HiLL PUBLISHING

Advances in Computer and Communication, 2026, 7(3), 167-171
https://www.hillpublisher.com/journals/acc/
ISSN Online: 2767-2875

Implementation of Lightweight Secure Transmission and Data Minimization Strategies in Multi-source Advertising Data Environments

Jinxin Li

Department of Electrical & Computer Engineering, University of Illinois Urbana-Champaign, Urbana, IL 61801, USA.

How to cite this paper: Jinxin Li. (2026) Implementation of Lightweight Secure Transmission and Data Minimization Strategies in Multi-source Advertising Data Environments. *Advances in Computer and Communication,* 7(3), 167-171.
DOI: 10.26855/acc.2026.09.011

Received: July 3, 2026
Accepted: August 2, 2026
Published: August 31, 2026

***Corresponding author:** Jinxin Li, Department of Electrical & Computer Engineering, University of Illinois Urbana-Champaign, Urbana, IL 61801, USA.

© 2026 by the author(s).
This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution-NonCommercial-NoDerivatives (CC BY-NC-ND) license, which permits non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited and is not modified or adapted.
https://creativecommons.org/licenses/by-nc-nd/4.0/

Abstract

Multi-source advertising data have great heterogeneity, dynamic operating environments, and inherent privacy risks, which lead to contradictions between the real-time lightweight transmission needs and the strict privacy security restrictions. By integrating lightweight encryption and secure transmission theories, a three-layer hierarchical encrypted transmission framework is established, using a dynamically optimized lightweight block encryption algorithm suitable for advertising scenarios. Strategies such as dynamic key updating, security authentication, and parallel secure transmission scheduling are designed to reduce the computation burden and transmission delay under high-concurrency conditions. According to the principle of data minimization, advertising data screening, redundancy removal, and feature simplification algorithms are proposed. A lightweight differential privacy-oriented desensitization strategy and an adaptive data minimization regulation mechanism are also developed. These approaches achieve a balance between transmission efficiency, computational lightness, and privacy protection reliability, guaranteeing stable data utility while limiting the risk of privacy leakage for multi-source advertising data in complex open network environments.

Keywords

Multi-source advertising data; lightweight secure transmission; data minimization; differential privacy

With the quick increase in the digital advertising business, advertising data from different delivery systems and user terminals has become increasingly abundant. This data has heterogeneity in structure, changing network conditions, and important user privacy characteristics, so traditional single-source data security transmission methods are not suitable. Real-time and frequent transmission needs to have low delay and small overhead, while the browsing, clicking, and conversion records in the data must satisfy strict privacy protection requirements. Conventional complex encryption algorithms consume much computation, and static data reduction rules cannot meet varying business situations. The existing security measures can not well balance transmission efficiency, light performance, and privacy compliance. Therefore, it is necessary to research targeted lightweight secure transmission and data reduction strategies to meet the secure, efficient, and low-latency transmission demands of multi-source heterogeneous advertising data.

1. Characteristics and Environmental Properties of Multi-source Advertising Data

Advertising data produced by various advertising distribution systems and user contact devices have special attribute features and complicated operational rules that are different from the traditional single-source network data. The data itself shows obvious heterogeneity in its structural form, information granularity, and sensitive attributes since

different advertising channels generate structured delivery parameters, semi-structured user operation logs, and unstructured interaction feedback during the business processes. The operating environment of the advertising data includes dynamic network changes and high-speed data access, which leads to unstable transmission bandwidth and varying data generation rates in real-time advertising services. Moreover, the data contains inherent privacy-related attributes such as user browsing habits, click traces, and conversion histories, which can indicate personal consumption preferences and user profiles. These inherent data characteristics and the operational environment give rise to a contradiction between the need for efficient real-time transmission and lightweight computing and the strict requirements for privacy and security, which forms the main background for implementing lightweight secure transmission and data reduction methods in advertising situations [1].

2. Basic Theory of Lightweight Encryption and Secure Transmission

Lightweight encryption and secure transmission theories aim at designing security protection systems with less computational and energy consumption for resource-limited network services, differing from the complicated encryption and transmission structures of the traditional methods [2]. The main theory of lightweight encryption mainly concentrates on eliminating redundant cryptographic operations while maintaining effective confusion and diffusion properties to decrease the requirement of computing resources in the encryption and decryption procedures. Secure transmission theories formulate the entire process of data interaction protection in the open network environment by controlling the data encryption, transmission, verification, and anti-interference rules. The integration of these two theories can coordinate the security and real-time transmission efficiency of multi-source advertisement data, which overcomes the adaptability issue of complex encryption algorithms in frequent advertisement data transmission conditions [3]. These fundamental theories give an essential theoretical basis for the construction of hierarchical encryption structures and lightweight optimization algorithms in our study and establish a solid theoretical groundwork for achieving low-latency and high-security transmission of diversified advertisement data streams.

3. Design of Lightweight Secure Transmission Strategy for Multi-source Advertising Data

3.1 Lightweight Hierarchical Encrypted Transmission Architecture Design

The complex heterogeneous features of multi-source advertising data from various publishing platforms and user terminal environments result in serious conflicts between transmission security and lightweight transmission efficiency in the present unified encryption methods. This framework divides the transmission into a three-level hierarchical system according to the sensitivity and transmission priority of the advertising data, which includes security preprocessing at the data perception layer, encryption protection in the intermediate transmission layer, and security verification at the terminal receiving layer [4]. Thus, the conventional advertising flow data can be transmitted quickly with simple encryption restrictions, while the sensitive user behavior data receives comprehensive security protection by using more secure encryption techniques. The entire architecture avoids the redundant security components in the usual integrated encryption schemes and simplifies the data interaction between different layers to greatly decrease the computational load and the time consumption in the data transmission process.

3.2 Improvement of Lightweight Encryption Algorithm Adapted to Advertising Scenarios

Most common lightweight encryption algorithms keep the number of encryption rounds and the key iteration rules unchanged, which cannot meet the changing and fluctuating characteristics of data volume and real-time transmission demands in the multi-source advertising business environment. In this research, we modify the traditional lightweight block encryption algorithm by changing the cyclic encryption rounds according to the attribute characteristics of the advertising data, such as its data size sensitivity level and transmission delay limit [5]. The modified algorithm eliminates the unnecessary repetitive operations for the low-sensitivity advertising data streams and keeps the essential encryption and confusion-diffusion procedures to ensure the basic security features while decreasing the computing workload of the devices. For the sensitive advertising user profile data and conversion behavior data, the algorithm increases some key mixing operations to compensate for the security deficiencies due to the simplification of the algorithm. The optimized algorithm can maintain consistent encryption efficiency even when a large amount of concurrent transmission occurs in the multi-source advertising data, and it achieves an appropriate balance between encryption security and transmission lightness.

3.3 Design of Dynamic Key Update and Security Authentication Mechanism

In the traditional advertising data transmission system, static keys and a single authentication method are easily

attacked by replay and key leakage in open networks. A dynamic key updating scheme has been designed, that includes two types of update rules, time-based and data flow volume-based, to periodically and reactively replace the transmission keys for multiple sources of advertising data [6]. This scheme introduces a key division verification approach to achieve the simultaneous update and matching verification of the keys between the sending terminals and receiving terminals without interrupting the normal advertising data transmission. The matching bidirectional identification authentication method integrates the verification of terminal's characteristics and the credibility of the data source to detect illegal access requests and abnormal data modification behaviors in the transmission channel. The entire scheme can eliminate the security defects caused by the long-term use of fixed keys and decrease the authentication delay of the complicated identity verification methods in order to meet the high-speed and low-delay requirements of the advertising business.

3.4 Parallel Secure Transmission Scheduling Strategy for Multi-source Data

Advertising data collected from various sources on different platforms have heterogeneous transmission features, such as varying data arrival rates and different priorities for business, which may lead to network congestion and resource wasting under the current method of unified serial transmission scheduling [7]. The proposed parallel secure transmission scheduling scheme sorts the multi-source advertising data streams based on their business priority and real-time transmission urgency, and assigns different network bandwidth and computing resources to each data stream. It constructs a dynamic queue adjustment model to modify the transmission order of encrypted data packets in real time according to changes in network load, so that the high-priority advertising data can obtain optimal transmission resources, while the low-priority log data can be transmitted in parallel in the background. This scheduling mechanism also includes conflict detection and coordination rules for the parallel data transmission to prevent loss and encryption failures caused by the competition for resources. The strategy effectively enhances the total transmission rate of multi-source advertising data and guarantees the stability and security of the parallel transmission in high-concurrency situations.

4. Implementation of Advertising Data Preprocessing and Desensitization Strategy Based on Data Minimization

4.1 Classification and Screening Mechanism of Advertising Data

Mixed content with different sensitivities and business values obtained from various sources and media channels leads to difficulty in implementing precise data minimization and targeted privacy protection. A systematic classification method is established based on the application environment, user privacy characteristics, and the transmission requirements of the advertising data [8]. The collected advertising data is categorized into public advertisement display data, general behavior interaction data, and sensitive user profile data by using multidimensional feature matching and rule screening. The designed hierarchical screening model specifies different identification standards and classification rules for various data types to accomplish the automatic classification and tagging of heterogeneous advertising data in complex multi-source situations. The classified data provides different processing restrictions for the later elimination of redundancy and privacy de-sensitization processes, so that the whole data minimization procedure can be conducted with targeted processing instead of general simplification and can well balance the usefulness of advertising business data and the privacy protection compliance.

4.2 Implementation of Redundant Data Elimination and Feature Simplification Algorithm

Massive advertising data from multiple sources collect a lot of duplicated samples, invalid noise data, and redundant feature dimensions during the cross-platform collection and integration, which causes extra transmission burden and potential privacy leakage problems. The proposed redundant elimination algorithm first finds the repeated data samples by using feature similarity matching and deletes the invalid interfering data, which does not affect the advertisement delivery and user behavior analysis. A feature dimension screening model is established to assess the correlation between different data features and the advertising business processes in order to keep the essential feature information that is closely related to advertising conversion prediction and user matching, while eliminating unrelated redundant dimensions. This algorithm optimizes the feature extraction procedure of the conventional advertising data processing methods and decreases the total data scale under the condition of maintaining the useful business information completely. The simplified data structure can greatly reduce the computational load of the following de-sensitization processing and enhance the overall efficiency of the data reduction strategies.

4.3 Lightweight Data Desensitization Strategy Adapted to Differential Privacy

Traditional methods of differential privacy declassification add too much noise to ensure privacy security, which leads to the loss of useful information in advertising data and cannot satisfy the lightweight processing requirement of real-time advertising transmission situations. This lightweight declassification approach improves the noise injection mechanism of traditional differential privacy algorithms by adjusting the noise intensity according to the sensitivity level of classified advertising data. A low level of noise disturbance is used for the general advertising behavior data to maintain high data availability while proper enhanced noise protection is carried out for sensitive users' private information. The strategy eliminates the complicated iterative calculation steps in the traditional declassification procedures and accomplishes fast privacy protection processing for large-scale multi-source advertising data streams. The improved differential privacy framework strictly regulates the privacy leakage risk during the advertising data transmission and application process and maintains stable data usefulness to support normal advertising push and user behavior analysis tasks, thus achieving a win-win situation of lightweight processing and reliable privacy protection.

4.4 Adaptive Regulation Mechanism of Data Minimization

The fixed data processing rules used in traditional data minimization methods are not suitable for coping with the rapid variations of multi-source advertising data volume, network transmission conditions, and business privacy protection requirements in real time, which results in either too much or too little data processing, affecting business operations or leading to possible privacy risks. The designed adaptive regulation mechanism considers the real-time data scale and network load as well as the privacy security level as the comprehensive evaluation criteria to establish a dynamic decision-making model for data minimization processing. This mechanism can automatically adjust the degree of data redundancy removal, feature simplification, and privacy de-sensitization according to the variation of the external environment and business needs. When the network environment is complicated and the privacy risks increase, a higher standard of data minimization processing is activated, while under stable business conditions, less strict rules are applied to keep more useful data information. This mechanism overcomes the shortcomings of the static data minimization schemes and achieves the adaptive matching between the data processing intensity and the actual advertising business situations.

5. Conclusion

Due to the conflict between security and efficiency in the transmission of multi-source advertising data, our research combines light-weight encryption techniques with data minimization methods to establish an entire security processing system including the transmission structure, algorithm improvement, scheduling control, and privacy desensitization. The hierarchical transmission scheme and the enhanced lightweight encryption algorithm can decrease the network delay and computing burden, while the dynamic authentication and parallel scheduling improve the transmission stability in high-concurrency situations. The classification and elimination of data redundancy and the adaptive differential privacy de-sensitization ensure precise protection of privacy without losing the essential business information. The adaptive regulation mechanism solves the problem of fixed processing rules. These approaches provide practical technical routes for the secure transmission and privacy management of multi-source advertising data, and give suggestions for lightweight security study in other real-time big-data service fields.

References

[1] Zhang L, Yin X, Zong G. Disturbance observer-based SMC for nonlinear cyber-physical systems with FDI attacks and multi-source disturbances. Trans Inst Meas Control. 2026;48(9):1921-1931. doi:10.1177/01423312251335398

[2] Liu X, Deng W, Liu L, et al. Sea ice concentration estimation via physical information-guided multi-source data fusion and spatial continuity preservation. Int J Appl Earth Obs Geoinf. 2026;150:105339. doi:10.1016/J.JAG.2026.105339

[3] Han X, Zhang X, Zhang D. A novel multi-source attention-enhanced transformer U-net for sea surface salinity retrieval based on remote sensing data in the Northwest Pacific. Int J Appl Earth Obs Geoinf. 2026;150:105341. doi:10.1016/J.JAG.2026.105341

[4] Zhao Z, Kuang X, Zhou Y, et al. The impact of urban mixed land use on urban vitality with multi-source big data: a case study of Nanjing, China. Sustain Cities Soc. 2026;145:107494. doi:10.1016/J.SCS.2026.107494

[5] Lee J, Park SY, Wadhwa A, Packman AI, Nesbitt SW, Sharma A, et al. Comparing multi-source urban flood indicators: satellite, simulation, and citizen-reported data. Environ Res Water. 2025;1(3):035007.

[6] Meng H, Xinchi L, Wei T, et al. Multisource data integration for targeted bus exterior advertising. Front Environ Sci. 2022;10:962410. doi:10.3389/FENVS.2022.962410

[7] Wu J, Wang H, Shang J. Multi-sourcing and information sharing under competition and supply uncertainty. Eur J Oper Res. 2019;278(2):658-671. doi:10.1016/j.ejor.2019.04.039

[8] Greidanus H, Alvarez M, Eriksen T, et al. Basin-wide maritime awareness from multi-source ship reporting data. TransNav Int J Mar Navig Saf Sea Transp. 2013;7(2):185-192. doi:10.12716/1001.07.02.04