

Artificial intelligence-based multi-key security for protected and transparent medical cloud storage

Ravi Kiran Bagadi¹, Neelima Santoshi Koraganji¹, Bandreddi Venkata Seshukumari²,
Kavya Ramya Sree Karuturi³, Sireesha Abotula¹, Bodapati Venkata Rajanna⁴,
Mahalakshmi Annavarapu⁵, Nitalaksheswara Rao Kolukula¹, Jayasree Pinajala⁶,
James Stephen Meka⁷

¹Department of Computer Science and Engineering, School of Technology, GITAM University, Visakhapatnam, India

²Department of Information Technology, VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India

³Department of Artificial Intelligence and Machine Learning, Aditya University, Surampalem, India

⁴Department of Electrical and Electronics Engineering, MLR Institute of Technology, Hyderabad, India

⁵Department of Computer Science and Business Systems, RVR and JC College of Engineering, Guntur, India

⁶Department of Computer Science and Engineering, Chaitanya Engineering College, Visakhapatnam, India

⁷Ambedkar Chair Professor, Andhra University, Visakhapatnam, India

Article Info

Article history:

Received Apr 17, 2025

Revised Oct 27, 2025

Accepted Nov 9, 2025

Keywords:

Cloud-based healthcare
Elliptic curve cryptography
Multi-key encryption
Physics informed triangulation
aggregation neural networks
Secure authentication

ABSTRACT

Ensuring the security and privacy for the patient medical records and medical reports data is a crucial challenge as cloud-based healthcare technologies become more prevalent. For cloud-hosted medical data, internet of things (IoT) and artificial intelligence (AI) technologies shows best solutions for the challenges in the medical domain. This study suggests a Secure and Transparent Multi-Key Authentication Framework that makes use of AI. Using Z-score normalization, the framework first preprocesses the data before clustering to create a multi-level multi-key security structure. The physics-informed triangulation aggregation neural network (PITANN) model in the study reduces computation costs by minimizing overhead, ensuring secure handling of location-based and medical data for enhanced data classification and encryption effectiveness. A multi-key derivation of an elliptic curve, the ElGamal cryptography scheme is presented, which allows for safe multi-key encryption with little increase in the length of the ciphertext. This method guarantees safe, confidential access to cloud-hosted encrypted health information. An envisioned amalgamation improves flexibility by enhancing performance metrics such as speed of computation while safeguarding patient information through enhanced security measures and ensuring precise medical record integrity within virtual healthcare systems.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Nitalaksheswara Rao Kolukula

Department of Computer Science and Engineering, School of Technology, GITAM University

Visakhapatnam, India

Email: kolukulanitla@gmail.com

1. INTRODUCTION

An investigation examines how an artificial intelligence (AI)-driven approach employs multiple verification methods for safeguarding digital healthcare record accessibility. The proposed mechanism fortifies cybersecurity measures in line with regulatory standards utilizing dispersed cryptographic keys for managing data security, guarantees comprehensive audit trails via blockchain infrastructure, and integrates advanced machine learning techniques to identify potential risks [1]. Robust strategies involving

robust cryptographic methods ensure privacy of healthcare information housed within distributed computing environments shared among various users [2]. Intelligent software safeguards computer systems against unauthorized access through advanced authentication methods like two-step verification; it also manages who can use these systems securely by limiting their privileges appropriately. Switching from physical records to digital healthcare databases enhanced medical services significantly however, this transition heightened cybersecurity threats [3]. Enhancing data protection significantly occurs through integrating blockchain alongside lattice-based authentication mechanisms. A cryptographic method employing advanced artificial intelligence (AI) models ensures privacy of patient health information. Advanced AI-driven multifactor security significantly bolsters cloud safety protocols [4]. Users who authenticate themselves through restricted methods utilizing encrypted database systems safeguard sensitive patient information from unauthorized access. Sophisticated encryption methods are employed throughout various geographical areas of computer systems for safeguarding medical records [5]. Ensuring seamless availability of patient's healthcare data electronically is crucial in medicine. The document proposes implementing an electronic verification mechanism for enhancing data accuracy, privacy, and safeguarding measures [6]. Utilizing telemedicine via cloud-based systems enables AI for diagnosis; nonetheless, concerns about cyber security and data protection persist [7]. In dealing with electronic health records management, the elliptic curve cryptography (ECC) protected cryptography discussed below guarantees both safety and reliability.

Nowadays, managing patient data efficiently has become much easier due to significant advancements in AI alongside increased use of cloud-based health info storage systems. Nevertheless, concerns about data safety, confidentiality, and unauthorized use persist, necessitating robust identification authentication methods. Commonly employing weak passwords makes systems susceptible to threats such as identity theft and phishing scams [8].

2. LITERATURE SURVEY

The study [9] evaluated the safety of patient data files, highlighting issues related to conventional watermarks. By employing advanced machine learning techniques such as deep neural networks and incorporating invisible watermarks for verification purposes, their approach enhanced both resistance against attacks and ensured secure identification processes. Despite advancements in blockchain technology and cryptographic methods for enhancing security, challenges related to compatibility and performance remained unresolved. The study [10] discussed concerns related to securing health data through internet of things (IoT) technology in medical systems. Proposed was an anonymous system utilizing cryptography for its security features. They ensured effectiveness without compromising safety measures. Nevertheless, scalability and computational overhead concerns remained.

In [11] investigated processing of clinical notes using bidirectional long short-term memory (BiLSTM). AI, machine learning and internet of things plays very vital role for patient records monitoring in medical domain. In [12] designed a quantum-safe multi-factor authentication mechanism for medical IoT. Their approach improved security but encountered issues in complexity and efficiency. Further research was required for optimization.

In [13] suggested a safe authentication approach for cloud-based electronic health records. Their solution increased security and minimized key exchange, but it had scalability issues. Further research was required for real-world application.

2.1. Problem statement

High computational complexity, scalability problems, and vulnerabilities in key generation are some of the difficulties facing healthcare data management. These are addressed by secure and transparent multi-key authentication for cloud-hosted medical data using AI, which uses physics-informed triangulation aggregation neural network (PITANN) based classification and multilevel multi-key security. Secure encryption and little ciphertext expansion are guaranteed by a multi-key derivation elliptic curve ElGamal cryptography technique. This approach enhances productivity, confidentiality, and accuracy which is a secure and scalable online health care administration tool.

3. PROPOSED METHOD

The mobile health (MHEALTH) and UCI dataset is preprocessed using Z-score normalization, and data is clustered for multilevel multi-key security. To assure the privacy of the transmission and storage, the system utilises PITANN for protected location and medical data classification. This Section will outline how the derivation of multiple keys protects the information of the clustered data which is stored in the cloud using

elliptic curve cryptography with small sized ciphertext expansion. Data acquisition followed by pre processing, secure multiple key generations and the encryption of data are shown in the schematic representation as per Figure 1. In data collection initially it is collected two datasets namely MHEALTH and UCI. In secure multi key generation it is used Elliptic curve ElGamal cryptography. For data encryption to convert plain text to cipher text, it is used PITANN.

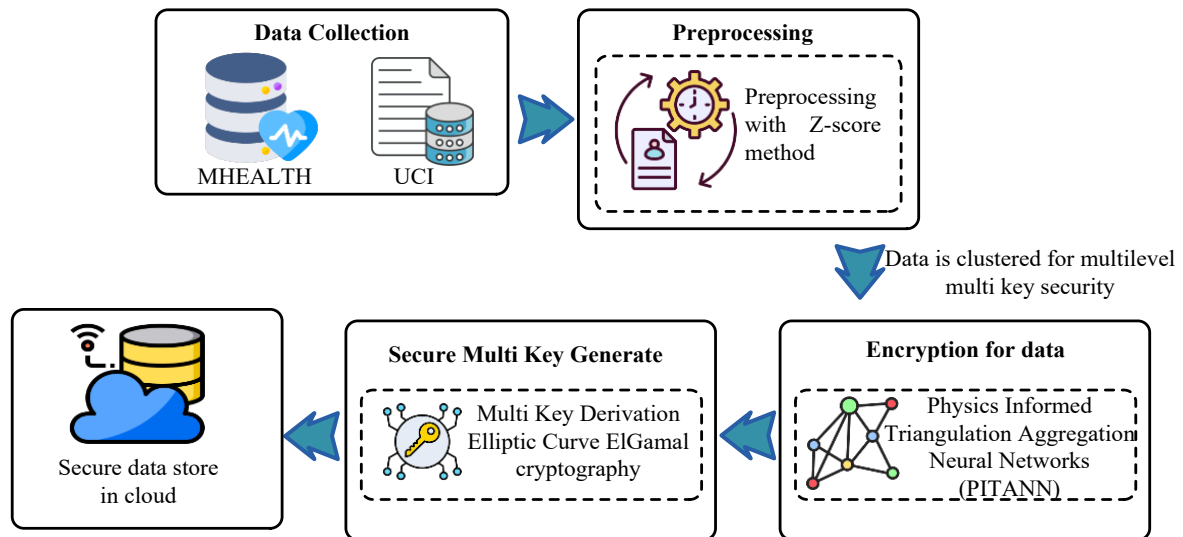


Figure 1. Overall schematic representation of proposed methodology

3.1. Data collection

The MHEALTH dataset is based upon activity recognition and healthcare with UCI machine learning repositories datasets [14], [15]. These datasets contain rich information that can be used for creating prediction model on high-quality medical information. The processing ensures that these data are accurate, reliable, and contribute to advance quality medical solutions. The MHEALTH dataset is an open dataset and it is specifically designed for human activity recognition under wearable sensors scenarios. This data set is utilized to promote scientific research activities in mobile health monitoring and activity identification. The UCI machine learning repository serves as a fundamental resource for numerous datasets utilized in machine learning research activities and testing purposes. The University of California, Irvine hosts this repository which delivers a broad spectrum of datasets encompassing classification, regression, clustering, and time series analysis domains.

3.2. Preprocessing

Preprocessing AI-operated authentication and secure key management for organized medical data guarantees. Preprocessing information has been supplied as stated below. In Z-score normalization, the preprocessing phase of normalization involves breaking the data into numerical properties that can be used to convert data values into a specific range. When normalizing data, many techniques are commonly used, such as decimal scaling, Z-score generalization and minimum-maximum normalization. In (1) shows how Z-score normalization from attribute D to u into a previously unknown range transforms to a u_i value [16].

$$u'_i = \frac{u_i - D_i}{std(D)} \quad (1)$$

Where u'_i result of normalization value of u_i . u is the value to be normalized in attribute D_i which is the mean value of attribute and $std(D)$ is the standard deviation for attribute D .

3.3. Physics informed triangulation aggregation neural networks

Physical rules are incorporated into neural network architecture to solve partial difference equations (PDEs), known as physics-informed neural networks (PINNs) [17]. But when it comes to handling complex geometric and odd domains, traditional pins often struggle with accuracy and efficiency. To deal with these

issues, we provide PITANN, a new structure that improves PINNs using triangle-based aggregation and domain discretionary methods. The purpose of the pit is to solve PDE in general as shown by (2).

$$Lu(x) = f(x)x \in \Omega \quad (2)$$

Where L is a differential operator, $u(x)$ is the solution function, and $f(x)$ represents source terms or external forces. In triangulation, PITANN uses Delaunay triangulation to extract a collection of non-overlapping triangular elements T_i from the computing domain Ω . This makes it possible to extract features locally and improves the neural network's ability to efficiently learn intricate boundary interactions [18]. For each triangular element T_i , we approximate the solution $u(x)$ using a set of basis functions shown in (3).

$$u(x) \approx \sum_{j=1}^N \phi_j(x) u_j \quad (3)$$

Where $u(x)$ is a specific spatial point x , the approximated solution function, N is the total number of nodes, $\phi_j(x)$ is the shape function associated with the triangulation, which are used to interpolate the solution within each triangular element, u_j is the nodal value of the solution function at the triangulation node. In aggregation, PITANN aggregates local solutions derived from individual triangular elements rather than treating the entire domain as a single entity [19]. The final solution $u(x)$ is computed as a weighted sum as shown in (4).

$$u(x) = \sum_{i=1}^M w_i u_i(x) \quad (4)$$

Where w_i is the aggregation weights learned during training, M is the number of such elements used in the aggregation process.

3.4. Multi key derivation elliptic curve ElGamal cryptography

ECC is a public-key cryptosystem that uses elliptic curves over finite fields, which have an algebraic structure. Shorter key lengths and robust security make it effective in contexts with limited resources, such as mobile devices and Internet of Things platforms. Known for its asymmetric encryption, the ElGamal cryptosystem bases its security on the difficulty of solving the discrete logarithm problem. Together, they improve security and computational efficiency in elliptic curve ElGamal (EC-ElGamal) encryption. The mathematical characteristics of elliptic curves as given by the following (5) which serve as the foundation for ECC.

$$y^2 = x^3 + ax + b \quad (5)$$

Where x, y are the coordinates of a point on the elliptic curve and a, b are the points which form the specific shape of the curve. The EC-ElGamal Cryptosystem EC-ElGamal is a modification of the ElGamal cryptosystem that uses elliptic curve point multiplication in place of modular arithmetic [20]. Key generation, select an elliptic curve E over a finite field F_q . Choose a base point G on E with a large prime order. Select a private key d , a random integer. Compute the public key $Q = dG$. Encryption: represent the plaintext message as a point M on the curve. Choose a random integer k . Compute the ciphertext as a pair of points (C_1, C_2) : $C_1 = kG$ $C_2 = M + kQ$. In Decryption, Compute $M = C_2 - dC_1$. Where C_1, C_2 is the first and second component of the ciphertext. M is the plaintext message. k is the random integer. Q is public key. G is a base point of curve [21]–[25].

3.5. Computational complexity

The proposed PITANN model performs training with a complexity of approximately $O(n \times t)$, where n is the number of training samples and t is the number of triangular elements used in domain discretization. The ECC-ElGamal encryption step performs point multiplication on elliptic curves with complexity $O(k \log k)$, where k is the key size. Overall, the combined framework achieves a near-linear complexity with respect to dataset size, making it feasible for large-scale healthcare data processing on modern cloud platforms [26].

4. RESULTS AND DISCUSSIONS

The system requires an Intel Core i3 processor, 32GB RAM, and a 1TB SSD for optimal performance. High-speed internet is needed so that the cloud works efficiently, while Google Cloud Storage

provides the necessary data storage. It can run on Windows 11 and uses Python 3.12 along with machine learning and encryption libraries like TensorFlow or PyTorch, Scikit-learn, NumPy, Pandas, Cryptography, and PyCryptodome. PostgreSQL is used as the database solution, while the cloud services are provided by Google Cloud Compute. Pandapower is a suggested power system analysis tool that provides complete computational capabilities. Heart disease prediction and analysis is shown and presented in [27].

4.1. Comparison analysis

The Table 1 presents a comparison of the performance of convolutional neural network (CNN), random forest (RF), and the suggested MHEALTH dataset. RF achieves accuracy of 95.56%, with precision, recall, and F1-score values of 93.50%, 91.83% and 93.25%, respectively. CNN improves with 90.4% accuracy. The MHEALTH dataset outperforms both, achieving 99.21% accuracy, with precision, recall, and F1-scores of 99.36%, 99.6%, and 99.14%, respectively. MHEALTH shows superior performance across all metrics.

Table 1. MHEALTH dataset comparison of existing methods with proposed model

Methods	Accuracy %	Precision %	Recall %	F1-score %
RF	95.56	93.50	91.83	93.25
CNN [23]	90.4	96	95.3	94.56
Proposed	99.21	99.36	99.6	99.14

Table 2 shows compares the performance of logistic regression (LR), BiLSTM, and the proposed UCI dataset. LR achieves accuracy of 88.14%, with precision, recall, and F1-score values of 88%, 89.10% and 88.36%, respectively. BiLSTM improves with 93.4% accuracy. The UCI dataset outperforms both, achieving 99.52% accuracy, with precision, recall, and F1-scores of 99.46%, 99.34%, and 99.25%, respectively. UCI shows superior performance across all metrics. Table 3 shows the error values for the proposed method compared to the existing method.

Table 2. UCI dataset comparison of existing methods with proposed model

Methods	Accuracy %	Precision %	Recall %	F1-score %
LR [24]	88.14	88	89.10	88.36
BiLSTM [25]	93.4	96.9	91.7	94.23
Proposed	99.52	99.46	99.34	99.25

Table 3. Error value for proposed with existing

Methods	R squared error	MSE	RMSE
DNN [17]	0.52	0.61	0.45
GNN [19]	0.41	0.47	0.55
Proposed	0.33	0.29	0.36

Figure 2 presents the training and validation performance over 100 epochs. For the MHEALTH dataset, (a) shows a training accuracy of 0.99 and a testing accuracy of 0.98, indicating a strong fit, while (b) reports a training loss of 0.79 and a testing loss of 0.80. Similarly, for the UCI dataset, (c) shows a training accuracy of 0.99 and a testing accuracy of 0.83, while (d) reports a training loss of 0.80 and a testing loss of 0.75, demonstrating good generalization.

Figure 3 shows the ciphertext expansion ratio in (a) encryption time and (b) decryption time which compares the cluster's encrypting and decryption times. The cluster routinely performs better than the others in both metrics. Both encryption and decryption durations increase linearly with data size, and the cluster maintains its highest efficiency throughout.

4.2. Limitations

While the proposed PITANN–ECC–ElGamal framework demonstrates excellent performance on the MHEALTH and UCI datasets, several limitations remain. First, the approach does not currently address post-quantum cryptographic threats; future work should consider lattice-based or code-based cryptography to mitigate quantum attacks. Second, actual clinical datasets were not evaluated because of accessibility limitations, and therefore further validation is needed on larger-scale heterogeneous medical data in order to have generalizability. Lastly, PITANN's computational complexity would grow with very dense or irregular data, and thus further optimization will be necessary for large-scale usages.

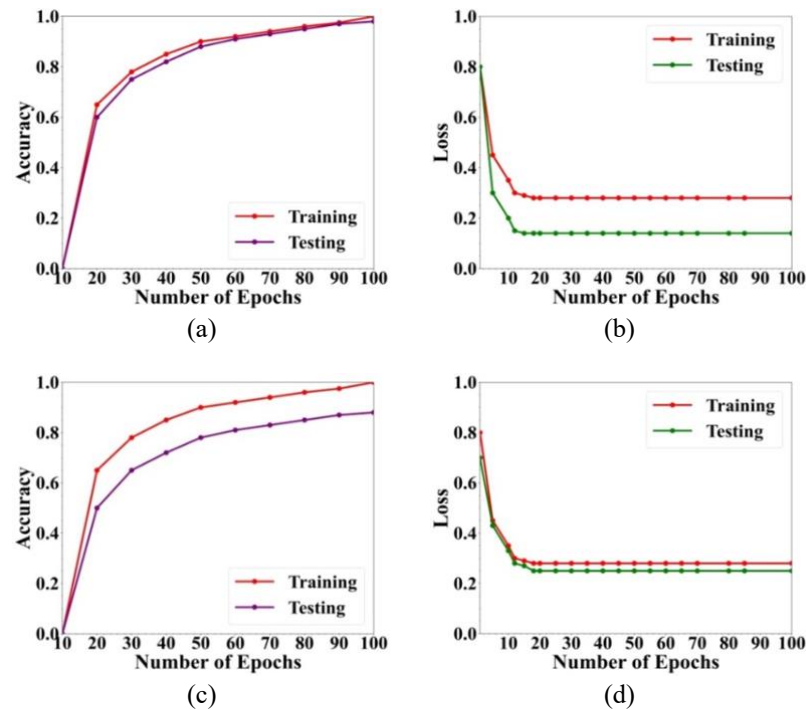


Figure 2. Training and testing performance analysis for two datasets in (a) training and testing accuracy MHEALTH, (b) training and testing loss MHEALTH, (c) training and testing accuracy UCI, and (d) training and testing loss UCI

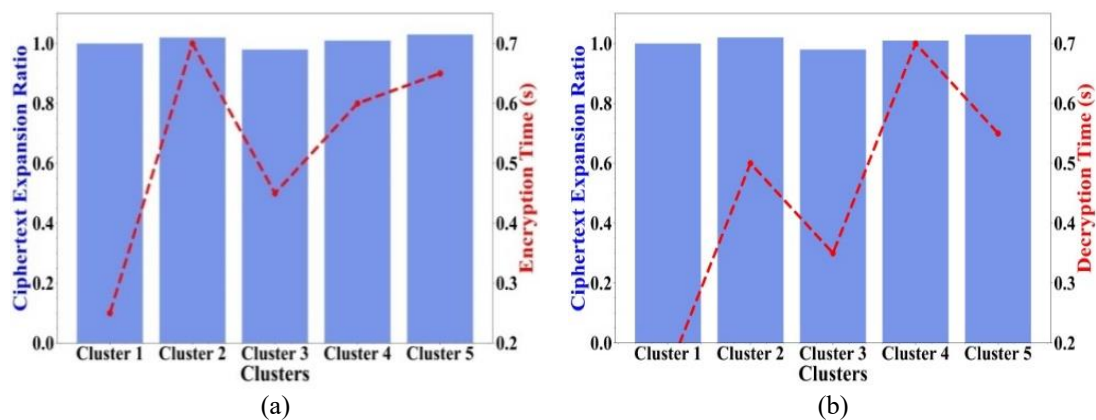


Figure 3. Ciphertext expansion ratio in (a) encryption time and (b) decryption time

5. CONCLUSION

A multi-key authentication method within the proposed architecture ensures secure and efficient storage of cloud-hosted medical data. Data privacy, integrity, and computational efficiency are enhanced by combining multi key derivation elliptic curve ElGamal cryptography and PITANN-based classification. Ensuring scalable cloud-based health solutions, the process minimizes ciphertext expansion but allows safe operations on ciphertext. With a strong encryption method, this hybrid architecture tackles important issues in medical data security. In the end, it offers a dependable, private solution for medical data kept in the cloud.

Future research will focus on integrating the proposed PITANN-ECC framework with federated learning and cloud-native deployment models to enhance scalability. We also plan to incorporate post-quantum cryptography for quantum-resistant security and perform comparative benchmarking with RSA, AES, lattice-based, and homomorphic encryption techniques. Finally, additional work will involve k-fold cross-validation, statistical significance testing, and validation on real-world clinical datasets.

FUNDING INFORMATION

There are no sources of funding agency that have supported the work. So, Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Ravi Kiran Bagadi	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Neelima Santoshi		✓				✓		✓	✓	✓	✓	✓		
Koraganji														
Bandreddi Venkata Seshukumari		✓				✓		✓	✓	✓	✓	✓		
Kavya Ramya Sree Karuturi		✓				✓		✓	✓	✓	✓	✓		
Sireesha Abotula	✓		✓	✓			✓			✓	✓		✓	✓
Bodapati Venkata Rajanna	✓	✓	✓	✓	✓		✓	✓	✓			✓		
Mahalakshmi Annavarapu	✓				✓		✓	✓	✓	✓	✓			
Nitalaksheswara Rao Kolukula	✓	✓	✓	✓	✓		✓	✓	✓			✓	✓	✓
Jayasree Pinajala		✓				✓		✓	✓	✓	✓	✓		
James Stephen Meka		✓				✓		✓	✓	✓	✓	✓		

C : **C**onceptualization

M : **M**ethodology

So : **S**oftware

Va : **V**alidation

Fo : **F**ormal analysis

I : **I**nterpretation

R : **R**esources

D : **D**ata Curation

O : **O**riginal Draft

E : **E**diting

Vi : **V**isualization

Su : **S**upervision

P : **P**roject administration

Fu : **F**unding acquisition

CONFLICT OF INTEREST STATEMENT

The authors state that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper. Authors State no conflict of interest.

DATA AVAILABILITY

The authors confirm that the data supporting the findings of this study are available within the article.




REFERENCES

- [1] A. S. Rajput, A. Agarwal, and K. B. Raja, "A robust multi-key authority system for privacy-preserving distribution and access control of healthcare data," *Computer Communications*, vol. 225, pp. 195–204, 2024, doi: 10.1016/j.comcom.2024.07.005.
- [2] B. S. Raj and S. Venugopalachar, "Multi-data multi-user end to end encryption for electronic health records data security in cloud," *Wireless Personal Communications*, vol. 125, no. 3, pp. 2413–2441, 2022, doi: 10.1007/s11277-022-09666-2.
- [3] T. Hariitha and A. Anitha, "Multi-level security in healthcare by integrating lattice-based access control and blockchain-based smart contracts system," *IEEE Access*, vol. 11, pp. 114322–114340, 2023, doi: 10.1109/ACCESS.2023.3324740.
- [4] J. A. Alzubi, O. A. Alzubi, M. Beseiso, A. K. Budati, and K. Shankar, "Optimal multiple key-based homomorphic encryption with deep neural networks to secure medical data transmission and diagnosis," *Expert Systems*, vol. 39, no. 4, 2022, doi: 10.1111/exsy.12879.
- [5] S. Gayathri and S. Gowri, "CUNA: A privacy preserving medical records storage in cloud environment using deep encryption," *Measurement: Sensors*, vol. 24, 2022, doi: 10.1016/j.measen.2022.100528.
- [6] C. L. Chen, P. T. Huang, Y. Y. Deng, H. C. Chen, and Y. C. Wang, "A secure electronic medical record authorization system for smart device application in cloud computing environments," *Human-centric Computing and Information Sciences*, vol. 10, pp. 1–31, 2020, doi: 10.1186/s13673-020-00221-1.
- [7] A. Alzahrani, "Developing a provable secure and cloud-centric authentication protocol for the e-healthcare system," *IEEE Access*, vol. 12, pp. 183665–183687, 2024, doi: 10.1109/ACCESS.2024.3500216.




- [8] L. Zhang, G. Hu, Y. Mu, and F. Rezaeiabagha, "Hidden ciphertext policy attribute-based encryption with fast decryption for personal health record system," *IEEE Access*, vol. 7, pp. 33202–33213, 2019, doi: 10.1109/ACCESS.2019.2902040.
- [9] A. Anand, J. Bedi, A. Aggarwal, M. A. Khan, and I. Rida, "Authenticating and securing healthcare records: a deep learning-based zero watermarking approach," *Image and Vision Computing*, vol. 145, 2024, doi: 10.1016/j.imavis.2024.104975.
- [10] X. Zhou, S. Wang, K. Wen, B. Hu, X. Tan, and Q. Xie, "Security-enhanced lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare," *IEEE Internet of Things Journal*, vol. 11, no. 6, pp. 9599–9609, 2024, doi: 10.1109/IJOT.2023.3323614.
- [11] N. R. Kolukula, S. Puli, C. Babi, and others, "Processing of clinical notes for efficient diagnosis with feedback attention-based BiLSTM," *Medical & Biological Engineering & Computing*, vol. 62, pp. 3193–3208, 2024, doi: 10.1007/s11517-024-03126-8.
- [12] A. Ahmad and S. Jagatheswari, "Quantum safe multi-factor user authentication protocol for cloud-assisted medical IoT," *IEEE Access*, vol. 13, pp. 3532–3545, 2025, doi: 10.1109/ACCESS.2024.3523530.
- [13] B. M. Singh and J. Natarajan, "A novel secure authentication protocol for e-health records in cloud with a new key generation method and minimized key exchange," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 7, 2023, doi: 10.1016/j.jksuci.2023.101629.
- [14] Kaggle, "MHealth dataset [data set]," Kaggle, 2024. [Online]. Available: <https://www.kaggle.com/datasets/mhealth>.
- [15] Kaggle, "UCI ML datasets [data set]," Kaggle, 2024. [Online]. Available: <https://www.kaggle.com/datasets/uciml>.
- [16] L. Peng, Z. Lu, T. Lei, and P. Jiang, "Dual-structure elements morphological filtering and local Z-score normalization for infrared small target detection against heavy clouds," *Remote Sensing*, vol. 16, no. 13, 2024, doi: 10.3390/rs16132343.
- [17] Z. Zou, X. Meng, and G. E. Karniadakis, "Correcting model misspecification in physics-informed neural networks (PINNs)," *Journal of Computational Physics*, vol. 505, 2024, doi: 10.1016/j.jcp.2024.112918.
- [18] J. Chen, D. Wu, P. Song, F. Deng, Y. He, and S. Pang, "Multi-view triangulation: systematic comparison and an improved method," *IEEE Access*, vol. 8, pp. 21017–21027, 2020, doi: 10.1109/ACCESS.2020.2969082.
- [19] M. Bilal *et al.*, "An aggregation of aggregation methods in computational pathology," *Medical Image Analysis*, p. 102885, 2023, doi: 10.1016/j.media.2023.102885.
- [20] S. Baccouri, H. Farhat, T. Azzabi, and R. Attia, "Lightweight authentication scheme based on elliptic curve El Gamal," *Journal of Information and Telecommunication*, vol. 8, no. 2, pp. 231–261, 2023, doi: 10.1080/24751839.2023.2281143.
- [21] O. A. Imran, S. F. Yousif, I. S. Hameed, W. N. A. D. Abed, and A. T. Hammid, "Implementation of El-Gamal algorithm for speech signals encryption and decryption," *Procedia Computer Science*, vol. 167, pp. 1028–1037, 2020, doi: 10.1016/j.procs.2020.03.402.
- [22] O. Abayomi-Alli, S. Misra, and A. Abayomi-Alli, "A deep learning method for automatic SMS spam classification: performance of learning algorithms on indigenous dataset," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 17, 2022, doi: 10.1002/cpe.6989.
- [23] J. Miah, M. Mamun, M. M. Rahman, M. I. Mahmud, S. Ahmad, and M. H. B. Nasir, "MHfit: mobile health data for predicting athletics fitness using machine learning models," in *2022 2nd International Seminar on Machine Learning, Optimization, and Data Science (ISMODE)*, 2022, pp. 584–589. doi: 10.1109/ISMODE56940.2022.10180967.
- [24] M. A. Khatun *et al.*, "Deep CNN-LSTM with self-attention model for human activity recognition using wearable sensor," *IEEE Journal of Translational Engineering in Health and Medicine*, vol. 10, pp. 1–16, 2022, doi: 10.1109/JTEHM.2022.3177710.
- [25] S. Pati, S. Kumar, A. Varma, and others, "Privacy preservation for federated learning in health care," *Patterns*, vol. 5, no. 7, 2024, doi: 10.1016/j.patter.2024.100974.
- [26] S. Li *et al.*, "Post-quantum security: opportunities and challenges," *Sensors*, vol. 23, no. 21, 2023, doi: 10.3390/s23218744.
- [27] N. R. Kolukula, P. N. Pothineni, V. M. K. Chinta, V. G. Boppana, R. P. Kalapala, and S. Duvvi, "Predictive analytics of heart disease presence with feature importance based on machine learning algorithms," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 32, no. 2, pp. 1070–1077, 2023, doi: 10.11591/ijeecs.v32.i2.pp1070-1077.

BIOGRAPHIES OF AUTHORS






Ravi Kiran Bagadi    is an Associate Professor in the Department of Computer Science Engineering at GITAM School of Technology, Visakhapatnam. With over 14 years of experience, he holds a Ph.D., M.Tech, and B.Tech in Computer Science and Engineering. He has published extensively in international journals and conferences, focusing on areas such as computer vision and image processing. He can be contacted at email: rbagadi@gitam.edu.






Neelima Santoshi Koraganji    received her B.Tech (CS and SE) from GITAM College of Engineering and M.Tech (CST) from Andhra University and pursuing her Ph.D. at Andhra University. She has 19 years of teaching experience and is currently working as an Assistant Professor in the Computer Science and Engineering department, GITAM Deemed to be University, Visakhapatnam. She is passionate to work with the young minds. She is the life member of Computer Society of India (CSI). Her current research interest includes quantum computing, artificial intelligence, machine learning, deep learning and cloud computing. She can be contacted at email: bvp.neelima@gmail.com.






Bandreddi Venkata Seshukumari    is an Associate Professor in the Department of Information Technology at VNRVJiet, boasts a remarkable academic career marked by dedication to both teaching and research. She was awarded a Ph.D. (CSE) and M.Tech. (CSE), and B.Tech. (CS and IT) from JNTUH. She has 20 years of teaching experience and 10 years of dedicated research experience. She has published 30 papers in esteemed journals like ACM, Elsevier and Springer, and Inder Science. She has served in various departmental roles like HOD, M.Tech., and various administrative roles, demonstrating her commitment to student development. She can be contacted at email: seshukumari_bv@vnrvjiet.in.






Kavya Ramya Sree Karuturi    pursuing Ph.D. in Aditya University, Surampalem, Andhrapradesh, India. She received her Masters Degree M.Tech in Information Technology in 2018 from SRKR Engineering College, Bhimavaram. Now, she is working as an Assistant Professor in the department of Artificial Intelligence and Machine Learning at Aditya University, Surampalem, Andhra Pradesh, India. She has experience more than 7 years in teaching and 4 years as Software Engineer in Industry. Her current research on machine learning, deep learning, computer vision and image processing. She can be contacted at email: kavayamyasreek@adityauniversity.in.






Sireesha Abotula    pursuing her Ph.D. in Andhra University, Visakhapatnam India. She received her Master's degree M.Tech in Computer Science and Systems Engineering in 2010 from Andhra University. Now, she is working as an Assistant Professor in the department of AI and DS at GITAM University Visakhapatnam Andhra Pradesh India. She has more than 18 years of teaching and 6 years of research experience. She is the life member of IAENG. Her current research interest includes AI, machine learning, deep learning, software engineering, IoT, and cloud computing. She can be contacted at email: sabotula85@gmail.com.






Bodapati Venkata Rajanna    is currently working as an Associate Professor in Department of Electrical and Electronics Engineering at MLR Institute of Technology, Hyderabad, India. He received B.Tech. degree in Electrical and Electronics Engineering from Chirala Engineering College, JNTU, Kakinada, India, in 2010, M.Tech. degree in Power Electronics and Drives from Koneru Lakshmaiah Education Foundation, Guntur, India, in 2015 and Ph.D. in Electrical and Electronics Engineering at Koneru Lakshmaiah Education Foundation, Guntur, India, in 2021. His current research includes, dynamic modeling of batteries for renewable energy storage, battery management systems (BMS) for electric vehicles and portable electronics applications, renewable energy sources integration with battery energy storage systems (BESS), smart metering and smart grids, micro-grids, automatic meter reading (AMR) devices, GSM/GPRS and power line carrier (PLC) communication, and various modulation techniques such as QPSK, BPSK, ASK, FSK, OOK, and GMSK. He can be contacted at email: rajannabv2012@gmail.com.






Mahalakshmi Annavarapu    completed her B.Tech (Computer Science and Engineering) from Chirala Engineering College, Chirala affiliated to JNTU, Kakinada. She completed her M.Tech (Computer Science and Engineering) from Avanathi Institute of Engineering and Technology affiliated to JNTU, Hyderabad. She had experience in different academic and administrative roles at various academic institutes for more than 9 years. Currently working as an Assistant Professor at RVR and JC College of Engineering (Autonomous) in Department of Computer Science and Business System, Guntur. She had two patents. She attended and presented papers in different conferences, workshops and symposiums. She published various papers in different international and national journals. She can be contacted at email: mahalakshmi.valluri09@gmail.com.






Nitalaksheswara Rao Kolukula    obtained his Ph.D. in Computer Science and Systems Engineering at Andhra University Visakhapatnam India. He received his Master's degree M.Tech in Computer Science and engineering in 2009. Now, he is an Assistant Professor in department of CSE at GITAM University Visakhapatnam Andhra Pradesh India. His current research interest includes AI, machine learning, deep learning software engineering, data engineering, and quality assurance. He can be contacted at email: kolukulanitla@gmail.com.



Jayasree Pinajala    is currently a Research Scholar and Pursuing her Ph.D. at Godavari Global University, Rajamahendravaram. She Completed her B.Tech (Information Technology) in 2011 from VRS and YRN College of Engineering and Technology, Chirala affiliated to JNTU, Kakinada. She completed her M.Tech (Computer Science and Engineering) in 2013 from Narasaraopeta Engineering College affiliated to JNTU, Kakinada. She had Experience in different academic and administrative roles at various academic institutes for more than 7 years. Currently working as an Assistant Professor at Chaitanya Engineering College Visakhapatnam in Department of Computer Science and Engineering. She attended and presented papers in different conferences, workshops and symposiums. She published various papers in different international and national journals. She can be contacted at email: jayasreep4@gmail.com.



James Stephen Meka    is a respected academician, currently serving as the National Chair Professor at the Dr. B.R. Ambedkar Chair, Andhra University, under the Ministry of Social Justice and Empowerment, Government of India. With over 22 years of teaching and research experience, and more than 11 years in administrative roles, he has made significant contributions to the academic and research landscape of the Institutions, he served. During his tenure as the Registrar of Andhra University, his leadership as the Dean of the A.U. Trans-disciplinary Research Hub (TDR-HUB) was marked by his efforts to foster research beyond the confines of the university, extending opportunities to affiliated institutions. He played a pioneering role in establishing standard protocols in line with UGC guidelines, contributing to the research growth of young scholars. He can be contacted at email: jamesstephenm@gmail.com.