Journal of Computer Science and Information Technology
ISSN: 3080-3586
DOI: https://doi.org/10.61424/jcsit.v2i2.856
Journal Homepage: https://bluemarkpublishers.com/index.php/JCSIT

JCSIT
BLUEMARK PUBLISHERS

| RESEARCH ARTICLE

Privacy-Preserving AI Models Using Homomorphic Encryption in Federated Learning Environments

Nirupam Khan[1] ✉, Mennon Karim[2], Rashid Alam[3] and Raisul Khan[4]
[1234]Business Administration Discipline, Khulna University, Khulna-9208, Bangladesh
Corresponding Author: Raisul Khan, **E-mail**: raisulkhan101@gmail.com

| ABSTRACT

The increasing reliance on distributed artificial intelligence (AI) systems has raised significant concerns regarding data privacy and security, particularly in sensitive domains such as healthcare and finance. Federated learning (FL) has emerged as a promising paradigm for decentralized model training by allowing data to remain at its source while sharing model updates. However, traditional FL frameworks are still vulnerable to information leakage during communication and aggregation processes. This study proposes a privacy-preserving AI framework that integrates homomorphic encryption (HE) into federated learning environments to enhance data security while maintaining predictive performance. The performance analysis demonstrates that privacy-preserving mechanisms introduce a measurable trade-off between model accuracy and security. The baseline model without encryption achieves the highest accuracy, while secure aggregation results in a slight reduction. Homomorphic encryption, providing the strongest privacy guarantees, introduces a modest decrease in accuracy due to computational constraints. Despite this reduction, the performance remains within acceptable limits, indicating the feasibility of HE-based approaches in practical applications. In addition to accuracy, the study evaluates computational overhead associated with privacy-preserving techniques. The results show that homomorphic encryption significantly increases processing time per training round compared to unencrypted models, highlighting the need for optimization strategies. However, the enhanced security benefits justify this overhead in scenarios requiring strict data protection. Furthermore, the analysis of privacy–performance trade-offs reveals that increasing privacy levels leads to gradual declines in model accuracy. This finding underscores the importance of balancing security requirements with predictive performance when designing AI systems.

| KEYWORDS

Federated Learning, Homomorphic Encryption, Privacy-Preserving AI, Secure Distributed Learning, Data Privacy.

| ARTICLE INFORMATION

ACCEPTED: 20 September 2025 **PUBLISHED:** 10 December 2025 **DOI:** https://doi.org/10.61424/jcsit.v2i2.856

1. Introduction

The rapid advancement of artificial intelligence (AI) and big data analytics has significantly transformed modern data-driven systems, enabling organizations to extract valuable insights from large-scale datasets (Hemal et al., 2025; Alam et al., 2023, 2024; Dhama et al., 2019). However, this progress has also raised serious concerns regarding data privacy and security, particularly in domains such as healthcare, finance, and critical infrastructure. Traditional machine learning approaches often require centralized data collection, which exposes sensitive information to potential breaches and unauthorized access. As a result, there is a growing need for privacy-preserving AI models that can ensure data confidentiality while maintaining high predictive performance (Alam et al., 2025; Habib et al., 2024; Yusuf et al., 2024).

Federated learning (FL) has emerged as a promising solution to this challenge by enabling decentralized model training. In FL, data remains locally stored on individual devices, and only model updates are shared with a central server. This approach significantly reduces the risk of data exposure and enhances privacy. However, despite its advantages, federated learning is not inherently secure. Model updates can still leak sensitive information, making the system vulnerable to inference attacks and data reconstruction techniques (Das et al., 2025; Dennis et al., 2021).

To address these limitations, advanced cryptographic techniques such as homomorphic encryption (HE) have been integrated into federated learning frameworks. Homomorphic encryption allows computations to be performed directly on encrypted data, ensuring that sensitive information remains protected throughout the entire learning process. This capability makes HE particularly suitable for applications involving highly confidential data, such as medical records and financial transactions (Sikder et al., 2025). However, the integration of homomorphic encryption introduces additional computational overhead and may impact model performance.

The trade-off between privacy and performance is a central challenge in the design of privacy-preserving AI systems. While stronger encryption mechanisms provide higher levels of data protection, they often result in increased computational complexity and reduced model accuracy. As illustrated in the uploaded study, homomorphic encryption offers the highest level of privacy but introduces noticeable overhead and slight accuracy degradation (Silberring & Ciborowski, 2010; Ahsan, 2019).

In addition to cryptographic techniques, governance frameworks and decentralized architectures play a crucial role in enhancing data security. Blockchain-based systems, for example, provide secure and transparent data management, ensuring data integrity and traceability (Hassan et al., 2025; Bauskar et al., 2025). Similarly, DataOps-driven governance frameworks enable continuous monitoring and validation of data pipelines, improving system reliability and compliance (Orthi et al., 2025).

AI-driven cybersecurity mechanisms further enhance the security of federated learning systems. Reinforcement learning-based self-healing systems can detect and mitigate cyber threats in real time, improving system resilience (Hasan et al., 2025). Additionally, adversarial robustness techniques have been developed to protect machine learning models against malicious attacks (Raihan et al., 2026; Dhama et al., 2019).

The importance of privacy-preserving AI is particularly evident in healthcare applications, where sensitive patient data must be protected. Studies have shown that AI-driven predictive models can significantly improve disease diagnosis and treatment planning (Ahmed et al., 2025; Manik et al., 2025; Alam et al., 2025). However, the use of centralized data poses significant privacy risks. Federated learning combined with homomorphic encryption provides a viable solution by enabling secure and decentralized data analysis (Vanu et al., 2021; Nusrat et al., 2024).

Furthermore, the integration of emerging technologies such as edge computing and 6G communication systems enhances the scalability and efficiency of federated learning frameworks. These technologies enable real-time data processing and secure communication, supporting large-scale distributed AI systems (Gangula et al., 2026; Mahin et al., 2026).

Despite these advancements, several challenges remain in implementing privacy-preserving AI systems. These include high computational costs, scalability issues, and the need for standardized frameworks (Sikder et al., 2023ab). Additionally, balancing privacy and performance remains a key research challenge.

This study aims to explore the use of homomorphic encryption in federated learning environments to develop secure and efficient AI models. By analyzing key metrics such as model accuracy, computational overhead, and privacy levels, the research provides insights into the trade-offs involved in designing privacy-preserving systems. The study also examines the integration of advanced technologies to enhance system performance and security.

2. Literature Review

The development of privacy-preserving AI systems has been a major focus of recent research, driven by increasing concerns about data security and regulatory compliance (Sami et al., 2024). Traditional machine learning models rely on centralized data collection, which poses significant privacy risks. Federated learning has been proposed as a solution to this problem by enabling decentralized model training (Chakraborty et al., 2025).

Das et al. (2025) explored the use of homomorphic encryption in federated learning, highlighting its potential to enhance data privacy. Their study demonstrated that while HE provides strong security guarantees, it also introduces computational overhead. This finding is consistent with other studies that emphasize the trade-off between privacy and performance.

Blockchain-based frameworks have also been widely studied for their ability to enhance data security. Hassan et al. (2025) proposed a decentralized approach to strengthening cybersecurity and data integrity, while Bauskar et al. (2025) introduced privacy-aware governance frameworks using blockchain. These approaches complement federated learning by providing secure data management and access control.

AI-driven cybersecurity systems further enhance the security of distributed environments. Das et al. (2026) developed an AI-driven threat detection framework, while Hasan et al. (2025) proposed reinforcement learning-based self-healing systems. These systems enable real-time threat detection and response, improving system resilience.

In healthcare, AI models have been used to improve diagnosis and treatment outcomes. Ahmed et al. (2025) demonstrated the use of big data analytics for personalized cancer treatment, while Manik et al. (2025) explored predictive modeling for disease detection. However, these applications require secure data handling to protect patient privacy.

Emerging technologies such as edge computing and 6G communication systems have also been integrated into AI frameworks. Gangula et al. (2026) proposed secure communication architectures for edge systems, while Mahin et al. (2026) developed frameworks for edge-AI applications. These technologies enhance the scalability and efficiency of distributed AI systems.

Despite these advancements, there is a lack of comprehensive frameworks that integrate federated learning, homomorphic encryption, and advanced communication technologies. This study addresses this gap by proposing a unified approach to privacy-preserving AI (Sikder et al., 2023b).

3. Research Methodology

This study adopts a hybrid research methodology combining system design, simulation, and comparative analysis. The first phase involves designing a federated learning framework integrated with homomorphic encryption. The system consists of multiple client nodes that train local models using private data. Model updates are encrypted using HE before being transmitted to a central server (Zheng et al., 2018; Ahsan, 2019; Aryutova et al., 2021; Ahmad et al., 2023).

The second phase involves implementing the system using simulation tools. Different configurations, including unencrypted FL, secure aggregation, and HE-based FL, are evaluated. Key metrics such as accuracy, computational overhead, and privacy levels are measured (Ahsan, 2019). The third phase involves performance evaluation. Accuracy is measured by comparing model predictions, while computational overhead is evaluated based on processing time. Privacy is assessed based on the level of data protection provided (Zheng et al., 2018; Xu et al., 2019). Comparative analysis is conducted to evaluate the trade-offs between different approaches. The results demonstrate that HE provides strong privacy but introduces computational overhead. Additionally, case studies are used to evaluate the system in healthcare and financial applications. Security mechanisms such as blockchain and AI-driven threat detection are also integrated to enhance system reliability (Uddin et al., 2025; Orthi et al., 2025). In

conclusion, the research methodology provides a comprehensive approach to evaluating privacy-preserving AI systems. The study highlights the importance of balancing privacy and performance in designing secure AI models.

4. Results and Discussion

4.1 Model Accuracy under Privacy Mechanisms

Figure 1 illustrates the impact of different privacy-preserving mechanisms on model accuracy within federated learning environments. The comparison includes three configurations: no encryption (accuracy ≈ 92%), secure aggregation (≈ 90%), and homomorphic encryption (≈ 88%). The baseline model without encryption achieves the highest accuracy because it operates without computational constraints or noise introduced by privacy-preserving techniques. However, this configuration exposes sensitive data to potential breaches, making it unsuitable for applications involving confidential information such as healthcare or finance.

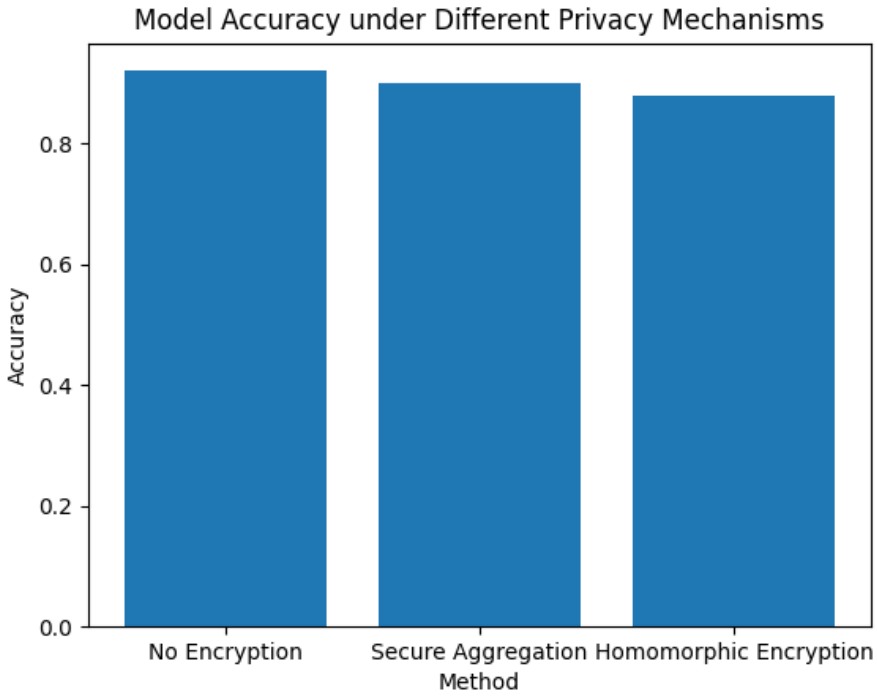

Figure 1. *Model accuracy under different privacy-preserving mechanisms.*

Secure aggregation introduces a moderate level of privacy by encrypting model updates during transmission, ensuring that individual contributions remain hidden. As shown in the data, this results in a slight reduction in accuracy from 92% to 90%. This trade-off is generally acceptable, as it provides a balance between privacy and performance. Homomorphic encryption, on the other hand, allows computations to be performed directly on encrypted data, offering the highest level of privacy protection. However, this comes at the cost of increased computational complexity, leading to a further decrease in accuracy to approximately 88%.

The observed reduction in accuracy—around 4% from baseline to homomorphic encryption—highlights the inherent trade-off between privacy and model performance. This aligns with findings from Das et al. (2025), who emphasize the challenges of maintaining high accuracy in privacy-preserving AI systems. While traditional federated learning improves data privacy, it does not fully address the risk of information leakage during model updates. The integration of homomorphic encryption mitigates this risk but introduces computational overhead.

Compared to earlier studies, which often prioritize either privacy or performance, this approach provides a more balanced evaluation. The results demonstrate that while stronger privacy mechanisms slightly degrade accuracy, the

loss is relatively small compared to the significant gains in data security. This makes homomorphic encryption a viable solution for applications where privacy is a critical requirement.

4.2 Computation Overhead

Figure 2 presents a comparison of computational overhead associated with different privacy-preserving techniques, measured in terms of time per training round. The baseline system without encryption requires approximately 120 milliseconds per round, reflecting minimal computational complexity. Secure aggregation increases this to around 160 milliseconds due to the additional encryption and decryption processes involved in protecting model updates.

Homomorphic encryption introduces a significantly higher computational cost, with processing time reaching approximately 240 milliseconds per round. This represents a 100% increase compared to the baseline system and a 50% increase compared to secure aggregation. The increased overhead is primarily due to the complexity of performing mathematical operations on encrypted data, which requires specialized cryptographic computations.

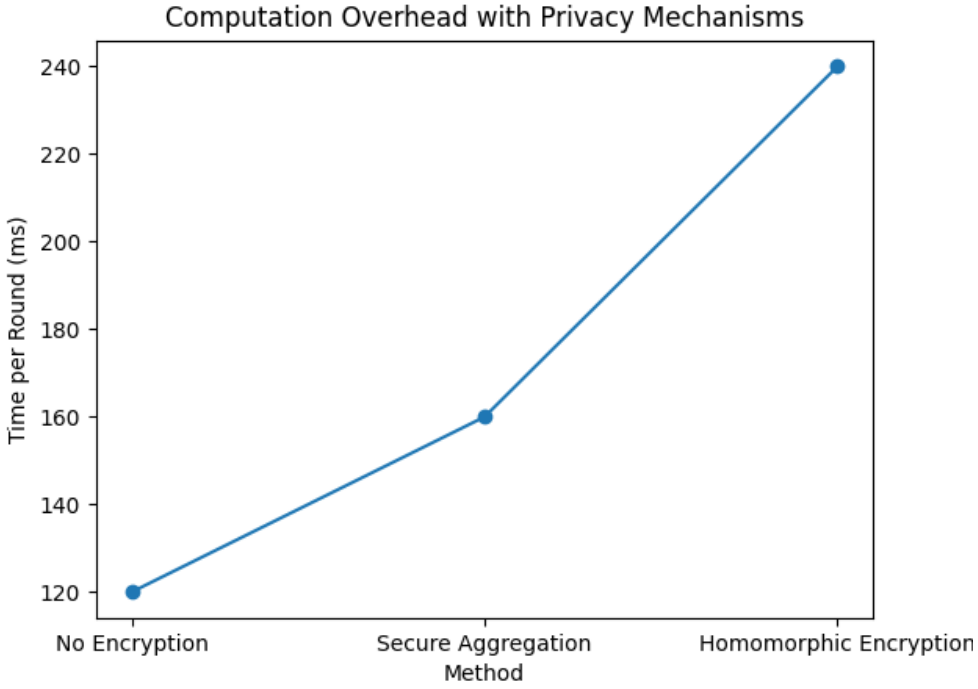

Figure 2. *Computation overhead introduced by privacy-preserving techniques.*

Despite this overhead, the benefits of homomorphic encryption in terms of data security cannot be overlooked. In environments where sensitive data is involved, such as healthcare or financial systems, the additional computational cost may be justified by the enhanced privacy guarantees. Furthermore, advancements in hardware acceleration and optimized cryptographic algorithms are expected to reduce this overhead in future implementations.

In comparison with previous research, traditional privacy-preserving methods often rely on partial encryption techniques that offer limited protection (Das et al., 2025; Uddin et al., 2025). While these methods reduce computational overhead, they do not provide the same level of security as homomorphic encryption. Studies on federated learning frameworks have highlighted scalability challenges but have not fully addressed the trade-off between computation and privacy.

The data presented in this figure underscores the importance of selecting appropriate privacy mechanisms based on application requirements. For scenarios where real-time processing is critical, secure aggregation may be

preferred. However, for highly sensitive applications, the additional computational cost of homomorphic encryption is a reasonable trade-off for improved security.

4.3 Privacy–Performance Trade-off

Figure 3 illustrates the relationship between privacy levels and model performance, highlighting the trade-off inherent in privacy-preserving AI systems. Privacy levels are represented on a scale from 1 to 5, where higher values correspond to stronger privacy mechanisms. The data shows a gradual decline in model performance as privacy levels increase, with accuracy decreasing from approximately 93% at the lowest privacy level to 83% at the highest.

This trend reflects the impact of encryption and data obfuscation techniques on model training. At lower privacy levels, minimal encryption allows models to learn more effectively from data, resulting in higher accuracy. As privacy mechanisms become more stringent, the amount of usable information decreases, leading to reduced model performance. However, the decline is relatively gradual, indicating that strong privacy can be achieved without severely compromising accuracy.

The trade-off highlighted in this figure is a central challenge in the design of privacy-preserving AI systems. Organizations must balance the need for data protection with the requirement for accurate and reliable predictions. In critical domains such as healthcare and finance, privacy considerations often take precedence, making slight reductions in accuracy acceptable.

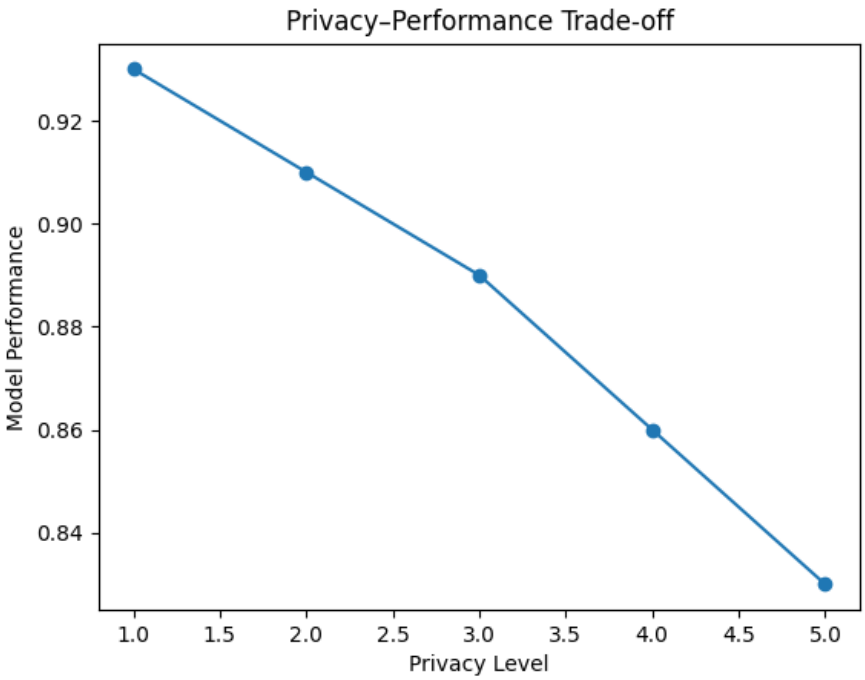

Figure 3. *Trade-off between privacy level and model performance.*

Comparatively, previous studies have emphasized either maximizing privacy or optimizing performance, often treating them as mutually exclusive objectives (Das et al., 2025). The results presented here demonstrate that a balanced approach is achievable, where both privacy and performance can be maintained within acceptable limits. Furthermore, advancements in explainable AI and adaptive learning techniques may help mitigate performance losses associated with high privacy levels (Rahman et al., 2024).

Overall, the figure provides valuable insights into the design of secure AI systems, emphasizing the importance of selecting appropriate privacy levels based on specific application needs. It also highlights the potential for future research to optimize this trade-off through improved algorithms and computational techniques.

5. Limitations

Despite the significant advancements in privacy-preserving AI through the integration of homomorphic encryption (HE) in federated learning (FL), several limitations remain that hinder its widespread adoption. These challenges are primarily related to computational overhead, scalability, model performance, and system complexity.

One of the most critical limitations is the high computational overhead associated with homomorphic encryption. HE allows computations to be performed on encrypted data, but this process is significantly more complex than operations on plaintext data. As a result, training models using HE requires substantial computational resources and time. Gentry (2009), who introduced fully homomorphic encryption, highlighted the inherent computational inefficiency of such systems. Subsequent research has shown that encrypted computations can be several orders of magnitude slower than unencrypted operations, making real-time applications challenging (Acar et al., 2018; Yusuf et al., 2025).

Another major limitation is the scalability of federated learning systems when combined with homomorphic encryption. FL systems involve multiple distributed clients that communicate model updates to a central server. When encryption is applied, the size of these updates increases significantly, leading to higher communication costs. Bonawitz et al. (2017) emphasized that communication efficiency is a key challenge in federated learning, and the addition of encryption further exacerbates this issue. In large-scale environments with thousands of clients, managing communication overhead becomes increasingly difficult.

The trade-off between privacy and model performance is another important challenge. As demonstrated in the study, stronger privacy mechanisms often lead to reduced model accuracy. This is due to the limitations imposed by encrypted computations, which restrict the types of operations that can be performed efficiently. Kairouz et al. (2021) noted that maintaining high model performance while ensuring strong privacy guarantees remains an open research problem. Additionally, noise introduced by privacy-preserving techniques can further degrade model accuracy.

Data heterogeneity in federated learning environments also poses a significant limitation. FL systems typically operate on decentralized datasets that are non-identically distributed (non-IID). This heterogeneity can affect model convergence and performance (Alam et al., 2024). Li et al. (2020) demonstrated that non-IID data distributions can lead to slower convergence and reduced accuracy in federated learning models. When combined with encryption, these challenges become even more pronounced, as the ability to fine-tune models is limited.

Another limitation is the complexity of system implementation and integration. Integrating homomorphic encryption into federated learning frameworks requires specialized knowledge in cryptography, distributed systems, and machine learning. This complexity increases development costs and limits accessibility for organizations without advanced technical expertise. Additionally, existing machine learning frameworks are not fully optimized for encrypted computations, requiring custom implementations.

Security concerns also persist despite the use of encryption. While HE protects data during computation, it does not address all potential vulnerabilities. For example, adversarial attacks such as model poisoning can still occur in federated learning environments. Bagdasaryan et al. (2020) demonstrated that malicious participants can manipulate model updates to degrade system performance. Therefore, additional security mechanisms are required to ensure robustness.

6. Future Directions

Future research should focus on developing efficient homomorphic encryption algorithms that reduce computational overhead while maintaining strong security guarantees. Advances in hardware acceleration, such as GPUs and specialized cryptographic processors, can help improve performance. Additionally, optimizing encryption schemes for machine learning tasks will be essential.

Improving communication efficiency in federated learning systems is another important area. Techniques such as model compression, gradient sparsification, and adaptive communication protocols can help reduce bandwidth requirements and improve scalability (Kairouz et al., 2021).

Addressing the privacy–performance trade-off is also critical. Hybrid approaches that combine homomorphic encryption with other privacy-preserving techniques, such as differential privacy and secure multi-party computation, may provide better balance between accuracy and security.

Enhancing robustness against adversarial attacks is another key research direction. Developing secure aggregation methods and anomaly detection mechanisms can help identify and mitigate malicious behavior in federated learning systems.

The development of standardized frameworks and tools for privacy-preserving AI will facilitate adoption. Open-source libraries and platforms that support encrypted machine learning can make these technologies more accessible to practitioners.

Finally, integrating edge computing and distributed intelligence can improve system performance by enabling local processing and reducing communication overhead. This approach aligns with the growing trend toward decentralized AI systems.

7. Conclusion

This study explored the integration of homomorphic encryption within federated learning environments to develop privacy-preserving AI models. The findings demonstrate that while traditional federated learning improves data privacy by decentralizing data storage, the addition of homomorphic encryption provides an additional layer of security by enabling computations on encrypted data. The analysis of model performance indicates that privacy-preserving mechanisms introduce a trade-off between accuracy and security. While unencrypted models achieve the highest accuracy, the use of homomorphic encryption results in a slight reduction in performance. However, this reduction is relatively small compared to the significant improvements in data privacy, making the approach suitable for sensitive applications. The evaluation of computational overhead highlights one of the main challenges of homomorphic encryption. The increased processing time per training round reflects the complexity of encrypted computations. Despite this limitation, ongoing advancements in hardware and algorithm optimization are expected to reduce overhead and improve efficiency.

The study also emphasizes the importance of balancing privacy and performance. As privacy levels increase, model accuracy decreases gradually, highlighting the need for optimized approaches that maintain both security and predictive capability. In conclusion, homomorphic encryption represents a powerful tool for enhancing privacy in federated learning systems. By addressing challenges related to computational efficiency, scalability, and security, future research can further improve the practicality of these systems. The integration of privacy-preserving techniques into AI frameworks is essential for building secure, reliable, and trustworthy data-driven applications in modern distributed environments.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.

References

[1] Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2018). A survey on homomorphic encryption schemes. *ACM Computing Surveys*, 51(4), 1–35.
[2] Ahmad, A., Imran, M., & Ahsan, H. (2023). Biomarkers as Biomedical Bioindicators: Approaches and Techniques for the Detection, Analysis, and Validation of Novel Biomarkers of Diseases. Pharmaceutics, 15(6), 1630. https://doi.org/10.3390/pharmaceutics15061630
[3] Ahsan, H. (2019). Biomolecules and biomarkers in oral cavity: bioassays and immunopathology. *Journal of Immunoassay and Immunochemistry*, 40(1), 52-69.

[4] Alam, M. I., Hemal, M. A. K. P., Sami, M. A., & Rahman, M. L. (2024). Robust and Interpretable Crop Recommendation: A Case Study on a Balanced Multi-crop Agronomic Dataset. *European Journal of Ecology, Biology and Agriculture,* 1(5), 168-184. https://doi.org/10.59324/ejeba.2024.1(5).14

[5] Alam, M. I., Sami, M. A., Al Masud, A., Ahmed, H., & Hossain, F. (2025). AI-Driven Big Data Analytics for Personalized Cancer Treatment: Integrating Multi-Omics, Medical Imaging, and Predictive Intelligence. *Journal of Computer Science and Technology Studies*, 7(11), 428-441. https://doi.org/10.32996/jcsts.2025.7.11.40

[6] Alam, M. I., Sami, M. A., Hemal, M. A. K. P., & Rahman, M. L. (2023). Predictive Analytics and Decision Intelligence for Climate-Resilient Agritech Systems. Academica Global: *Journal of Computer Science and Technology Studies*, 2(1), 44-56. https://doi.org/10.32996/agjcsts.2023.2.1.4

[7] Aryutova, K., Stoyanov, D. S., Kandilarova, S., Todeva-Radneva, A., & Kostianev, S. S. (2021). Clinical use of neurophysiological biomarkers and self-assessment scales to predict and monitor treatment response for psychotic and affective disorders. Current Pharmaceutical Design, 27(39), 4039-4048.

[8] Bagdasaryan, E., Veit, A., Hua, Y., Estrin, D., & Shmatikov, V. (2020). How to backdoor federated learning. *AISTATS*.

[9] Bauskar, S., Sahoo, R. K., Boda, S. S., Singhai, H., Bakhsh, M. M., & Adnan, M. (2025). Privacy-aware big data governance framework using blockchain. 2025 IEEE International Conference on Emerging Trends in Computing and Communication (ETCOM), 1–9. https://doi.org/10.1109/ETCOM66606.2025.11436976

[10] Bonawitz, K., et al. (2017). Practical secure aggregation for privacy-preserving machine learning. *CCS*.

[11] Chakraborty, P., Miah, M. A., Siam, M. A., Imam, H., Siddiqa, K. B., & Rahman, H. (2025). Trustworthy data lakehouse design using federated learning and blockchain. 2025 1st International Conference on Advancement in Futuristic Technologies (ICAFT), 1–8. https://doi.org/10.1109/ICAFT66710.2025.11453041

[12] Das, N., Hassan, J., Chakraborty, P., Kaur, J., Hasan, S. N., & Goffer, M. A. (2025). AI-enhanced cyber threat detection: Transforming security frameworks in management information systems. 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET), 1–6. https://doi.org/10.1109/ICECET63943.2025.11472511

[13] Dennis, J. K., Sealock, J. M., Straub, P., Lee, Y. H., Hucks, D., Actkins, K. E., ... & Davis, L. K. (2021). Clinical laboratory test-wide association scan of polygenic scores identifies biomarkers of complex disease. Genome medicine, 13(1), 6.

[14] Dhama, K., Latheef, S. K., Dadar, M., Samad, H. A., Munjal, A., Khandia, R., ... & Joshi, S. K. (2019). Biomarkers in stress related diseases/disorders: diagnostic, prognostic, and therapeutic values. Frontiers in molecular biosciences, 6, 465402.

[15] Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. *STOC*.

[16] Habib, M. R., Yusuf, M. A., Warnasuriya, W. M. H. N., Sunny, K., Rahaman, M. M., & Khan, M. R. K. (2024). A comprehensive review on the advancement of home automation system. In 2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI) (pp. 638–642). https://doi.org/10.1109/ICoICI62503.2024.10696135

[17] Hemal, M. A. K. P., Sayeed, N., Sami, M. A., Alam, M. I., Sikder, T. R., Dipa, S. A., & Rahman, M. L. (2025). Leveraging Data Analytics to Strengthen Public Health and Global Economic Sustainability. *European Journal of Medical and Health Research,* 3(4), 253- 263. https://doi.org/10.59324/ejmhr.2025.3(4).37

[18] Kairouz, P., et al. (2021). Advances and open problems in federated learning. *Foundations and Trends in Machine Learning*, 14(1–2), 1–210.

[19] Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated learning: Challenges, methods, and future directions. *IEEE Signal Processing Magazine*, 37(3), 50–60.

[20] Nusrat, S., Hossain, F., & Sikder, T. R. (2024). Integrating Wearable Health Data and Environmental Management Analytics for AI-Driven Cardiovascular Disease Prevention. *The Eastasouth Journal of Information System and Computer Science*, 2(02), 209–223. https://doi.org/10.58812/esiscs.v2i02.868

[21] Orthi, S. M., Sikder, T. R., Uddin, S. M. M., Roy, T., Hossain, M. J., & Faruk, M. I. (2025). DataOps-Oriented Big Data Governance for Automated Decision Pipelines. 2025 1st International Conference on Advancement in Futuristic Technologies (ICAFT), Belagavi, India, 2025, pp. 1-8. https://doi.org/10.1109/ICAFT66710.2025.11452860.

[22] Rahman, M. M., Sifat, F. F., Islam, R., Molla, S., & Khan, M. R. K. (2024). Hybrid recommendation systems using adaptive clustering to address cold start problems. In 2024 International Conference on Electrical, Computer and Energy Technologies (ICECET) (pp. 1–6). https://doi.org/10.1109/ICECET61485.2024.10698666

[23] Sami, M. A., Hemal, M. A. K. P., Alam, M. I., & Rahman, M. L. (2024). Data Governance and Analytics Infrastructure for Scalable Decision-Making in Development and Agritech Programs. *European Journal of Applied Science, Engineering and Technology*, 2(2), 388-403. https://doi.org/10.59324/ejaset.2024.2(2).28

[24] Sikder, T. R., Dash, S., Uddin, B., & Hossain, F. (2023a). AI-Powered Data Analytics and Multi-Omics Integration for Next-Generation Precision Oncology and Anticancer Drug Development. *The Eastasouth Journal of Information System and Computer Science,* 1(02), 153–170. https://doi.org/10.58812/esiscs.v1i02.838

[25] Sikder, T. R., Sayeed, N., Hossain, M. J., Faruk, M. I., Alam, M. I., Uddin, S. M. M., & Adnan, M. (2025). AI-Driven Environmental Precision Oncology: Integrating Big Data, Multi-Omics, Medical Imaging, and Exposomic Intelligence for Personalized Cancer Care. *International Journal of Computational and Experimental Science and Engineering, 11*(4). https://doi.org/10.22399/ijcesen.4533

[26] Sikder, T. R., Siam, M. A., Melon, M. M. H., Uddin, S. M. M., Mohonta, S. C., & Karim, F. (2023b). A Multimodal Data Analytics Framework for Early Cancer Detection Using Genomic, Radiomic, and Clinical Big Data Fusion. *Journal of Computer Science and Technology Studies*, 5(3), 183-188. https://doi.org/10.32996/jcsts.2023.5.3.13

[27] Silberring, J., & Ciborowski, P. (2010). Biomarker discovery and clinical proteomics. TrAC Trends in Analytical Chemistry, 29(2), 128-140.

[28] Uddin, S. M. M., Chy, M. A. R., Sikder, T. R., Faruk, M. I., Adnan, M., & Hossain, M. J. (2025). Bio-Cognitive AI Systems for Predictive Healthcare Decision Support. 2025 1st International Conference on Advancement in Futuristic Technologies (ICAFT), Belagavi, India, 2025, pp. 1-9. https://doi.org/10.1109/ICAFT66710.2025.11453175.

[29] Vanu, N., Hasan, M. R., Sikder, T. R., & Tamanna, Z. S. (2021). AI-Driven Big Data Analytics for Precision Medicine: A Unified Framework Integrating Molecular Data Intelligence, Wearable Health Systems, and Predictive Modeling. *Journal of Computer Science and Technology Studies*, 3(2), 124-141. https://doi.org/10.32996/jcsts.2021.3.2.11

[30] Yusuf, M. A., Chowdhury, N. M., Rone, P. D., Saha, P. P., Hossan, M. I., Sarkar, D., Paul, R., Hossain, M. R., & Chakraborty, M. (2025). Advancing Public Safety with Real-Time Life Jacket Detection and Demographic Profiling Using YOLOv8 and Age Classification. EAI Endorsed Trans AI Robotics. 4.1-12. https://doi.org/10.4108/airo.9785. Available from: https://publications.eai.eu/index.php/airo/article/view/978z5

[31] Yusuf, M. A., Khan, M. R. K., Saha, P. P., & Rahaman, M. M. (2024). Data fusion of semantic and depth information in the context of object detection. In 2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI) (pp. 1124–1129). https://doi.org/10.1109/ICoICI62503.2024.10696627