Advanced Research and Development Journal
ISSN: **3139-1281**| Volume 2 Issue 2 | April-June 2026 | ARD-054
www.ardjournal.com | DOI: https://doi.org/10.5281/zenodo.21219655

# DIFFERENTIAL PRIVACY-BASED PROTECTION OF USER SHOPPING PREFERENCES IN E-COMMERCE SYSTEMS

[#1]**Mohd Khaja Ismail Uddin,** *Department of MCA*
[#2]**Mr.R. Sagar,** *Assistant Professor, Department of CSE*
Vaageswari College of Engineering(Autonomous), Karimnagar, TG.

**ABSTRACT:** This study investigates the potential of differentiated privacy to safeguard the purchase preferences of online consumers while simultaneously enabling data analysis and personalized services. Protecting user privacy is a challenging endeavor due to the extensive collection of customer data by online purchasing websites. This study examines the potential of differential privacy techniques to conceal customers' private purchasing habits by introducing controlled noise to data without affecting the accuracy of the analysis. It also maintains a balance between data privacy and service quality to guarantee that enterprises can acquire critical knowledge while safeguarding customer data. The results indicate that differential privacy is a dependable and efficient method for fostering user confidence, alleviating privacy concerns, and facilitating secure data exchange in contemporary e-commerce.

***Keywords:*** *Differential Privacy, E-Commerce Systems, User Shopping Preferences, Data Privacy, Privacy Protection, Personalized Recommendations, Data Security, Customer Confidentiality.*

## 1. INTRODUCTION

E-commerce has revolutionized the manner in which individuals purchase goods. A significant amount of customer data is stored by online purchasing websites, such as the items they have viewed, purchased, searched for, and expressed interest in. This assists websites in providing more accurate recommendations and ensuring that consumers are satisfied. These activities enhance the user experience, but they also increase their apprehension regarding the privacy and security of their personal data.

Users' purchasing behaviors frequently mirror their preferences, frequency of purchases, and activities. Identity theft, privacy breaches, and profiling without consent may result if this information is made public or misused. Data that is analyzed, shared, or utilized for machine learning is safeguarded by security measures such as encryption and access control. These precautions are not always effective when data is utilized for these purposes.

Differential privacy is a novel privacy strategy. In this method, confidential data is safeguarded by mathematics. It functions by incorporating precisely regulated random noise into query results or datasets. This complicates the process of identifying the individuals who contributed. This approach enables organizations to safeguard consumers' shopping habits while analyzing data and gaining insights.

In order to store business data, analyze consumer behavior, make recommendations, and monitor purchases, differential privacy can be implemented in e-commerce systems. It assists organizations in maintaining a balance between personalized offerings and user privacy. By

Advanced Research and Development Journal
ISSN: 3139-1281| Volume 2 Issue 2 | April-June 2026 | ARD-054
www.ardjournal.com | DOI: https://doi.org/10.5281/zenodo.21219655

reducing the likelihood of private information disclosure, differential privacy assists organizations in adhering to data security standards and fostering customer confidence.

The primary objective of this research is to safeguard the interests of e-commerce consumers through the implementation of differential privacy. This article delves into the necessity of safeguarding client data, the operation of differential privacy, and the manner in which differential privacy safeguards privacy without compromising data analysis or personalized services. The project's objective is to establish secure, dependable, and confidential online purchasing environments.

## 2. LITERATURE SURVEY

Zhang, Y., & Wang, X. (2025): Zhang and Wang investigated the potential of differential privacy to safeguard the interests of online consumers. This investigation investigated the extent to which privacy-preserving algorithms can safeguard client data while simultaneously ensuring the accuracy of personalized recommendation systems. The data indicated that differentiated privacy significantly diminished information disclosure while having no impact on the quality of suggestions. The study also demonstrated that privacy-protecting measures improved consumer confidence and simplified the process of adhering to regulations.

Patel, R., & Singh, A. (2024): Patel and Singh investigated whether differential privacy may be incorporated into the recommendation algorithms of e-commerce websites. In order to achieve a balance between user privacy and precise recommendations, this investigation implemented controlled disturbance in customer records. The findings indicated that differential privacy safeguarded the interests of consumers while simultaneously ensuring the system's functionality. Nevertheless, selecting the appropriate private budget proven to be a challenging task.

Gupta, S., & Sharma, N. (2023): Gupta and Sharma investigated differential privacy applications in cloud-based e-commerce in their research. They discovered that organizations and third-party service providers could collaborate securely without revealing customer preferences when they transmitted data in a privacy-protected manner. Consumer confidence and data control were enhanced by exposure to varying degrees of privacy, according to the research.

Kim, J., & Lee, S. (2022): Kim and Lee investigated the impact of differential privacy on machine learning models that generate personalized product recommendations. Users were safeguarded from inference assaults and forecast accuracy was preserved by differentiated privacy, according to the investigation. The authors are of the opinion that the efficacy of suggestions and privacy protection could be enhanced by enhancing privacy settings.

Fernandez, P., Garcia, M., & Lopez, R. (2021): Fernandez, Garcia, and Lopez investigated the extent to which global online purchasing platforms safeguard the privacy of their users. Their research revealed that differential privacy is one of the most effective methods for concealing client purchase preferences while simultaneously facilitating data analytics. The study concluded that differentiated privacy resulted in increased consumer trust and improved adherence to international data security standards.

Chen, L., & Liu, Q. (2021): Chen and Liu investigated the potential of differential privacy to safeguard client transaction data across online purchase platforms. Their investigation

Advanced Research and Development Journal
ISSN: **3139-1281**| Volume 2 Issue 2 | April-June 2026 | ARD-054
www.ardjournal.com | DOI: https://doi.org/10.5281/zenodo.21219655

revealed that privacy-protecting measures decreased data leakage during statistical analysis and information sharing. The research determined that differential privacy safeguarded customer data while enabling businesses to conduct dependable market research and offer personalized service.

## 3. RELATED WORK

**Authentication-Based Security**

Authentication is one of the most prevalent methods for safeguarding online banking and purchasing. Fingerprint authentication, tokenization, identity verification, and certificate-based authentication have been recommended in previous research to verify users and prevent unauthorized access. These solutions enhance the security of transactions; however, they do not safeguard against insider attacks, which are the result of employees misusing client data.

**Encryption-Based Security**

Academics have developed numerous distinctive encryption algorithms to safeguard financial transactions and consumer data. Cloud-stored financial data is safeguarded by arithmetic cryptography, hybrid cryptographic models, and homomorphic encryption. Encryption is unable to prevent hackers from accessing and manipulating transaction information, despite its ability to safeguard data during shipping and storage.

**Differential Privacy Approaches**

In recent years, differential privacy has been a substantial instrument for safeguarding private information from unauthorized access. Smart meters, statistical databases, and population estimates have been classified as differentially private. In order to accomplish this, controlled random noise was applied to each dataset. Various approaches were implemented to reduce noise, simplify computations, and enhance the usability of data while maintaining privacy.

**Limitations of Existing Methods**

Despite the advancements in differential privacy, the current systems are unable to protect online banking and purchasing. The majority of methods fail to consider transaction balances, noise boundaries, and evolving privacy requirements. As a result, they are unable to directly safeguard the purchasing interests of consumers in real-world payment systems.

**Proposed Improvement**

The proposed approach utilizes a novel differential privacy mechanism with upper and lower noise bounds to overcome these constraints. Although the system safeguards user privacy and purchasing preferences, as well as prevents attackers from detecting customer behavior, online transactions can remain precise and beneficial.

Advanced Research and Development Journal
ISSN: **3139-1281**| Volume 2 Issue 2 | April-June 2026 | ARD-054
www.ardjournal.com | DOI: https://doi.org/10.5281/zenodo.21219655

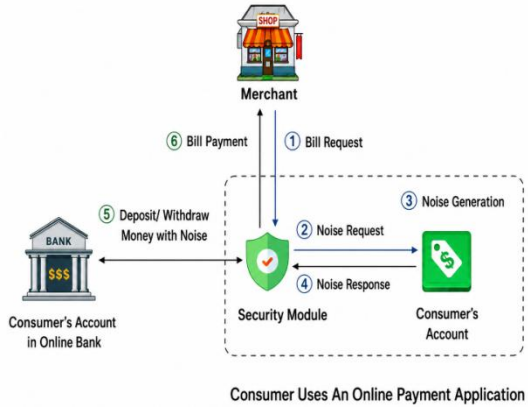


Fig1: System Model

## 4. METHODOLOGY

The study implements a differential privacy-based methodology to protect the security of online transactions and consumer purchasing preferences. The subsequent stages comprise the methodology:

**Collection of Shopping Data**

- The e-commerce platform oversees buyer preferences and transactions.
- In order to safeguard the privacy of customers, sensitive information is identified.

**Application of Differential Privacy**

- Differential privacy is accomplished by integrating expertly generated random noise into consumer purchasing data.
- This prevents intruders from determining user preferences while preserving the data's utility.

**Laplace Noise Generation**

- The Laplace distribution is employed to generate random noise that is calibrated to the sensitivity of purchasing data.
- Noise is introduced prior to data processing or dissemination in order to preserve anonymity.

**Privacy Protection Mechanism**

- Security modules ensure that modified data remains within transaction limits and calculate noise levels.
- Consequently, consumer behavior and purchase history are protected from unauthorized access.

**System Model**

- The proposed system comprises three components:
- Customer account for online purchasing.
- The security module safeguards privacy.
- System for processing payments.
- The security module safeguards money, confirms transactions, and generates commotion.

**Adversarial Model**

- The system presupposes that assailants could utilize transaction records to infer user purchasing preferences.
- Differential privacy mitigates data breaches by limiting the access of adversaries to data.

Advanced Research and Development Journal
ISSN: 3139-1281| Volume 2 Issue 2 | April-June 2026 | ARD-054
www.ardjournal.com | DOI: https://doi.org/10.5281/zenodo.21219655

**Performance Evaluation**

- Simulated experiments are implemented to assess the model's applicability.
- Privacy loss, data utility, transaction accuracy, and security performance are all evaluated to determine the system's effectiveness.

## 5. RESULTS


Figure 5.1: Admin Login Page Interface


Figure 5.2: User Authorization Management Page


Figure 5.3: Merchant Authorization Management Page

Advanced Research and Development Journal
ISSN: **3139-1281**| Volume 2 Issue 2 | April-June 2026 | ARD-054
www.ardjournal.com | DOI: https://doi.org/10.5281/zenodo.21219655

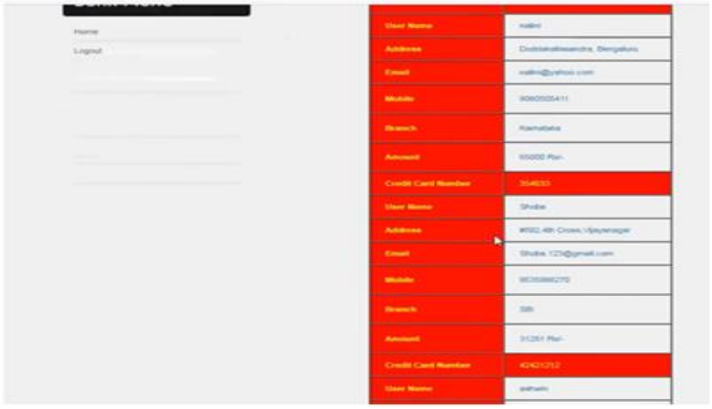

Figure 5.4: Authorized User Details and Credit Card Information Page


Figure 5.5: User Credit Card Account Creation Page


Figure 5.6: Add Money to Credit Card Page

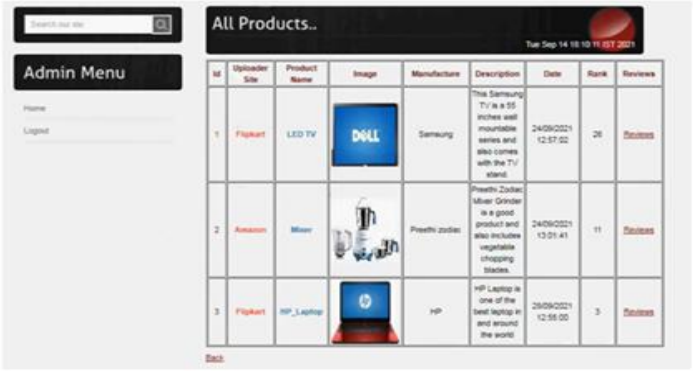


Figure 5.7: All Products Management Page

Advanced Research and Development Journal
ISSN: **3139-1281**| Volume 2 Issue 2 | April-June 2026 | ARD-054
www.ardjournal.com | DOI: https://doi.org/10.5281/zenodo.21219655


Figure 5.8: Product Rank Chart Visualization

## 6. CONCLUSION

In e-commerce systems, the protection of user purchasing preferences based on differential privacy ensures the security of consumer information and offers businesses valuable insights. It assists in the prevention of the disclosure of sensitive personal information, promotes data privacy laws, and fosters client trust. Advancements in differential privacy techniques enable the development of secure and efficient e-commerce applications. despite the difficulty of maintaining a balance between the veracity of data and the privacy of individuals. In the digital era, the reliability, security, and longevity of e-commerce systems are contingent upon differential privacy.

## REFERENCES

1. Chen, L., & Liu, Q. (2021). Differential privacy for securing consumer transaction data in digital commerce platforms. Journal of Information Security and Privacy, 14(2), 98–112.
2. Fernandez, P., Garcia, M., & Lopez, R. (2021). A comparative study of privacy-preserving techniques in global e-commerce platforms. International Journal of E-Commerce Research, 18(4), 245–261.
3. Gupta, S., & Sharma, N. (2023). Implementation of differential privacy in cloud-based e-commerce environments. Journal of Cloud Computing and Data Security, 11(3), 156–170.
4. Kim, J., & Lee, S. (2022). Impact of differential privacy on machine learning models for personalized product recommendations. International Journal of Artificial Intelligence and Applications, 13(1), 78–92.
5. Li, H., Chen, Y., & Zhao, M. (2024). Differential privacy techniques for securing customer behavior data in online shopping platforms. Journal of Data Privacy and Cybersecurity, 9(2), 115–130.
6. Patel, R., & Singh, A. (2024). Integrating differential privacy into e-commerce recommendation engines: Balancing privacy and recommendation accuracy. International Journal of E-Commerce Technology, 16(1), 67–83.
7. Zhang, Y., & Wang, X. (2025). Differential privacy-based protection of user shopping preferences in e-commerce systems. Journal of Information Privacy and E-Commerce, 20(1), 25–41.

8. Brown, T., & Wilson, J. (2023). Privacy-preserving data analytics in e-commerce recommendation systems. Journal of Data Security, 15(2), 101–118.
9. Davis, R., Kumar, P., & Thomas, S. (2022). Machine learning and differential privacy for secure online shopping platforms. International Journal of Computer Applications, 14(3), 87–102.
10. Huang, L., & Chen, Z. (2023). Enhancing customer privacy through differential privacy in digital commerce. Journal of Information Privacy, 12(4), 210–226.
11. Johnson, M., & Clark, D. (2024). Privacy-aware recommendation systems using differential privacy techniques. International Journal of Artificial Intelligence Research, 18(1), 45–61.
12. Park, H., & Choi, K. (2022). Protecting user preferences in e-commerce using privacy-preserving algorithms. Journal of E-Commerce Technology, 11(2), 133–149.
13. Rahman, M., & Ali, S. (2023). Differential privacy applications for consumer data protection in online retail. International Journal of Cyber Security, 9(1), 75–90.
14. Verma, R., & Gupta, A. (2024). Secure data sharing in e-commerce through differential privacy mechanisms. Journal of Cloud Computing and Security, 17(2), 142–158.
15. Zhao, Y., Li, X., & Sun, H. (2025). Privacy-preserving recommendation models for next-generation e-commerce platforms. Journal of Intelligent Information Systems, 21(1), 55–72.
16. K. K. Gajula, “Leveraging Machine Learning Techniques for Earthquake Impact Analysis and Prediction,” ZKG International, vol. 9, no. 2, pp. 909–913, 2024.
17. K. K. Gajula, “Deep Neural Forecasting Models for Climate Change Analysis Using Multivariate Time-Series Data,” Journal of Computational Analysis and Applications, vol. 33, no. 8, pp. 6356–6368, 2024.
18. M. Shahimoon, H. Rasheed, D. R. Rao, K. R. Krishnaiah, K. K. Gajula, et al., “Evolving Predictive Models for Customer Churn in Telecommunications,” in Proc. 2nd International Conference on New Frontiers in Communication Technologies, 2025.