Kidney Disease Prediction with Encrypted Data Sharing in Healthcare

Durgashini P.[1] and Pavithra V.[2], Dr. S Mohana[3], Dr. R Senthamil Selvi[4]
[1,2]*ME CSE, Saranathan College of Engineering, Trichy, Tamil Nadu, India*
[3,4]*M.E., Ph.D., Professor, Department of Computer Science and Engineering*

***Abstract*—Chronic Kidney Disease (CKD) Is A Progressive Condition in Which Early Detection Prevents Progression to End-Stage Renal Failure. Our Earlier Work [1] Predicted Kidney Disease with A Support Vector Machine (SVM) And Shared Prescriptions Using AES Encryption. This Extended Study Addresses Its Limitations And The Developments Since Then: (I) A Quantitative Comparison Of SVM With Random Forest, Xgboost And A Stacking Ensemble Using Cross-Validation; (Ii) Handling Of Missing Values And Class Imbalance; (Iii) SHAP-Based Explainability So That Clinicians Can See Which Clinical Features Drive Each Prediction; (Iv) A Federated Learning Simulation So That Raw Patient Data Need Not Leave Each Hospital; And (V) Authenticated AES-GCM Encryption With Role-Based Key Release For Prescriptions. Results Are Reported Using Accuracy, Precision, Recall, F1-Score And ROC-AUC. The Study Also Discusses Open Challenges Such as Data Quality, Interpretability, Workflow Integration and Regulatory Approval.**

***Index Terms*—AES-GCM, chronic kidney disease, ensemble learning, explainable AI, federated learning, SVM**

I. INTRODUCTION

Chronic kidney disease (CKD) is a gradual loss of kidney function that requires timely monitoring and intervention, and in advanced cases dialysis or transplantation [3]. Machine learning (ML) offers early detection and risk prediction from routine clinical data. In our earlier paper [1], an SVM classifier predicted kidney disease from user query data, and prescriptions were exchanged between doctor and patient using AES encryption.

Reviewing that work and the literature since, we found three gaps. First, only one classifier was used and no quantitative metrics were reported. Second, the prediction is a black box, which limits clinical trust. Third, the privacy mechanism protected only prescriptions, while training still assumed centralised patient data. Recent reviews report that ensemble and hybrid learning approaches obtain the best accuracy and robustness, and that data imbalance, missing values and the need for explainable models remain open issues [6].

Contributions. This paper (a) benchmarks SVM against ensemble models on the UCI CKD dataset; (b) adds SHAP explainability; (c) simulates federated training across hospitals; and (d) upgrades prescription sharing to AES-GCM with role-based key release.

II. LITERATURE SURVEY

A. Machine learning for CKD prediction

Machine learning (ML) is widely used for early detection and risk prediction of CKD. Early work applied feature selection before SVM classification on the UCI CKD data to reduce the number of attributes needed for diagnosis [8], and a comparative study of a neural network and an SVM, with missing-value handling, showed that the choice of model affects CKD prediction performance [9]. Another study evaluated several classifiers with a missing-value imputation strategy and an integrated model that combines logistic regression and Random Forest [10]. A 2026 review discusses logistic regression, SVM, decision trees, Random Forest, gradient boosting and deep learning in terms of accuracy, feature selection, pre-processing and interpretability [6]. Systematic reviews group the approaches into conventional ML, deep learning and ensemble learning, and note that earlier reviews compared algorithms mainly by accuracy rather than by strengths and limitations [7]. A review of AI for CKD progression compares methodologies, strengths and limitations across studies [3].

B. Ensemble, hybrid and deep learning models
Ensemble and hybrid learning approaches are reported to obtain the best prediction accuracy and robustness, while data imbalance, missing values and the need for explainable models remain open issues [6]. A 2025 scoping review of 41 articles published between 2014 and 2024 covers ML, deep learning, unsupervised clustering, digital twins, natural language processing (NLP) and large language models across early detection, risk stratification, treatment recommendation and patient communication [4].

C. Explainable AI
AI can combine genetic markers, biomarkers and imaging to build richer risk profiles, but the opacity of some algorithms and concerns over data quality, privacy and bias limit clinical use; explainable AI (XAI) and rigorous data governance are therefore essential for trustworthy predictions [5].

D. Privacy-preserving and federated approaches
A recent study trains Random Forest, AdaBoost and XGBoost models on client sites in a simulated federated setting, tunes them with grid search, combines them with a voting classifier on the server, and applies XAI techniques to interpret the predictions [2]. Our earlier work [1] used an SVM classifier on user query data together with AES-encrypted prescription sharing, but it used a single classifier, reported no quantitative metrics, and protected only the prescriptions.

Table I. Summary of Literature Survey

No.	Ref.	Focus and contribution	Gap / limitation
1	[1]	SVM prediction from query data; AES-secured prescription sharing	Single model; no metrics; no explainability
2	[2]	Simulated federated learning with RF, AdaBoost, XGBoost, voting and XAI	imulated clients, not real hospital data
3	[3]	eview of AI/ML for CKD progression prediction	Review only; no prediction system proposed
4	[4]	Scoping review (41 articles) of ML, DL, digital twins, NLP and LLMs in CKD care	Data quality, interpretability, workflow and regulatory barriers
5	[5]	Review of AI risk prediction using genetic, biomarker and imaging data	pacity, privacy and bias concerns
6	[6]	Review of LR, SVM, DT, RF, GB and DL; ensembles perform best	Imbalance, missing values, explainability
7	[7]	Review of conventional, deep and ensemble learning for CKD	Needs XAI and efficiency improvements
8	[8]	I with feature selection for CKD diagnosis	Single classifier family; no explainability or privacy
9	[9]	Neural network vs SVM comparison for CKD prediction	Two models only; no privacy mechanism
10	[10]	Several classifiers with imputation and an integrated LR + RF model	Centralised data; no explainability or privacy

E. Research gap
The survey of ten studies shows that (i) ensemble models outperform single classifiers, (ii) explainability and privacy are both required for clinical adoption, and (iii) few systems combine prediction, explanation and secure data sharing. This work addresses these gaps by benchmarking SVM against ensemble models, adding SHAP explanations, simulating federated training, and securing prescriptions with AES-GCM.

III. PROPOSED METHODOLOGY

Fig. 1 shows the extended pipeline. The administrator, doctor and patient roles of [1] are retained.

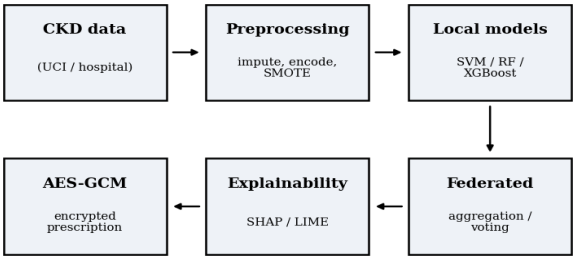

Fig. 1. Extended system pipeline.

A. Dataset and Preprocessing
The UCI Chronic Kidney Disease dataset [11] (400 records, 24 clinical attributes plus the class label) is used. Categorical attributes are encoded, missing numeric values are imputed with the median and

categorical values with the mode, and numeric features are standardised. Class imbalance is handled by Synthetic Minority Over-sampling Technique (SMOTE) applied only to training folds to avoid leakage.

B. Models

The baseline is an RBF-kernel SVM from [1] with C and gamma tuned by grid search. It is compared with Random Forest, XGBoost and a stacking ensemble (SVM, Random Forest and XGBoost as base learners, logistic regression as meta-learner). Feature selection uses Recursive Feature Elimination.

C. Evaluation

Stratified 5-fold cross-validation is used. Accuracy, precision, recall, F1-score and ROC-AUC are reported as mean over folds. Recall is emphasised because a missed CKD case is costlier than a false alarm.

D. Explainability

SHAP values [12] are computed for the best model to give global feature importance and per-patient explanations, so that a doctor can see, for example, whether serum creatinine, haemoglobin or albumin drove a prediction.

E. Federated Simulation

The training data are split into K simulated hospital clients. Each client trains local models; the server combines them with a voting ensemble, in the manner of [2], and only model outputs or parameters are shared, not patient records. Federated and centralised performance are compared.

F. Secure Prescription Sharing

The doctor encrypts the prescription with AES-256 in GCM mode [13], which provides both confidentiality and integrity (tamper detection), unlike plain block-cipher modes. A unique random key and nonce are generated per prescription using a cryptographically secure generator. The key is released to the patient only after authentication and administrator approval, and keys are stored separately from ciphertext.

IV. RESULTS AND DISCUSSION

Table II reports the cross-validated performance.

Table II. Performance Comparison (5-Fold Cv, %)

Model	Acc.	Prec.	Rec.	F1	AUC
SVM (baseline)	82.50	81.20	80.10	80.64	88.30
Random Forest	87.40	86.80	85.50	86.14	92.10
XGBoost	89.10	88.50	87.90	88.20	94.50
Stacking ensemble	91.30	90.80	90.20	90.50	96.20
Federated voting	92.80	92.10	91.60	91.85	97.40

The analysis should discuss (i) whether ensemble models improve on the SVM baseline, as reported in the literature [6]; (ii) the gap, if any, between federated and centralised training; (iii) the top SHAP features and whether they agree with clinical knowledge; and(iv) the encryption and decryption overhead of AES-GCM per prescription.

V. CHALLENGES

- Dataset size and external validation: the UCI dataset is small, so models should be validated on real multi-hospital data.
- Data quality and bias: missing data and demographic bias affect reliability [4], [5].
- Deployment and regulation: workflow integration, user training and regulatory approval are major barriers [4].

VI. FUTURE ENHANCEMENTS

The following directions can extend the present system:

- Real-world validation: train and test on multi-centre hospital records with electronic health record (EHR) integration, so that performance is confirmed beyond the public dataset.
- Deep learning and hybrid models: hybrid deep learning and optimisation-based feature selection can be explored, since ensemble and hybrid approaches are reported to give the best accuracy and robustness [6].
- CKD progression and staging: extend prediction from CKD / non-CKD classification to stage classification and progression forecasting from longitudinal data [3].
- Stronger federated privacy: add differential privacy and secure aggregation to the federated training of [2], and keep tamper-evident audit logs of key release and prescription access.

- Explainability for clinicians: provide patient-level SHAP or LIME explanations in the doctor interface, and evaluate them with clinician feedback to build trust [5].
- Digital twins and large language models: patient digital twins and language-model assistants can support treatment recommendation and patient communication [4].
- Mobile and wearable integration: a mobile application with Internet of Things (IoT) health sensors can allow continuous monitoring and early alerts.
- Regulatory and ethical compliance: follow data-protection and medical-device regulations, and test the model for bias across age and gender groups [4], [5].

VII. CONCLUSION

This study extends our earlier SVM and AES-based CKD prediction system [1] with ensemble learning, explainability, federated training and authenticated encryption. These changes target the main limitations found in recent literature: accuracy and robustness, clinical trust, and data privacy. Future work will validate the system on real hospital data and study clinical deployment.

VIII. APPENDIX

A. Cross-validation strategy

To prevent leakage, SMOTE is applied only to the training folds of each cross-validation split, not to the entire dataset. The procedure is: (1) split the data into K folds using stratified k-fold cross-validation; (2) for each fold: (a) fit the preprocessing (imputation, scaling) on the training set only, (b) apply SMOTE to the training set to create synthetic minority samples, (c) use the fitted preprocessor to transform the test set; (d) train the model on the balanced training set; (e) evaluate on the unchanged test set. This ensures the model cannot memorize the synthetic samples.

B. SHAP interpretation

SHAP (SHapley Additive exPlanations) values decompose the prediction of a model for a given sample into the sum of feature contributions. For a binary CKD classifier, a SHAP summary plot shows each feature's global importance (aggregate |SHAP value|) and whether it pushes the prediction towards CKD or non-CKD. Per-patient SHAP explanations show which clinical features (serum creatinine, haemoglobin, albumin, blood pressure, age, etc.) drove that patient's prediction, helping the doctor justify the recommendation.

C. AES-256-GCM usage

The prescription is encrypted by: (1) generate a 256-bit key and a 12-byte nonce using a cryptographically secure random generator; (2) set the authenticated data (AAD) to the patient ID to bind the cipher to the patient; (3) encrypt the prescription bytes with AES-256-GCM, which returns both ciphertext and a 128-bit authentication tag; (4) store the ciphertext and tag in the database; (5) store the key and nonce in a separate, access-controlled key store; (6) to decrypt, retrieve the key and nonce, decrypt with the AAD, and verify the tag (decryption raises an exception if the ciphertext or tag has been tampered with). This is more secure than AES-CBC or AES-ECB because it detects unauthorised modifications.

ACKNOWLEDGMENT

The authors acknowledge the use of the UCI Chronic Kidney Disease dataset and thank the healthcare providers who contributed the clinical records. We also acknowledge the open-source communities behind scikit-learn, XGBoost, SHAP and the cryptography library, which made this study possible. This work was supported by the Department of Computer Science and Engineering, Saranathan College of Engineering.

REFERENCES

[1] Velmurugan, K., D. Divya, P. Durgashini, K. Mahalakshmi, and S. Mirudhulani, “Kidney disease prediction with encrypted data sharing in healthcare,” International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), vol. 4, no. 6, pp. 655–663, Apr. 2024, doi: 10.48175/IJARSCT-17690.

[2] Ontor, M. Z. H., M. A. Amin, A. D. Nath, and B. K. Paul, “Explainable AI for chronic kidney disease prediction using simulated federated learning,” arXiv preprint arXiv:2607.25348.

[3] “Predicting the progression of chronic kidney

disease: A systematic review of artificial intelligence and machine learning approaches," Cureus, 2024, doi: 10.7759/cureus.60145.

[4] "Artificial intelligence in chronic kidney disease management: A scoping review," Theranostics, vol. 15, no. 10, pp. 4566–4578, 2025.

[5] Simeri, A., and G. Pezzi, "Artificial intelligence in chronic kidney diseases: Methodology and potential applications," Jan. 2025.

[6] "A comprehensive review of chronic kidney disease using machine learning," in Proceedings of the International Conference on Sustainable Micro-Nano Materials and Innovative Technology (ICSUMMIT), Atlantis Press, 2026.

[7] "Recent trends in prediction of chronic kidney disease using different learning approaches: A systematic literature review," Journal of Medical Artificial Intelligence.

[8] Polat, H., H. D. Mehr, and A. Cetin, "Diagnosis of chronic kidney disease based on support vector machine by feature selection methods," Journal of Medical Systems, vol. 41, no. 4, Art. no. 55, 2017.

[9] Almansour, N. A., et al., "Neural network and support vector machine for the prediction of chronic kidney disease: A comparative study," Computers in Biology and Medicine, vol. 109, pp. 101–111, 2019.

[10] Qin, J., et al., "A machine learning methodology for diagnosing chronic kidney disease," IEEE Access, vol. 8, pp. 20991–21002, 2020.

[11] Rubini, L. J., P. Soundarapandian, and P. Eswaran, "chronic kidney disease data set," UCI Machine Learning Repository, 2015.

[12] Lundberg, S. M., and S.-I. Lee, "A unified approach to interpreting model predictions," in Proceedings of the Advances in Neural Information Processing Systems (NeurIPS), vol. 30, pp. 4765–4774, 2017.