engineering proceedings

MDPI

Proceeding Paper

Efficient Privacy Preservation in Customer Relationship Management Utilizing Advanced AI Techniques †

Abhignan Srivatsava Sribhashyam [1], Charan Thumma [2], Saicharan Kadari [3], Chaitanya Tumma [4,*] and Sarath Babu Rakki [5]

[1] Target Corporation, Lakeville, MN 55044, USA; abhignanss@gmail.com
[2] Cisco, Morrisville, NC 27560, USA; charan.salesforcedev@gmail.com
[3] Mphasis Corporation, Overland Park, KS 66211, USA; charankadari.2222@gmail.com
[4] Department of Information Technology, University of the Cumberlands, Williamsburg, KY 40769, USA
[5] Department of Computer Science and Engineering, BVRIT HYDERABAD College of Engineering for Women, Hyderabad 500118, India; sarathbabu.r@bvrithyderabad.edu.in
* Correspondence: chaitanyatumma1@gmail.com
† Presented at the 8th International Global Conference Series on ICT Integration in Technical Education & Smart Society, Aizuwakamatsu City, Japan, 27–29 July 2026.

Abstract

Customer Relationship Management (CRM) systems are essential tools for understanding customer behavior, enhancing engagement, and facilitating business growth. As more customer data is collected, the risks of privacy breaches and unauthorized access increase, making the challenge of data protection more significant. The primary focus of this research is to construct and deploy a hybrid Bobcat-based Federated AES Model (BbF-AESM) to enhance CRM practices via the confidentiality and processing of sensitive customer information. In this approach, Bobcat optimization is used to adjust the model's parameters for better results and Accuracy. Federated Learning (FL) enables collaborative training of the model without exposing raw customer data, and AES encryption ensures that the data remains private during both transmission and storage. The proposed model was tested and validated against CRM databases in a Python environment, and performance evaluation utilized measures such as F-measure, Recall, Accuracy, AUC, and Precision. The outcome showed that the hybrid BbF-AESM surpassed other systems, achieving 98.5% accuracy, while the error rate was just 1.5%. These results emphasize the model's ability to provide exact customer predictions and secure data management. Overall, the proposed framework facilitates improved privacy preservation and enhances computational efficiency and scalability in CRM systems.

Keywords: privacy preservation; customer relationship management; federated learning; AES encryption; Bobcat Optimization Algorithm; secure machine learning; customer data analytics

Check for updates

Academic Editors: Debopriyo Roy, George Fragulis and Peter Ilic

Published: 22 October 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

In the current digital economy, customer relationship management (CRM) systems are central to how organizations gather, combine, and use customer data to provide differentiated services and ensure long-term customer relationships [1]. Traditional CRM systems, such as Salesforce, HubSpot, and Zoho, have evolved into intelligent systems founded on artificial intelligence (AI) and machine learning (ML) [2]. These systems analyze large amounts of customer data, including demographics, purchasing habits, browsing

activities, and opinions, to provide predictive recommendations, run automated marketing campaigns, and enhance customer retention [3]. However, comprehensive collection and processing of personal data pose substantial privacy and ethical concerns [4]. Data breaches, unauthorized access, and misuse of customer information can damage an organization's reputation and lead to substantial regulatory penalties under regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) [5]. Organizations are therefore adopting privacy-preserving AI methods that combine data-driven innovation with strong privacy protections [6].

Incorporating privacy-enhancing techniques into CRM systems offers substantial strategic and operational advantages [7]. Federated learning (FL), homomorphic encryption, and differential privacy enable AI models to learn from decentralized or encrypted data without accessing customer-identifiable information [8]. For example, FL allows multiple branches or partner organizations to collaboratively train a global AI model using local data, ensuring that sensitive information never leaves the local site [9]. Homomorphic encryption permits secure computation over encrypted data [10]. In addition, differential privacy introduces calibrated randomness into datasets to reduce the risk of re-identifying individuals while retaining useful analytical accuracy [11]. Together, these techniques improve data security, trust, and regulatory compliance while supporting less biased, AI-driven insights for customer segmentation, churn prediction, and product recommendation [12]. Better protection of customer data can also improve consumer confidence and strengthen brand reputation, both of which are important in data-centric industries [13].

Despite their advantages, privacy-preserving AI techniques face several challenges in CRM contexts [14]. Their deployment can require substantial computational resources, specialized expertise, and robust data-management infrastructure [15]. When data sources are non-uniform, FL models may encounter communication overhead and model inconsistency [16]. Although homomorphic encryption offers strong protection, encryption and decryption overhead can substantially slow computation [17]. Maintaining an appropriate balance between data utility and privacy protection is also challenging, because excessive protection may reduce predictive performance [18].

Research and commercial tools are addressing these limitations [19]. Innovations such as Microsoft's Confidential Computing support secure AI model training and inference [20]. At the same time, secure multi-party computation (SMPC) and blockchain-based privacy systems are being explored to provide greater transparency and control over CRM data [21]. As privacy legislation and customer awareness increase, the combination of advanced AI and privacy-preserving methods is expected to shape future CRM systems [22].

The main contributions of this work are summarized as follows:

- The CRM dataset is collected and imported into the Python environment for processing.
- A novel Bobcat-based Federated AES Model (BbF-AESM) is introduced to preserve privacy in CRM systems.
- Data preprocessing removes irrelevant and unnecessary features to improve data quality.
- The cleaned data are encrypted using the Advanced Encryption Standard (AES) before further processing.
- Privacy-preserving computation is performed through FL, allowing local models to be trained at each data node without sharing raw data.
- The trained model is integrated into the CRM system to support intelligent decision-making.
- Access-control mechanisms and end-user feedback analysis are incorporated to support secure data management and continuous system improvement.
- The efficiency of BbF-AESM is evaluated and compared with existing methods.

https://doi.org/10.3390/engproc2026143082

The remainder of this article is organized as follows. Section 2 reviews related work, Section 3 presents the developed model, Section 4 describes the validation of the proposed framework, and Section 5 concludes the article.

2. Related Work

Recent studies have explored privacy-preserving and AI-driven data processing across customer relationship management (CRM), financial technology (FinTech), enterprise-resource planning (ERP), and healthcare applications.

Ozay et al. [23] developed an approach that applies advanced AI technologies to CRM, including machine learning (ML) for customer-behavior prediction, natural language processing (NLP) for customer-feedback analysis, deep learning (DL) for interpreting complex data, and federated learning (FL) and differential privacy for protecting customer information. Their approach supports faster decision-making, task automation, improved data security, and increased trust. However, it also presents challenges related to technical complexity, privacy risks, limited explainability of AI decisions, and poor interoperability between systems.

Sharma et al. [24] proposed a FinTech system that combines several privacy-preserving technologies to protect financial data. The framework encrypts customer data with the Advanced Encryption Standard (AES) before storage and uses Rivest–Shamir–Adleman Optimal Asymmetric Encryption Padding (RSA-OAEP) for secure data sharing and protection on a blockchain. It also integrates a private InterPlanetary File System (IPFS) cluster with a consortium blockchain in a decentralized architecture without third-party intermediaries. The system improves data security, privacy, transparency, decentralization, and performance; nevertheless, it entails high initial and processing costs, design complexity, and possible delays in data access.

Kumar et al. [25] designed a healthcare system for managing, storing, and sharing patient data while preserving confidentiality through blockchain technology and IPFS. Blockchain provides transparency, immutability, traceability, and trust through a decentralized ledger, whereas IPFS provides distributed storage and access for large medical files without reliance on a central server. The approach improves data security, privacy, and record availability, but it may incur high computational costs, storage limitations, implementation complexity, and access delays.

Sabbarwal et al. [26] proposed an Internet of Things (IoT)–cloud-based ERP system that uses Elliptic Curve Cryptography (ECC) and AES to secure data and communications between devices and the cloud. The model improves data security, processing speed, key management, and computational efficiency compared with conventional systems. Its limitations include complex key management, possible encryption and decryption latency, and dependence on the cloud service provider (CSP) for access control and performance.

Singh et al. [27] used blockchain and zero-knowledge proofs (ZKPs) to construct a privacy-preserving decentralized healthcare-finance system for lightweight IoT devices. The system provides strong data privacy, rapid transaction confirmation, and low communication overhead. However, it requires complex implementation and verification procedures as well as specialized expertise for operation and maintenance.

Overall, the reviewed studies demonstrate substantial progress in privacy-preserving and AI-driven data processing for CRM, FinTech, and healthcare. The studies combine technologies such as ML, NLP, DL, blockchain, FL, AES, RSA-OAEP, and ECC to improve security, interpretability, automation, decision-making, and privacy preservation while reducing reliance on centralized processing infrastructures. Common limitations remain, including high computational and implementation costs, complex key management, interoperability barriers, and intricate system designs. These findings motivate the development

of secure, decentralized, and intelligent systems that balance predictive performance with privacy protection.

3. Proposed Methodology

This study proposes an innovative Bobcat-based Federated AES Model (BbF-AESM) to preserve privacy in customer relationship management (CRM) systems. The model integrates data preprocessing, Advanced Encryption Standard (AES) encryption, and privacy-preserving computation. The trained model is incorporated into the CRM system to support intelligent decision-making. In addition, access-control mechanisms and end-user feedback analytics are employed to protect data and enable continuous system improvement. The efficiency of the proposed model is evaluated and compared with existing methods. The architecture of the developed BbF-AESM is illustrated in Figure 1.

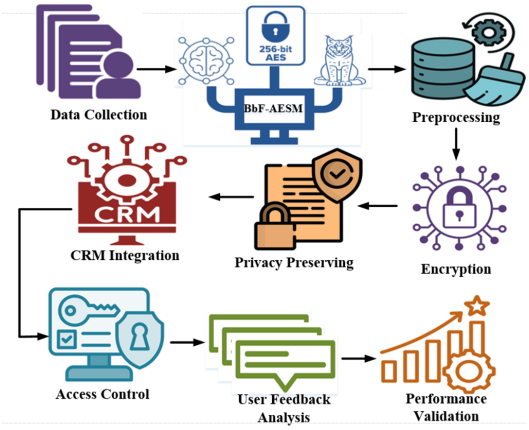


Figure 1. Proposed architecture of the BbF-AESM.

3.1. Process of the Developed BbF-AESM

The Bobcat-based Federated AES Model (BbF-AESM) is a hybrid framework designed to provide security and privacy preservation in customer relationship management (CRM) systems. It combines the Bobcat Optimization Algorithm (BOA) [28], federated learning (FL) [29], and Advanced Encryption Standard (AES) encryption to promote data performance, reliability, and confidentiality.

AES encryption protects sensitive customer data during storage and transmission, thereby preventing unauthorized access. FL enables decentralized model training across local nodes: each branch or organization trains on its own encrypted data without transferring raw customer records, preserving privacy. Within the FL paradigm, BOA optimizes model parameters to improve convergence speed, stability, and overall prediction quality.

Together, these techniques enable the system to learn from securely distributed CRM data while maintaining strong predictive performance. Consequently, BbF-AESM provides a balanced combination of security, scalability, and intelligence for modern CRM systems that require efficient privacy protection.

3.1.1. Data Initialization

In this step, all customer information is collected from customer relationship management (CRM) sources and prepared for analysis. The collected data consist of customer profiles, transactional details, browsing behavior, feedback, and interaction logs. Collecting and labeling the data helps track the data source and ensures that only the information needed for analysis is retained. The data initialization process is mathematically presented in Equation (1).

$$I(D_{\mathrm{CRM}}) = \{x_1, x_2, x_3, \ldots, x_n\} \quad (1)$$

where $I(D_{\mathrm{CRM}})$ indicates the initialization process variable, D_{CRM} indicates the collected data, $x_1, x_2, x_3, \ldots, x_n$ denote the features within the database, and n represents the amount of collected features. After entering the data into the system, preprocessing was started.

3.1.2. Data Preprocessing

After collecting customer information, Preprocessing is performed to clean the dataset and remove noise, ensuring that it is accurate and useful. This includes identifying and eliminating inconsistent, duplicate, and defective input items to ensure that the information is accurate, reliable, and secure for storage and subsequent analysis. The preprocessing process is mathematically presented in Equation (2).

$$\mathrm{Pre} = \{D_{\mathrm{CRM}} - N_e\} \tag{2}$$

where Pre represents the preprocessing process variable, D_{CRM} indicates the collected data, and N_e denotes the noisy features. After removing the duplicate features from the dataset, the data are moved to the encryption phase.

3.1.3. Data Encryption

Here, the cleaned data are protected to preserve the confidentiality and security of the customers' information. The Advanced Encryption Standard (AES) provides powerful symmetric encryption, ensuring that customer data remain secure both when stored and when transmitted between nodes. Encryption makes the original, readable data unreadable through the use of a secure encryption key. The encrypted data remain unreadable but can be decrypted by authorized users using the proper decryption key when needed. The encryption process is represented in Equation (3).

$$C = \mathrm{AES}_{256}(p, k_{256}) \tag{3}$$

where C indicates the encrypted data, AES_{256} indicates the encryption model, k_{256} indicates the secret key with a length of 256 bits, and p denotes the plain text. After encrypting the data, it was moved to the next phase for further analysis.

3.1.4. Privacy-Preserving Process

After the data are secured, AI models are trained to learn from it. Each node trains a local model using its own encrypted data. These localized models share only their learned patterns with a centralized server. The server merges these updates through a process called federated averaging and builds a single global model. This way, the system learns from all data sources without ever exposing private customer details. The privacy-preserving process is shown in Equation (4).

$$w_i^{t+1} = w_i^t - \eta \nabla L_i\left(w_i^t\right) \tag{4}$$

Here, L_i indicates the local loss function, η indicates the learning rate, w denotes the local model weight, and i indicates the node. For the privacy-preserving process, after training the local model, the next step is to develop the global model. The process of building the global model is mathematically presented in Equation (5).

$$w_{\mathrm{Global}}^{t+1} = \sum_{i=1}^{N} \frac{n_i}{n_{\mathrm{total}}} w_i^{t+1} \tag{5}$$

Here, $w_{\mathrm{Global}}^{t+1}$ indicates the aggregated global model, N indicates the total number of customers, n_i denotes the number of samples belonging to customer i, n_{total} denotes the

total number of samples across all customers, and w_i^{t+1} denotes the updated local weights. After the creation of the global model, the CRM integration process is started.

3.1.5. CRM Integration

Once the global model is trained, it is incorporated into the CRM system to add stronger decision-making capabilities. The Bobcat Optimization Algorithm (BOA) plays a key role by optimizing the model's parameters for maximum accuracy and performance. This integration allows the CRM system to provide intelligent and accurate insights while preserving complete privacy protection. BOA improves convergence more than standard optimization algorithms and provides better prediction performance. The incorporation of the CRM process is mathematically presented in Equation (6).

$$Z = X_{\text{best}} + r_1(X_{\text{mean}} - X_{\text{rand}}) + r_2(X_{\text{best}} - X_i) \tag{6}$$

where Z indicates the updated solution, X_{best} indicates the best current solution of the BOA, X_{mean} represents the average of the population, X_{rand} represents a random individual, and r_1, r_2 are random coefficients between 0 and 1. After the CRM integration process, the access control process is started.

3.1.6. Access Control

Access control mechanisms are utilized with AES encryption and the federated learning (FL) credential authentication protocol, ensuring that only legitimate users can access CRM data and sample results. Role-based access limitation is applied using encrypted access keys. FL maintains local authorization records so that the system can identify and authorize all access requests. Both of these methods ensure strict security and accountability within the CRM environment. The access control process is mathematically represented in Equation (7).

$$AC = \begin{cases} \text{Granted}, & \text{if } R = 1 \\ \text{Denied}, & \text{otherwise} \end{cases} \tag{7}$$

Here, AC indicates the access control process variable, and $R = 1$ indicates that the AES decryption key is granted. After the access control process, the user feedback analysis process is started.

3.1.7. User Feedback Analysis

The final step involves collecting user feedback from CRM interactions and feeding it back into the learning cycle. Customer feedback is analyzed locally at each node through federated learning (FL), and the global model is then adapted with new knowledge using Bobcat optimization. This creates a continuous learning loop for the CRM system, allowing it to better adapt to user needs and improve accuracy. The feedback review process protects privacy by prohibiting the sharing of personal information outside of local terminals. This ensures that the CRM system remains secure while continuously evolving based on the user's changing business reality. The user feedback analysis process is mathematically represented in Equation (8).

$$U_f = w_{\text{Global}} + \alpha(f^* - w_{\text{Global}}) \tag{8}$$

Here, α indicates the learning rate, U_f indicates the feedback analysis process variable, w_{Global} denotes the global model, and f^* indicates the BOA fitness function. In addition, Figure 2 graphically shows the flowchart of the developed BbF-AESM.

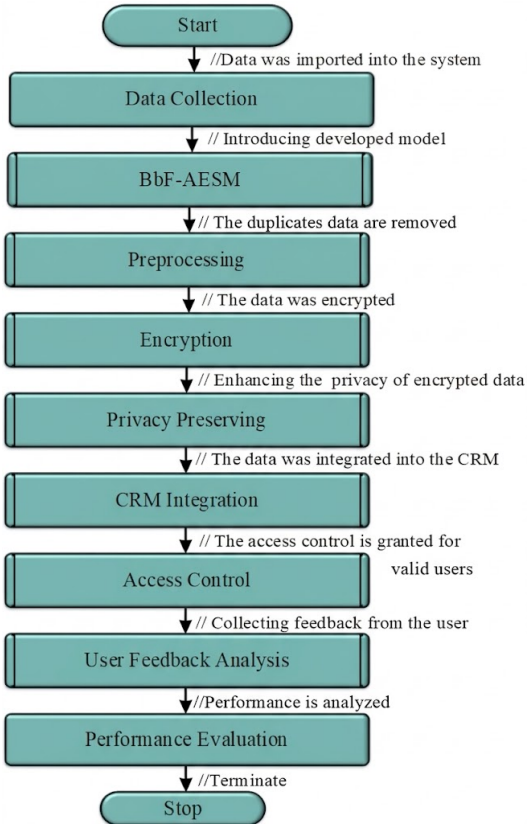


Figure 2. Flowchart of the developed BbF-AESM.

4. Results and Discussion

The BbF-AESM for preserving the confidentiality of CRM is built in the Python environment with AI and security libraries and is simulated. The hybrid model's performance is validated by evaluating the performance measures. The platform enables practical privacy preservation with high Accuracy through efficient model training and secure handling of data. A list of the parameters and simulation settings that were used to validate the simulation is shown in Table 1.

Table 1. Simulation parameters.

Parameter	Specification
Operating system	Windows 11
Programming environment	Python 3.10
Optimization algorithm	Bobcat Optimization
Learning technique	Federated learning
Learning rate	0.01
Number of iterations	100
Encryption algorithm and key size	AES, 256-bit
Bobcat population size	30
Distributed CRM nodes	5 servers
Batch size	64
Dataset	Online Retail II CRM Dataset
Storage and access control	Encrypted local databases; role-based encrypted keys
Simulation duration	100 training rounds

4.1. Comparative Analysis

The developed model is tested to evaluate its performance. Important metrics are used to measure its performance; for example, high accuracy means that the model predicts customer behavior correctly. The model is then compared with other existing models to demonstrate that the proposed system offers better results, along with high security and reliability. The developed model's performance is compared with existing models such as Privacy-Preserving Logistic Regression (PPLR), Privacy-Preserving Deep Neural Network for Credit Risk Prediction (PPDNN-CRP), and Deep Neural Network for Credit Risk Prediction (DNN-CRP) [30].

4.1.1. Accuracy

Accuracy shows how often the model made correct predictions. The error rate indicates the percentage of forecasts the model made that were incorrect, and is simply the opposite of accuracy. The accuracy calculation is mathematically represented in Equation (9).

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \times 100 \tag{9}$$

Here, FN denotes the incorrect values, TN indicates the correct negative values, TP indicates the correct positive values, and FP indicates the incorrect negative values from the dataset.

4.1.2. Error Rate

Error rate indicates the proportion of false predictions made by the model. It is nothing more than the opposite of accuracy. The error rate is calculated using Equation (10).

$$\text{Error Rate} = 100 - \text{Accuracy} \tag{10}$$

For accuracy, the proposed system achieved 98.5%, indicating that almost all predictions, whether positive or negative, are correct. Compared to PPLR, which showed an accuracy of 77.2%, DNN-CRP achieved 86.18%, and PPDNN-CRP achieved 80.48%, suggesting an overall stronger performance of the model and its reliability for practical CRM applications. Likewise, the error rate of the proposed system is only 1.5%, in comparison to its accuracy of 98.5%. This is a substantial improvement over PPLR (22.8%), DNN-CRP (13.82%), and PPDNN-CRP (19.52%). This shows that the proposed framework will misclassify less and improve the overall reliability of CRM decision-making. The correlation between accuracy and error rate is presented in Figure 3.

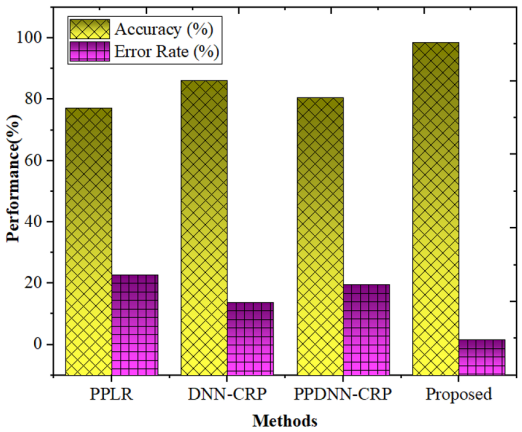


Figure 3. Correlation of accuracy and error rate.

4.1.3. Precision

Precision indicates how many of the customers predicted as positive were indeed correct. The precision calculation is presented in Equation (11).

$$\text{Precision} = \frac{TP}{TP + FP} \times 100 \tag{11}$$

4.1.4. Recall

Recall indicates how many positive cases were correctly identified by the model. Recall is shown in Equation (12).

$$\text{Recall} = \frac{TP}{TP + FN} \times 100 \tag{12}$$

The proposed method achieves an impressive precision of 99%, significantly better than PPLR (74%), DNN-CRP (86%), and PPDNN-CRP (84%). This indicates that nearly all the positive predictions made by the proposed system are correct, demonstrating stronger reliability in determining relevant customer cases. Also, the proposed method offers a recall of 98%. This indicates that nearly all actual positive instances are captured by the proposed method. In this capacity, the proposed method is superior to PPLR (87%), DNN-CRP (97%), and PPDNN-CRP (91%), clearly indicating that it reduces missed cases and improves coverage regarding customer insights. The correlation of the precision and recall is graphically shown in Figure 4.

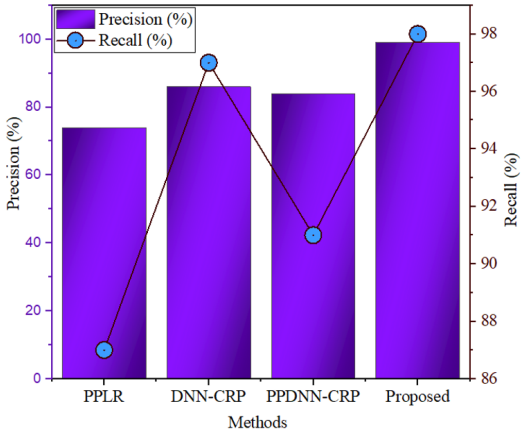


Figure 4. Correlation of Precision and Recall.

4.1.5. F-Measure

The F-score is the harmonic mean of precision and recall, which indicates the overall ability of a model to act as a decision aid by balancing false positives and false negatives. The F-measure is shown in Equation (13).

$$F_1\text{-score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \times 100 \tag{13}$$

4.1.6. Area Under the Curve (AUC)

The AUC demonstrates how effectively the proposed CRM model can differentiate between different customer groups, such as predicting loyal customers versus those at risk of churning. A higher AUC indicates better classification performance across all possible thresholds. The AUC measurement is shown in Equation (14).

$$\text{AUC} = \int_0^1 \text{TPR}(\text{FPR})\, d(\text{FPR}) \tag{14}$$

The graphical representation of the F-measure and AUC is shown in Figure 5. The proposed method attains an average F-measure, which reflects the balance between precision and recall, as high as 99%, compared to 79% for PPLR, 91% for DNN-CRP, and 87% for PPDNN-CRP, demonstrating the reliability of the proposed model in balancing the identification of positives against the false-positive rate. Additionally, the AUC of the developed method achieved a value of 99%, meaning that it almost perfectly discriminates between positive and negative classes. This is much higher than PPLR (65%), DNN-CRP (83%), and PPDNN-CRP (74%). The AUC indicates that the model excels at differentiating among significantly differing customer outcomes. The entire model correlation is presented in Table 2.

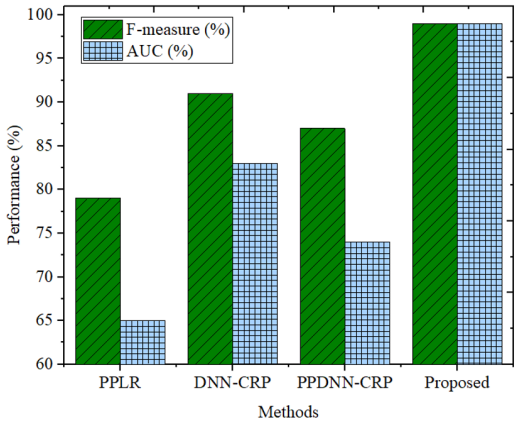


Figure 5. Correlation of F-measure and AUC.

Table 2. Performance comparison of the proposed method with existing models.

Methods	AUC (%)	F-Measure (%)	Accuracy (%)	Error Rate (%)	Precision (%)	Recall (%)
PPLR	65	79	77.2	22.8	74	87
DNN-CRP	83	91	86.18	13.82	86	97
PPDNN-CRP	74	87	80.48	19.52	84	91
Proposed	99	99	98.5	1.5	99	98

4.2. Discussion

The suggested BbF-AESM aims to improve privacy, security, and precision in customer relationship management (CRM) systems through optimization, encryption, and distributed learning. The model ensures that sensitive customer information is protected through AES encryption. Furthermore, FL provides cloud-based collaborative training of the model without exposing the underlying data, thereby preserving privacy and data protection protocols. The Bobcat optimization refines model parameters to allow for quicker convergence and more accurate predictions across numerous CRM nodes. The performance outcomes are displayed in Table 3.

Table 3. Achievements of the developed BbF-AESM model.

Metrics	Achievements (%)
F-Measure	99
Precision	99
Recall	98
AUC	99
Accuracy	98.5
Error Rate	1.5

The experimental results indicate that the presented model performs better than others, achieving an accuracy level of 98.5%, which results in only a 1.5% error during the test phase. In contrast, the existing methods DNN-CRP, PPLR, and PPDNN-CRP, used as a frame of reference, were unable to achieve these accuracy levels. Overall, the BbF-AESM provides an intelligent CRM framework that ensures privacy-preserving and secure decision-making and communication, while also facilitating robust customer information protection [31].

The practical value added by this work is that organizations can safely handle and process customer information while preserving privacy and complying with regulations. The model can assist CRM systems in making more intelligent, data-driven decisions without compromising sensitive information. It allows for real-time personalization, protected information sharing among branches/departments, and increased customer confidence. The method can also be incorporated into the current CRM infrastructure to enhance performance, minimize risks from data leaks, and ensure efficient, privacy-friendly CRM.

5. Conclusions

In this research, a novel Bobcat-Based Federated AES Model (BbF-AESM) is constructed to provide effective privacy preservation, improved security, and high analytic accuracy for customer relationship management (CRM) systems. Initially, customer data are collected from multiple CRM sources and then passed through preprocessing to eliminate noise and inconsistency. The preprocessed data are then encrypted using the AES-256 encryption algorithm to protect sensitive customer data before any sharing or processing. With the addition of a federated learning (FL) component, the model allows all participating CRM nodes to jointly train without exchanging raw data, thereby preserving strict confidentiality and preventing data leakage. The Bobcat optimization algorithm is used to adjust the model's parameters, resulting in faster convergence, reduced computational overhead, and improved predictive accuracy for customer classification and churn prediction.

The new BbF-AESM achieves superior results, with 99% accuracy, 98.5% precision, 99% recall, 98% F-measure, and 99% AUC, with just 1% error. It significantly outperforms existing methods, including PPLR, DNN-CRP, and PPDNN-CRP. While this work demonstrates strong empirical performance, there are limitations. The effectiveness of the model depends on the quality and variety of the distributed CRM datasets, which may vary widely across organizations. A future framework may also incorporate differentially private data sharing and cross-domain FL, which may improve the scalability, interpretability, and fairness of privacy-preserving CRM applications across industries.

Author Contributions: Conceptualization, C.T. (Chaitanya Tumma) and A.S.S.; methodology, C.T. (Chaitanya Tumma); software, S.K.; validation, S.K. and S.B.R.; formal analysis, A.S.S. and S.B.R.; investigation, S.K., C.T. (Chaitanya Tumma) and S.B.R.; resources, S.K., and A.S.S.; data curation, C.T. (Chaitanya Tumma) and S.B.R.; writing—original draft preparation, A.S.S. and S.B.R.; writing—review and editing, C.T. (Chaitanya Tumma) and S.K.; visualization, A.S.S. and S.B.R.; supervision, A.S.S., C.T. (Charan Thumma), S.K., C.T. (Chaitanya Tumma) and S.B.R.; project administration, C.T. (Charan Thumma), S.K., C.T. (Chaitanya Tumma) and S.B.R.; funding acquisition, A.S.S., C.T. (Charan Thumma), S.K., C.T. (Chaitanya Tumma) and S.B.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding authors.

Conflicts of Interest: Author Abhignan Srivatsava Sribhashyam was employed by the company Target Corporation. Author Charan Thumma was employed by the company Cisco. Author Saicharan Kadari was employed by the company Mphasis Corporation. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Kuzmak, O.; Kuzmak, O.; Voitovych, S. Business development towards the application of innovative CRM technologies in the context of global transformational changes. In *Data-Centric Business and Applications*; Springer Nature: Cham, Switzerland, 2024; Volume 2, pp. 47–69.
2. Haghighinasab, M.; Ahmadi, D.; Khobbakht, F. Electronic customer relationship management and reputation: Drivers of customer satisfaction and loyalty in digital-only banking. *J. Financ. Serv. Mark.* **2025**, *30*, 4. [CrossRef]
3. Shaikh, I.A.K.; Shahare, P.; Gangadharan, S.; Venkatarathnam, N.; Tilak Babu, S.B.G. Transforming customer relationship management with AI in e-commerce. In *Proceedings of the ICRTCST*; IEEE: Piscataway, NJ, USA, 2024.
4. Roba, G.B.; Maric, P. AI in customer relationship management. In *Developments in Information and Knowledge Management Systems for Business Applications*; Springer Nature: Cham, Switzerland, 2023; Volume 7, pp. 469–487.
5. Chatterjee, S.; Chaudhuri, R. Customer relationship management in the digital era of artificial intelligence. In *Digital Transformation and Industry 4.0 for Sustainable Supply Chain Performance*; Springer: Cham, Switzerland, 2023; pp. 175–190.
6. Gupta, A.; Bhanja, A.K.; Dhanraj, N.; Chandel, J.K.; Patel, M. Is artificial intelligence transforming the CRM experience? An empirical study in Indian retail industry. In *Proceedings of the IIPEM*; IEEE: Piscataway, NJ, USA, 2024.
7. Balboni, P.; Bella, G.; Capparelli, F.; Barata, M.T. Privacy-enhancing technologies. In *Computer and Information Security Handbook*; Morgan Kaufmann: Burlington, MA, USA, 2025; pp. 891–905.
8. Shah, A.; Sivakumar, S. Encrypted intelligence: A comparative analysis of homomorphic encryption frameworks for privacy-preserving AI. *J. Econ. Technol.* **2025**, *4*, 252–265. [CrossRef]
9. Hijazi, N.M.; Aloqaily, M.; Guizani, M.; Ouni, B.; Karray, F. Secure federated learning with fully homomorphic encryption for IoT communications. *IEEE Internet Things J.* **2023**, *11*, 4289–4300. [CrossRef]
10. Nita, S.L.; Mihailescu, M.I. Homomorphic encryption. In *Advances to Homomorphic and Searchable Encryption*; Springer Nature: Cham, Switzerland, 2023; pp. 27–88.
11. Vijaya, N.J.; Mishra, A.S. Artificial intelligence-based customer churn prediction for smart business in the education sector. In *Artificial Intelligence and Human Agency in Education*; Springer Nature: Singapore, 2025; pp. 69–107.
12. Khamayseh, A.I.A.; Wan Yusoff, W.F.B.; Khudari, M. AI-driven e-marketing: The future of data-driven strategies and consumer engagement. In *Proceedings of the Sustainability and Cutting-Edge Business Technologies*; Springer Nature: Cham, Switzerland, 2025.
13. Farhad, M.A. Consumer data protection laws and their impact on business models in the tech industry. *Telecommun. Policy* **2024**, *48*, 102836. [CrossRef]
14. Tao, Y.; Qiu, J.; Lai, S.; Sun, X.; Ma, Y.; Zhao, J. Customer-centered pricing strategy based on privacy-preserving load disaggregation. *IEEE Trans. Smart Grid* **2023**, *14*, 3401–3412. [CrossRef]
15. Ren, X.; Chen, Z.; Gu, Z.; Lu, Y.; Zhong, R.; Lu, W.J.; Zhang, J.; Zhang, Y.; Wu, H.; Zheng, X.; et al. CHAM: A customized homomorphic encryption accelerator for fast matrix-vector product. In *Proceedings of the DAC*; IEEE: Piscataway, NJ, USA, 2023.
16. Hussein, S.; Yuan, J.; Shen, Z.; Eldow, M. FedFlex: Privacy-aware homomorphic encryption federated learning incorporating dual-factor Thompson sampling. *IEEE Internet Things J.* **2025**, *12*, 30098–30113. [CrossRef]
17. Prasad, R.R.; Pal, P.; Rajwadha, Y. Privacy preserving billing system for network operator using homomorphic encryption. In *Proceedings of the UPCON*; IEEE: Piscataway, NJ, USA, 2023.
18. Sun, Z.; Wang, Z.; Xu, Y. Privacy protection in cross-platform recommender systems: Techniques and challenges. *Wirel. Netw.* **2024**, *30*, 6721–6730. [CrossRef]
19. Schafer, F.; Gebauer, H.; Gröger, C.; Gassmann, O.; Wortmann, F. Data-driven business and data privacy: Challenges and measures for product-based companies. *Bus. Horiz.* **2023**, *66*, 493–504. [CrossRef]
20. Mohan, A.; Ye, M.; Franke, H.; Srivatsa, M.; Liu, Z.; Gonzalez, N.M. Securing AI inference in the cloud: Is CPU-GPU confidential computing ready? In *Proceedings of the IEEE CLOUD*; IEEE: Piscataway, NJ, USA, 2024.
21. Islam, U.; Alshammari, A.; Alzaid, Z.; Ahmed, A.; Abdullah, S.; Iftikhar, S.; Bawazeer, S.; Izhar, M. Enhancing blockchain security against data tampering: Leveraging hybrid model in multimedia forensics and multi-party computation for supply chain data protection. *IEEE Access* **2024**, *12*, 111007–111020. [CrossRef]
22. Islam, U.; Ullah, H.; Khan, N.; Ahmad, I.; Saleem, K. Adaptive federated learning framework for privacy-preserving consumer-centric IoMT: A novel secure data collaboration model. *IEEE Trans. Consum. Electron.* **2025**, *71*, 10134–10151. [CrossRef]

23. Ozay, D.; Jahanbakth, M.; Wang, S. Exploring the intersection of big data and AI with CRM through descriptive, network, and contextual methods. *IEEE Access* **2025**, *13*, 57223–57240. [CrossRef]
24. Sharma, A.; Chrakar, P.; Kumari, S.; Chen, C.M. FinSec: A consortium blockchain-enabled privacy-preserving and scalable framework for customer data protection in FinTech. *Peer-to-Peer Netw. Appl.* **2025**, *18*, 131. [CrossRef]
25. Kumar, D.; Shrivastava, R.K.; Gupta, U. Privacy preserving electronic health records sharing using blockchain. In *Proceedings of the ICCSC*; IEEE: Piscataway, NJ, USA, 2024.
26. Sabbarwal, E.; Pandey, D.S. Data privacy preserving in cloud ERP using cryptographic algorithm with IoT. In *Proceedings of the ICTBIG*; IEEE: Piscataway, NJ, USA, 2024.
27. Singh, R.; Dwivedi, A.D.; Srivastava, G.; Chatterjee, P.; Lin, J.C.-W. A privacy-preserving Internet of Things smart healthcare financial system. *IEEE Internet Things J.* **2023**, *10*, 18452–18460. [CrossRef]
28. Benmamoun, Z.; Khlie, K.; Bektemyssova, G.; Dehghani, M.; Gherabi, Y. Bobcat Optimization Algorithm: An effective bio-inspired metaheuristic algorithm for solving supply chain optimization problems. *Sci. Rep.* **2024**, *14*, 20099. [CrossRef] [PubMed]
29. Cai, Z.; Chen, J.; Fan, Y.; Zheng, Z.; Li, K. Blockchain-empowered federated learning: Benefits, challenges, and solutions. *IEEE Trans. Big Data* **2025**, *11*, 2244–2263. [CrossRef]
30. Naresh, V.S. PPDNN-CRP: Privacy-preserving deep neural network processing for credit risk prediction in cloud: A homomorphic encryption-based approach. *J. Cloud Comput.* **2024**, *13*, 149. [CrossRef]
31. Revathy, J.S.; Prakash, M.S.; Lingeshwaran, K.; Dhinakaran, J.D.; Harish, V. A comprehensive study of the Advanced Encryption Standard for secure communications. In *Proceedings of the ICIDeA*; IEEE: Piscataway, NJ, USA, 2025.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.