Jurnal TICOM: Technology of Information and Communication
Volume 13, Nomor 2, Januari 2024 Hal: 74-78 E-ISSN: 2962-7982

Optimasi Penggunaan Enkripsi Homomorfik untuk Keamanan dan Privasi Data Kesehatan (Studi Literatur)

Muhammad Harun Yahya[1]*, Chrisdiego Chrisanto[2], Abdu Afin Arsy[3]

[1,2,3]Fakultas Matematika dan Ilmu Pengetahuan Alam Militer, Matematika, Universitas Pertahanan RI, Bogor, Indonesia
Kawasan IPSC Sentul, Sukahati, Kec. Citeureup, Kabupaten Bogor, Jawa Barat 16810
E-mail: [1]harunyahya119@gmail.com, [2]chrisdiegoc@gmail.com, [3]aaarsy01@gmail.com
(*: corresponding author)

Abstrak— **Digitalisasi dalam sektor kesehatan menghadirkan tantangan baru terkait privasi dan keamanan data medis. Artikel ini mengulas optimalisasi penggunaan enkripsi homomorfik (HE) untuk melindungi data kesehatan dalam kerangka Federated Learning (FL) dan Internet of Medical Things (IoMT). Kajian ini memaparkan tantangan implementasi HE, seperti konsumsi daya tinggi dan keterbatasan perangkat IoT, serta solusi untuk mengatasi kendala tersebut. Hasil tinjauan literatur menunjukkan bahwa inovasi algoritma HE hemat daya dan integrasi dengan teknologi blockchain mampu meningkatkan efisiensi dan keamanan dalam sistem kesehatan berbasis IoT. Studi ini menekankan pentingnya pengembangan teknologi enkripsi yang efisien guna mendukung interoperabilitas data medis dan meningkatkan kepercayaan publik terhadap sistem kesehatan digital.**

Kata Kunci— **Enkripsi homomorfik, privasi data, Federated Learning, IoMT, blockchain.**

Abstract— ***The digital transformation in the healthcare sector presents new challenges regarding privacy and security of medical data. This article reviews the optimization of homomorphic encryption (HE) for safeguarding healthcare data within the frameworks of Federated Learning (FL) and the Internet of Medical Things (IoMT). The study highlights challenges such as high power consumption and IoT device limitations, alongside solutions to address these constraints. Findings from the literature review indicate that innovative energy-efficient HE algorithms and blockchain integration significantly enhance efficiency and security in IoT-based healthcare systems. This study underscores the importance of developing efficient encryption technologies to support medical data interoperability and improve public trust in digital healthcare systems.***

Keyword— **Homomorphic encryption, data privacy, Federated Learning, IoMT, blockchain.**

I. PENDAHULUAN

Transformasi digital di sektor kesehatan telah membawa perubahan besar dalam cara data kesehatan dikumpulkan, disimpan, dan dianalisis. Dengan kemajuan teknologi *Internet of Things* (IoT), perangkat medis pintar dan jaringan terintegrasi telah memungkinkan pengumpulan data pasien secara real-time [1]. Hal ini membuka peluang besar untuk meningkatkan kualitas perawatan kesehatan melalui diagnosa yang lebih cepat, personalisasi terapi, dan pengelolaan data pasien yang lebih efisien. Namun, manfaat ini diiringi oleh tantangan besar terkait keamanan dan privasi data [2]. Data kesehatan bersifat sangat sensitif karena menyangkut informasi pribadi yang dapat memengaruhi keamanan pasien jika disalahgunakan. Pelanggaran privasi data tidak hanya berdampak pada individu, tetapi juga dapat mengurangi kepercayaan masyarakat terhadap layanan kesehatan berbasis teknologi [3].

Salah satu pendekatan yang muncul untuk menangani tantangan ini adalah *federated learning* (FL), yang membuat pelatihan model kecerdasan buatan secara terdistribusi tanpa memindahkan data mentah dari perangkat pengguna ke server pusat [4]. FL mengatasi risiko kebocoran data dengan hanya mengirim parameter model yang telah diperbarui, bukan data asli. Namun, penelitian menunjukkan bahwa parameter yang dikirim dalam FL tetap rentan terhadap serangan, seperti inferensi parameter atau rekonstruksi data [5]. Untuk meningkatkan keamanan dalam FL, *homomorphic encryption* (HE) menjadi salah satu solusi yang efektif. HE memungkinkan komputasi dilakukan langsung pada data yang telah dienkripsi, sehingga data sensitif tetap terlindungi sepanjang proses komputasi [6].

Namun, penerapan HE dalam perangkat IoT mempunyai tantangan yang signifikan. Perangkat IoT umumnya memiliki sumber daya terbatas, seperti daya baterai rendah, kapasitas memori terbatas, dan kemampuan komputasi yang tidak memadai [7]. Penggunaan HE pada perangkat ini sering kali menghasilkan *overhead* komputasi yang besar, waktu proses yang lama, dan konsumsi energi yang tinggi. Hal ini membatasi adopsi luas HE dalam sistem kesehatan berbasis IoT [8]. Selain itu, heterogenitas perangkat dan data yang tersebar di berbagai institusi kesehatan memperumit proses agregasi data dalam *federated learning*, sehingga membutuhkan algoritma yang lebih efisien dan adaptif.

Urgensi penelitian ini terletak pada meningkatnya kebutuhan akan solusi privasi dalam lingkungan kesehatan yang semakin terhubung secara digital. Regulasi seperti GDPR di Eropa dan HIPAA di Amerika Serikat semakin menekankan pentingnya perlindungan data pasien, sementara kebutuhan

akan interoperabilitas dan efisiensi tetap tinggi [9]. Tanpa solusi yang tepat, potensi besar IoT dalam meningkatkan layanan kesehatan tidak dapat dimanfaatkan sepenuhnya [10]. Oleh karena itu, penelitian studi literarur ini bertujuan untuk mengoptimalkan HE agar dapat diterapkan pada perangkat dengan sumber daya terbatas, tanpa mengorbankan privasi data maupun efisiensi operasional sistem. Optimasi ini melibatkan desain algoritma HE yang hemat daya dan rendah biaya komunikasi, serta integrasi dengan arsitektur FL untuk memastikan keberlanjutan sistem dalam skala besar [11].

Implementasi HE yang dioptimalkan diharapkan mampu mengatasi tantangan yang ada, seperti waktu enkripsi dan dekripsi yang panjang, serta kebutuhan penyimpanan yang besar [12]. Pendekatan ini juga membuka peluang untuk mengintegrasikan teknologi blockchain sebagai mekanisme tambahan untuk meningkatkan keamanan, stabilitas, dan transparansi data dalam sistem kesehatan berbasis IoT. Dengan demikian, penelitian studi literatur ini tidak hanya berkontribusi pada pengembangan teknologi privasi di sektor kesehatan, tetapi juga memberikan dasar bagi pengembangan sistem kesehatan digital yang lebih aman, efisien, dan dapat diandalkan.

II. METODE PENELITIAN

Metodologi penelitian ini disusun untuk mengkaji penerapan ekripsi homomorfik dalam menjaga privasi data medis. Kajian ini mencakup penentuan ruang lingkup yang berfokus pada diagnosis medis berbasis machine learning dalam lingkungan IoMT dan *edge computing*. Literatur dipilih secara selektif dari sumber akademik terpercaya untuk menjamin relevansi dan validitas kajian. Analisis dilakukan dengan pendekatan tematik dan komparatif, disertai visualisasi data dalam tabel dan grafik untuk mendukung interpretasi hasil. Pendekatan ini diharapkan memberikan wawasan mendalam tentang potensi dan tantangan enkripsi homomorfik dalam sistem diagnosis medis berbasis privasi.

A. *Penentuan Ruang Lingkup*

Pada bagian ini, ruang lingkup kajian difokuskan pada pemanfaatan *homomorphic encryption* dalam menjaga privasi data medis. Kajian ini mencakup bagaimana enkripsi homomorfik diterapkan dalam diagnosis medis berbasis *machine learning*. Fokus literatur diarahkan pada sistem yang mendukung privasi data pasien saat proses diagnosis dan prediksi penyakit, termasuk penerapannya pada lingkungan *Internet of Medical Things* (IoMT) dan layanan berbasis edge computing. Adapun tujuan dari literatur ini adalah untuk memahami peran enkripsi homomorfik dalam meningkatkan privasi, mengidentifikasi tantangan implementasinya, serta menemukan solusi efektif dalam menjaga keamanan data dalam sistem diagnosis medis.

B. *Penentuan Literatur*

Proses pencarian literatur dilakukan dengan memanfaatkan berbagai database akademik terkemuka, seperti IEEE Xplore, SpringerLink, dan Google Scholar. Pencarian difokuskan pada kata kunci yang relevan, seperti *"homomorphic encryption," "privacy-preserving," "medical diagnosis," "logistic regression," "support vector machine," "Internet of Medical Things,"* dan *"edge computing."* Teknik pencarian menggunakan operator *Boolean* seperti AND dan OR untuk memperluas cakupan pencarian sekaligus mempersempit hasil yang lebih spesifik. Selain itu, filter diterapkan pada rentang publikasi lima tahun terakhir agar hanya artikel yang paling relevan dan mutakhir yang dipertimbangkan. Publikasi yang dipilih berasal dari jurnal dan konferensi ternama di bidang kriptografi, kecerdasan buatan, dan aplikasi medis, untuk memastikan kualitas dan relevansi penelitian.

Literatur yang dipilih memiliki keterkaitan erat dengan penggunaan enkripsi homomorfik dalam sistem diagnosis medis berbasis privasi. Beberapa karya ilmiah yang menjadi acuan dalam penelitian ini meliputi berbagai pendekatan inovatif. *PPFLHE: A privacy-preserving federated learning scheme with homomorphic encryption for healthcare data*. Membahas peningkatkan efisiensi privasi, akurasi model, dan mengurangi latensi komunikasi dalam FL [13]. *Integrating homomorphic encryption in IoT healthcare blockchain system*. Menjelaskan pengintegrasian IoT, blockchain, dan enkripsi homomorfik untuk meningkatkan keamanan dan efisiensi dalam sistem kesehatan berbasis IoT [14]. *Homomorphic encryption-based privacy-preserving federated learning in IoT-enabled healthcare system*. Menjelaskan mengenai perlindungan data medis dalam FL dengan mempertimbangkan kualitas data sebagai faktor kontribusi model global [15].

Dengan mengintegrasikan hasil-hasil dari literatur tersebut, penelitian ini berupaya menyusun analisis yang lebih komprehensif tentang potensi dan tantangan penerapan enkripsi homomorfik dalam diagnosis medis berbasis privasi, khususnya dalam konteks Federated Learning dan IoT di sektor kesehatan.

C. *Analisis Literatur*

Analisis literatur dilakukan dengan menggunakan beberapa metode untuk mendapatkan pemahaman yang komprehensif. Pertama, analisis komparatif diterapkan untuk membandingkan algoritma dalam hal efisiensi dan tingkat akurasi saat dienkripsi menggunakan *homomorphic encryption*. Selanjutnya, analisis tematik digunakan untuk mengidentifikasi tema-tema utama dalam literatur, seperti privasi data pasien, efisiensi komputasi dalam proses inferensi, dan penerapan model dalam lingkungan IoMT dan edge computing. Selain itu, keterbatasan dari setiap pendekatan turut dikaji, terutama terkait dengan tingginya kebutuhan komputasi dan kompleksitas enkripsi dalam skala besar.

D. *Data*

Pelaporan data hasil analisis dilakukan dengan menyajikan temuan dalam bentuk tabel dan grafik untuk mempermudah perbandingan. Tabel perbandingan digunakan untuk menggambarkan perbedaan dan persamaan antara berbagai pendekatan enkripsi homomorfik dalam diagnosis medis. Selain itu, jika relevan, grafik atau diagram juga digunakan untuk memvisualisasikan hasil prediksi dan tingkat akurasi dari model yang diteliti. Sintesis temuan difokuskan pada peran penting homomorphic encryption dalam menjaga privasi

selama proses diagnosis dan prediksi medis. Tantangan implementasi, seperti kebutuhan daya komputasi yang tinggi dan kompleksitas teknis, juga dibahas untuk memberikan rekomendasi bagi penelitian di masa mendatang. Kajian ini diharapkan dapat menjadi landasan bagi pengembangan sistem diagnosis medis yang lebih aman dan efisien dengan memanfaatkan teknologi enkripsi homomorfik.

III. HASIL DAN PEMBAHASAN

Hasil studi ini memaparkan beberapa metode yang digunakan oleh beberapa jurnal artikel dalam pengoptimalan penggunaan enkripsi homomorfik untuk keamanan dan privasi data Kesehatan.

A. Mengurangi Overhead Komunikasi serta Penggunaan Enkripsi Berskema Elgamal

Artikel [15] membahas mekanisme Federated Learning (FL) untuk sistem kesehatan berbasis *Internet of Things* (IoT) yang menggunakan enkripsi homomorfik untuk menjaga privasi data medis. FL memungkinkan berbagai institusi medis berkolaborasi dalam membangun model global tanpa berbagi data mentah, yang sangat penting untuk melindungi privasi pasien. Model FL dikembangkan dengan metode backward propagation berbasis Stochastic Gradient Descent (SGD) yang digambarkan dalam fungsi loss $L(DS, w)$ dengan $L2$-norm, seperti pada Persamaan (1)

$$L(DS, w) = \frac{1}{|DS|} \sum_{(x_k, y_k) \in DS} |f(x_k, w) - y_k|^2 \quad (1)$$

Kontribusi utama mencakup pengenalan skema masking menggunakan enkripsi homomorfik yang diadaptasi dari algoritma ElGamal untuk memungkinkan agregasi data dengan keamanan privasi. Penulis mendeskripsikan penyesuaian ElGamal untuk mendukung homomorfisme aditif, sebagaimana ditunjukkan pada modifikasi cipher $Enc(m)$

$$Enc(m_a) \oplus Enc(m_b) = Enc(m_a + m_b) \quad (2)$$

Modifikasi ini memungkinkan penjumlahan aman antar ciphertext. Mekanisme ini digabungkan dengan secret sharing dan pseudo-random generators untuk mendukung toleransi dropout klien dan mengurangi dampak komunikasi berlebih.

Salah satu inovasi artikel ini adalah pengukuran kualitas data lokal berdasarkan gradien lokal dibandingkan gradien global. Dalam setiap iterasi, kualitas data Q_i^t dihitung sebagai:

$$Q_i^t = \frac{d}{|g_i^t - g_{\text{global}}^{t-1}|_2^2} \quad (3)$$

di mana g_i^t adalah gradien lokal klien i, dan g_{global}^{t-1} adalah gradien global dari iterasi sebelumnya. Model global diperoleh melalui rata-rata tertimbang berdasarkan kualitas data:

$$w_{\text{global}}^{t+1} = \frac{\sum_i Q_i^t w_i^t}{\sum_i Q_i^t} \quad (4)$$

Pendekatan ini memastikan kontribusi lebih besar dari klien dengan data berkualitas tinggi.

Artikel ini membahas keamanan skema masking dan enkripsi homomorfik terhadap berbagai serangan. Keamanan mekanisme masking didasarkan pada ketidakmampuan pihak jahat untuk memulihkan data lokal dari model yang telah diacak. Kompleksitas kriptografis dikurangi dengan hanya mengenkripsi metrik kualitas data Q_i^t, sehingga overhead komputasi tetap rendah dibandingkan dengan pendekatan tradisional yang mengenkripsi seluruh parameter model.

Implementasi metode ini dilakukan pada dataset medis HAM10000 untuk klasifikasi lesi kulit. Hasil eksperimen menunjukkan bahwa metode ini memberikan kinerja akurasi yang sebanding dengan pendekatan lain, namun dengan keuntungan tambahan privasi yang lebih baik. Kecepatan konvergensi model juga dipertahankan meskipun terdapat dropout klien, menunjukkan efisiensi tinggi dari pendekatan yang diusulkan.

B. *Integrasi dengan Internet of Things (IOT) dan Blockchain serta Penggunaan Enkripsi Berskema Linier Ultraringan*

Artikel [14] memperkenalkan arsitektur untuk integrasi perangkat IoT, blockchain, dan enkripsi homomorfik yang tertanam, difokuskan pada aplikasi di sektor kesehatan. IoT memungkinkan perangkat untuk berkomunikasi tanpa intervensi manusia, namun tantangan utama meliputi keamanan, privasi, dan integritas data. Penelitian ini menggunakan teknik enkripsi ultraringan yang memungkinkan operasi aritmatika seperti penjumlahan homomorfik pada data terenkripsi, memastikan bahwa privasi data tetap terjaga selama proses komputasi.

Proses enkripsi terdiri atas tiga tahapan utama:

1) *Pembangkit kunci (KeyGen):* Menghasilkan pasangan kunci privat dan publik (Ski, Pki), dengan $Ski = ki$ dan $Pki = ki + \alpha \cdot p$, di mana p dan α adalah bilangan prima besar.

2) *Enkripsi (Enc):* Data dibagi menjadi bagian $m_1, m_2, \ldots, m_i$ dan dienkripsi dengan:

$$c = \left(\sum_{j=1}^{i} m_j \cdot Pk_j \right) \bmod n \quad (5)$$

di mana $n = p \cdot q$, dengan p dan q bilangan prima.

3) *Dekripsi (Dec):* Menggunakan kunci privat Ski, data diekstraksi dengan:

$$m_j = \frac{c}{Ski}, \quad c \leftarrow c - (c \bmod Ski) \quad (6)$$

Arsitektur ini memanfaatkan properti homomorfik aditif, dinyatakan dengan persamaan (2) yang memungkinkan operasi pada data terenkripsi tanpa mendekripsi. Misalnya, dalam kasus agregasi data pasien (seperti kadar glukosa darah), nilai terenkripsi dari beberapa sampel dapat dijumlahkan, dan hasil

akhirnya dapat didekripsi oleh pengguna yang berwenang dengan:

$$s = \sum_{j=1}^{t} record_j \quad (7)$$

$$Dec(s) = \sum_{j=1}^{t} m_j. \quad (8)$$

Hasil uji coba menunjukkan bahwa teknik ini efisien baik dari segi waktu komputasi maupun konsumsi komunikasi. Dengan kunci 256-bit, waktu enkripsi dan dekripsi masing-masing adalah 0,19 ms dan 0,87 ms, lebih cepat dibanding teknik lain. Teknik ini juga mengurangi ukuran komunikasi data hingga 1 KB per record, dibandingkan 5 KB pada metode lain. Skema ini berhasil menggabungkan beberapa bidang data dalam satu nilai, menurunkan beban penyimpanan blockchain.

Aplikasi di sektor kesehatan menunjukkan potensi signifikan, terutama dalam pengelolaan data pasien secara anonim dan terdesentralisasi. Properti blockchain seperti transparansi, stabilitas, dan anonimitas, memastikan rekaman data tidak dapat dimanipulasi. Penelitian ini memberikan fondasi untuk pengembangan lebih lanjut pada sektor lain, seperti pertanian dan sistem IoT lainnya, di mana efisiensi dan privasi menjadi prioritas utama.

C. *Pertimbangan kualitas data dan Penggunaan Enkripsi Berskema Pailier*

Artikel [13] mengusulkan PPFLHE (Privacy-Preserving Federated Learning with Homomorphic Encryption), sebuah kerangka federated learning (FL) yang dirancang untuk meningkatkan privasi data kesehatan dengan enkripsi homomorfik. Masalah utama yang diatasi adalah kebocoran privasi dalam FL, terutama selama pertukaran parameter model dan partisipasi pengguna yang tidak dapat dipercaya. PPFLHE menggunakan skema enkripsi Paillier, serta mekanisme pengakuan (ACK) untuk mengelola pengguna yang tidak responsif, guna meminimalkan latensi komunikasi.

Federated Learning memungkinkan kolaborasi antar klien untuk melatih model global tanpa berbagi data mentah. Proses pelatihan dinyatakan secara matematis sebagai:

$$W_{t+1}^{i} = W_t^i - \eta_t \nabla F_i(W_t, X_t) \quad (9)$$

di mana W_t adalah parameter model, η_t adalah learning rate, dan ∇F_i adalah gradien data klien ke-i. Model ini bertujuan untuk meminimalkan fungsi loss global:

$$\min_{W} \sum_{i=1}^{K} \frac{n_i}{n} F_i(W) \quad (10)$$

dengan n_i adalah jumlah data klien i dan n total data.

Skema enkripsi Paillier mendukung operasi aditif pada ciphertext. Tahapan utamanya adalah:

1) Pembangkit kunci: Kunci terdiri dari kunci publik (n, g), di mana $n = p \cdot q$, dan kunci privat (λ, μ) dengan $\lambda = \text{lcm}(p-1, q-1)$

2) Enkripsi*:*

$$c = (g^m \cdot r^n) \bmod n^2 \quad (11)$$

di mana m adalah *plain* text dan r bilangan acak.

3) Dekripsi*:*

$$m = \frac{L\left(c^{\lambda} \backslash mod n^2\right) \cdot \mu}{n} \bmod n \quad (12)$$

dengan $L(x) = \frac{x-1}{n}$

Hasil uji coba menunjukkan bahwa PPFLHE mempertahankan akurasi klasifikasi tinggi (81,53%) menggunakan model ringan MobileNetV2. Meskipun waktu enkripsi dan dekripsi meningkat dengan panjang kunci, penggunaan kunci 512-bit memberikan keseimbangan antara keamanan dan efisiensi. Selain itu, mekanisme ACK mengurangi latensi komunikasi server hingga 160 detik dengan menyingkirkan klien yang tidak responsif.

PPFLHE meningkatkan privasi dengan mempertahankan utilitas data dalam FL untuk aplikasi kesehatan. Mekanisme ini relevan untuk skenario dengan distribusi data yang tidak merata. Namun, overhead komunikasi dari enkripsi homomorfik menjadi tantangan yang perlu diatasi dalam penelitian lanjutan. Artikel ini menyarankan eksplorasi teknologi blockchain dan konsistensi model untuk meningkatkan solusi di masa depan.

IV. KESIMPULAN

Berdasarkan tinjauan literatur terhadap beberapa artikel yang membahas penerapan enkripsi homomorfik dalam sistem *Federated Learning* (FL) di bidang kesehatan, dapat disimpulkan bahwa meskipun ketiganya bertujuan untuk melindungi privasi data, masing-masing memiliki pendekatan yang berbeda dalam hal teknik dan kompleksitas sistem yang digunakan. Artikel pertama, PPFLHE (*Privacy-Preserving Federated Learning with Homomorphic Encryption*), fokus pada peningkatan efisiensi privasi dan pengurangan latensi komunikasi dalam FL. Dengan menggunakan enkripsi homomorfik Paillier dan mekanisme kontrol akses yang ketat, artikel ini bertujuan untuk mengurangi overhead komunikasi sambil tetap menjaga akurasi model yang tinggi. Artikel kedua, IoT *Healthcare Blockchain*, mengintegrasikan teknologi IoT, blockchain, dan enkripsi homomorfik untuk meningkatkan keamanan dan efisiensi dalam sistem kesehatan berbasis IoT. Artikel ini menggunakan teknik enkripsi linier ultraringan untuk mempercepat komputasi serta mengadopsi kontrol akses granular guna memastikan bahwa hanya data relevan yang dapat diakses oleh pihak tertentu, sambil meminimalkan konsumsi energi dan biaya komunikasi. Sementara itu, artikel ketiga, *Homomorphic Encryption in FL for IoT-Enabled Healthcare*, berfokus pada perlindungan data medis dalam FL dengan mempertimbangkan kualitas data sebagai faktor kontribusi model global. Artikel ini menggunakan variasi enkripsi homomorfik ElGamal dan mengimplementasikan skema toleransi dropout serta resistensi kolusi untuk meningkatkan efisiensi dan keamanan sistem.

Perbedaan utama antara ketiga pendekatan ini terletak pada fokus pengembangan, teknik enkripsi, dan kompleksitas sistem yang digunakan. PPFLHE lebih menekankan pada efisiensi privasi dan pengurangan latensi, *IoT Healthcare Blockchain* mengintegrasikan blockchain untuk meningkatkan keamanan data, sedangkan *Homomorphic Encryption in FL for IoT-Enabled Healthcare* berfokus pada pengelolaan kualitas data dan toleransi terhadap dropout dalam FL. Meskipun ketiganya menggunakan enkripsi homomorfik, teknik yang diterapkan berbeda, dengan PPFLHE dan artikel ketiga menggunakan variasi Paillier/ElGamal, sementara artikel kedua mengusulkan teknik enkripsi linier ultraringan untuk meningkatkan efisiensi komputasi.

Secara keseluruhan, beberapa artikel yang dibahas menunjukkan potensi besar dalam meningkatkan privasi, keamanan, dan efisiensi sistem kesehatan berbasis IoT dan FL. Namun, masing-masing pendekatan memiliki keunggulan tersendiri yang sesuai dengan konteks aplikasi yang berbeda. Oleh karena itu, penelitian lebih lanjut diperlukan untuk mengeksplorasi integrasi dan optimasi teknik-teknik ini dalam sistem kesehatan yang lebih luas, serta untuk mengidentifikasi solusi terbaik dalam mengelola data kesehatan yang sensitif.

REFERENSI

[1] Nidhi, B. S. Rawat, A. Srivastava, and N. Garg, "Health Monitoring Transforming Using IoT: A Review," in *2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT)*, IEEE, Feb. 2024, pp. 17–22.

[2] M. Ali, F. Naeem, M. Tariq, and G. Kaddoum, "Federated Learning for Privacy Preservation in Smart Healthcare Systems: A Comprehensive Survey," *IEEE J Biomed Health Inform*, vol. 27, no. 2, pp. 778–789, 2023.

[3] Vinola. C, G. Premi, P. Solainayagi, C. Srinivasan, and P. G. Kuppusamy, "Data Privacy and Confidentiality in Healthcare Applications of IoT-Enabled Wireless Sensor Networks," in *2023 Second International Conference On Smart Technologies For Smart Nation (SmartTechCon)*, IEEE, 2023, pp. 610–614.

[4] S. K. Lo *et al.*, "Toward Trustworthy AI: Blockchain-Based Architecture Design for Accountability and Fairness of Federated Learning Systems," *IEEE Internet Things J*, vol. 10, no. 4, pp. 3276–3284, 2023.

[5] B. C. Das, M. Hadi Amini, and Y. Wu, "Privacy Risks Analysis and Mitigation in Federated Learning for Medical Images," in *2023 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*, IEEE, 2023, pp. 1870–1873.

[6] J. Park and H. Lim, "Privacy-Preserving Federated Learning Using Homomorphic Encryption," *Applied Sciences*, vol. 12, no. 2, p. 734, 2022.

[7] H. M. Reddy, S. P C, and S. Sankaran, "On the Feasibility of Homomorphic Encryption for Internet of Things," in *2022 IEEE 8th World Forum on Internet of Things (WF-IoT)*, IEEE, 2022, pp. 1–6.

[8] M. Matsumoto and M. Oguchi, "Speeding Up Encryption on IoT Devices Using Homomorphic Encryption," in *2021 IEEE International Conference on Smart Computing (SMARTCOMP)*, IEEE, 2021, pp. 270–275.

[9] M. Qi, Z. Wang, Q.-L. Han, J. Zhang, S. Chen, and Y. Xiang, "Privacy Protection for Blockchain-Based Healthcare IoT Systems: A Survey," *IEEE/CAA Journal of Automatica Sinica*, vol. 11, no. 8, pp. 1757–1776, 2024.

[10] W. F. Shah, "Preserving Privacy and Security: A Comparative Study of Health Data Regulations - GDPR vs. HIPAA," *Int J Res Appl Sci Eng Technol*, vol. 11, no. 8, pp. 2189–2199, 2023.

[11] P. Yao, H. Wang, C. Zheng, J. Yang, and L. Wang, "Efficient Federated Learning Aggregation Protocol Using Approximate Homomorphic Encryption," in *2023 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, IEEE, 2023, pp. 1884–1889.

[12] K. Shivdikar *et al.*, "Accelerating Polynomial Multiplication for Homomorphic Encryption on GPUs," in *2022 IEEE International Symposium on Secure and Private Execution Environment Design (SEED)*, IEEE, Sep. 2022, pp. 61–72.

[13] B. Wang, H. Li, Y. Guo, and J. Wang, "PPFLHE: A privacy-preserving federated learning scheme with homomorphic encryption for healthcare data," *Appl Soft Comput*, vol. 146, p. 110677, 2023.

[14] H. Aissaoua, A. Laouid, M. Kara, A. Bounceur, M. Hammoudeh, and K. Chait, "Integrating Homomorphic Encryption in IoT Healthcare Blockchain Systems," *Ingénierie des systèmes d information*, vol. 29, no. 5, pp. 1667–1677, 2024.

[15] L. Zhang, J. Xu, P. Vijayakumar, P. K. Sharma, and U. Ghosh, "Homomorphic Encryption-Based Privacy-Preserving Federated Learning in IoT-Enabled Healthcare System," *IEEE Trans Netw Sci Eng*, vol. 10, no. 5, pp. 2864–2880, 2023.