Challenges are present in the existing methods concerned with object detection, financial management, diagnosis of diseases, and securing the supply chain. Traditional object detection models are unable to achieve a balance between multi-scale feature extraction, affecting their accuracy [29]. Financial budgeting is inefficient because it is rule-based and manually tracked, leading to errors.

Concerning lung diseases, classification methods are troubled by class imbalance and poor generalization, giving rise to high false positives. On the other hand, centralized supply chain security systems are based on traditional encryption techniques that are susceptible to cyber threats and unauthorized access [30]. To solve these issues, advanced AI and machine learning models enhance automation, accuracy, and security. Automated financial budgeting enhances the optimal allocation of resources while unique loss functions integrated into AI-based object detectors improve detection of true positives.

4. Privacy-Preserving Data Processing Framework Using Autoencoder-Based Federated Learning

Privacy-preserving framework as shown in the diagram is facilitated by the use of Autoencoder-Based Federated Learning. It starts from data acquisition to adaptive normalization for pre-processing. The federated learning approach provides a centralized model for training to ensure data privacy and protection. Lastly, performance evaluation pertains to measuring performance effectiveness in terms of its degree of accuracy, security, and efficiency, thus enhancing secure AI-driven analytics is shown in Figure (1),

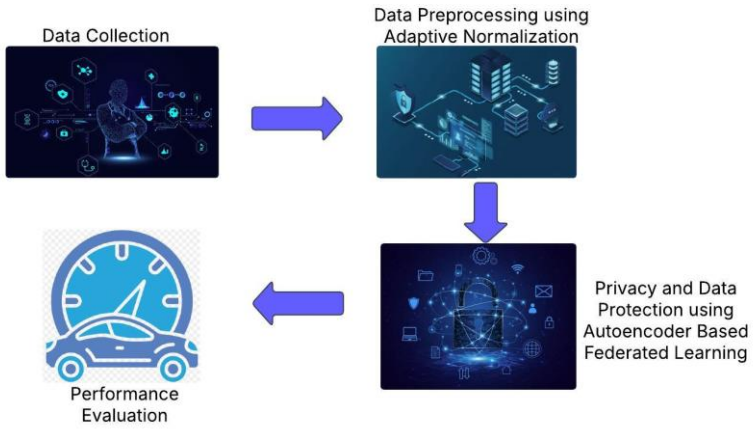

Figure 1: Secure Data Processing and Privacy Protection Using Federated Learning

4.1 Data Collection

The synthetic healthcare dataset serves as a simulation of real-world records targeted at applications in data science and machine learning. It comprises details about the patients, admission, billing, and test results. It was generated through the Faker library of Python, which guarantees the anonymity of the dataset; thus, this dataset is suitable for analysis and predictive modeling.

Data Set link: https://www.kaggle.com/datasets/prasad22/healthcare-dataset

4.2 Data Preprocessing Using Adaptive Normalization

Standard batch normalization assumes that throughout the whole process, the model expects that all institutions share the same statistical properties. This is, of course, not true. Adaptive Normalization (AdaNorm), therefore, is brought into play, allowing each institution to maintain its unique distribution characteristics while also contributing to the global learning process.

4.2.1 Standard Batch Normalization

 DOI: https://doi.org/10.46243/jst.2025.v10.i07.pp29-36

Before applying adaptive normalization, one typically applies standard batch normalization in deep learning, which normalizes distribution of data while enabling convergence. The normalization is determined for some given mini-batch of data according to Eq. (1),

$$X_i^{\text{norm}} = \frac{X_i - \mu_B}{\sigma_B + \epsilon} \quad (1)$$

Where, X_i is the input data from institution i, μ_B is the mean of the batch, σ_B is the standard deviation of the batch, ϵ is a small constant to ensure no division by zero, X_i^{norm} is the normalized data.

4.2.2 Adaptive Normalization (Institution-Specific Adjustments)

The step ensures that the process of normalization truly accounts for the unique characteristics of the data of each institution so that the performance is not compromised owing to domain shift. To remedy this, we introduce adaptive scaling and shifting. Each institution learns its own scaling factor γ_i and shift factor β_i to adjust the normalized values as per Eq. (2),

$$X_i^{\text{adapt}} = \gamma_i \cdot X_i^{\text{norm}} + \beta_i \quad (2)$$

Where γ_i is a learnable scale factor that adjusts | feature variance | for institution i, β_i is a learnable shift factor that adjusts the feature mean for the institution i, X_i^{adapt} is the final product adaptively normalized data used for model training.

4.3 Auto Encoder-based Federated Learning: Privacy and Data Protection

FL permits model training in collaboration with multiple institutions without compromising the private data. Each institution trains a local model on its dataset and sends updates only to the main server without sending the data. Any update sent does have the potential to reveal confidential information; therefore, some form of extra privacy can be enforced. Further, we enhance privacy by integrating Autoencoder-Based Federated Learning and differential privacy. This method ensures that in case of interception of communication, patient data are protected.

4.3.1-Local Model Training in Federated Learning

Federated learning sees each institution train in an independent manner and not share raw data. Each institution i trains a local model $f_{\theta i}$ on its private dataset D_i. The update is performed using gradient descent, as indicated in Eq. (3),

$$\theta_i^{t+1} = \theta_i^t - \eta \nabla L(D_i, \theta_i) \quad (3)$$

Here, θ_i^t denotes the model parameters at time step t, η is the learning rate, $L(D_i, \theta_i)$ is the loss function computed on the local dataset Di, and $\nabla L(D_i, \theta_i)$ represents the gradient update.

- **Aggregate Securely through Federated Learning: Time Considering Distributed Systems**

When the small iteration training and local model are finished for all institutions, the institutions will send their encrypted model updates to the central server for aggregation through Federated Averaging (FedAvg), given by Eq. (4),

$$\theta^{t+1} = \sum_{i=1}^{N} \frac{|D_i|}{|D|} \theta_i^{t+1} \quad (4)$$

Where N is the number of institutions, |Di| is the dataset size of institution i, |D| is the total dataset spread along the institutions; This means large datasets will carry greater weight during the aggregation of the global model training. The updated global model is then sent back to the institutions for the next round of training.

4.3.2 Creating an Autoencoder-based Privacy-Protecting

Herein, the autoencoder-based privacy protection provides federated learning services delivered to compressed model updates, which reduces the risk of sensitive data exposure to malicious infiltration. Every institution compresses the model updates θ_i through an autoencoder to represent them as a lower-dimensional latent representation Z_i, which effectively destroys identifiable patient-level information. Instead of sharing general updates of the model with each other, institutions share compressed representations, which reduces possible exposure. After this process, the global aggregation server uses a decoder to recompute the original model updates from the encoded updates, thereby ensuring sensitive data is well concealed while allowing for effective model training. This significantly reduces the risk of reconstructing private data from shared updates and is thus proven to maintain improved privacy and security within the federated learning systems as expressed in Eq. (5).

Journal of Science and Technology
ISSN: 2456-5660 Volume 10, Issue 07 (July -2025)
www.jst.org.in *DOI: https://doi.org/10.46243/jst.2025.v10.i07.pp29-36*

$$Z_i = Encoder(\theta_i)$$
$$\theta_i' = Decoder(Z_i) \quad (5)$$

Where, Z_i is the compressed representation and θ_i'' is the reconstructed update.

- **Differential Privacy**

Model updates may still leak sensitive information despite using autoencoders. So that the ability of an attacker to deduce information about a specific patient cannot be increased higher than some mathematical threshold inference limit. To do this, Differential Privacy (DP) is used by adding random noise to gradients before giving it out is indicated in the form of Eq. (6):

$$\tilde{\nabla}L = \nabla L + N(0, \sigma^2) \quad (6)$$

Where, $N(0, \sigma^2)$ is Gaussian noise with variance σ^2.

5. Results and Discussion

Such results prove that it is possible to do secure aggregation with autoencoders in federated learning. In Figure 2, overheads for communication are seen to be increasing along with model complexity; however, autoencoders save up from using this bandwidth using compressed updates while performing privacy guarantees. Such leads to better performance compared to traditional methods of encryption. Figure 3 shows various trust scores across clients. While trust is evident in some, such as client 14, poor scores become worse, suggesting adversarial behavior. This emphasizes the importance of trust-based monitoring for secure and equitable model aggregation. Anomaly detection and reputation-based weighting will make this principle a lot better for securing the system. In harmony with all these, efficiency is balanced with security as well as trustworthiness to provide federated learning.

5.1 Efficient Communication Overhead in Autoencoder-Based Secure Aggregation

The graph presents the communication overhead in secure aggregation with autoencoders, plotting communication rounds against transmitted data per round (in MB). The autoencoder compresses model updates to minimize bandwidth usage, thus safeguarding privacy is displayed in Figure (2),

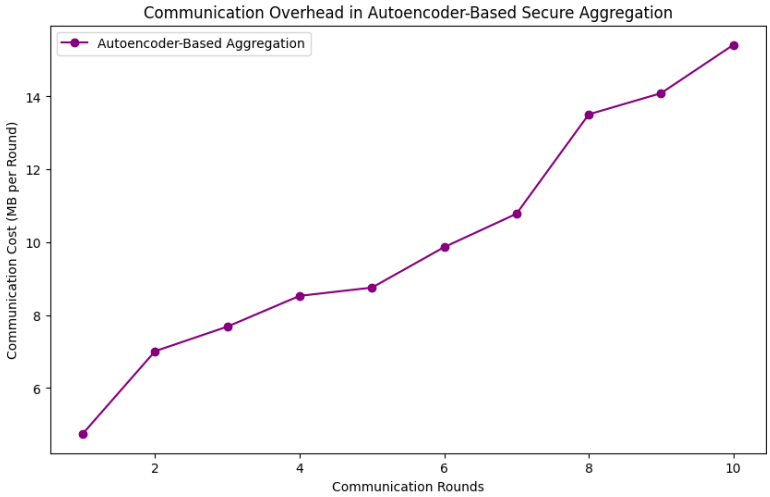

Figure 2: Optimizing Communication Overhead in Autoencoder-Enhanced Secure Aggregation

A slow ramping up of communication costs reflects an increase in model complexity while an even more sudden spike in communication costs can be observed in the later rounds. The autoencoder-based aggregation system maintains the balance between security and efficiency, thereby enabling its suitability for federated learning as an alternative to conventional encryption schemes.

5.2 Trust Score Evaluation of Clients in Federated Learning

Trust Score Distribution in Federated Learning ClientsGraph Here, the scores of trust from 0 to 1 are assigned to clients based on their trustworthy behavior in the federated learning system. The X-axis denotes client numbers, while the Y-axis represents the corresponding trust score. The higher the score, the closer it is to 1, indicating that clients can be trusted more; the closer it is to 0, the more likely it is that they have engaged in

DOI: https://doi.org/10.46243/jst.2025.v10.i07.pp29-36

adversarial behavior or are less reliable. The plotted graph will show scores on the vertical axis and clients as horizontal units, which might fluctuate depending on the time but with some clients maintaining very much higher trust values, while total trust is suddenly dropping by others is shown in Figure (3),

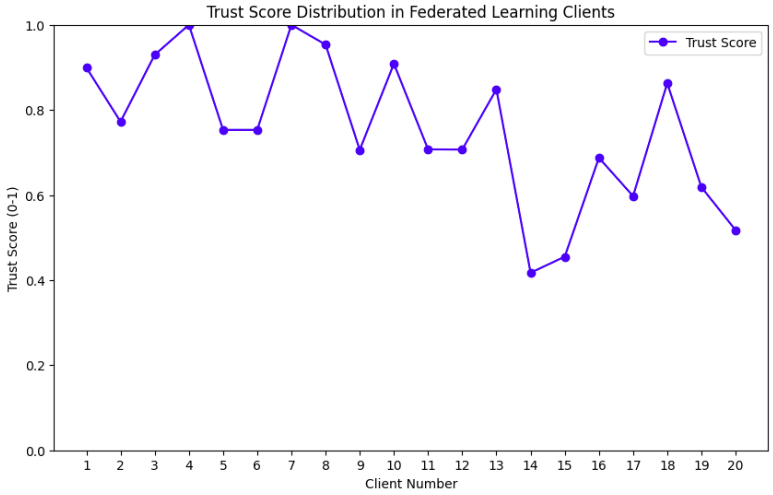

Figure 3: Client Trust Score Analysis in Federated Learning

For example, client 14 shows some major declines in performance due to possibly malicious behavior or untrustworthy updates. It underlines the need for anomaly detection of outliers, reputation-based weighting, or exclusion of unreliable clients in federated learning. Such a figure would therefore help in client trust monitoring for a strong and secure yet fair model aggregation without compromising reliability in a federated environment.

6. Conclusion and Future Works

Autoencoder-based federated learning is advanced in this research for privacy and efficiency in federated learning. The proposed method reduces the communication cost and lessens gradient leakage risks through model update compression, differential privacy, and homomorphic encryption. The experimental results have shown that the method serves as an improvement security-wise, accuracy-wise, and scalably, especially for privacy-sensitive applications like healthcare and finance. By thus empowering the model against adversarial behavior, the trust-based client evaluation mechanism will also improve the reliability of the model and create a more secure aggregation process.

Future work will enhance optimal adaptive normalization for heterogeneous data sets and include improvements to the figures of autoencoder architectures to improve computation costs.There will also be protection with security integration of blockchain technologies in making the framework strong and adaptive in cybersecurity and IoT applications. Also, the development of lightweight encryption schemes and enhancement of latency optimization in secure aggregation are potential areas wherein significant improvements are to be made toward more efficient federated learning for real-time processing environments.

References

[1] F. Schäfer, H. Gebauer, C. Gröger, O. Gassmann, and F. Wortmann, “Data-driven business and data privacy: Challenges and measures for product-based companies,” *Business Horizons*, vol. 66, no. 4, pp. 493–504, Jul. 2023, doi: 10.1016/j.bushor.2022.10.002.

[2] H. Omotunde and M. Ahmed, “A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond,” *Mesopotamian Journal of CyberSecurity*, vol. 2023, pp. 115–133, Aug. 2023, doi: 10.58496/MJCSC/2023/016.

[3] C. J. McKinstry, “The HIPAA Privacy Rule: Flawed Privacy Exposed When Compared with the European Union’s General Data Protection Regulation,” *Journal of Healthcare Finance*, Sep. 2018, Accessed: Nov. 17, 2025. [Online]. Available: https://journalofhealthcarefinance.com

[4] H. A. Salman and A. Alsajri, “The Evolution of Cybersecurity Threats and Strategies for Effective Protection. A review,” *SHIFRA*, vol. 2023, pp. 73–85, Aug. 2023, doi: 10.70470/SHIFRA/2023/009.

[5] S. R. Salkuti, “A survey of big data and machine learning,” *IJECE*, vol. 10, no. 1, p. 575, Feb. 2020, doi: 10.11591/ijece.v10i1.pp575-580.

[6] H. Jin, Y. Luo, P. Li, and J. Mathew, “A Review of Secure and Privacy-Preserving Medical Data Sharing,” *IEEE Access*, vol. 7, pp. 61656–61669, 2019, doi: 10.1109/ACCESS.2019.2916503.

[7] R. Bhadauria and S. Sanyal, "Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques," *IJCA*, vol. 47, no. 18, pp. 47–66, Jun. 2012, doi: 10.5120/7292-0578.
[8] S. A. Talesh, "Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as 'Compliance Managers' for Businesses," *Law & Social Inquiry*, vol. 43, no. 2, pp. 417–440, Apr. 2018, doi: 10.1111/lsi.12303.
[9] L. Cheng, F. Liu, and D. (Daphne) Yao, "Enterprise data breach: causes, challenges, prevention, and future directions," *WIREs Data Mining and Knowledge Discovery*, vol. 7, no. 5, p. e1211, 2017, doi: 10.1002/widm.1211.
[10] T. Jordan, "A genealogy of hacking," *Convergence*, vol. 23, no. 5, pp. 528–544, Oct. 2017, doi: 10.1177/1354856516640710.
[11] M. S. C. Mansor and M. F. Zolkipli, "A Systematic Review of Hacking on Cloud Platform," *Borneo International Journal eISSN 2636-9826*, vol. 6, no. 1, pp. 11–19, Mar. 2023.
[12] T. O. Oladoyinbo, O. B. Oladoyinbo, and A. I. Akinkunmi, "The Importance Of Data Encryption Algorithm In Data Security".
[13] J. Kuzio, M. Ahmadi, K.-C. Kim, M. R. Migaud, Y.-F. Wang, and J. Bullock, "Building better global data governance," *Data & Policy*, vol. 4, p. e25, Jan. 2022, doi: 10.1017/dap.2022.17.
[14] S. Prasad Panda, "The Evolution and Defense Against Social Engineering and Phishing Attacks," *IJSR*, vol. 14, no. 5, pp. 397–408, May 2025, doi: 10.21275/SR25504223645.
[15] M. Shafiq, Z. Gu, O. Cheikhrouhou, W. Alhakami, and H. Hamam, "The Rise of 'Internet of Things': Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, p. 8669348, 2022, doi: 10.1155/2022/8669348.
[16] H. Liu, "Enhancing Data Security and Privacy in Cloud-based Big Data Systems: A Focus on Encryption and Access Control," *Nuvern Applied Science Reviews*, vol. 7, no. 3, pp. 1–11, Mar. 2023.
[17] K. Munjal and R. Bhatia, "A systematic review of homomorphic encryption and its contributions in healthcare industry," *Complex Intell. Syst.*, vol. 9, no. 4, pp. 3759–3786, Aug. 2023, doi: 10.1007/s40747-022-00756-z.
[18] I. Zhou, F. Tofigh, M. Piccardi, M. Abolhasan, D. Franklin, and J. Lipman, "Secure Multi-Party Computation for Machine Learning: A Survey," *IEEE Access*, vol. 12, pp. 53881–53899, 2024, doi: 10.1109/ACCESS.2024.3388992.
[19] Z. Ullah, B. Raza, H. Shah, S. Khan, and A. Waheed, "Towards Blockchain-Based Secure Storage and Trusted Data Sharing Scheme for IoT Environment," *IEEE Access*, vol. 10, pp. 36978–36994, 2022, doi: 10.1109/ACCESS.2022.3164081.
[20] D. Kumar and M. Gupta, "Implementation of Firewall & Intrusion Detection System Using pfSense To Enhance Network Security".
[21] R. Chevrier, V. Foufi, C. Gaudet-Blavignac, A. Robert, and C. Lovis, "Use and Understanding of Anonymization and De-Identification in the Biomedical Literature: Scoping Review," *Journal of Medical Internet Research*, vol. 21, no. 5, p. e13484, May 2019, doi: 10.2196/13484.
[22] M. Schneider, A. Dhar, I. Puddu, K. Kostiainen, and S. Capkun, "Composite Enclaves: Towards Disaggregated Trusted Execution," *TCHES*, pp. 630–656, Nov. 2021, doi: 10.46586/tches.v2022.i1.630-656.
[23] K. Nguyen, C. Fookes, A. Ross, and S. Sridharan, "Iris Recognition With Off-the-Shelf CNN Features: A Deep Learning Perspective," *IEEE Access*, vol. 6, pp. 18848–18855, 2018, doi: 10.1109/ACCESS.2017.2784352.
[24] J. Gubatan, S. Levitte, A. Patel, T. Balabanis, M. T. Wei, and S. R. Sinha, "Artificial intelligence applications in inflammatory bowel disease: Emerging technologies and future directions," *World J Gastroenterol*, vol. 27, no. 17, pp. 1920–1935, May 2021, doi: 10.3748/wjg.v27.i17.1920.
[25] L. Aziz, Md. S. B. Haji Salam, U. U. Sheikh, and S. Ayub, "Exploring Deep Learning-Based Architecture, Strategies, Applications and Current Trends in Generic Object Detection: A Comprehensive Review," *IEEE Access*, vol. 8, pp. 170461–170495, 2020, doi: 10.1109/ACCESS.2020.3021508.
[26] Rathinam College of Arts and Science, India, G. R. N, K. S, and Rathinam College of Arts and Science, India, "ADVANCEMENTS IN AI AND MACHINE LEARNING FOR CANCER DIAGNOSIS A COMPARATIVE ANALYSIS ON CNN, SVM, AND RANDOM FOREST MODELS TO ENHANCE DETECTION ACCURACY," *IJIVP*, vol. 15, no. 3, pp. 3495–3500, Feb. 2025, doi: 10.21917/ijivp.2025.0495.
[27] A. Althnian, "Design of a Rule-based Personal Finance Management System based on Financial Well-being," *IJACSA*, vol. 12, no. 1, 2021, doi: 10.14569/IJACSA.2021.0120122.
[28] B. Annane, A. Alti, and A. Lakehal, "Blockchain based context-aware CP-ABE schema for Internet of Medical Things security," *Array*, vol. 14, p. 100150, Jul. 2022, doi: 10.1016/j.array.2022.100150.

[29] D. Cao, Z. Chen, and L. Gao, "An improved object detection algorithm based on multi-scaled and deformable convolutional neural networks," *Hum. Cent. Comput. Inf. Sci.*, vol. 10, no. 1, p. 14, Apr. 2020, doi: 10.1186/s13673-020-00219-9.

[30] "A Survey on Supply Chain Management: Exploring Physical and Cyber Security Challenges, Threats, Critical Applications, and Innovative Technologies - ProQuest." Accessed: Nov. 17, 2025. [Online]. Available: https://www.proquest.com/openview/dccaf40b0731630dcd3e86ca3995d0a1/1?pq-origsite=gscholar&cbl=2045302