

Recent Advances in Privacy-Preserving Cybersecurity Using Homomorphic Encryption and Federated Learning

Mr. Raman Kumar

Assistant Professor, Department of Computer Science and Applications, Mandsaur

raman.kumar@meu.edu.in

Corresponding Author: *Raman Kumar (raman.kumar@meu.edu.in)

Received: 1 August 2026 | Revised: 5 August 2026 | Accepted: 25 August 2026

Abstract—Cybersecurity threats and the need to secure sensitive data have grown significantly as connected devices, IoT, cloud computing, and digital services have all exploded. This review examines the most recent developments in privacy-preserving cybersecurity, with a particular emphasis on Federated Learning (FL) and Homomorphic Encryption (HE). Digital signatures, hash functions, zero-knowledge proofs, Secure Multi-party Computation, and Denial-of-Service, Malware, Phishing, SQL Injection, Session Hijacking, Man-in-the-Middle, and Cross-Site Scripting are some of the methods covered. There are three main varieties of HE covered in the study: Partial Homomorphic Encryption, Somewhat Homomorphic Encryption, and Fully Homomorphic Encryption. HE is a method for computing without decrypting the data. Additionally, FL is covered as a decentralized ML strategy that uses data retention at the local level and updates models through distribution, similar to Horizontal, Vertical, and Federated Transfer Learning. Issues with data heterogeneity, straggler effects, privacy protection, and security are also covered, along with other FL difficulties. Applications in the healthcare, financial, internet of things (IoT), edge computing, and industrial sectors are highlighted, and HE and FL are shown to provide more privacy in new areas of application as well as safer, more collaborative, and more efficient cybersecurity solutions.

Keywords—Privacy-Preserving Cybersecurity, Homomorphic Encryption, Federated Learning, Data Privacy, Secure Computation.

I. INTRODUCTION

Cybersecurity and data privacy are essential to protect sensitive digital information, prevent unauthorized access and cyber threats, ensure regulatory compliance, and maintain trust in increasingly interconnected digital environments. The rapid growth of cyber dangers has made cybersecurity and data privacy the most pressing issues of the modern digital age. Businesses and individuals using systems that rely on digital infrastructure are susceptible to cyber dangers including phishing, malware, ransomware, and unauthorized intrusions due to the fact that data is processed and stored over digital networks. In order to secure critical information and

establish reliable cyber security systems, enterprises must conquer two formidable obstacles. Due to the increased transmission of sensitive data through online platforms, the requirement for privacy protection in cybersecurity operations is on the rise. Cyberattacks and data breaches both result in financial losses, damaged reputations, and infractions of regulatory norms. Modern data breaches show how thieves may get private information by taking advantage of loopholes in computer systems, which poses a major security risk in the form of fraud and identity theft. As their need grows, organizations must adopt privacy-protecting techniques that help them to protect their data without harming their cybersecurity procedures [1].

The inherent sensitivity of the data being evaluated is one of the most critical issues. Confidential information like user behavior, IP addresses and application data are often included in network traffic [2]. Multiple parties or external analysts sharing the information creates significant privacy concerns. In traditional methods of protecting network data, encryption techniques are used that secure the data while it is being transferred and stored [3]. These approaches are used for analysis, however, they involve decrypting the data, which can leave them vulnerable to threats and risks. A solution to the challenge is homomorphic encryption (HE), which has been attracting attention as a new paradigm in secure data-sharing systems for network traffic analysis. The advantage of homomorphic encryption is that it enables operations on encrypted data without the need to decrypt it, maintaining the confidentiality of the underlying data. This distinctive feature allows analysts to gain insights from sensitive network traffic without compromising the privacy of the users [4].

FL has come up as one of the probable solutions that would enable decentralized model training. One kind of distributed model has clients training local models with their own data and then sending the weights (or gradients) of those models to a centralized unit. Without revealing the real facts, the central server gathers the modifications to enhance the global model [5]. Difficulties arise for traditional ML techniques in the context of security of CPS. The challenge

lies in centralizing data to train the models, which can be problematic for privacy and security, particularly with sensitive data from distributed sources. Traditional methods also fail miserably when faced with massive volumes of diverse data stored in a wide range of CPS devices and environments. Federated learning provides an encouraging alternative to these problems by allowing for the collaborative training of models over decentralized edge devices without compromising data privacy. FL spreads out the learning process across several edge devices instead of concentrating the data into a single center, which decreases the danger of data breaches and privacy issues [6].

This paper is organized as follows: Section II introduces the topic of Privacy-Preserving Cybersecurity, Section III discusses Homomorphic Encryption and Federated Learning, Section IV summarizes the recent research works, and Section V concludes this paper and discusses possible future research directions.

II. PRIVACY-PRESERVING CYBERSECURITY

Advances in computer power, data analytics, and artificial intelligence have accelerated the creation of privacy-preserving techniques for cybersecurity [7]. The primary methods by which organizations protected their sensitive data in the early days of cybersecurity were encryption, access control systems, and firewalls [8]. These safeguards failed to provide adequate privacy protection due to the proliferation of illegal data access and breaches.

A. Privacy Threats in Cybersecurity

These are the steps done to disrupt a system's normal operations or cause harm to it by taking advantage of security flaws utilizing different methods and tools [9].

1) Denial-of-service (DoS)

This form of attack aims to block access to a computer or network resource that legitimate users are trying to utilize. It occurs when a network's ability to carry out its intended purpose is impaired or destroyed.

2) Malware

This kind of attack takes advantage of security holes in order to gain unauthorized access to systems through the use of malicious software [10][11]. Malware occurs when an attacker has access to a large financial or political reward, which increases their desire to hack a large number of network devices in order to achieve their malevolent goals.

3) Phishing

This practice is illegal since it harvests personal information from online users using social engineering and technological means. A variety of communication channels, including email, instant messaging, pop-up messages, and web pages, are utilized in phishing strategies.

4) SQL Injection attack

The goal of this attack is to alter or manipulate the SQL query in the attacker's favor by inserting an input string into the program. Unauthorized users can access and manipulate the database, and sensitive information might be exposed as a result of this attack. Data loss or abuse by unauthorized organizations, leading to the destruction of functionality and secrecy, is a real possibility in the event of this assault, making it dangerous.

5) Session Hijacking and Man-in-the-Middle Attacks

An MITM attack happens when an unauthorized third party stealthily assumes control of the communication channel between several endpoints. There are a few other names for this attack in the literature: MIM, MitM, MiM, and MITMA. An attacker that uses man-in-the-middle techniques can listen in on, change, or even hijack their targets' communication flow.

6) Cross-Site Scripting (XSS)

An attacker tries to steal sensitive client data by running malicious JavaScript code in the victim's browser. Recent websites have been shown to routinely leverage this vulnerability.

B. Privacy-Preserving Technologies in Cybersecurity

Privacy-Preserving Technologies in Cybersecurity are techniques designed to protect sensitive information while enabling secure data processing, sharing, and communication. These solutions mitigate privacy concerns such as unwanted access, data leakage, and information inference while ensuring cybersecurity.

1) Digital Signatures

The digital signature relies on the message and the sender to give cryptographic value [12]. Digital signatures are a great way to make sure that data stays intact, that messages are updated when sent, and that they are valid.

2) Hash Functions and Data Integrity

A hash function can also be called a one-way function. Many applications in computer science have made use of the hash function [13]. A mathematical operation known as a hash function is used to convert an input string's variable length into a fixed length.

3) Zero-Knowledge Proofs

The 1985-proposed cryptographic method known as Zero-Knowledge Proof (ZKP) [14] enables a prover to prove a statement is true to a verifier without disclosing no information other than the statement's validity [15].

4) Homomorphic Encryption

Homomorphic Encryption (HE) is a key cryptographic method in blockchain construction, which enables the processing of encrypted data without revealing the plaintext, guaranteeing data protection and availability [16].

5) Secure Multi-party Computation (SMPC)

SMPC allows for multiple parties to jointly process private data without revealing anything about the data elements that are used by each party [17].

C. Privacy-Preserving Machine Learning

Privacy-preserving ML is a growing paradigm aimed at tackling the difficulties of data security and individual privacy in the digital age [18]. Traditional gadgets for learning procedures frequently demand centralized information aggregation for education, producing substantial privacy difficulties, especially with the rising attention and regulation of data security.

1) Differential Privacy

This method incorporates controlled noise into the data in such a manner that it guarantees a mathematical limitation on privacy leakage, regardless of whether an adversary observes the training data or the trained model.

2) Federated Learning

The training is divided between several devices or servers, where the original data remains in place [19]. The model updates are shared rather than the specific data points.

3) Homomorphic Encryption

Enables computation on encrypted data basic operations such as addition and multiplication and is fundamental for more complex operations.

4) Secure multi-party computation (SMPC)

This technique enables secure cooperation but allows no third party to be trusted: computations are made on encrypted data, without revealing any information about the data or the computed results.

5) Data Anonymization

This strategy entails deleting or obscuring personally identifiable information (PII) from the data before training.

D. Privacy-Preserving Cybersecurity in Emerging Environments

Privacy-Preserving Cybersecurity in Emerging Environments focuses on protecting sensitive information in modern environments such as IoT, edge computing. It integrates privacy-enhancing techniques with cybersecurity mechanisms to prevent data leakage, unauthorized access, and privacy attacks while supporting secure and efficient data processing.

1) Internet of Things (IoT)

The fast rise of the IoTs has enabled billions of internet gadgets, which has exacerbated cybersecurity issues. Encrypting and safeguarding these IoT devices is not totally practicable because of a lack of power, various security-related difficulties arise [20].

2) Edge Computing

In edge computing, the "edge" refers to any resource situated between data sources and cloud centers [21]. This paradigm enables terminal devices to offload storage and computational tasks to nearby edge nodes, such as base stations (BS), wireless access points (WAP), or edge servers.

3) Blockchain-Based Systems

Implementing state-of-the-art security measures like perturbation, encryption (including differential privacy and homomorphic encryption), onion routing, zero-knowledge proofs (ZKPs), Tor networks, and trusted hardware can improve blockchain-based privacy-preserving methods [22][23].

III. HOMOMORPHIC ENCRYPTION AND FEDERATED LEARNING

One privacy-preserving cryptographic method is Homomorphic Encryption (HE), which allows calculations to be executed directly on encrypted data without decryption being necessary. It allows sensitive information to remain confidential while supporting secure data processing and analysis, making it valuable in cloud computing, healthcare, finance, and cybersecurity applications.

A. Types of Homomorphic Encryption

Homomorphic Varieties One way to categorize encryption is by the kind and level of computations that can be done directly on encrypted data. Different from one another in terms of the operations they enable and the computing power they offer, the three primary kinds of homomorphic encryption are PHE, SHE, and FHE, as seen in Fig. 1.

1) Somewhat Homomorphic Encryption (SHE)

There is a cap on how many times this cryptosystem permits operations like addition and multiplication on encrypted data before it introduces noise [24]. Hence, the data is irretrievable after a certain amount of noise is added.

2) Partially Homomorphic Encryption (PHE)

Encrypted data may be added or multiplied using this cryptosystem. Here are a few instances of PHE: Algorithm for Goldwasser-Micali [25] that has semantic security based on the quadratic residuality problem.

3) Fully Homomorphic Encryption

Multiple addition and multiplication operations on encrypted data are possible with this cryptosystem. The semantic security of this cryptosystem relies on sparse subset sum problem (SSSP) and assumptions.

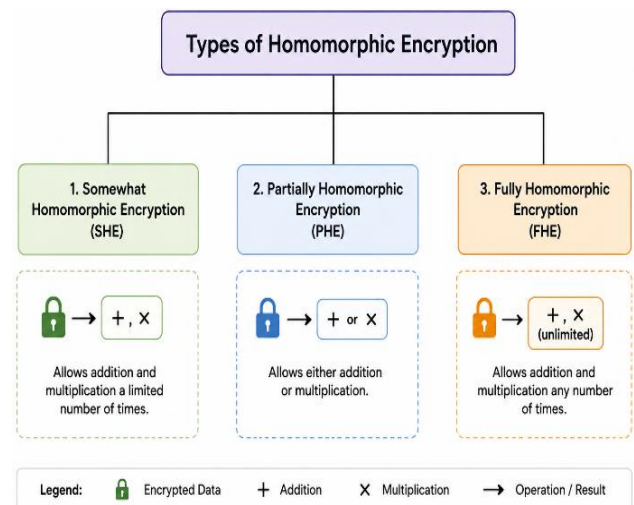


Fig. 1. Types of Homomorphic Encryption

B. Homomorphic Encryption Framework

Secure sensitive data, particularly in healthcare, while addressing important privacy concerns with Homomorphic Encryption (HE), a powerful encryption method:

- **Data Encryption:** Data owners (such as individuals or organizations) begin by encrypting their data, converting it into a secure format that cannot be read.
- **Encrypted Data Transmission:** The data is securely transmitted to external services or cloud storage when encrypted[26].
- **External Processing Entity:** These external entities (such as cloud providers) store or process the encrypted data, but cannot access the actual contents of the data since they do not have the decryption keys [27].
- **Function Execution on Ciphertext:** The data can still be subject to computations or analyzes with homomorphic encryption in place, eliminating the need for decryption.

C. Federated Learning

FL is a distributed ML method that enables several entities to collaborate on a model without disclosing their original data to a single server. Safeguards sensitive data by storing it locally and basely sharing model parameters or updates, enhancing data privacy and security. The healthcare industry greatly benefits from FL when it comes to handling patient

records and guaranteeing data security. Security of sensitive information, including financial transactions, can be achieved through its use in the financial sector. Security of data and systems in the IoT and cybersecurity relies heavily on FL.

D. Types of Federated Learning

FL is a novel ML solution that overcomes privacy and data decentralization challenges by letting different devices or organizations to interact without having to disclose their raw data to train ML models, as seen in Fig. 2.

1) Horizontal federated learning (HFL)

The HFL architecture is a configuration where data is split horizontally across clients, each holding a different portion of data but the same features. It's appropriate when privacy is an issue and clients want to work together on a common ML project without sharing their entire datasets.

2) Vertical federated learning (VFL)

This is used when the data sets have complementary attributes [28]. This method is where the features are separated and the client's collaborate to train a model.

3) Federated transfer learning (FTL)

FL is combined with transfer learning. Clients work together, contributing a pretrained model and then fine-tuning it with their own data.

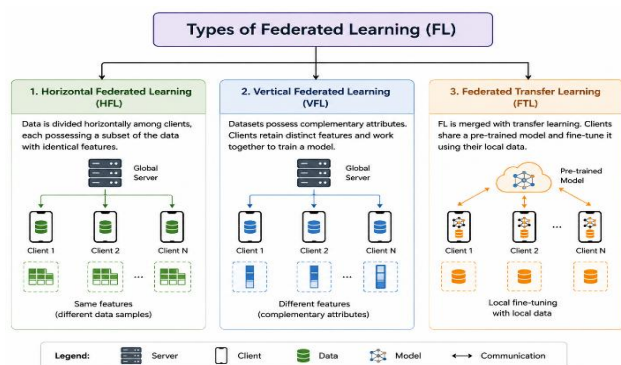


Fig. 2. Types of Federated Learning

E. Current Challenges in Federated Learning

FL has a lot of potential and promising developments, but it also has many challenges. The difficulties arise frequently because of the distributed nature of the paradigm and the complexity of data distribution and networks in the real world.

1) Data Heterogeneity (Non-IID Data)

Data heterogeneity, or client data that is not independent and identically distributed (non-IID), is a prevalent and challenging issue in FL. In an idealized FL scenario where data is IID across all clients, classical FL algorithms like FedAvg can deliver high-quality model performance and quick convergence.

2) Straggler Effect and Client Selection

The perfect world of FL, in which every client takes part in every cycle, isn't always doable in practice [29]. Because client devices naturally vary in hardware, network connectivity, and data volume, the straggler effect is one of the biggest obstacles in FL.

3) Privacy Protection and Security

FL takes privacy seriously from the start, yet it still faces the same security and privacy risks as any other system. Even

without raw data, the simple process of exchanging model changes might inadvertently expose sensitive information.

F. Applications of Federated Learning

FL's collaborative model training solutions and privacy-preserving features are causing waves in several industries. Detailed applications are provided below for various applications.

- **Healthcare:** FL has the ability to revolutionize the healthcare industry by addressing the critical issues of data security and privacy. Without compromising patient privacy or violating laws like HIPAA or GDPR, medical facilities can work together to train disease diagnostic models (for example, cancer detection using MRI data).
- **Finance:** FL solves data privacy problems and enhances model performance in finance. Banking institutions train models together to identify fraudulent transactions in multiple banks without sharing sensitive transaction data [30].
- **Internet of Things (IoT) and Edge Computing:** FL's distributed structure perfectly adapts to the context of IoT and Edge Computing where devices produce an enormous amount of data [31]. Distributed sensor applications may safely aggregate data from one another with FL's help, including traffic management, energy efficiency, pollution monitoring, and more.
- **Industrial Applications:** industries where data is siloed between entities can make use of FL to securely share data and learn collaboratively. Co-training enhances inventory control and demand forecasting while maintaining trade secrets. FL models can accurately foresee equipment failure in distributed manufacturing units, minimizing downtime and costs.

It emphasizes what they do, how they apply to privacy and cyber security, the communication needs, challenges and benefits. The comparison reveals that by combining HE with FL it is possible to offer improved privacy and security for distributed cybersecurity systems. The comparative analysis of Homomorphic Encryption (HE), FL and their Hybrid variant is shown in Table I for Cybersecurity problems.

TABLE I. CYBERSECURITY USING HOMOMORPHIC ENCRYPTION AND FEDERATED LEARNING

Aspect	Homomorphic Encryption (HE)	Federated Learning (FL)	HE + FL
Purpose	Secure computation on encrypted data	Collaborative learning without sharing raw data	Privacy-preserving collaborative learning
Privacy	Protects data during computation	Keeps data at local devices	Protects data and model updates
Cybersecurity Use	Secure threat and intrusion analysis	Intrusion and malware detection	Privacy-preserving attack detection
Communication	Encrypted data transfer	Model updates are exchanged	Encrypted model updates are exchanged
Main Challenge	High computational cost	Communication and data heterogeneity	Higher computation and communication cost
Key Benefit	Strong data confidentiality	Decentralized learning	Enhanced privacy and security

IV. LITERATURE REVIEW

The following section provides an overview of relevant research on Homomorphic Encryption (HE) and FL for privacy-preserving cybersecurity. The research focuses on their functions in various cybersecurity and emerging environments, including secure data processing, collaborative threat detection, privacy protection, computational efficiency, and secure model training.

Zhansaya Myrzakul et al. (2026) introduces a modified homomorphic encryption scheme for ESP32 based IoT devices. The proposed scheme enables secure data encryption and decryption while supporting limited processing on encrypted data. The ESP32 microcontroller was used to execute the algorithm, and its performance was assessed by measuring its memory usage and execution time. Experimental results demonstrate that the modified scheme reduces computational overhead while maintaining an adequate level of security, confirming the feasibility of using homomorphic encryption in resource-constrained IoT devices for secure data processing [32]. P. Pushpa et al. (2025) proposed approach maximizes data security and privacy by encrypting data processing using homomorphic encryption (HE) and eliminating the need for decryption. Combining partially, moderately, and fully homomorphic encryption in this way allows for a wide variety of processing needs to be addressed. Advanced key management, end-to-end encryption, and continuous monitoring contribute to improved security, while assessment of performance shows lower processing time, memory use, and computational overhead. The functions, resource efficiency, and security balance offered by cloud-based systems outperform those of existing systems [33].

Wentao Yang et al. (2024) provide a method to lessen the communication and computational burden of homomorphic cryptographic FL by combining scarification with compressive sensing. The next step is to conduct trials to see how well Paillier homomorphic encryption FL works with the MNIST and Fashion-MNIST datasets. With a reduction in

computational overhead of 90% and an improvement in encryption speed from 7.75 seconds to 0.70 seconds, the findings show that the approach is effective. Similarly, you'll see that the computational overhead drops by 88%, and the decryption time goes down from 5.23 seconds to 0.66 seconds. The transmission overhead went down from 2494.56KB to 163.78KB, a decrease of 93.4%. While the MNIST dataset showed a decrease from 98.47% to 98.37%, the Fashion-MNIST dataset witnessed an improvement in model accuracy from 89.64% to 90.16% [34].

Pratik Thantharate & Anurag T et al. (2023) Introduces Cyberia, a platform for FL that can identify cyber threats together without exposing sensitive information. In order to create a global model, the decentralized method trains them on data from individual clients and only distributes updates at intermediate stages. Cyberia achieves far higher results than a centralized deep neural network (89.6% vs. 81.4%), as demonstrated on the Bot-IoT dataset. Data poisoning assaults, systematic bias, and statistical heterogeneity are some of the issues that arise in practice. Aggregation must be securely aggregated, with differentiated privacy and adversarial protections in place, for its adoption to be robust [35].

Josep Domingo-Ferrer et al. (2022) Creates a FL system that protects users from poisoning and Byzantine assaults while still allowing them to remain anonymous when interacting with their peers. A decentralized reputation management system encourages adherence to the framework's protocols, which are predicated on unlikable anonymity and co-utility. This method allows for the identification of faulty model updates with less computing expense than homomorphic encryption approaches, while being superior to update aggregation in preserving model update values and FL accuracy [36]. Table II presents a comparison of two forms of privacy-preserving cybersecurity—FL and homomorphic encryption—and discusses their respective methods, advantages, disadvantages, and potential future developments in the field of safe data processing.

TABLE II. COMPARATIVE ANALYSIS OF PRIVACY PRESERVING CYBERSECURITY USING HOMOMORPHIC ENCRYPTION AND FEDERATED LEARNING

Reference	Study Focus	Approach / Methodology	Key Findings	Challenges / Limitations	Future Directions
Zhansaya Myrzakul et al. (2026)	HE for resource-constrained IoT	Modified HE scheme implemented on ESP32-based IoT devices; evaluated using execution time and memory consumption	Reduces computational overhead while maintaining an adequate level of security; demonstrates feasibility for secure IoT data processing	Limited processing and resource capacity of ESP32-based IoT devices	Develop more lightweight and efficient HE schemes for resource-constrained IoT environments
P. Pushpa et al. (2025)	HE for secure data processing	Combination of PHE, SHE, and FHE with advanced key management, end-to-end encryption, and continuous monitoring	Improves security, resource efficiency, processing time, and memory usage; provides better cloud-based functionality	Computational and resource requirements of HE; balancing security and efficiency	Optimize HE schemes for efficient cloud-based processing and stronger key management
Wentao Yang et al. (2024)	HE-based Federated Learning optimization	Scarification and compressive sensing applied to Paillier HE-FL using MNIST and Fashion-MNIST	Encryption time reduced by 90%, decryption overhead by 88%, and communication overhead by 93.4%, with comparable model accuracy	Slight accuracy variation; HE still introduces computational and communication overhead	Further optimize compression and sparsification techniques for large-scale HE-FL systems
Pratik Thantharate & Anurag T et al. (2023)	Privacy-preserving cyber threat detection	Cyberia federated learning framework for collaborative intrusion detection using decentralized client data; evaluated on Bot-IoT	Achieved 89.6% accuracy, compared with 81.4% for centralized DNN; improves collaborative cyber threat detection	Statistical heterogeneity, systemic bias, and data poisoning attacks	Integrate secure aggregation, differential privacy, and adversarial defense mechanisms
Josep Domingo-Ferrer et al. (2022)	Privacy and security in FL	Federated framework using unlinkable anonymity, co-utility, and decentralized reputation management to address Byzantine and poisoning attacks	Provides participant privacy and attack resistance while preserving model-update values; reduces computational overhead compared with HE-based methods	Complexity of decentralized reputation and incentive mechanisms; protection depends on protocol adherence	Develop scalable and robust FL frameworks with stronger privacy, security, and incentive mechanisms

V. CONCLUSION AND FUTURE WORK

The increasing adoption of interconnected digital systems has created a growing need for effective privacy-preserving cybersecurity mechanisms. This paper examined recent advances in HE and FL and highlighted their potential for protecting sensitive information during data processing and collaborative model training. The reviewed studies demonstrate that HE enables secure computation on encrypted data, while FL supports decentralized learning without requiring the sharing of raw data. The findings indicate that both techniques can strengthen data confidentiality, secure threat detection, and privacy-preserving ML across IoT, cloud, healthcare, finance, and cybersecurity environments. Scarification and compressive sensing are two methods that can lessen the computational and communication burden, and integrating HE with FL improves privacy and security. However, computational cost, communication efficiency, non-IID data, resource constraints and security of model updates are challenges. In conclusion, HE and FL offer a promising base for secure and scalable privacy preserving cybersecurity.

Future research is needed to devise efficient and light HE-FL for large scale and resource limited environments. Special focus must be paid to minimizing computation and communication overhead, addressing the challenge of non-IID data, preventing poisoning and inference attacks, enhancing secure aggregation, and testing integrated HE-FL solution in real-world scenarios of cybersecurity.

- **Funding:** This research received no external funding.
- **Institutional Review Board Statement:** Not applicable.
- **Informed Consent Statement:** Not applicable.
- **Data Availability Statement:** The data supporting the findings of this study are available from the corresponding author upon reasonable request.
- **Conflicts of Interest:** The author declares no conflict of interest.

How to cite this article:

R. Kumar, "Recent Advances in Privacy-Preserving Cybersecurity Using Homomorphic Encryption and Federated Learning," *Journal of Global Research in Electronics and Communication*, vol. 2, no. 8, pp. 01–07, Jul. 2026. Doi. XXXX

REFERENCES

- [1] T. R. Akash, N. J. Sany, L. Akter, and S. A. Sarna, "Privacy - Preserving Technique in cybersecurity: Balancing Data Protection and User Rights," *J. Comput. Sci. Technol. Stud.*, vol. 7, no. 4, pp. 248–263, 2025, doi: 10.32996/jcsts.2025.7.3.90.
- [2] Y. Muni, "Advanced Multi-Protocol Label Switching (MPLS)-Enabled Networks: A Survey of Emerging Approaches Via Traffic Engineering," *Eng. Technol. J.*, vol. 11, no. 01, Jan. 2026, doi: 10.47191/etj/v11i01.22.
- [3] A. Aleroud, F. Yang, S. C. Pallaprolu, Z. Chen, and G. Karabatis, "Anonymization of Network Traces Data through Condensation-based Differential Privacy," *Digit. Threat. Res. Pract.*, vol. 2, no. 4, pp. 1–23, Dec. 2021, doi: 10.1145/3425401.
- [4] D. Akinyele, "Secure Data Sharing Using Homomorphic Encryption for Network Traffic Analysis," 2024.
- [5] A. Kahate, R. Babulkar, R. Chakole, and S. Deote, "Review Paper : A Detailed Review of Federated Learning in Cybersecurity with a Focus on Sandbox Integration," vol. 12, no. 06, pp. 55–60, 2025, doi: 10.1109/TCLT52584.2020.0900497.
- [6] M. R. War, Y. Singh, Z. A. Sheikh, and P. Singh, "Review on the Use of Federated Learning Models for the Security of Cyber-Physical Systems," *Scalable Comput. Pract. Exp.*, vol. 26, pp. 16–33, 2025, doi: 10.12694/scpe.v26i1.3438.
- [7] S. Singamsetty, "AI-Enabled Data Stewardship Real-Time Alignment of Privacy and Storage Policies Across Global Systems using Deep CNN-RNN Techniques," in *2025 5th Asian Conference on Innovation in Technology (ASIANCON)*, IEEE, Aug. 2025, pp. 1–6, doi: 10.1109/ASIANCON66527.2025.11281010.
- [8] G. Longo, F. Lupia, A. Merlo, F. Pagano, and E. Russo, "A data anonymization methodology for security operations centers: Balancing data protection and security in industrial systems," *Inf. Sci. (Ny)*, vol. 690, no. October 2024, p. 121534, 2025, doi: 10.1016/j.ins.2024.121534.
- [9] M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study," *Arab. J. Sci. Eng.*, vol. 45, 2020, doi: 10.1007/s13369-019-04319-2.
- [10] S. Chatterjee, "Advanced Malware Detection in Operational Technology: Signature-Based Vs. Behaviour-Based Approaches," *ESP J. Eng. Technol. Adv.*, vol. 1, 2021, doi: 10.56472/25832646/JETA-V1I2P128.
- [11] R. Azmeera, "The Effects of Increased Software Errors on Software Product Functionality," University of the Cumberland, 2025, doi: 10.13140/RG.2.2.18820.80009.
- [12] H. Zebari and W. Abdullallah, "Cryptographic Techniques for Data Privacy Preservation: A Review," *East J. Appl. Sci.*, vol. 1, pp. 40–53, 2025, doi: 10.63496/ejas.Vol1.Iss1.50.
- [13] R. Bahri, M. A. Budiman, and B. B. Nasution, "Sign-Then-Encrypt Scheme with Cramer-Shoup Cryptosystem and Dissanayake Digital Signature," *3rd Int. Conf. Adv. Inf. Sci. Dev. (ICAISD 2023)*, pp. 131–138, 2023, doi: 10.5220/0012444900003848.
- [14] M. M. Islam, "Exploring the Applications of Artificial Intelligence across Various Industries," 2024.
- [15] S. C. Pallaprolu, "Zero-day Attack Identification in Streaming Data: Nearest Neighbor Heuristics and Dynamic Semantic Network Generation in the Spark Eco-system," University of Maryland, Baltimore County, 2017.
- [16] M. Sarker, "Revolutionizing healthcare: the role of machine learning in the health sector," 2024.
- [17] H. Padmanaban, "Revolutionizing Regulatory Reporting through AI/ML: Approaches for Enhanced Compliance and Efficiency," 2024.
- [18] N. Rashid and H. Maseeh, "Privacy-preserving machine learning: a review of federated learning techniques and applications," *Int. J. Sci. World*, vol. 11, pp. 30–39, 2025, doi: 10.14419/af03y111.
- [19] A. Iricanin, O. Ristic, and M. Milošević, "Privacy-Preserving in Machine Learning: Differential Privacy Case Study," 2024, pp. 89–96, doi: 10.46793/TIE24.0891.
- [20] T. Habibu and A. Julius, "Cybersecurity in the Internet of Things (IoT) - Review," *DS J. Cyber Secur.*, vol. 3, pp. 15–38, 2025, doi: 10.59232/CYS-V3I3P102.
- [21] R. Kumar and K. Patibandla, "Enhancing Data Security and Privacy in Edge Computing: A Comprehensive Review of Key Technologies and Future Directions," *SSRN Electron. J.*, vol. 11, p. 77, 2023, doi: 10.2139/ssrn.5187239.
- [22] R. Zhang, Y. Li, and L. Fang, "PBTMS: A Blockchain-Based Privacy-Preserving System for Reliable and Efficient E-Commerce," *Electronics*, vol. 14, no. 6, 2025, doi: 10.3390/electronics14061177.
- [23] T. Surve, A. K. Tyagi, S. Tiwari, and S. Sreevathsa, "Revolutionizing Blockchain Governance: Integrating Gamification, Reputation, and Education into Proxy Voting Systems," *Procedia Comput. Sci.*, vol. 282, pp. 316–325, 2026, doi: 10.1016/j.procs.2026.05.079.
- [24] S. Sarpong, S. Opuni-Basoa, and K. Awuah-Mensah, "Homomorphic Encryption: an Overview," *Int. J. Comput. Sci. Mob. Comput.*, vol. 14, no. 10, p., 2025.
- [25] S. Goldwasser and S. Micali, "Probabilistic encryption & how to play mental poker keeping secret all partial information", doi: 10.1145/800070.802212.
- [26] K. K. Mohammed, "The Future is Cloud : Modernizing Big Data for the Cloud Era," *Int. J. Sci. Res. Eng. Trends*, vol. 11, no. 5, pp. 1–5, 2025, doi: 10.5281/zenodo.17339856.
- [27] C. Gilbert and M. A. Gilbert, "The Effectiveness of Homomorphic Encryption in Protecting Data Privacy," *Int. J. Res. Publ. Rev.*, vol. 5, pp. 3235–3256, 2024, doi: 10.2139/ssrn.5259722.
- [28] M. Aggarwal, V. Khullar, and N. Goyal, "A comprehensive review of

- federated learning: Methods, applications, and challenges in privacy-preserving collaborative model training," *Appl. Data Sci. Smart Syst.*, vol. 2, pp. 570–575, 2024, doi: 10.1201/9781003471059-73.
- [29] A. Wajahat, K. Zhang, and J. Latif, "A Comprehensive Review Of Federated Learning: Advancements, Challenges, And Future Directions," *J. Intell. Syst. Appl. Data Sci.*, vol. 3, 2025, doi: 10.64680/jisads.v3i1.38.
- [30] R. Vishvakarma, "A Governance Model For Agentic Ai Use In Banking Systems," *Int. Res. J. Mod. Eng. Technol. Sci.*, vol. 8, no. 6, pp. 2917–2934, june, Jul. 2026, doi: 10.56726/IRJMETS100553.
- [31] P. K. Myakala, C. Bura, and A. K. Jonnalagadda, "Federated Learning and Data Privacy: A Review of Challenges and Opportunities," *Int. J. Res. Publ. Rev.*, vol. 5, no. 12, pp. 1867–1879, 2024, doi: 10.55248/gengpi.5.1224.3512.
- [32] Z. Myrzakul, Z. Temirbekova, and G. Myrzakul, "Development and Performance Evaluation of a Modified Homomorphic Encryption Scheme for ESP32-Based Resource-Constrained IoT Devices," in *2026 IEEE 6th International Conference on Smart Information Systems and Technologies (SIST)*, 2026, pp. 1–5. doi: 10.1109/SIST61674.2026.11596207.
- [33] P. Pushpa, S. Aravinth, B. Jackson, R. Shankari, J. Sasidevi, and M. S. Priya, "Homomorphic Encryption for Enhanced Cybersecurity Privacy-Preserving Data Processing in Cloud-based Systems," in *2025 6th International Conference for Emerging Technology (INCET)*, 2025, pp. 1–6. doi: 10.1109/INCET64471.2025.11140360.
- [34] W. Yang, Y. Bai, Y. Rao, H. Wu, G. Xing, and Y. Zhou, "Privacy-Preserving Federated Learning with Homomorphic Encryption and Sparse Compression," in *2024 4th International Conference on Computer Communication and Artificial Intelligence (CCAI)*, 2024, pp. 192–198. doi: 10.1109/CCAI61966.2024.10602929.
- [35] P. Thantharate and A. T, "CYBRIA - Pioneering Federated Learning for Privacy-Aware Cybersecurity with Brilliance," in *2023 IEEE 20th International Conference on Smart Communities: Improving Quality of Life using AI, Robotics and IoT (HONET)*, IEEE, Dec. 2023, pp. 56–61. doi: 10.1109/HONET59747.2023.10374608.
- [36] J. Domingo-Ferrer, A. Blanco-Justicia, J. Manjón, and D. Sánchez, "Secure and Privacy-Preserving Federated Learning via Co-Utility," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3988–4000, 2022, doi: 10.1109/JIOT.2021.3102155.