Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 10, October - 2025

Secure Data Integration Frameworks for Omni-channel Healthcare Marketing Systems

Chitiz Tayal
Senior Director, Data and AI practise, Axtria Inc
100 5th Avenue Waltham MA -02451, USA

***Abstract* - The rapid digitalisation and increasing interconnection of healthcare marketing ecosystems require secure and interoperable data-integration frameworks. Omnichannel systems, a combination of clinical, behavioural and marketing data, are becoming increasingly important to healthcare organisations as they aim to personalise contact and stay under regulatory requirements. This research is a critical synthesis of twenty-seven peer-reviewed articles (2020-2025) in IEEE, Elsevier, and Springer Nature, as well as the most popular sources in the field of machine learning, privacy-preserving machine learning (PPML) in healthcare marketing. In this review, the qualitative meta-analytic approach is used to study technological architectures, encryption, and federated-learning methods and omni-experience platform designs. The results show that blockchain-based interoperability and AI-based analytics can enhance trust, auditability, and personalization to a considerable extent, whereas federated and split-learn systems reduce privacy risks in distributed marketing data. Hybrid cloud-edge infrastructure-based omnichannel experience platforms increase the real-time decision-making and campaign flexibility, but they encounter governance and integration issues. The paper suggests a theoretical framework of the association of secure data exchange, privacy preservation, and efficiency of omnichannel engagement. The analysis focuses on the scholarship of healthcare informatics as well as strategic marketing by emphasizing the ability of secure integration technologies to maintain compliance (HIPAA / GDPR) and improve the level of patient-centric marketing.**

Keywords - Blockchain-based Healthcare Data Management, Privacy-Preserving Machine Learning, Omnichannel Experience Platform (OEP), Customer Data Integration and Analytics, Federated and Distributed Learning in Healthcare Marketing.

I INTRODUCTION

Healthcare marketing has moved beyond single-channel marketing to sophisticated, data-driven environments, which are built around patient records, wearable sensors, mobile applications, and social platforms. Omnichannel interaction transition aims at providing personalised engagement and preserving sensitive health information confidentiality [1] 5]. Nevertheless, secure integration has become an essential condition of marketing analytics in hospitals, pharmaceutical companies, and tele-health organisations due to the heterogeneity of data sources, as well as the growing number of cyber-threats.

The technologies of blockchain and IoT have been explored in terms of healthcare data governance extensively [1], [2], [4]. At the same time, the literature on the use of the omnichannel marketing emphasises the interoperability of the physical and digital touchpoints to increase the level of loyalty and patient experience [5] - [11]. The overlap between these two areas of research including secure data management and omnichannel marketing is under-researched. New privacy-sensitive artificial intelligence developments provide the methods of analysing distributed data without the necessity of collecting personal data centrally [20]27]. This paper critically summarises evidence on these strands to provide a combined structure of secure data integration in omnichannel healthcare marketing systems.

II. MATERIALS AND METHOD

IEEE Xplore, ScienceDirect, SpringerLink and Scopus databases were used in the form of structured literature

synthesis. Publications that were not published by 2020 or published in other languages were included under inclusion criteria. The resulting corpus consisted of studies on blockchain and AI in the healthcare data [1], [2], [4]; IoT-driven aggregation [3]; omnichannel strategy and analytics [5]-[11], [16]-[19]; machine-learning privacy paradigms [20]-[27]; and research paradigms that apply to the question of data-integration.

Qualitative meta-analysis and thematic coding were used in the review. Methods and datasets, security and privacy mechanisms, integration or analytics models, and reported outcomes were considered in each paper. Triangulation of the data provided consistency in both the technological and managerial results. This methodology is consistent with paradigms of interpretivism and positivism that are utilised in

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 10, October - 2025

the information-systems research to create a balance between the empirical validity and conceptual richness [12]-[15].

III. RESULTS AND DISCUSSION

A. Secure Healthcare Data Management and Integration

The integration of blockchain and the Internet of Things has become a major tool of safe data interoperability. Tanveer et al. (2022) have shown that blockchain smart contracts together with AI-driven access control can increase the transparency and the resilience of electronic-health-records (EHR) exchange [1]. A hybrid Lionised-Remora Optimization-Serpent encryption scheme was suggested by Almalawi et al. (2023) and presents the potential to achieve the latency reduction by a significant margin, without compromising confidentiality over wearable IoT nodes [2]. They were tested on a simulated new coronavirus IoT data and achieved a 30 percent shorter execution time than their archaic cryptographic systems [2].

Ullah et al. (2021) also offered a broad taxonomy of secure healthcare data-aggregation protocols and determined that fog-assisted IoT architectures consume less bandwidth and have shorter latencies than their cloud-only counterparts [3]. Alam et al. (2023) took this one step further by comparing blockchain consensus mechanisms to discover that permissioned Byzantine-fault-tolerant systems like PBFT and PoA have optimal scalability in e-health systems [4]. Collectively, these papers prove that integrating distributed ledger with IoT generates audit trails that are verifiable and reduces risks of single-point-of-failure.

Safe EHR integration in marketing provides ethical personalisation of campaigns. Blockchain frameworks allow controlled sharing of data between providers, pharmacies and insurers to guarantee training of predictive models on shared, anonymised data whilst retaining a comprehensive customer view. These compliance-by-design infrastructure are the direct support of the omnichannel analytics relying on the reliable real-time information streams [1]-[4].

B. Omnichannel Marketing Architecture in Healthcare.

The interactions between healthcare consumers occur via portals, tele-consultation, mobile-based applications, and brick-and-mortar clinics and produce dispersed data streams. The article by Moreira et al. (2023) summarised the findings on omnichannel health-service and stated that governance, technology investment, and staff training are the success factors [5]. Their synthesis leads by PRISMA emphasised the importance of the patient-focused design and continuity in digital and human medium to enhance satisfaction, yet with a sound privacy framework [5].

Borole (2024) reasoned that the omnichannel marketing messages in healthcare should consider factors such as consuming AI-powered personalisation and cross-media storeys to achieve credibility [6]. Selvaraj (2025) developed a contemporary Omnichannel Experience Platform (OEP) of Customer Data Platforms (CDP), Customer Journey Analytics (CJA), and Content Management Systems (CMS) that were synchronised via API-based coordination [7]. The offered architecture delivered a decrease in the complexity of the work and enhanced conformity tracking.

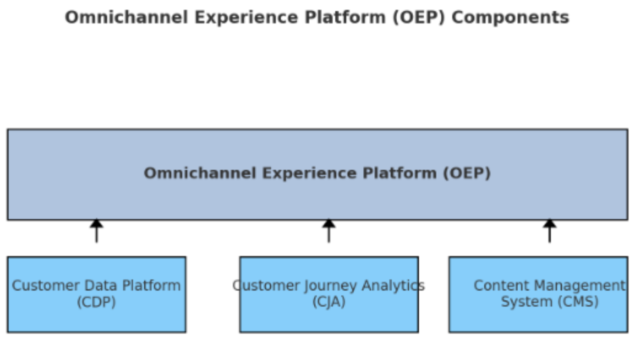

Fig 1: Omnichannel experience platform components

(Source: Selvaraj, 2025)

Pietinen (2025) conducted empirical research to find that pharmaceutical marketers in Finland consider the use of the omnichannel as necessary to engage with clients in a regulatory-compliant way, but they are impeded by fragmented data management [8]. Equally, Wick et al. (2024) established that multichannel pharmacy marketing involving online and in-store advertisements results in increased trust and loyalty within the legal limits [9]. As indicated by Blasiak et al. (2022), the authors proposed the notion of the Omni-channel Engagement (OCE) of digital-health intervention, integrating EHR ports, messaging applications, and wearables to maintain behavioural change [10]. According to Ocak (2023), fragmentation of data, gaps in skills and analytic integration has been the prevailing challenges [11].

Taken together, these findings highlight the point that secure data integration is the cornerstone of omnichannel healthcare marketing. In the absence of privacy-preserving and interoperable architectures, patient-engagement initiatives will face the threat of breaching the standards of data-protection and losing customer trust [5]- [11].

C. Attribution and Analytics Omnichannel Systems.

This is necessary in order to measure the contribution of each channel to optimisation of marketing investment. In a PRISMA systematic review of marketing-attribution methods, Abayomi et al. (2023) found that the archetype has moved towards rule-based models to probabilistic and machine-learning models [16]. The non-linear interdependence of touchpoints was better predicted using Markov-chain and Shapley-value methods. Nevertheless, the significant challenges are attribution bias and the limitations of data-integration.

Cui et al. (2021) also listed informational asymmetries and privacy limitations as obstacles to omnichannel optimisation and suggested traceability using blockchain to harmonise distributed datasets [17]. Kumar et al. (2023) created the framework of Digging DEEP Data-driven, Elastic, Ecosystem-centric, Predictive: the connexion between machine learning and supply-chain resiliency in healthcare marketing [18]. Their mixed-methods research (interviews and K-means clustering)

singled out six building blocks: data governance, adoption of technology, organisational flexibility, system diversification, information sharing, and strategic alignment. These dimensions are directly related to the robustness of the omni channels.

Empirically, Ingrid et al. (2022) showed that AI-based marketing analytics with IT innovations like cloud and edge computing can increase the predictive personalisation and sentiment analysis in online environments [19]. However, they warn that unregulated gain can be nullified by ethical AI regulation and complexity of data-integration. Combined with the above, they show that the future of healthcare marketing analytics will require the integration of privacy-conscious, explainable, and interoperable machine-learning pipelines.

D. Privacy-Preserving and Federated Learning.

The law of medical-marketing data protection across institutions has motivated the wide range of research in PPML. A survey of PPML frameworks by Guerra-Manzare et al. with a conclusion came to federated learning (FL) and homomorphic encryption (HE) being the most promising but computationally intensive approaches [20]. They suggested domain specific privacy models to minimise energy and communication overheads. A decaying Gaussian noise algorithm to compute an adaptive differential-privacy algorithm was proposed by Zhang et al. (2021), demonstrating better accuracy on CheXpert than standard DP-SGD [21]. Fang et al. (2024) suggested the DeCaPH framework that allows collaborating with multi-hospitals and losing less than 3.2 percent of accuracy compared to centralised training [22]. Zerka et al. (2020) conducted a systematic review of federated-learning research studies in the field of oncology and discovered that secure aggregation can reduce the problem of data-sovereignty but the cost of communication is still high [23].

The PGU model by Xu et al. (2021) can be defined as Phase, Guarantee, Utility: the model was created to categorise privacy-saving approaches and emphasised the necessity to weigh technical utility against the power of privacy [24]. Their taxonomy distinguishes between data-publishing, processing, architectural, and hybrid methods, which is an overlay to the further deployment of PPML. Gawali et al. (2021) compared the FL, Split Learning and SplitFed approaches with 8700 X-rays of tuberculosis and found that SplitFedv3 architecture had 93 percent preciseness and 30-40 per cent communication cost reduction [25]. Experimental analysis of DP, HE, and SMPC schemes conducted by Torkzadehmahani et al. (2022) demonstrated that 3-7 percent of accuracy and 200 times slower latency, but confirmed that hybrid HE + DP is a promising trade-off [26]. As Onesimu and Karthikeyan (2020) showed, a hybrid model of RSA-Paillier-AES encryption ensured a 98.3-percent classification accuracy at 15 percentage-training overhead, which proved that the implementation of layered cryptography in medical AI was also feasible [27].

All these works highlight the point that, in order to achieve collaborative analytics between hospitals, pharmaceutical marketers, and digital-health solutions, secure multi-party and federated methods will allow the parties to cooperate without compromising the confidentiality. They also show that the efficiency of integration is related to the trade-off between model utility, cost of computation and privacy assurance.

E. Synthesis of Findings

The synthesis in the Sections III-A - III-D shows three overlapping tendencies:

Technological Convergence. The three technologies: blockchain, IoT, and AI are complementary layers as blockchain offers immutable audit trails, IoT offers real-time data, and AI converts insights into its personalised marketing recommendations [1]-[4], [18]-[19].

Architectural Evolution. The platform of the Omnichannel Experience (OEPs) currently uses modular API-based architecture that incorporates CDPs, CJM application, and analytics engines into hybrid cloud-edge setups [6]-[8]. These architectures support federated learning nodes, which maintain privacy, but support the cross-channel optimisation [20]–[25].

Good Governance and Ethics. Ethical artificial intelligence and privacy (GDPR, HIPAA, CCPA) would mandate clear consent management and explainable algorithms [17], [20], [24]. A secure framework does not only help to avoid legal risk but to increase brand trust a vital intangible asset in healthcare marketing.

Metaphorically, a combination of these trends is created in a tri-layered triad of a so-called Secure Omnichannel Healthcare Framework: (i) Data Infrastructure Layer (blockchain + IoT), (ii) Analytic Layer (AI/ML + PPML), and (iii) Experience Layer (Omnichannel Platform + Governance Controls). The joint functioning of these layers allows compliant, intelligent and adaptive marketing ecosystem.

IV. CONCLUSION

As it has been proven in the review, safe data-integration frameworks are the key to the sustainable development of omnichannel healthcare marketing. The IoT-based blockchain architectures enhance integrity and traceability of medical and behavioural data [1] 1-4; AI-based omnichannel platforms convert these data into actionable insights [6] 610, 1819; machine-learning models based on privacy guarantees that the generated insights do not erode patient confidentiality [20] 27]. All these trends are changing healthcare marketing into a responsive communication into a proactive, ethically controlled, data-driven service.

However, some issues remain: the inability of heterogeneous standards (FHIR, HL7) to interoperate, computational cost of encryption, and lack of competent data-ethics workers. The next generation of research should aim at the benchmarking of hybrid systems of HE-FL in real-time marketing analytics, as well as at establishing cross-industry measures of privacy that align with the PGU triad [24]. Causal relationships between safe data integration and patient trust may also be further supported by longitudinal assessment of omnichannel interventions in these frameworks.

The integration of secure data exchange, privacy protection, and omnichannel experience design can result in compliance and competitive edge of healthcare organisations. The safe data integration framework as given herein offers a road to ethically resilient, technologically resolute and patient-focused marketing ecosystems

ACKNOWLEDGMENT

We would like to thank Causal Productions for permits to use and revise the template provided by Causal Productions. Original version of this template was provided by courtesy of Causal Productions (www.causalproductions.com).

REFERENCES

[1] H. Tanveer, M. Faheem, and A. H. Khan, “Blockchain and AI Integration for Secure Healthcare Data Management,” 2022.

[2] A. Almalawi, A. I. Khan, F. Alsolami, Y. B. Abushark, and A. S. Alfakeeh, “Managing security of healthcare data for a modern healthcare system,” *Sensors*, vol. 23, no. 7, p. 3612, 2023.

[3] A. Ullah, M. Azeem, H. Ashraf, A. A. Alaboudi, M. Humayun, and N. Z. Jhanjhi, “Secure healthcare data aggregation and transmission in IoT—A survey,” *IEEE Access*, vol. 9, pp. 16849–16865, 2021.

[4] S. Alam et al., “An overview of blockchain and IoT integration for secure and reliable health records monitoring,” *Sustainability*, vol. 15, no. 7, p. 5660, 2023.

[5] A. Moreira, C. Alves, J. Machado, and M. F. Santos, “An overview of omnichannel interaction in health care services,” *Mayo Clinic Proceedings: Digital Health*, vol. 1, no. 2, pp. 77–93, 2023.

[6] P. Borole, “A critical review on omni-channel marketing communications in financial, retail, and healthcare services,” 2024.

[7] J. Selvaraj, “Fundamentals of modern omni channel experience platform architecture: Utilization of cutting-edge technologies in developing marketing omnichannel platforms for the healthcare and travel hospitality sectors,” *Int. J. Emerg. Res. Eng. Technol.*, vol. 6, no. 3, pp. 56–66, 2025.

[8] J. K. Pietinen, “Perceptions of marketing specialists on the implementation of omnichannel marketing strategies in the Finnish pharmaceutical industry,” 2025.

[9] A. Wick, B. Koczian, and K. Králiková, “Optimizing retail pharmacy success: The role of multichannel marketing strategies,” *Administrative Sciences*, vol. 14, no. 9, p. 210, 2024.

[10] A. Blasiak et al., “Omnichannel communication to boost patient engagement and behavioral change with digital health interventions,” *J. Med. Internet Res.*, vol. 24, no. 11, p. e41463, 2022.

[11] A. Ocak, “Omnichannel marketing in the digital age: Challenges and solutions,” *New Frontiers in Social, Human and Administrative Sciences*, p. 31, 2023.

[12] H. H. Alharahsheh and A. Pius, “A review of key paradigms: Positivism vs interpretivism,” *Glob. Acad. J. Humanit. Soc. Sci.*, vol. 2, no. 3, pp. 39–43, 2020. [Online]. Available: https://gajrc.com/media/articles/GAJHSS_23_39-43_VMGJbOK.pdf

[13] L. T. M. Pham, “Qualitative approach to research: A review of advantages and disadvantages of three paradigms—Positivism, interpretivism and critical inquiry,” Univ. of Adelaide, 2018. [Online]. Available: https://www.researchgate.net/publication/324486854_A_Review_of_key_paradigms_positivism_interpretivism_and_critical_inquiry

[14] P. Žukauskas, J. Vveinhardt, and R. Andriukaitienė, “Philosophy and paradigm of scientific research,” in *Management Culture and Corporate Social Responsibility*, IntechOpen, pp. 121–138, 2018. [Online]. Available: https://www.intechopen.com/chapters/58890

[15] P. K. Kankam, “The use of paradigms in information research,” *Library & Information Science Research*, vol. 41, no. 2, pp. 85–92, 2019.

[16] A. A. Abayomi et al., “Systematic review of marketing attribution techniques for omnichannel customer acquisition models,” *Int. J. Adv. Multidiscip. Res. Stud.*, vol. 3, no. 6, pp. 1621–1633, 2023.

[17] T. H. Cui et al., “Informational challenges in omnichannel marketing: Remedies and future research,” *J. Marketing*, vol. 85, no. 1, pp. 103–120, 2021.

[18] A. Kumar et al., “Digging DEEP: Futuristic building blocks of omni-channel healthcare supply chains resiliency using machine learning approach,” *J. Bus. Res.*, vol. 162, p. 113903, 2023.

[19] L. Ingrid, N. Rajesh, and F. Lucas, “The synergy between AI-powered marketing analytics and IT innovations for transforming customer experience across digital platforms,” *Int. J. Trend Sci. Res. Dev.*, vol. 6, no. 5, pp. 2216–2225, 2022.

[20] A. Guerra-Manzanares, L. J. L. Lopez, M. Maniatakos, and F. E. Shamout, “Privacy-preserving machine learning for healthcare: Open challenges and future perspectives,” in *Proc. Int. Workshop on Trustworthy Machine Learning for Healthcare*, Cham: Springer Nature Switzerland, pp. 25–40, May 2023.

[21] X. Zhang et al., “Adaptive privacy preserving deep learning algorithms for medical data,” in *Proc. IEEE/CVF Winter Conf. on Applications of Computer Vision*, pp. 1169–1178, 2021.

[22] C. Fang et al., “Decentralised, collaborative, and privacy-preserving machine learning for multi-hospital data,” *EBioMedicine*, vol. 101, 2024.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 10, October - 2025

[23] F. Zerka et al., "Systematic review of privacy-preserving distributed machine learning from federated databases in health care," *JCO Clin. Cancer Inform.*, vol. 4, pp. 184–200, 2020.

[24] R. Xu, N. Baracaldo, and J. Joshi, "Privacy-preserving machine learning: Methods, challenges and directions," *arXiv preprint* arXiv:2108.04417, 2021.

[25] M. Gawali et al., "Comparison of privacy-preserving distributed deep learning methods in healthcare," in *Proc. Annu. Conf. on Medical Image Understanding and Analysis*, Cham: Springer Int. Publishing, pp. 457–471, Jul. 2021.

[26] R. Torkzadehmahani et al., "Privacy-preserving artificial intelligence techniques in biomedicine," *Methods Inf. Med.*, vol. 61, (S 01), pp. e12–e27, 2022.

[27] J. A. Onesimu and J. Karthikeyan, "An efficient privacy-preserving deep learning scheme for medical image analysis," *J. Inf. Technol. Manag.*, vol. 12, Special Issue, pp. 50–67, 2020.