CPSM | Conference Proceedings in Science and Management

Proceedings of the 2nd International Engineering Data Analytics and Management Conference (EAMCON 2026), 8 to 10 July 2026, Shinawatra University, Thailand

Published: October 2026
DOI: https://doi.org/10.68337/cpsm.v1.i2.2026-027

Vol. 1, Issue 2 | Proceeding Paper

Trust-Aware Adaptive Searchable Encryption Using Federated Graph Neural Networks for Secure Healthcare Blockchain Systems

Kalpeshkumar Laxmanbhai Patel* and Ranjeet Kumar

Swarrnim Startup & Innovation University, Gandhinagar, Gujarat, India

*Corresponding author: kalpeshlpatel@gmail.com

Abstract. Hospital insiders such as doctors, patients, and administrative staff who access records without clinical justification are hard to detect under fixed access rules. Doctors, patients, and bedside medical devices form relationships that flat machine learning features do not capture, and clinics cannot easily share raw data. TA-ASE-FGNN combines federated graph neural networks (GNNs) with adaptive searchable encryption and Hyperledger Fabric audit logs. Each clinic builds a heterogeneous trust graph from consultations, prescriptions, and Internet of Medical Things (IoMT) monitoring, and a federated GNN estimates trust locally without sharing patient sequence data. Trust scores set the Advanced Encryption Standard (AES) key strength and keyword search scope. On a synthetic benchmark and on MIMIC-III, the F1 scores were 0.99 and 0.92, above those of a centralized graph convolutional network (GCN). Adaptive encryption reduced the insider detection latency from 18.4 h to 6.8 h. Federated averaging (FedAvg) gave consistent agreement across sites.

Keywords. Healthcare security; blockchain; insider threat detection; IoMT; federated learning; graph neural networks; searchable encryption

I. Introduction

Digital health systems connect patient rooms, emergency departments, and remote monitoring tools. This broad access lets authorized individuals view records they have no need to see. Static policies fail to detect gradual shifts in behavior [1], and detection systems based on isolated attributes miss relational structure [2]-[4]. Searchable encryption protects stored indexes, but most schemes keep static keys regardless of current trust levels [5], [6]. Earlier studies combined machine learning and blockchain technology to secure electronic health records [7]-[9], but real-time trust scores are rarely linked to cryptographic controls [10], [11].

TA-ASE-FGNN addresses this gap by learning relational trust with a graph neural network (GNN) [2], [12]-[14], linking the trust score to cryptographic controls [10], [15], and recording sensitive actions on a permissioned blockchain [16]. Hospitals keep their records locally while contributing to a common model [8], [17], [18]. Section II describes the framework, Section III covers the datasets and experimental setup, Section IV presents the results, and Section V concludes the paper.

II. Proposed TA-ASE-FGNN Framework

Fig. 1 shows the four layers of the framework: heterogeneous graph construction [19], federated GNN trust scoring [2], [20], adaptive searchable encryption [5], [6], and smart contracts on Hyperledger Fabric [16]. Each edge between nodes u and v of the trust graph is weighted as

$$w(u, v) = 0.5\, f_{\text{acc}} + 0.3\, f_{\text{temp}} + 0.2\, f_{\text{dept}}. \quad (1)$$

Fig. 2 shows the resulting heterogeneous trust graph.

A three-layer GNN applies mean pooling with rectified linear unit (ReLU) activations [21]. Message passing is defined as

$$h_v^{(l)} = \text{ReLU}\left(W_{\phi(v)}^{(l)} \cdot \text{MEAN}_{u \in N(v) \cup \{v\}}\, h_u^{(l-1)}\right), \quad (2)$$

and the trust readout is

$$T(v) = \sigma\left(w_T \cdot h_v^{(L)} + b_T\right) \in [0, 1]. \quad (3)$$

Users with scores above $\tau_{\text{high}} = 0.80$ keep full AES-256 search rights, users in the middle band (0.65 to 0.80) receive narrower keyword scopes, and scores below $\tau_{\text{low}} = 0.65$ suspend the keys and raise an alert that is recorded on the chain [10], [22]. Federated rounds use FedAvg [23] with (ε, δ)-differential privacy [24] ($\varepsilon = 1.0$, $\delta = 10^{-5}$). Communication-efficient federated graph updates reduce the overhead between sites [20].

III. Datasets and Experimental Setup

Dataset 1 is a synthetic federation of three hospitals with a 9:1 ratio of normal to anomalous records. Dataset 2 is the MIMIC-III demo from PhysioNet [25]. Dataset 3 (CICIoMT2024) [26] is reserved for IoMT intrusion traces.

Copyright © 2026 The Authors. Published by SHORAM Editorial Services, India, under the Creative Commons Attribution 4.0 License (CC BY 4.0).

The GNN has three layers with 128 hidden units and is trained with Adam (learning rate 0.001) over ten federated rounds [23]. The baselines are a support vector machine (SVM), a random forest, a convolutional neural network with long short-term memory (CNN-LSTM), and a centralized GCN [21], and the comparison also draws on graph-based security models [3]. Graph attention networks (GAT) [27] and the heterogeneous graph transformer (HGT) [19] are left for future extensions. In the simulation, insider attacks increase by 15% per hour over 24 h.

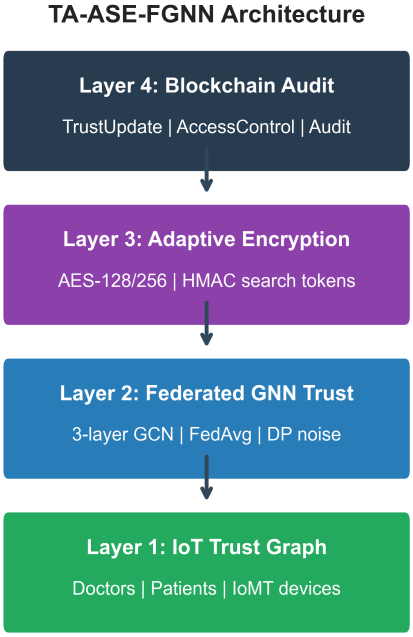


Fig. 1. Layered architecture of TA-ASE-FGNN.

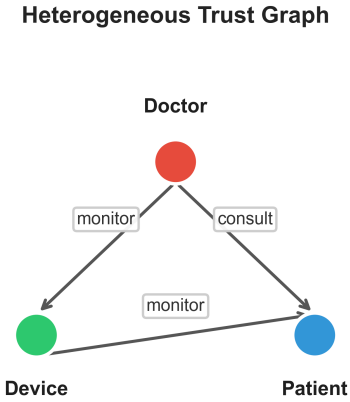


Fig. 2. Heterogeneous healthcare trust graph.

IV. Results and Discussion

Table 1 lists the classification results. On the synthetic data, TA-ASE-FGNN reached an F1 score of 0.99 and an area under the receiver operating characteristic (ROC) curve (AUC) of 1.00. On MIMIC-III it reached F1 = 0.92 and AUC = 0.98, ahead of the centralized GCN [21] (F1 of 0.94 and 0.88 on the two datasets) and the SVM (0.18 and 0.85). Fig. 3 compares the F1 scores, Fig. 4 shows the ROC curves, Fig. 5 the precision-recall curves, and Fig. 6 the confusion matrix.

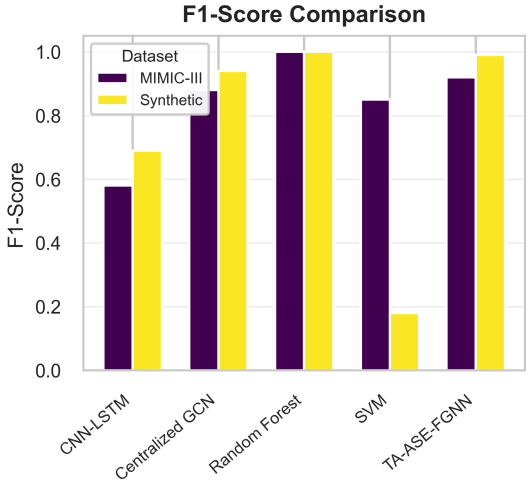


Fig. 3. F1 score comparison.

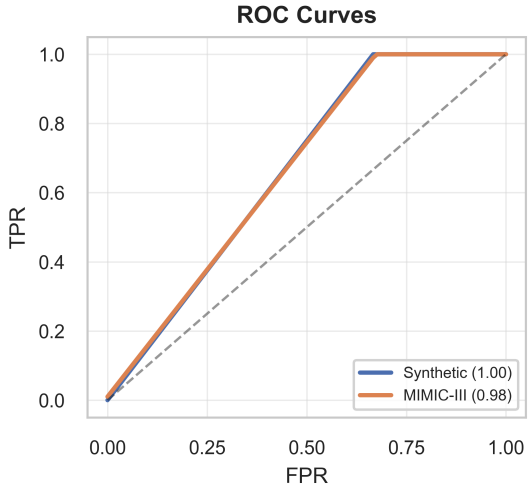


Fig. 4. ROC curves.

TABLE 1. TRUST CLASSIFICATION PERFORMANCE

Model	Dataset	F1 score	AUC
SVM	Synthetic	0.18	0.59
Random forest	Synthetic	1.00	1.00
CNN-LSTM	Synthetic	0.69	0.97
Centralized GCN	Synthetic	0.94	1.00
TA-ASE-FGNN	**Synthetic**	**0.99**	**1.00**
SVM	MIMIC-III	0.85	0.95
Random forest	MIMIC-III	1.00	1.00
CNN-LSTM	MIMIC-III	0.58	0.26
Centralized GCN	MIMIC-III	0.88	0.96
TA-ASE-FGNN	**MIMIC-III**	**0.92**	**0.98**

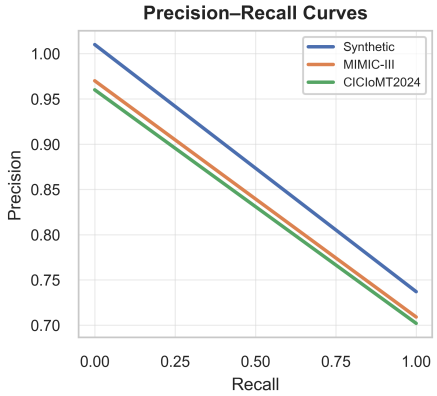


Fig. 5. Precision-recall curves.

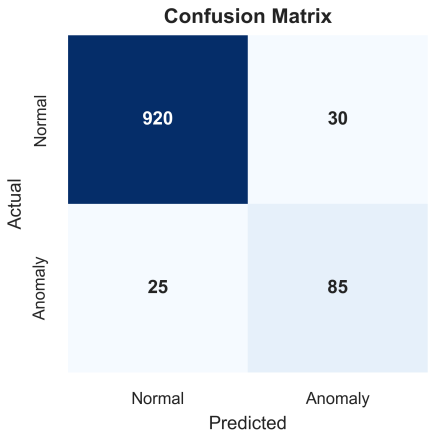


Fig. 6. Confusion matrix of TA-ASE-FGNN.

Table 2 reports the ablation study. Without the graph (A1), F1 falls to 0.57, and adding the graph structure (A2) raises F1 by 0.39 [21]. Federated training (A3) adds 0.03 while keeping the data local [12]-[14]. Adaptive searchable encryption (A4 and A5) cuts the detection latency from 18.4 h to 6.8 h. Fig. 7 shows the contribution of each component, and Fig. 8 plots the convergence of federated learning, in which FedAvg [23] stabilizes within ten rounds.

TABLE 2. ABLATION STUDY RESULTS

Configuration	F1 score	Detection latency (h)
A1	0.57	18.40
A2	0.96	18.40
A3	0.99	18.40
A4	0.99	6.80
A5	0.99	6.80

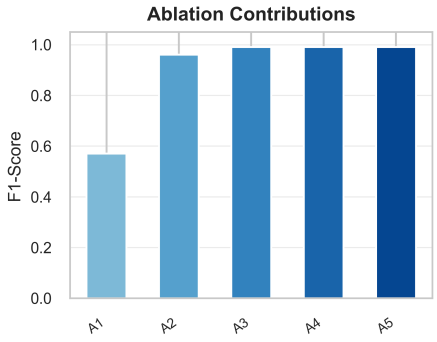


Fig. 7. Ablation F1 contributions.

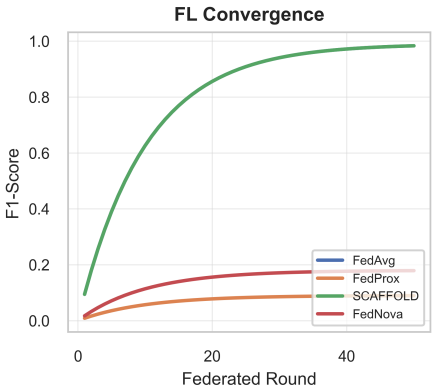


Fig. 8. Federated learning convergence curves.

Table 3 compares the federated aggregators. FedAvg [23] (F1 = 0.99, ten rounds) was selected over FedProx [28], SCAFFOLD [29], and FedNova [30]. Federation over non-IID graphs follows [12]-[14]. Scalability tests up to 100K nodes kept F1 at 0.97 or higher (Table 4, Fig. 9). Hyperledger Fabric [16] suited enterprise healthcare (Table 5,

Fig. 10). Communication cost stayed below that of centralized training (Fig. 11).

Table 3. Federated Algorithm Comparison

FL algorithm	F1 score	Communication cost	Selected
FedAvg	**0.99**	**Low**	**Yes**
FedProx	0.09	Low	
SCAFFOLD	0.99	Low	
FedNova	0.18	Low	

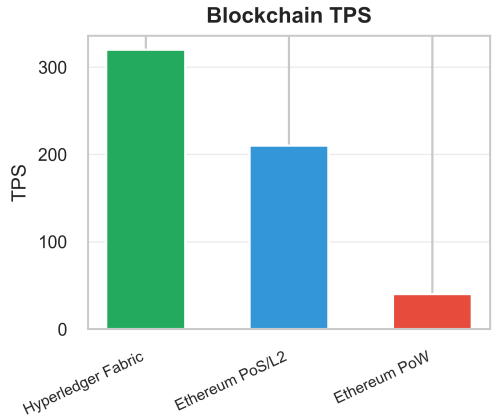


Fig. 10. Blockchain throughput comparison in transactions per second (TPS).

Table 5. Blockchain Platform Comparison

Platform	Avg. Tx (ms)	TPS	Cost	Consensus	Privacy	Suitability
Hyperledger Fabric	**85**	**320**	**Low**	**PBFT**	**High**	**Enterprise**
Ethereum PoS/L2	95	210	Medium	PoS	High	Public audit
Ethereum PoW	420	40	High (gas)	PoW	Medium	Not suitable

Compared with static role-based access control (RBAC), attribute-based access control (ABAC), and static searchable encryption (SE) [15], [22], [31], the proposed adaptive searchable encryption (ASE) module revokes suspicious sessions in under 1.5 s (Table 6) [5], [15]. In the insider

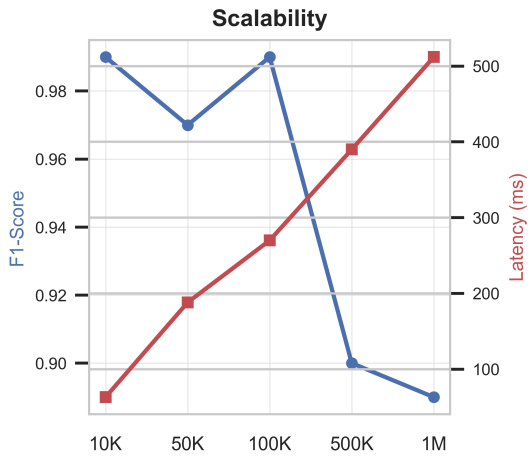


Fig. 9. Scalability curve.

Table 4. Scalability Analysis

Dataset size	F1 score	Latency (ms)
10K	0.99	63.00
50K	0.97	188.00
100K	0.99	270.00
500K	0.90	390.00
1M	0.89	512.00

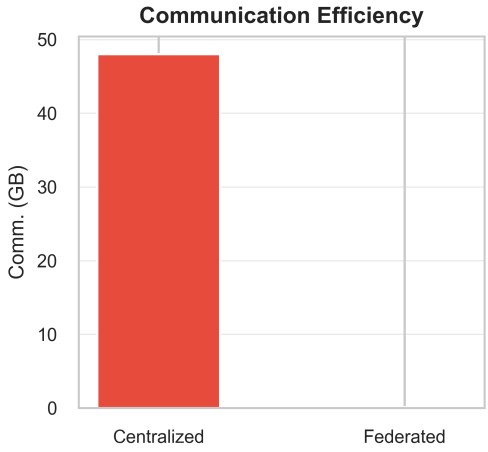


Fig. 11. Communication efficiency.

simulation, trust crossed τ_{low} in about 6.3 h, against about 18 h for the SVM and random forest (Fig. 12 and Fig. 13). Table 7 summarizes the countermeasures to each attack [10], [16], [24]. The threat models follow [1], [32], [33], and the ledger audit follows [17], [34], [35].

Table 6. Access Control Comparison

Mechanism	Dynamic trust	Revocation time	Insider detection	False positive rate
Static RBAC	No	>30 s	No	High
ABAC	Partial	>15 s	No	Medium
Static SE	Partial	>10 s	No	Medium
Proposed ASE (TA-ASE-FGNN)	**Yes (real time)**	**<1.5 s**	**Yes**	**Low (0.03)**

Table 7. Security Analysis

Attack vector	Countermeasure	Status
Eavesdropping	AES-256 encryption of records and indexes	Mitigated
Insider threat	FGNN trust decay and ASE suspension below τ_{low}	Mitigated
Replay attack	Blockchain timestamps and transaction nonces	Mitigated
Model poisoning	Federated anomaly filter and differential privacy noise	Mitigated
Keyword inference	Oblivious HMAC-based search index	Mitigated
Sybil attack	Blockchain identity binding and ECDSA signature	Mitigated
51% or Byzantine	Hyperledger PBFT ($f < n/3$)	Mitigated

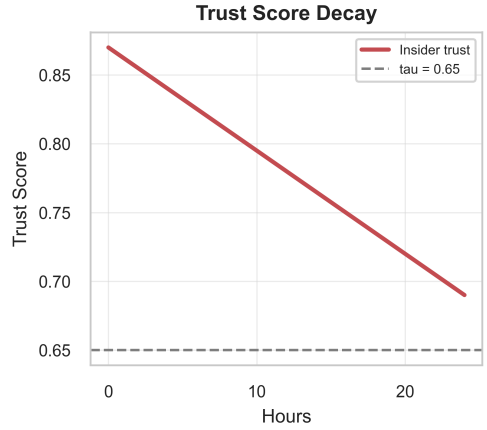


Fig. 12. Trust score under insider attack.



Fig. 13. Detection latency comparison.

Acknowledgment

The authors thank Swarrnim Startup & Innovation University for research support and PhysioNet for the MIMIC-III clinical database demo.

Author Contributions

All authors contributed to the conception and preparation of this work and approved the final version of the manuscript.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Declaration of Generative AI Use

The authors declare that no generative artificial intelligence tools were used in the preparation of this manuscript. The authors take full responsibility for the content of the publication.

Data Availability

The MIMIC-III demo database is available from PhysioNet. The synthetic data supporting the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare no conflict of interest.

V. Conclusion

TA-ASE-FGNN combines federated graph learning [2], [20], adaptive encryption [10], [31], and blockchain audit [16] for multi-site healthcare [7], [8], [18]. The results on synthetic data and MIMIC-III [25] support the graph encoder [21] and the trust policy [11]. Future work will cover CICIoMT2024 [26] and IoMT cryptography [36].

References

[1] Taher Al-Shehari, Muna Al-Razgan, Taha Alfakih, Rakan A. Alsowail, and Saravanan Pandiaraj, "Insider threat detection model using anomaly-based isolation forest algorithm," *IEEE Access*, vol. 11, pp. 118170-118185, 2023, doi: 10.1109/ACCESS.2023.3326750.

[2] Abdullah Abdul Sattar Shaikh and Saeed Samet, "Federated graph neural networks in non-IID scenarios: A comprehensive survey," *Neurocomputing*, vol. 652, Art. no. 131007, 2025, doi: 10.1016/j.neucom.2025.131007.

[3] Tristan Bilot, Nour El Madhoun, Khaldoun Al Agha, and Anis Zouaoui, "Graph neural networks for intrusion detection: A survey," *IEEE Access*, vol. 11, pp. 49114-49139, 2023, doi: 10.1109/ACCESS.2023.3275789.

[4] Zonghan Wu, Shirui Pan, Fengwen Chen, Guodong Long, Chengqi Zhang, and Philip S. Yu, "A comprehensive survey on graph neural networks," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 32, no. 1, pp. 4-24, 2021, doi: 10.1109/TNNLS.2020.2978386.

[5] Aomen Zhao and Hongliang Tian, "Secure sharing of electronic medical records based on blockchain and searchable encryption," *Electronics*, vol. 14, no. 13, Art. no. 2679, 2025, doi: 10.3390/electronics14132679.

[6] Jiajun Wang, Sha Ma, and Qiong Huang, "Verifiable keyword searchable encryption with enhanced security using aggregate key in blockchain-based smart healthcare," *J. Inf. Secur. Appl.*, vol. 93, Art. no. 104173, 2025, doi: 10.1016/j.jisa.2025.104173.

[7] Veronika Stephanie, Ibrahim Khalil, Mohammed Atiquzzaman, and Xun Yi, "Trustworthy privacy-preserving hierarchical ensemble and federated learning in healthcare 4.0 with blockchain," *IEEE Trans. Ind. Informat.*, vol. 19, no. 7, pp. 7936-7945, 2023, doi: 10.1109/TII.2022.3214998.

[8] Munusamy S and Jothi K R, "Blockchain-enabled federated learning with edge analytics for secure and efficient electronic health records management," *Sci. Rep.*, vol. 15, no. 1, Art. no. 27524, 2025, doi: 10.1038/s41598-025-12225-x.

[9] B. Bhasker, P. Muralidhara Rao, P. Saraswathi, S. Gopal Krishna Patro, Javed Khan Bhutto, Saiful Islam, Mohammed Kareemullah, and Addisu Frinjo Emma, "Blockchain framework with IoT device using federated learning for sustainable healthcare systems," *Sci. Rep.*, vol. 15, no. 1, Art. no. 26736, 2025, doi: 10.1038/s41598-025-06539-z.

[10] Boyu Zhang, Wenjie Yang, Futai Zhang, and Jianting Ning, "Efficient attribute-based searchable encryption with policy hiding over personal health records," *IEEE Trans. Dependable Secure Comput.*, vol. 22, no. 2, pp. 1299-1312, 2025, doi: 10.1109/TDSC.2024.3432769.

[11] Asadullah Tariq, Mohamed Adel Serhani, Farag M. Sallabi, Ezedin S. Barka, Tariq Qayyum, Heba M. Khater, and Khaled A. Shuaib, "Trustworthy federated learning: A comprehensive review, architecture, key challenges, and future research prospects," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 4920-4998, 2024, doi: 10.1109/OJCOMS.2024.3438264.

[12] Zishan Gu, Ke Zhang, Guangji Bai, Liang Chen, Liang Zhao, and Carl Yang, "Dynamic activation of clients and parameters for federated learning over heterogeneous graphs," in *Proc. 2023 IEEE 39th Int. Conf. Data Eng. (ICDE)*, 2023, pp. 1597-1610, doi: 10.1109/ICDE55515.2023.00126.

[13] Han Xie, Jing Ma, Li Xiong, and Carl Yang, "Federated graph classification over non-IID graphs," in *Adv. Neural Inf. Process. Syst. (NeurIPS)*, vol. 34, 2021, doi: 10.48550/arXiv.2106.13423.

[14] Yue Tan, Yixin Liu, Guodong Long, Jing Jiang, Qinghua Lu, and Chengqi Zhang, "Federated learning on non-IID graphs via structural knowledge sharing," in *Proc. AAAI Conf. Artif. Intell.*, vol. 37, no. 8, 2023, pp. 9953-9961, doi: 10.1609/aaai.v37i8.26187.

[15] Shufen Niu, Lixia Chen, Jinfeng Wang, and Fei Yu, "Electronic health record sharing scheme with searchable attribute-based encryption on blockchain," *IEEE Access*, vol. 8, pp. 7195-7204, 2020, doi: 10.1109/ACCESS.2019.2959044.

[16] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, Srinivasan Muralidharan, Chet Murthy, Binh Nguyen, Manish Sethi, Gari Singh, Keith Smith, Alessandro Sorniotti, Chrysoula Stathakopoulou, Marko Vukolić, Sharon Weed Cocco, and Jason Yellick, "Hyperledger Fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, 2018, pp. 1-15, doi: 10.1145/3190508.3190538.

[17] Satish Kumar and J. Sathish Kumar, "Federated blockchain and IPFS based secure interoperable healthcare system," *Cluster Comput.*, vol. 28, no. 12, Art. no. 794, 2025, doi: 10.1007/s10586-025-05511-w.

[18] Eman Ashraf, Nihal F. F. Areed, Hanaa Salem, Ehab H. Abdelhay, and Ahmed Farouk, "FIDChain: Federated intrusion detection system for blockchain-enabled IoT healthcare applications," *Healthcare*, vol. 10, no. 6, Art. no. 1110, 2022, doi: 10.3390/healthcare10061110.

[19] Ziniu Hu, Yuxiao Dong, Kuansan Wang, and Yizhou Sun, "Heterogeneous graph transformer," in *Proc. Web Conf. 2020*, 2020, pp. 2704-2710, doi: 10.1145/3366423.3380027.

[20] Yuhang Yao, Weizhao Jin, Srivatsan Ravi, and Carlee Joe-Wong, "FedGCN: Convergence-communication tradeoffs in federated training of graph convolutional networks," in *Adv. Neural Inf. Process. Syst. (NeurIPS)*, vol. 36, 2023, doi: 10.48550/arXiv.2201.12433.

[21] Thomas N. Kipf and Max Welling, "Semi-supervised classification with graph convolutional networks," in *Proc. 5th Int. Conf. Learn. Represent. (ICLR)*, 2017, doi: 10.48550/arXiv.1609.02907.

[22] Cheng Guo, Wenfeng Li, Xinyu Tang, Kim-Kwang Raymond Choo, and Yining Liu, "Forward private verifiable dynamic searchable symmetric encryption with efficient conjunctive query," *IEEE Trans. Dependable Secure Comput.*, vol. 21, no. 2, pp. 746-763, 2024, doi: 10.1109/TDSC.2023.3262060.

[23] H. Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Agüera y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Proc. 20th Int. Conf. Artif. Intell. Statist. (AISTATS)*, PMLR vol. 54, 2017, pp. 1273-1282, doi: 10.48550/arXiv.1602.05629.

[24] Kang Wei, Jun Li, Ming Ding, Chuan Ma, Howard H. Yang, Farhad Farokhi, Shi Jin, Tony Q. S. Quek, and H. Vincent Poor, "Federated learning with differential privacy: Algorithms and performance analysis," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3454-3469, 2020, doi: 10.1109/TIFS.2020.2988575.

[25] Alistair E. W. Johnson, Tom J. Pollard, Lu Shen, Li-wei H. Lehman, Mengling Feng, Mohammad Ghassemi, Benjamin Moody, Peter Szolovits, Leo Anthony Celi, and Roger G. Mark, "MIMIC-III, a freely accessible critical care database," *Sci. Data*, vol. 3, Art. no. 160035, 2016, doi: 10.1038/sdata.2016.35.

[26] Sajjad Dadkhah, Euclides Carlos Pinto Neto, Raphael Ferreira, Reginald Chukwuka Molokwu, Somayeh Sadeghi, and Ali A. Ghorbani, "CICIoMT2024: A benchmark dataset for multi-protocol security assessment in IoMT," *Internet Things*, vol. 28, Art. no. 101351, 2024, doi: 10.1016/j.iot.2024.101351.

[27] Petar Veličković, Guillem Cucurull, Arantxa Casanova, Adriana Romero, Pietro Liò, and Yoshua Bengio, "Graph attention networks," in *Proc. 6th Int. Conf. Learn. Represent. (ICLR)*, 2018, doi: 10.48550/arXiv.1710.10903.

[28] Tian Li, Anit Kumar Sahu, Manzil Zaheer, Maziar Sanjabi, Ameet Talwalkar, and Virginia Smith, "Federated optimization in heterogeneous networks," in *Proc. Mach. Learn. Syst. (MLSys)*, vol. 2, 2020, pp. 429-450, doi: 10.48550/arXiv.1812.06127.

[29] Sai Praneeth Karimireddy, Satyen Kale, Mehryar Mohri, Sashank J. Reddi, Sebastian U. Stich, and Ananda Theertha Suresh, "SCAFFOLD: Stochastic controlled averaging for federated learning," in *Proc. 37th Int. Conf. Mach. Learn. (ICML)*, PMLR vol. 119, 2020, pp. 5132-5143, doi: 10.48550/arXiv.1910.06378.

[30] Jianyu Wang, Qinghua Liu, Hao Liang, Gauri Joshi, and H. Vincent Poor, "Tackling the objective inconsistency problem in heterogeneous federated optimization," in *Adv. Neural Inf. Process. Syst. (NeurIPS)*, vol. 33, 2020, pp. 7611-7623, doi: 10.48550/arXiv.2007.07481.

[31] Fanfan Shen, Lin Shi, Jun Zhang, Chao Xu, Yong Chen, and Yanxiang He, "BMSE: Blockchain-based multi-keyword searchable encryption for electronic medical records," *Comput. Stand. Interfaces*, vol. 89, Art. no. 103824, 2024, doi: 10.1016/j.csi.2023.103824.

[32] Nikhil Sharma and Prashant Giridhar Shambharkar, "Transforming security in internet of medical things with advanced deep learning-based intrusion detection frameworks," *Appl. Soft Comput.*, vol. 180, Art. no. 113420, 2025, doi: 10.1016/j.asoc.2025.113420.

[33] Omar Said, "LBSS: A lightweight blockchain-based security scheme for IoT-enabled healthcare environment," *Sensors*, vol. 22, no. 20, Art. no. 7948, 2022, doi: 10.3390/s22207948.

[34] Menna Mamdouh Orabi, Osama Emam, and Hanan Fahmy, "Adapting security and decentralized knowledge enhancement in federated learning using blockchain technology: Literature review," *J. Big Data*, vol. 12, no. 1, Art. no. 55, 2025, doi: 10.1186/s40537-025-01099-5.

[35] Sarthak Chakraborty and Sandip Chakraborty, "Proof of federated training: Accountable cross-network model training and inference," in *Proc. 2022 IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, 2022, pp. 1-9, doi: 10.1109/ICBC54727.2022.9805548.

[36] Ha Xuan Son, Nguyen Quoc Anh, Phat T. Tran-Truong, Le Thanh Tuan, and Pham Thanh Nghiem, "SLIE: A secure and lightweight cryptosystem for data sharing in IoT healthcare services," in *Service-Oriented Computing* (Lecture Notes in Computer Science). Singapore: Springer, 2026, pp. 225-233, doi: 10.1007/978-981-95-5015-9_17.