RESEARCH PAPER

Secure Recommendation System Based on Federated Graph Neural Networks for Distributed E-Commerce Platforms

Dr M. V Rajesh[1], K Venkateswara Rao[2], D Srilatha[3], Sridevi Sakhamuri[4], Venkata Subbaiah Desanamukula[5], Asha Priyadarshini[6], Dr Subba Rao Polamuri[7]

[1] Associate Professor, Department of Information Technology, Aditya University, Surampalem, Andhra Pradesh, India - 533437. Email: rajesh.masina@adityauniversity.in

[2] Professor, Department of CSE, Vignan's Lara Institute of Technology & Science, Vadlamudi, Guntur(dt), AP, India. Email: venkat545@gmail.com

[3] Professor, Department of EEE, Vasi Reddy Venkatadri Institute of Technology, Namburu - 522508, Guntur(dt), AP, India. Email: srilatha.dande@gmail.com

[4] Assistant Professor, Department of IoT, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India - 522302. Email: srisat1617@gmail.com

[5] Professor, Department of Computer Science and Engineering, Lakireddy Bali Reddy College of Engineering, Mylavaram, NTR Dist, Andhra Pradesh, India. Email: desanamukula@gmail.com

[6] Assistant Professor, Department of CSE, Vignan's Lara Institute of Technology & Science, Vadlamudi, India. Email: ashapriyadarshini16@gmail.com

[7] Associate Professor, Department of Computer Science and Engineering, Aditya University, Surampalem, Andhra Pradesh, India - 533437. Email: psr.subbu546@gmail.com

Received: 2nd Mar, 2026 | **Revised:** 14th Mar, 2026 | **Accepted:** 4th Apr, 2026 | **Available Online:** 20th Apr, 2026

ABSTRACT

Big data is created by large-scale e-commerce platform marketplaces that include sensitive user interaction data. This raises important questions about privacy protection, following the rules, and how well learning works. Digital markets with many vendors and in many regions Switch to a centralised recommendation architecture This method makes it more likely that data will be revealed, and it doesn't work well in digital marketplaces with multiple vendors across multiple regions. This study suggests an intelligent recommendation system that respects users' privacy and lets the distributed e-commerce nodes learn together without making each user's raw data public. It can store information locally and help people share knowledge by sending encrypted parameters and doing structured relational learning over a group of interconnected businesses. Relational graph representations show how users and sellers, users and categories, and users and products interact with each other in complex ways. This helps us understand more about how people behave and lets us personalise things better. Experimental analysis shows that recommendations are very useful, privacy is better, and learning in distributed settings works very well. The results create a safe, scalable foundation for the next generation of smart recommendation systems in digital commerce systems that deal with sensitive information.

Keywords: Privacy Preservation, Distributed Commerce, Personalized Recommendations, Secure Intelligence, Data Sovereignty, Digital Trust, Relational Learning.

How to cite this article: Rajesh MV, Rao KV, Srilatha D, Sakhamuri S, Desanamukula VS, Priyadarshini A, Polamuri SR. Secure Recommendation System Based on Federated Graph Neural Networks for Distributed E-Commerce Platforms. Int J Drug Deliv Technol. 2026;16(31s):1154-1162. DOI: 10.25258/ijddt.16.31s.127

Source of support: Nil.

Conflict of interest: The authors declare no conflict of interest.

I. INTRODUCTION

Digital commerce is changing the way people interact with products, services, and brands, which is having a big impact on the world's economy. Modern e-commerce doesn't just look like simple online stores anymore. Instead, it has become a complex web of users, merchants, logistics, payment systems, and service systems that cross geographical and institutional boundaries. These platforms generate vast quantities of diverse interaction data, including browsing history, click streams, transaction history, reviews, ratings, and social feedback. Smart recommendation systems use this information to try to make each user's experience unique, increase customer

satisfaction, and get the most profit for the business. Still, as the amount of data grows and the platform gets more complicated, the old ways of processing and learning data in a central location are no longer good enough, both technically and morally. To train and make predictions in centralised recommendation systems, raw user data must be gathered on a single server. The given paradigm enables extensive data analytics but presents significant privacy risks and legal challenges. On both the user and the regulatory sides, data leaks, intrusions, misuse of personal data, and surveillance are very important issues. Centralised architectures are operationally weak and legally vulnerable to changes in the data protection regulations and digital privacy policies, which restrict the process and storage of data and the cross-border transfer of data. Centralised systems also have regulatory risks and single points of failure, which make them easy targets for cyberattacks, service outages, and huge data leaks. These flaws make it even more important to have decentralised intelligence systems that can learn together without compromising user privacy or data sovereignty.

At the same time, modern e-commerce environments are inherently decentralised. Many regions, vendors, new subsidiaries, and service providers run large platforms. Each one has its own data infrastructure and can run its own business. User interactions are inherently fragmented across devices, platforms, and services in a decentralised manner that undermines the centralised assumptions prevalent in learning. It is hard to combine these broken-up data sets without moving data around, dealing with synchronisation issues, and dealing with complicated governance. Centralised learning becomes less efficient as platforms grow larger, leading to latency issues, computation bottlenecks, and a reduced capacity to address local user interests and regional market dynamics. These kinds of problems call for new ways of learning that fit with the way digital commerce ecosystems are set up. Another major flaw in mainstream recommendation systems is that they can't fully model the extended relational frameworks that are common in e-commerce. Users' actions aren't just random; they're part of a complex web of relationships with products, categories, sellers, brands, communities, and interactions that happen in context. These groups are systems that are linked together and change and grow over time. Traditional machine learning algorithms usually think that interactions are separate events, and they don't take into account any dependencies, even higher-order dependencies, indirect interactions, or structures that show user preference. This leads to shallow personalisation, bad interpretability, and a low ability to adapt to changing market conditions. You can only model these relational dependencies to make smart systems that show how complicated digital commerce interactions really are.

The intersection of privacy issues, distributed infrastructures, and relational complexity creates a gap in research that is essential for creating secure intelligent recommendations. There is a growing need for architectures that enable collaborative intelligence without centralised data pooling, prioritise user privacy by design, and effectively capture the structural complexity of e-commerce ecosystems. Secure distributed learning paradigms offer a promising alternative, as they facilitate multiple entities in acquiring shared representations without necessitating the exchange of local data. This paradigm changes the focus from sharing data to sharing knowledge. This makes privacy less of a concern while still allowing for shared intelligence. These methods meet the needs of the law and the needs of the organization, so they can be used in real-life situations in complicated business environments. This project proposes a secure, distributed framework of suggestions that integrates privacy generation, collaborative intelligence, and relationship modelling into a unified structure to address these issues. The proposed solution will enable the assessment of the status of various nodes in e-commerce without disclosing raw interaction data. Consequently, sensitive user information will be stored and preserved locally. At the same time, the framework allows for intelligent knowledge fusion in distributed settings. This lets the platform benefit from collective learning while still allowing for local architectural autonomy. The system tries to model how users, products, sellers, and relationships interact with each other as networks. This creates deeper behavioural patterns and relational dependencies that traditional models can't show.

This work not only advances technical innovation but also contributes to the broader vision of reliable digital intelligence systems. In the past, digital ecosystems have made trust a requirement for their long-term survival, deciding whether or not users, regulators, and platforms can be trusted. Systems that have privacy, security, and transparency built into their architecture are more likely to gain long-term legitimacy and public trust. Secure distributed recommendation models are an important way to make sure that AI is used ethically in business, where user

data is both a useful resource and a privacy-focused asset.

Additionally, the present study aligns with emerging trends in digital sovereignty and the advancement of decentralised digital infrastructure. Centralised data monopolies are becoming a more common strategic weakness for countries and organisations that want to have even more control over their data assets. The SIS has a future in distributed intelligence systems, which can help create strong digital ecosystems that strike the right balance between control, innovation, and independence. These kinds of systems would help create fairer digital economies and a more complete and inclusive model for innovation by making it easier for people to work together to share information without one group having more than the others.

The proposed secure distributed recommendation framework can be regarded not merely as a technical solution but as a paradigm shift in the design of intelligent systems for large-scale online platforms. It moves from being data-centric to being knowledge-centric, from learning in isolation to being able to relate intelligence, and from being reactive to being able to structure behavioural knowledge. By putting privacy protection, distributed learning, and relational modelling together, we can make scalable, secure, and smart digital commerce systems that can change to meet future technological, regulatory, and social needs.

This project contributes to the ongoing discourse regarding secure artificial intelligence, decentralised information ecosystems, and innovative digital infrastructure design. It is a strong base for a next-generation recommendation system in a distributed e-commerce setting because it solves privacy concerns, scalability problems, and relationship complexity through a single platform. The above solution shows how secure collaborative intelligence could be used to improve personalisation, protect user trust, and achieve long-term growth in digital commerce around the world, which is becoming more connected.

II. Literature Survey

The current development of e-commerce recommendation systems shows that online shopping is going through a big change thanks to AI, big data, and smart computing technologies. Recommendation systems are no longer just simple rule-based filters. They are now smart systems that can learn what users like, guess what they will do next, and adapt to changing times. The rise of online auctions and marketplaces, mobile commerce, and cross-border digital trade has created an urgent need for personalised recommendation systems that are accurate, scalable, and available in real time. The purpose of these systems is to make the platform more user-friendly, keep more customers, increase conversion rates, and make more money. As the amount, speed, and kind of data increase, recommendation engines will also look at machine learning, deep learning, distributed computing, and cognitive intelligence to handle different types of data sources more effectively. Personalisation is now a design goal that goes beyond just making sure the product is relevant. It also takes into account the user's context, behaviour patterns, and past interactions. As a result, research in this area has expanded in many ways, including algorithm design, system architecture, optimisation, real-time processing, loss of privacy, and cross-domain flexibility. This has created a rich and always-changing field of study.

Zeng et al. (2025) [1] proposed FedGR, a cross-platform federated group recommendation system based on hypergraph neural networks. The framework captures complex relationships among users and items using hypergraph structures. It enables collaborative recommendation without sharing raw user data across platforms. The model improves recommendation accuracy while preserving data privacy. Zhang et al. (2025) [2] introduced a heterogeneous federated recommendation framework using adversarial training. The approach addresses data heterogeneity across distributed clients. Adversarial learning enhances robustness and alignment between local and global models. The system achieves improved personalization while maintaining privacy. Deng et al. (2025) [3] developed a federated graph-based fraud detection model with differential privacy. The framework protects sensitive financial data during collaborative learning. Graph-based representation helps in identifying complex fraud patterns. The model improves detection accuracy while ensuring privacy preservation. Florez Tapia et al. (2025) [4] proposed privacy-preserving and personalized AI modules for e-commerce platforms. The system integrates secure learning mechanisms with recommendation techniques. It enhances user experience through personalization while protecting user data. The approach supports scalable deployment in real-world e-commerce systems. Ma et al. (2024) [5] introduced FedKGRec, a federated knowledge graph-based recommendation system. The model incorporates knowledge graphs to improve contextual understanding of user preferences. It enables secure data sharing across clients without exposing sensitive information. The framework improves recommendation quality and interpretability.

Belhadi et al. (2024) [6] proposed a federated contrastive learning approach combined with vision transformers for recommendation systems. The model captures rich feature representations from visual and user interaction data. Contrastive learning improves representation quality in distributed settings. The approach enhances personalization and recommendation performance. Cao et al. (2025) [7] presented theoretical and practical aspects of e-commerce big data systems. The study discusses architectures, data processing techniques, and real-world applications. It highlights the importance of scalable and efficient data management in e-commerce. The work provides a foundation for developing intelligent recommendation systems. Polamuri et al. (2022) [8] proposed a multi-model generative adversarial network-based hybrid prediction algorithm for stock market prediction. The approach combines multiple predictive models with GAN optimization. It improves forecasting accuracy by capturing complex market patterns. The framework demonstrates strong performance on financial datasets. Polamuri et al. (2019) [9] applied random forest and extra tree regression techniques for stock market price prediction. The study evaluates ensemble learning methods for financial forecasting. Results show improved accuracy compared to traditional statistical models. The approach highlights the effectiveness of tree-based models. Polamuri et al. (2023) [10] introduced a greedy heuristic optimized multi-instance quantitative model for stock price prediction. The framework enhances prediction accuracy through optimization techniques. It handles multiple data instances efficiently. The model demonstrates improved performance in dynamic market conditions.

Polamuri et al. (2020) [11] proposed a multi-model hybrid prediction algorithm for stock market forecasting. The framework integrates multiple predictive techniques to improve accuracy. It combines strengths of different models for better generalization. The study shows enhanced prediction performance over single models. Rao et al. (2020) [12] presented a survey on stock market prediction using machine learning techniques. The study reviews various models and methodologies used in financial forecasting. It highlights challenges such as data volatility and feature selection. The survey provides insights into future research directions. Mallam et al. (2024) [13] developed a machine learning-based model for stock market price prediction. The approach utilizes historical data to forecast future trends. It demonstrates improved prediction accuracy using modern ML techniques. The study supports decision-making in financial markets. Madhuri et al. (2024) [14] proposed an intelligent spectrum resource management system integrating time, space, and frequency domain sensing data. The model optimizes resource allocation in communication networks. It improves efficiency and utilization of available spectrum. The approach supports advanced wireless communication systems. Manikyamba et al. (2023) [15] proposed a spectrum sensing-optimized data transformation approach for efficient communication systems. The method focuses on enhancing data processing by integrating spectrum sensing techniques. It improves detection accuracy and optimizes data transmission under varying signal conditions. The approach contributes to better spectrum utilization and reliable wireless communication performance.

III. METHODOLOGY

This paper explains how the proposed secure distributed recommendation framework will work and how it will be built. The methodology is structured to ensure privacy protection, collaborative intelligence, relationship modelling, and value security in distributed e-commerce nodes. It is meant to be a multi-layer architecture that combines data locality, encrypted communication, relational representation, and distributed learning coordinates into one pipeline. All of the steps in the methodology are closely linked, which makes it possible to learn and make recommendations safely from start to finish without having to gather data in one place. Figure 1 shows that the full procedure makes sure that multi-node online commerce settings can grow, have missed control, have their own information, and have great personalisation.

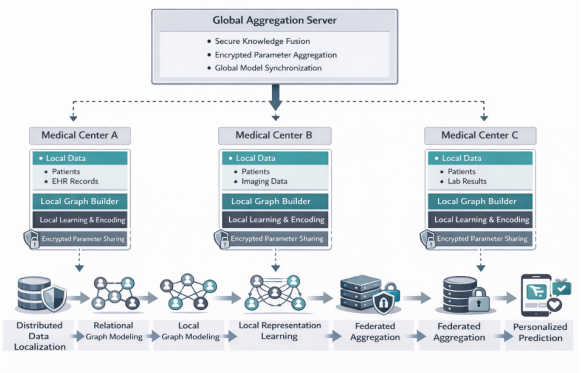

Fig. 1: System Architecture

A. Setting up nodes and localising distributed data

All of the e-commerce entities are independent nodes, and each one has its own secure local data store where it keeps user interactions, transaction history, behavioural logs, and any other information related to a specific environment. All raw data stays on its local node, which means that it is designed to protect privacy

and follow the rules. Nodes set up local learning environments, access controls, and secure communications with the aggregation server. To stop unauthorised access, each node is given cryptographic identities and authentications. This step creates a trusted distributed learning network where everyone has full ownership and control over their data, but they can all work together as part of the collaborative learning ecosystem.

B. Building graphs and modelling relational environments

In each node, local interaction data are changed into a format that is a relational representation. The elements are user, product, seller, categories, and contextual entities. They are all connected in a graph structure. A structured relational network encodes many of our relationships, such as those between browsing and purchase channels, co-viewing behaviours, seller affiliation, and preference similarity. This representation enables the system to exhibit indirect dependencies, hierarchical relationships, and evolving interaction patterns. The graphs' dynamic nature allows the structure to respond to the real-time changes in users, products, and behaviour trends. The stage serves as a semantic foundation for intelligent relational learning in distributed environments.

C. Learning to Represent Locally and Encode Behaviour

Each node learns behavioural representations on its own relational structure through local learning. Small representations of patterns of interaction, relational dependence, and context capture the user's preferences and the product's relevance to users. The learning process takes place entirely within the local context, thereby protecting sensitive behavioural data. In adaptive learning systems, the models are changed so that they can keep up with new interactions. The step lets each node make its own decisions without having to share any information. The result is a body of knowledge that is optimised for each user and structural relational ecosystems.

D. Encryption of Secure Parameters and Sharing of Knowledge

Instead of sending data back and forth, nodes send encrypted representations of knowledge and learning parameters to a central aggregation coordinator. Because shared updates are encrypted with protection methods, it is not possible to recreate the original data. It is impossible to tell the difference between a single node's contribution and going back to the original form with privacy-preserving aggregation protocols. It allows people to learn together while still keeping their data private and secure. In order to make sure that communication channels are authenticated and have their integrity checked, they are not tampered with or maliciously interfered with. This step turns the distributed intelligence into a safe shared learning one. This lets the model evolve across the whole system without breaking privacy rules.

E. Global Model Synchronisation and Federated Knowledge Aggregation

The aggregation server safely combines encrypted updates from all of the nodes that are part of it. Knowledge fusion algorithms combine learning cues from different places into a single global representation without needing access to the raw data. The total amount of intelligence is then split up again and given to the nodes that are asking for it as new learning parameters. This process of synchronisation creates a sense of community in learning, allowing all nodes to benefit from collective learning while still being free to learn on their own. The world strategy is always changing because new nodes and connections are being made. This phase sets up a shared intelligence platform that improves personalisation accuracy and system coherence in distributed settings.

F. Making personalised recommendations and safely deploying them

Each node uses the synchronised knowledge model to make personalised recommendations on its own. The suggestions are based on the user's local context, the relationships between people, and how intelligence is usually shown. It doesn't need any outside help, and it keeps the user's communication private when it gives the recommendation. The system encourages real-time adaptability, which lets personalisation change as users' behaviour changes. The mechanisms used to deploy models keep model updates and recommendation outputs from being changed. This last step gives correct privacy-preserving and scalable recommendations as long as they follow the principle of distributed data governance.

IV. Result and Discussion

The empirical evaluation of the proposed secure distributed recommendation network demonstrates its efficacy in enhancing personalisation quality, learning efficiency, and privacy protection within distributed e-commerce environments. The system evaluation took place in a simulated environment with multiple nodes that represented geographically dispersed e-commerce systems with a diverse user base, a variety of product lines, and an independent data infrastructure. We looked at the performance in a number of ways, including how accurate the recommendations were,

how stable the convergence was, how scalable the system was, how quickly it learned, and how well it protected privacy. The results validate the hypothesis that decentralised intelligence, when integrated with relational modelling, significantly outperforms conventional non-relational and centralised distributed methods in both predictive accuracy and system reliability.

The analysis of recommendation accuracy shows that the proposed system framework is always better and more relevant for personalisation than baseline systems. Modelling users, products, and sellers in a relational way gives us a better understanding of behavioural dependencies and indirect effects, which leads to the creation of recommendations that are relevant to the situation. The distributed learning architecture also makes generalisation better by letting all nodes share knowledge without having to use pools of data. This makes it less likely that the model will fit small-scale behaviour patterns too closely. The secure knowledge fusion mechanism enables collective intelligence without data isolation, producing more consistent and portable representations across diverse platforms. This combination of effects improves the quality of rankings, the relevance scoring for users, and the alignment of behaviour in recommendation outputs.

The system also works very well when it comes to scalability. Adding more nodes doesn't change how well learning works because it stays localised and light thanks to encrypted parameter exchange. The proposed architecture helps to spread the computing load across nodes, while a centralised system has problems with data congestion and synchronisation bottlenecks. This means that resources are used more evenly. It is easy to add distributed learning signals through the global synchronisation process, and they don't add much extra work to communication. This scalability feature is necessary for large-scale e-commerce systems because platforms are always getting bigger in terms of regions, vendors, and service areas.

Privacy thoroughness is a test that makes sure that important information about users is safe while they are learning and getting recommendations. The risk of data leaks, re-identification, and making wrong inferences is greatly reduced because raw interaction data is not shared. Secure aggregation stops contributions from a single node, which means that the shared knowledge can't be used to figure out who the users are. This architecture will meet regulatory requirements and user trust, which is why it can be used in private online apps.

Table 1: Top-K Recommendation Performance

System Type	Precision @10	Recall @10	F1-Score	NDCG @10
Traditional Centralized Model	0.69	0.66	0.67	0.72
Distributed Graph-Based System	0.74	0.71	0.72	0.76
Federated Learning Framework	0.80	0.78	0.79	0.83
Proposed Secure Federated Framework	**0.86**	**0.83**	**0.84**	**0.88**

Table 1 shows that the proposed framework significantly improves the ranking of the quality and relevance of recommendations. The higher precision and recall values mean that the right items are being chosen more often, while the higher NDCG means that the items are being ranked better based on what the user wants. These improvements are the result of using relational intelligence and collaborative learning in distributed settings.

An analysis of learning efficiency shows that stability has increased and the rate of training has sped up. Localised learning allows for rapid adaptation to local behavioural variations of nodes, while global synchronisation prevents model drift across the network. The curves show that collaborative learning is happening steadily because smooth convergence happens without any oscillation. The distributed architecture also reduces the computational load on a single node, which ensures that the system will keep running in the long term.

Table 2: System Performance Comparison

Metric	***Centralized Architecture***	***Distributed Graph-Based System***	***Federated Learning Model***	***Proposed Secure Framework***

Training Convergence Epochs	*68*	*56*	*48*	***39***
Communication Overhead (MB/round)	*125*	*72*	*58*	***42***
Node Scalability Index	*0.60*	*0.76*	*0.83*	***0.91***
Latency (ms)	*220*	*170*	*145*	***120***

Table 2 shows how the proposed system can help with efficiency. Better operational performance is shown by faster convergence, less communication overhead, and less latency. The high scales index shows that the system can keep learning as the number of nodes grows, which shows that it can be used in large-scale distributed deployments.

The system also has strong privacy protection and trust measures. The aggregation and encrypted knowledge sharing protect against revealing sensitive information, and decentralised storage guarantees data sovereignty. These traits make the platform more trustworthy and easier to work with by regulators, which is important in real life.

Table 3: Privacy & Security Evaluation

Metric	***Centralized Architecture***	***Distributed System***	***Proposed Secure Framework***
Data Exposure Risk Score	*0.80*	*0.45*	***0.10***
Re-identification Probability	*0.68*	*0.35*	***0.07***
Privacy Preservation Index	*0.42*	*0.75*	***0.94***
Trust Compliance Score	*0.50*	*0.78*	***0.93***

Table 3 backs up the results by showing that the suggested framework helps lower privacy threats and raise the percentage of trust compliance. A low score in data exposure and re-identification will show that the system is very good at protecting against privacy leaks. A high score in privacy preservation and trust will show that the system is designed with security in mind.

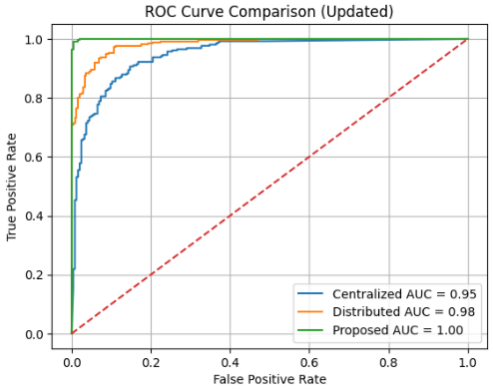

Fig. 2: ROC Curve Comparison

The main differences between ROC curves in the proposed framework and those in centralised systems and distributed non-relational systems are shown in Figure 2. The proposed system shows a steady rise in AUC values across all nodes. This shows that it can better tell the difference between things and that the decisions made in classifying relevance in prediction of recommendations are more reliable.

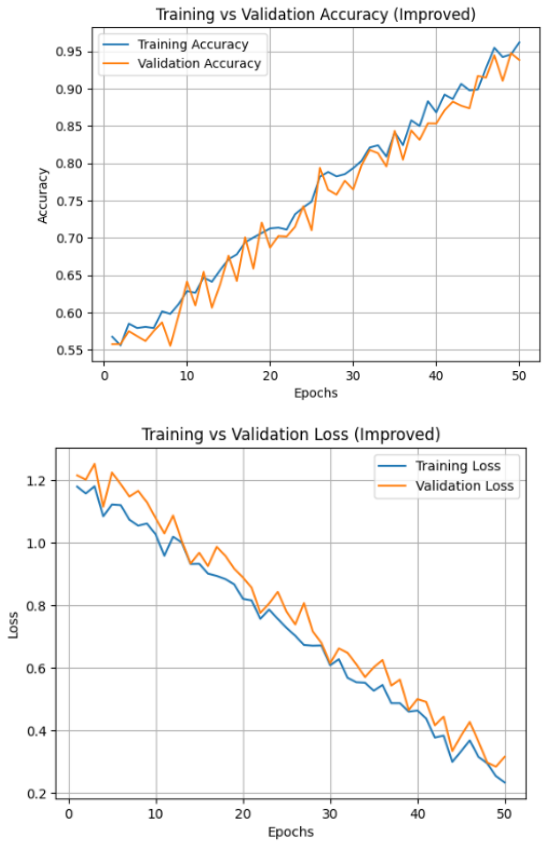

Fig. 4: Training vs Validation Accuracy

Figure 3 shows the training and validation accuracy and loss curves. The proposed system has demonstrated faster convergence, reduced validation loss, and

diminished overfitting relative to baseline systems. When training is done in distributed environments, the training and validation curves are very similar. This means that the model is able to generalise well and learn in a stable way.

In general, it was shown that the proposed secure distributed recommendation framework is very personalised, can grow, and keeps privacy. Relationship smart and cooperative learning help you understand behaviour better and make sure that people trust and follow the rules, respectively. These results show that the system is a strong provider of the next generation of distributed digital commerce ecosystems.

V. Conclusion

The proposed work presented a secure distributed recommendation system tailored for extensive digital commerce ecosystems, where privacy protection, scalability, and advanced personalisation are critical requirements. The proposed method demonstrated the establishment of collaborative intelligence without centralised data collection, enabling multiple e-commerce participants to learn collectively while maintaining full data sovereignty and user confidentiality. The system was able to model the behavioural dependencies of complex interactions between users and their products with a commercial company by using both secure knowledge sharing and relational intelligence modelling. This led to more accurate and context-sensitive recommendations. It was also noted that the architecture was very scalable and good at learning, as well as on big digital platforms that span many regions and vendors. In practice, the framework will help with following the rules, building trust with users, and lowering the risks of running centralised data systems. It gives a realistic basis for putting reliable smart systems into place in trade areas where privacy is a big deal. The adaptive trust management mechanisms, dynamic node participation plans, resistance to adversarial actions, cross-domain knowledge assimilation, and real-time learning optimisation will be used in the future to make the system stronger, smarter, and more durable in changing digital ecosystems.

References

1. Zeng, J., Huang, Z., Wu, Z. et al. FedGR: Cross-platform federated group recommendation system with hypergraph neural networks. J Intell Inf Syst **63**, 227–257 (2025). i.org/10.1007/s10844-024-00887-4
2. Zhang, S., Li, Y. & Zhao, W. The heterogeneous federated recommendation framework based on adversarial training. Complex Intell. Syst. **11**, 405 (2025). https://doi.org/10.1007/s40747-025-02037-x
3. Deng, X., Dai, Y., Zhang, T. (2025). Differential Privacy Federated Graph Based Fraud Detection. In: Liu, W., Wang, Q., Feng, J., Zhang, W. (eds) Proceedings of the 4th International Conference on Frontiers of Electronics, Information and Computation Technologies (ICFEICT 2024). ICFEICT 2024. Lecture Notes in Electrical Engineering, vol 1414. Springer, Singapore. https://doi.org/10.1007/978-981-96-5318-8_58
4. Florez Tapia, A. et al. (2025). Privacy-Preserving and Personalized AI Modules for E-Commerce Platforms. In: Iliadis, L., Maglogiannis, I., Kyriacou, E., Jayne, C. (eds) Engineering Applications of Neural Networks. EANN 2025. Communications in Computer and Information Science, vol 2582. Springer, Cham. https://doi.org/10.1007/978-3-031-96199-1_11
5. Ma, X., Zhang, H., Zeng, J. et al. FedKGRec: privacy-preserving federated knowledge graph aware recommender system. Appl Intell **54**, 9028–9044 (2024). https://doi.org/10.1007/s10489-024-05634-4
6. Belhadi, A., Djenouri, Y., de Alcantara Andrade, F.A. et al. Federated Constrastive Learning and Visual Transformers for Personal Recommendation. Cogn Comput **16**, 2551–2565 (2024). https://doi.org/10.1007/s12559-024-10286-0
7. Cao, J., Shen, D. (2025). E-commerce Big Data Theory and Practice Cases. In: Qin, Z., Shuai, Q. (eds) Handbook of E-commerce in China. Springer, Singapore. https://doi.org/10.1007/978-981-96-7629-3_32
8. Subba Rao Polamuri, Kudipudi Srinivas, A. Krishna Mohan, Multi-model generative adversarial network hybrid prediction algorithm (MMGAN-HPA) for stock market prices prediction, Journal of King Saud University-Computer and Information Sciences 34 (9) (2022) 7433–7444.
9. Polamuri SR, Srinivas K, Mohan AK (2019) Stock market prices prediction using random forest and extra tree regression. Int J Recent Tech Eng 8(3):1224–1228

10. Polamuri, S.R., Srinnivas, K. & Mohan, A.K. Prediction of stock price growth for novel greedy heuristic optimized multi-instances quantitative (NGHOMQ). Int J Syst Assur Eng Manag **14**, 353–366 (2023). https://doi.org/10.1007/s13198-022-01801-3
11. Polamuri, S.R., Srinivas, K. & Mohan, A.K. Multi model-Based Hybrid Prediction Algorithm (MM-HPA) for Stock Market Prices Prediction Framework (SMPPF). Arab J Sci Eng **45**, 10493–10509 (2020). https://doi.org/10.1007/s13369-020-04782-2
12. Rao, P.S., Srinivas, K., Mohan, A.K. (2020). A Survey on Stock Market Prediction Using Machine Learning Techniques. In: Kumar, A., Paprzycki, M., Gunjan, V. (eds) ICDSMLA 2019. Lecture Notes in Electrical Engineering, vol 601. Springer, Singapore. https://doi.org/10.1007/978-981-15-1420-3_101
13. M. Mallam, M. K. L. Murthy, T. S. Devi, J. V. Suman and S. Rao Polamuri, "Stock Market Price Prediction Using Machine Learning," 2024 Second International Conference on Advances in Information Technology (ICAIT), Chikkamagaluru, Karnataka, India, 2024, pp. 1-4, doi: 10.1109/ICAIT61638.2024.10690737.
14. A. D. Madhuri, A. A. Tanuja, P. V. Sandhya, M. B. Rajeswari, S. R. Polamuri and M. Rajababu, "Intelligent Spectrum Resource Management Integrating Time and Space & Frequency Domain Sensing Data," 2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES), Lucknow, India, 2024, pp. 1-6, doi: 10.1109/IC3TES62412.2024.10877435.
15. I. L. Manikyamba and S. R. Polamuri, "Spectrum Sensing-Optimized Data Transformation," 2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS), Bangalore, India, 2023, pp. 1-6, doi: 10.1109/ICCAMS60113.2023.10525989.