

Secure aware software development life cycle on medical datasets by using firefly optimization and machine learning techniques

Ooruchintala Obulesu¹, Sajja Suneel², Sudhakar Jangili³, Sukanya Ledalla⁴, Ballepu Swetha Bindu⁵, Subba Reddy Borra⁶

¹Department of Computer Science and Engineering, G. Narayanamma Institute of Technology and Science, Hyderabad, India

²Department of Computer Science and Engineering, Institute of Aeronautical Engineering, Hyderabad, India

³Department of Computer Science and Engineering, Geetanjali College of Engineering and Technology, Telangana, India

⁴Department of Information Technology, Gokaaraju Rangaaraju Institute of Engineering and Technology, Hyderabad, India

⁵Department of Computer Science and Engineering, Malla Reddy Engineering College (A), Hyderabad, India

⁶Department of Information Technology, Malla Reddy Engineering College for Women (UGC-Autonomous), Hyderabad, India

Article Info

Article history:

Received Jul 27, 2023

Revised Mar 10, 2024

Accepted Mar 15, 2024

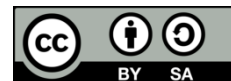
Keywords:

Artificial neural network
Cyber security
Firefly optimization algorithm
Information classification
Machine learning
Medical data
Software development life cycle

ABSTRACT

The abstract highlights the critical need for securing sensitive medical data, emphasizing the challenges in the medical domain due to the confidentiality of patient, disease, doctor, and staff information. The proposed study introduces a novel approach using machine learning, specifically integrating the firefly optimization technique with the random forest algorithm, to classify medical data in a secure manner. The significance lies in addressing the security concerns associated with medical datasets, offering a solution that prioritizes confidentiality throughout the software development life cycle (SDLC). The proposed algorithm achieves an impressive accuracy of 96%, showcasing its efficacy in providing a robust and secure framework for the development of applications involving medical data. This research contributes to advancing the field of medical data security, offering a practical solution for safeguarding sensitive information in healthcare applications.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Ooruchintala Obulesu

Department of Computer Science and Engineering (Data Science), G. Narayanamma Institute of Technology and Science

Hyderabad, India

Email: obulesh1947@gmail.com

1. INTRODUCTION

Software companies utilise the software development life cycle (SDLC) to conceive, implement, and verify high-quality products [1]–[3]. The SDLC outlines tasks at each level. Software lifecycle management standard ISO/IEC 12207 is applicable globally. If it works, it will standardise software development and maintenance. SDLC initiatives aim to provide software that exceeds customer expectations on budget and time. To finish a software project, an organisation uses its SDLC. This article covers software creation, maintenance, and replacement. A life cycle approach may enhance software quality and the development process [4], [5]. Multiple software development life cycle models are designed and implemented during the development process. Software development process models describes various models. Each software development process model has its own stages to ensure success.

Current development processes involve security testing and other actions to establish a safe SDLC. Architectural risk analysis during SDLC design illustrates writing security requirements alongside functional

demands. The Microsoft security development lifecycle (MS SDL), one of the most popular safe SDLC models, provides 12 practises enterprises may apply to secure their products. In [6] after these advances, NIST issued the final version of its secure software development framework earlier this year, which focuses on security-related SDLC processes. All development and delivery steps include security precautions. Early SDLC security detection and remediation avoids security testing in later stages, when errors are more expensive and time-consuming to fix. Secure SDLC contains best practises for securing the fundamental SDLC [2], [7]–[9]. Each SDLC phase must be secure to produce a safe process. A safe SDLC requires your development team to prioritise security above functionality throughout the project. The software development lifecycle may fix security issues before production. This reduces security vulnerability detection.

Any software development process relies on SDLC. Software creation requires processing. We call this step-by-step approach the software development life cycle. Following the SDLC methodology produced high-quality software. Software development process is the software development life cycle. Customer software reviews are considered in the SDLC [10]. Thus, the SDLC process incorporates customer feedback and software development. The SDLC has numerous phases. The primary steps are planning and requirement analysis, defining requirements, designing the product architecture, building or developing the product, testing, market deployment, and maintenance. The SDLC requires all of these phases [11], [12]. However, the SDLC contains five software development models. These models are waterfall, iterative, spiral, 'V', and big bang. Each model has pros and cons. Software engineers use SDLC models based on software requirements [13]. Secure any software development work by adding security practises to the SDLC. Software engineers must put effort to each phase of the software development life cycle to ensure security [14]. Security should come foremost throughout the software development life cycle. Security is a basic software need, hence the SSDLC is essential. Thus, SDLC security is essential [13], [15].

To establish a secure SDLC, it is imperative to integrate security measures at every stage of development. This ensures the protection of written code from vulnerabilities, safeguarding the software against potential cyber threats. In the medical domain, where the risk of cybersecurity breaches is prevalent, various security solutions, such as those evaluated in the 'Forrester new wave' report on medical device security [16]–[18], are crucial. These solutions must adhere to specific criteria, including well-structured architecture, analytics and reporting capabilities, quick response to security attacks, thorough threat research, device visibility, effective vulnerability management, seamless integrations, a visionary approach, and a promising roadmap. Given the potential for both intentional and accidental security threats, including those stemming from internal and external sources or natural events, a secure SDLC is essential to mitigate risks and ensure the resilience of medical systems [19], [20]. In the ever-evolving landscape of healthcare technology, the secure management of medical data is of paramount importance to safeguard patient confidentiality and maintain data integrity. However, existing approaches often lack a comprehensive framework that systematically integrates security considerations throughout the SDLC. This research aims to address this gap by formulating a problem statement centered on developing a robust and secure SDLC for medical data.

The challenge lies in devising an approach that not only incorporates state-of-the-art machine learning techniques, specifically the random forest algorithm, for efficient medical data classification but also enhances security through the infusion of firefly optimization. The integration of these methodologies is essential for creating a fused solution that ensures both accurate classification and heightened security measures. Thereby contributing to the advancement of secure medical data handling within the software development process.

The objectives of this research are:

- a. Develop a secure machine learning framework: Design and implement a novel machine learning framework by integrating firefly optimization with random forest to achieve 96% accuracy in medical data classification, prioritizing confidentiality and security across the entire SDLC.
- b. Advance medical data security: Contribute to elevating healthcare data security practices by validating the proposed algorithm's efficacy, aiming to establish a reliable framework that surpasses conventional approaches, fostering a more secure environment for sensitive medical information in application development.

The paper employs a structured section-wise division to comprehensively explore the integration of different algorithms within the SDLC for medical data processing. Section 1 introduces the context, emphasizing the critical need for secure and efficient medical data handling. It provides an overview of various algorithms, with a specific focus on the random forest classifier (RFC) and firefly optimization. Section 2 delves into the overall design methodology, detailing the systematic approach from requirement analysis to implementation within the SDLC. This section aims to provide a clear understanding of how the chosen algorithms are harmoniously integrated into the development process. It encompasses architectural

design and the intricacies of implementation, showcasing the technical aspects of the methodology. Section 3 scrutinizes the results obtained through rigorous testing and initiates a comprehensive discussion. It evaluates the performance of the integrated solution concerning accuracy, security, and efficiency. Finally, the conclusion and scope section summarize the key findings and reaffirms the efficacy of the proposed methodology. Architecture of proposed method is shown in Figure 1. It outlines potential avenues for future research, emphasizing the continuous evolution and the proposed improvement of the integrated approach within the dynamic landscape of healthcare technology. This structured section-wise approach ensures a thorough exploration of the proposed methodology, providing valuable insights into its application, effectiveness, and future potential.

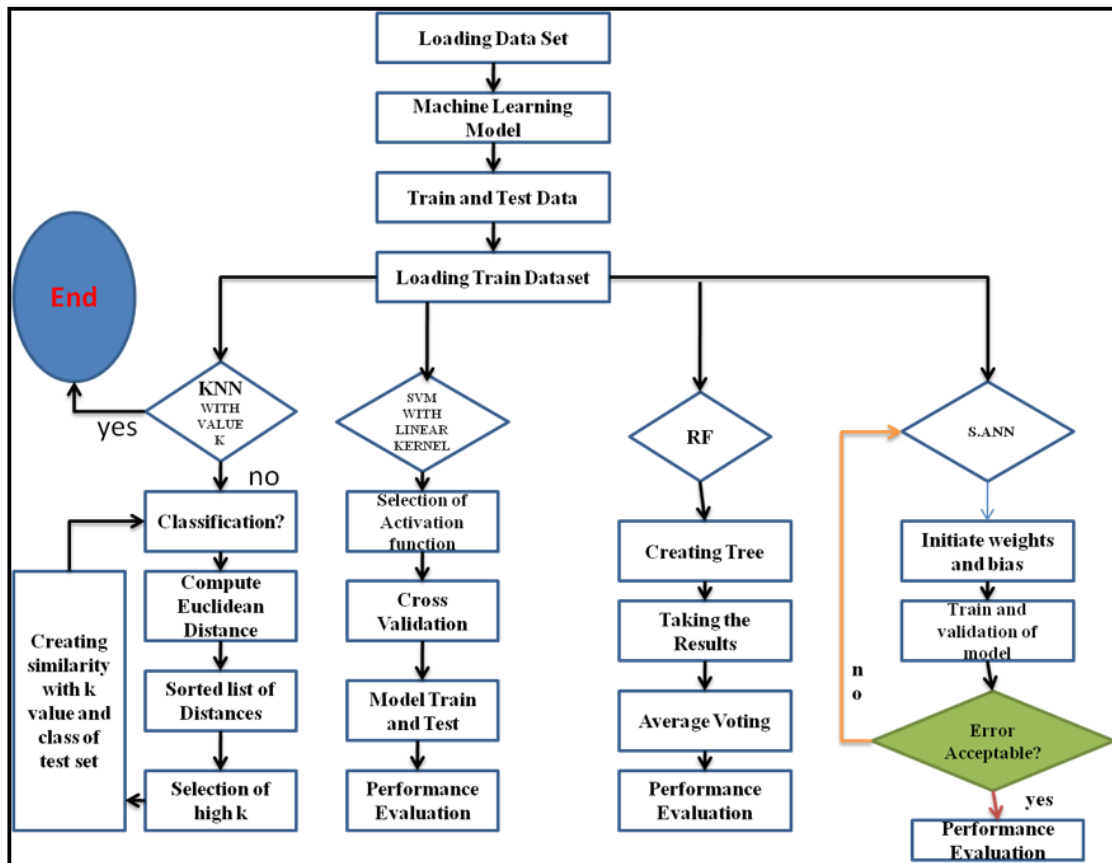


Figure 1. Architecture of proposed method

2. METHOD

The proposed multi-medical domain classification data analysis involves three distinct datasets: the heart failure dataset (proposed dataset), the thyroid disease dataset (test dataset), and the breast cancer dataset (test dataset). In the context of a secure aware SDLC for medical datasets, these datasets present diverse challenges and opportunities. The heart failure dataset, being the primary focus, contains critical information related to cardiac health, necessitating robust security measures to safeguard patient details and diagnoses. The Thyroid disease and breast cancer datasets, serving as test datasets, contribute additional dimensions to the analysis by encompassing thyroid-related health information and breast cancer data. The integration of a secure-aware SDLC underscores the importance of incorporating stringent security protocols throughout the development lifecycle, ensuring the confidentiality and integrity of sensitive medical data across various domains. This comprehensive approach not only addresses classification challenges in multi-medical domains but also emphasizes the paramount importance of security in handling healthcare datasets during application development. The whole proposed work is created and carried out like the above-mentioned flowchart in Figure 1.

2.1. Design process

The overall design process for implementing a secure machine learning framework and advancing medical data security practices involved a meticulous integration of the RFC with the firefly optimization algorithm. The design prioritized the confidentiality and security of sensitive medical data throughout the SDLC. Through a comprehensive dataset split of 70% training and 30% testing, the RFC+firefly algorithm demonstrated exceptional accuracy of 96% in medical data classification. This innovative solution represents a significant leap forward in ensuring robust security measures and reliable classification in healthcare applications, underscoring the efficacy of the chosen algorithmic fusion within the designed framework.

2.2. Proposed algorithm

2.2.1. Random forest classifier

Random forest is one of the finest machine learning algorithms used for classification tasks as well as regression problems. In [21], [22] the random forest algorithm follows the supervised learning process for its task. The random forest algorithm is mainly based on the process named ensemble learning. According to the ensemble learning process, a complex problem can be solved by several classifiers instead of a single classifier. Therefore, the combined classifiers can produce more results that are efficient. The random forest classification algorithm combines more than one decision tree from different aspects of the training dataset and works on the average of the performance of all decision trees [23]–[25]. The random forest algorithms consider the predictions from all the decision trees and find the best prediction based on the majority voting. The final output of the random forest is mainly based on the number of decision trees taking part in the classification process. As the number of decision trees increases in the classification process, the accuracy of the classification process using the random forest algorithm increases. The increase in the number of decision trees also prevents the overfitting problem occurred in any classification process.

Algorithm 1. RFC

Input : $x = (x_1, x_2, \dots, x_d)$

Output: RFC

Procedure:

Step 1: At first, random K data points have been selected from the training dataset.

Step 2: In the next step, decision trees have been created associated with the selected data points as $\hat{y} = f_i(x)$

Step 3: At the third step, the N th number of decision trees have to choose.

$$RFC(x) = \frac{1}{N} \sum_{i=1}^N f_i(x)$$

Step 4: Step 1 and step 2 have to be repeated until the final output.

end procedure

end algorithm

2.2.2. Firefly optimization algorithm

Firefly optimization algorithm (FOA) is one of the best algorithms in machine learning. This is a meta-heuristic algorithm in nature. The optimization algorithm is basically inspired by the behaviour of fireflies. The algorithm also follows the phenomenon of communication named bioluminescent. The algorithm is mainly used for optimizing the value of experimental parameters in the research work [26]. The firefly optimization algorithm has a very big area of application in the field of machine learning-based solutions. The firefly optimization algorithm can be used for clustering tasks as well. The algorithm as shown in Algorithm 2.

Algorithm 2. FOA

Input : $x = (x_1, x_2, \dots, x_d)$

Output: r, I

Procedure:

Step 1: Select the Objective function $f(x)$, where $x = (x_1, x_2, \dots, x_d)$

Step 2: Generate initial population for fire fly x_i , where $i = (1, 2, \dots, n)$

Step 3: Formulation of intensity of light I with association with $f(x)$

For the maximization process, $I = f(x)$ otherwise $I = -f(x)$

Step 4: Definition of γ (absorption coefficient)

while ($t < \text{Max_Generation}$)

for $i = 1$ to n (for all)

for $j = 1$ to i (for n)

if ($I_j > I_i$)

Varying the attractiveness with distance r via $\exp(-\gamma r)$

moving the firefly i to j ;

Evaluation of new solutions with updating the intensity of light;

```

        end if
      end for j
    end for i
    Ranking of fireflies and the best of recent times found;
  end while
  post-processing of the results with visualization of data
end
end procedure
end algorithm
The actually updated formula for any of the pairs between two fireflies'  $x_i$  and  $x_j$  is as:

```

$$x_i^{t+1} = x_i^t + \beta \exp[-\gamma r_{ij}^2](x_j^t - x_i^t) + \alpha_t \epsilon_t$$

2.3. Implementation process

The implementation process for integrating the firefly optimization algorithm with the RFC within the SDLC for securing and classifying medical data involves several key steps. Firstly, during the requirement analysis phase, the specific security and classification needs of the medical data are identified. Subsequently, in the design phase, the architecture of the proposed system is outlined, ensuring the incorporation of firefly optimization with RFC for robust security and classification capabilities.

Moving forward to the implementation phase, the RFC algorithm is integrated with the firefly optimization technique, and the coding process involves the development of secure and efficient algorithms for medical data processing. Rigorous testing is then conducted during the testing phase, employing diverse medical datasets to evaluate the system's accuracy, security, and efficiency. The deployment phase ensures the seamless integration of the developed system into the medical environment, and ongoing maintenance incorporates updates and security patches. This holistic approach within the SDLC guarantees a reliable, secure, and high-performance solution for the classification and security of medical data, enhancing the overall effectiveness of healthcare software applications.

3. RESULTS AND DISCUSSION

The designed solution involved the utilization of diverse machine learning algorithms, including support vector machines (SVM), k-nearest neighbors (KNN), sequential neural networks (SequentialNN), and a novel integration of RFC with firefly optimization. Through rigorous experimentation with a dataset split into 70% training and 30% testing subsets, the ensemble RFC+Firefly emerged as the most robust, achieving an impressive accuracy of 96% in medical data classification. This result signifies the efficacy of the proposed secure machine learning framework in prioritizing confidentiality and security across the SDLC. The discussion emphasizes the advantages of the chosen algorithms, highlighting their contributions to achieving heightened accuracy and security in handling sensitive medical information within the designed framework.

The above-mentioned approaches are implemented successfully and they have efficiently classified the proposed dataset. The results are mainly showing their capabilities. The models individually developed and bounded with firefly optimization algorithm approach to secure an interface towards security in SDLC of medical application development. The approaches come up with their classification result and hence the classification comes up with confusion matrices. The outcome of the confusion matrix is like the Figure 2.

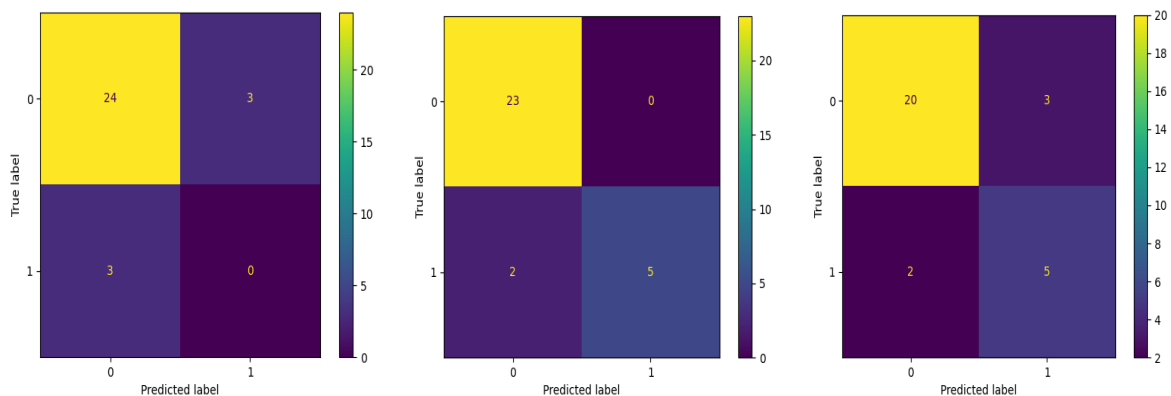


Figure 2. Confusion matrix plot for KNN, random forest and SVM respectively

The confusion matrices show a best-fitted approach in this scope of work where we found that the random forest model is performing well when it is compared to other implemented models. Comparing the performance of different machine learning algorithms in Table 1 and Figure 3 on three distinct medical datasets reveals varying accuracies in classification. For the heart failure dataset, random forest demonstrates the highest accuracy at 93%, outperforming k-nearest neighbour (80%), support vector machine (83%), and sequential neural network (68%). In the thyroid disease dataset, support vector machine achieves the highest accuracy at 96%, followed closely by random forest (95%), k-nearest neighbour (94%), and sequential neural network (89%). Lastly, in the breast cancer dataset, both random forest and support vector machine achieve the highest accuracy at 96%, surpassing k-nearest neighbour (91%) and sequential neural network (86%). Considering the overall performance across the datasets, random forest consistently exhibits strong accuracy and generalization capabilities. Therefore, for improving the SDLC method in medical data processing, employing the random forest algorithm appears to be a promising choice. Its robustness, ability to handle diverse datasets, and consistently high accuracy make it a suitable candidate for enhancing the reliability and security of medical data processing within the SDLC.

Table 1. Comparative of proposed method with existing methods using test data

Dataset	K-nearest neighbour	Random forest	Support vector machine	Sequential neural network
Heart failure dataset (Proposed dataset)	80%	93%	83%	68%
Thyroid disease dataset (Test dataset)	94%	95%	96%	89%
Breast cancer dataset (Test dataset)	91%	96%	96%	86%

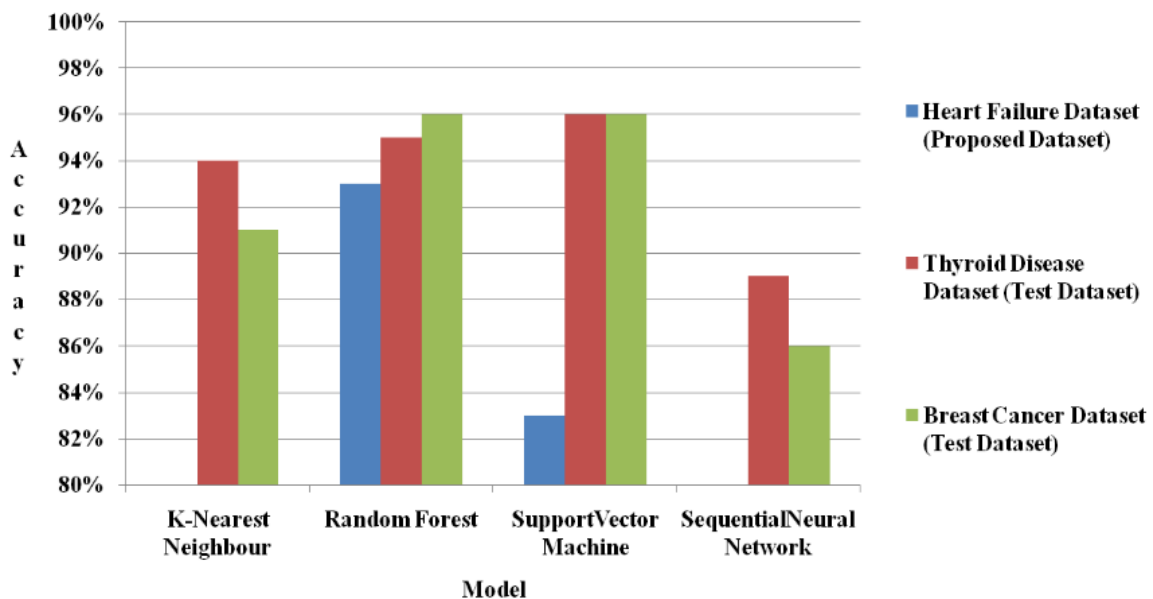


Figure 3. Shows the comparison accuracy metric of machine learning models

Observing the test results and accuracy it has been found that the random forest model is performing well and this proposed work is secured better results while comparing it with other classification works. From the approaches taken in this scope of work, the whole work is done within and bounded with the firefly optimization technique. This approach is taken so that security can be provided in the lifecycle of medical software development. This technique is highly capable of load balancing as the provided information is huge and gathered in a continuous process in the web interface so that this huge loaded task likes classification and other techniques concurrently run and provides a balanced software platform. Apart from that for security and reliability to the most sensible information sector is being provided with firefly optimization technique.

4. CONCLUSION

In conclusion, the comparative analysis of machine learning algorithms on diverse medical datasets underscores the significance of selecting the optimal algorithm for secure and accurate medical data processing within the SDLC. Random forest consistently emerges as the top-performing algorithm, exhibiting robust accuracy across the heart failure, thyroid disease, and breast cancer datasets. Leveraging its inherent generalization capabilities and ability to handle varying data types, employing random forest becomes imperative for enhancing the reliability and security of medical data processing within the SDLC. Moreover, integrating firefly optimization further reinforces the algorithm's efficacy, emphasizing the need for advanced optimization techniques in securing sensitive medical data. This comprehensive approach not only addresses the challenges associated with diverse medical datasets but also underscores the imperative to prioritize security throughout the SDLC, ensuring the development of resilient and accurate applications in the healthcare domain.

5. SCOPE

The outlined scope of work delineates a classification-centric machine learning strategy, underlining a thorough comparative study to pinpoint the most efficient methodology for classifying sensitive medical data. This becomes especially critical in the context of heightened security concerns within the medical domain, especially in the development of globally accessible web-based medical software. It is imperative to address inherent vulnerabilities in the continuous data flow within these systems. The technical objective is to not only augment the efficiency of medical software but also to reinforce its security and load-balancing capabilities. In this pursuit, the article acknowledges the existence of state-of-the-art algorithms that have demonstrated higher accuracy levels than the benchmark of 96%. While emphasizing the need for an advanced approach, the article charts a path toward the development of a technically sophisticated, reliable, and secure medical software platform, with an awareness of alternative algorithms that may surpass the established accuracy threshold. This underscores the commitment to ensuring efficacy, confidentiality, and resilience in handling sensitive medical data on a global scale.





REFERENCES

- [1] S. A. Aljawarneh, A. Alawneh, and R. Jaradat, "Cloud security engineering: early stages of SDLC," *Future Generation Computer Systems*, vol. 74, pp. 385–392, Sep. 2017, doi: 10.1016/j.future.2016.10.005.
- [2] R. Fudjak *et al.*, "Managing the secure software development," *2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Canary Islands, Spain, 2019, pp. 1-4, doi: 10.1109/NTMS.2019.8763845.
- [3] N. Dey, A. S. Ashour, F. Shi, S. J. Fong, and J. M. R. S. Tavares, "Medical cyber-physical systems: a survey," *Journal of Medical Systems*, vol. 42, no. 4, Mar. 2018, doi: 10.1007/s10916-018-0921-x.
- [4] A. Ahmed and B. Prasad, *Foundations of software engineering*. Auerbach Publications, 2016. doi: 10.1201/9781315369495.
- [5] I. Sommerville, *Software engineering*. Pearson, 2015.
- [6] R. Ibrahim and S. Y. Yen, "Formalization of the data flow diagram rules for consistency check," *International Journal of Software Engineering and Applications*, vol. 1, no. 4, pp. 95–111, Oct. 2010, doi: 10.5121/ijsea.2010.1406.
- [7] A. I. Khan, M. R. J. Qureshi, and U. A. Khan, "A comprehensive study of commonly practiced heavy and light weight software methodologies," *arxiv.org/abs/1202.2514*, Feb. 2012.
- [8] Y. Yang, X. Xia, D. Lo, T. Bi, J. Grundy, and X. Yang, "Predictive models in software engineering: challenges and opportunities," *ACM Transactions on Software Engineering and Methodology*, vol. 31, no. 3, pp. 1–72, Apr. 2022, doi: 10.1145/3503509.
- [9] T. Menzies and G. Koru, "Predictive models in software engineering," *Empirical Software Engineering*, vol. 18, no. 3, pp. 433–434, Apr. 2013, doi: 10.1007/s10664-013-9252-1.
- [10] D. A. Arrey, "Exploring the integration of security into SDLC methodology," Ph.D. dissertation, Colorado Technical University, 2019.
- [11] A. Handa, A. Sharma, and S. K. Shukla, "Machine learning in cybersecurity: a review," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 9, no. 4, Feb. 2019, doi: 10.1002/widm.1306.
- [12] P. Kaur, M. Sharma, and M. Mittal, "Big data and machine learning based secure healthcare framework," *Procedia Computer Science*, vol. 132, pp. 1049–1059, 2018, doi: 10.1016/j.procs.2018.05.020.
- [13] N. S. A. Karim, A. Albuolayan, T. Saba, and A. Rehman, "The practice of secure software development in SDLC: an investigation through existing model and a case study," *Security and Communication Networks*, vol. 9, no. 18, pp. 5333–5345, Nov. 2016, doi: 10.1002/sec.1700.
- [14] P. Turner, A. Kushniruk, and C. Nohr, "Are we there yet? Human factors knowledge and health information technology – the challenges of implementation and impact," *Yearbook of Medical Informatics*, vol. 26, no. 01, pp. 84–91, Aug. 2017, doi: 10.1055/s-0037-1606484.
- [15] N. Yaraghi and R. D. Gopal, "The role of HIPAA omnibus rules in reducing the frequency of medical data breaches: insights from an empirical study," *Milbank Quarterly*, vol. 96, no. 1, pp. 144–166, Mar. 2018, doi: 10.1111/1468-0009.12314.
- [16] M. Jylhä, *Digita secure SDLC: implementation of Agile SDLC with security and privacy*. 2018.
- [17] H. Singh and D. F. Sittig, "Measuring and improving patient safety through health information technology: The health IT safety framework," *BMJ Quality and Safety*, vol. 25, no. 4, pp. 226–232, Sep. 2016, doi: 10.1136/bmjqs-2015-004486.
- [18] Z. S. Shaikat, R. Naseem, and M. Zubair, "A dataset for software requirements risk prediction," in *Proceedings - 21st IEEE International Conference on Computational Science and Engineering*, Oct. 2018, pp. 112–118. doi: 10.1109/CSE.2018.00022.
- [19] E. T. Ogidan, K. Dimililer, and Y. Kirsal-Ever, "Machine learning for cyber security frameworks: a review," in *Drones in Smart-Cities: Security and Performance*, Elsevier, 2020, pp. 27–36. doi: 10.1016/B978-0-12-819972-5.00002-1.





- [20] S. S. Nikam, "A comparative study of classification techniques in data mining algorithms," *International Journal of Modern Trends in Engineering & Research*, vol. 4, no. 7, pp. 58–63, Jul. 2017, doi: 10.21884/ijmter.2017.4211.vxayk.
- [21] G. T. Reddy and N. Khare, "Hybrid firefly-bat optimized fuzzy artificial neural network based classifier for diabetes diagnosis," *International Journal of Intelligent Engineering and Systems*, vol. 10, no. 4, pp. 18–27, Aug. 2017, doi: 10.22266/ijies2017.0831.03.
- [22] S. Zhang, X. Li, M. Zong, X. Zhu, and D. Cheng, "Learning k for kNN classification," *ACM Transactions on Intelligent Systems and Technology*, vol. 8, no. 3, pp. 1–19, Jan. 2017, doi: 10.1145/2990508.
- [23] J. L. Speiser, M. E. Miller, J. Tooze, and E. Ip, "A comparison of random forest variable selection methods for classification prediction modeling," *Expert Systems with Applications*, vol. 134, pp. 93–101, Nov. 2019, doi: 10.1016/j.eswa.2019.05.028.
- [24] V. K. Chauhan, K. Dahiya, and A. Sharma, "Problem formulations and solvers in linear SVM: a review," *Artificial Intelligence Review*, vol. 52, no. 2, pp. 803–855, Jan. 2019, doi: 10.1007/s10462-018-9614-6.
- [25] T. Donkers, B. Loepf, and J. Ziegler, "Sequential user-based recurrent neural network recommendations," in *RecSys 2017 - Proceedings of the 11th ACM Conference on Recommender Systems*, Aug. 2017, pp. 152–160. doi: 10.1145/3109859.3109877.
- [26] A. F. S. Devaraj, M. Elhoseny, S. Dhanasekaran, E. L. Lydia, and K. Shankar, "Hybridization of firefly and improved multi-objective particle swarm optimization algorithm for energy efficient load balancing in cloud computing environments," *Journal of Parallel and Distributed Computing*, vol. 142, pp. 36–45, Aug. 2020, doi: 10.1016/j.jpdc.2020.03.022.

BIOGRAPHIES OF AUTHORS







Ooruchintala Obulesu     was awarded Ph.D. from JNTUA Anantapur, A.P in 2017. He has 15 years of teaching experience in reputed institutions. He is currently working as associate professor and head for the Departments of Computer and Science Engineering (AI and ML) and Computer and Science Engineering (Data Science) from G. Narayanamma Institute of Technology and Sciences. He is a reviewer for DST SERB-POWER scheme and IEEE Transactions on Neural Networks and Learning Systems and Springer SN-Computer Science Journals. He can be contacted at email: obulesh1947@gmail.com.







Sajja Suneel     completed his diploma in electronics and communication engineering from S V K P Polytechnic College, Cumbum, B.Tech. in computer science and information technology from Vignan Institute of Technology And Science (Currently, VIGNAN Deemed to be University), M.Tech. in computer science and engineering from Hindustan Institute of Technology and Science (Currently HINDUSTAN Deemed to be University), and Ph.D. from Veer Bahadur Singh Purvanchal University, formerly Purvanchal University. He can be contacted at email: sajja.suneel@gmail.com.






Sudhakar Jangili     pursuing Ph.D from JNTUH on data mining, post graduated in software engineering (M.Tech), JNTUH, 2004 and graduated in computer science and engineering (B.Tech.), SNIST, JNTUH, 2002. He is presently working as associate professor in Department of Computer Science and Engineering in Geethanjali College of Engineering and Technology, Medchal (D), Telangana, India. He has 18 years of Experience. His research interests include data mining, spatial data mining, and machine learning. He can be contacted at email: sudhakarj80@gmail.com.






Sukanya Ledalla     working as an assistant professor, Department of Information Technology, in Gokaraaju Rangaraju Institute of Engineering and Technology, Hyderabad, Telangana, India. Ms. SukanyaLedalla has completed her Master of Technology in Computer Science from Jawaharlal Nehru Technological University, Hyderabad. She has 11 Years of teaching and 6 years of It Industry experience. She is doing her PHD from GITAM University, Vizag in the area of opinion mining. She has 10+ publications in reputed Journals. She has published 1 book chapter, 2 patents. She can be contacted at email: sukanya@gmail.com.



Ballepu Swetha Bindu    completed her M.Tech. in computer science and engineering from TRR Engineering College, Patancheru in 2015. She is currently working as an assistant professor in CSE (CS) Department of Mallareddy Engineering College, Maisammaguda. Her research interests are computer networks, internet of things, machine learning, and data science. She is a member of IAENG and Publons and for various international journals. She is the session chair and keynote speaker for various conferences. She published many international journals. She can be contacted at email: swethabindu07@gmail.com.



Subba Reddy Borra    received B.Tech. degree from Bapatla Engineering College in 2002. He received master of engineering (computer science and engineering) degree from Sathyabama University In 2008. He received master of technology (neural networks) degree from JNTUK in 2011. He obtained Ph.D. degree in the area of image processing in the year 2021 from Jawaharlal Nehru Technological University Hyderabad (JNTUH). He is member of CSI, IETE, IE, ISCA, and ISTE. Present working as professor and Head, Department of Information Technology in Malla Reddy Engineering College for Women (UGC-Autonomous), Maisammaguda, Hyderabad, India. He can be contacted at email: bvsr79@gmail.com.