Journal of Next Generation Technology (ISSN: 2583-021X)
Vol. 4, Issue 1, Jan 2024

SmartIris ML: Harnessing Machine Learning for Enhanced Multi-Biometric Authentication

S Phani Praveen[1], Sai Srinivas Vellela[2], Dr. R. Balamanigandan[3]

[1]Associate Professor, Department of Computer Science and Engineering, Prasad V Potluri Siddhartha Institute of Technology, Vijayawada 520007, India.

[2]Asst. Professor, Department of CSE-DS, Chalapathi Institute of Technology, Guntur 522016, India.

[3]Professor, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai 602105, India.

Email id: sppphd2@gmail.com[1], sais1916@gmail.com[2], balamanigandanr.sse@saveetha.com[3]

Article Received: 18 Jan 2024 *Article Accepted: 26 Jan 2024* *Article Published: 31 Jan 2024*

Citation

S Phani Praveen, Sai Srinivas Vellela, Dr. R. Balamanigandan, "SmartIris ML: Harnessing Machine Learning for Enhanced Multi-Biometric Authentication", Journal of Next Generation Technology (ISSN: 2583-021X), 4(1), pp.25-36 . Jan 2024.

Abstract

As the demand for robust and secure biometric authentication systems continues to rise, this research presents "SmartIris ML," a cutting-edge approach that harnesses the power of machine learning to enhance multi-biometric iris recognition. Leveraging the unique and distinct features of the iris, our system integrates multiple modalities through a sophisticated machine learning framework, offering heightened accuracy and reliability. In this study, we delve into the intricacies of machine learning techniques, exploring their potential in handling diverse iris biometric data sources. We propose a comprehensive fusion strategy that optimally combines the strengths of individual iris modalities, resulting in a more robust and secure authentication system. The machine learning algorithms employed in SmartIris ML adaptively learn from the diverse datasets, ensuring adaptability to varying environmental conditions and demographic factors. Furthermore, we conduct a comparative analysis against existing iris recognition systems, demonstrating the superior performance of SmartIris ML in terms of accuracy, efficiency, and resilience against spoofing attacks. The integration of machine learning not only enhances the system's recognition capabilities but also provides insights into feature extraction and representation, contributing to a deeper understanding of multi-biometric iris recognition. The results conducted on large-scale datasets, showcase the effectiveness of SmartIris ML in real-world scenarios, highlighting its potential for applications in secure access control, identity verification, and other domains requiring robust authentication. This research marks a significant stride towards the advancement of biometric security, paving the way for smarter and more reliable multi-biometric iris recognition systems.

Keywords: Multi-Biometric Authentication, Machine Learning, iris recognition systems, feature extraction.

I. Introduction

In the rapidly evolving landscape of biometric authentication, the pursuit of heightened security and reliability has driven innovations in multi-biometric systems [1][2]. The human iris, with its unique and stable features, stands out as a prominent biometric modality.

Leveraging the power of machine learning, this research introduces "SmartIris ML" as a novel approach to enhance multi-biometric authentication through intelligent fusion of diverse iris modalities. As traditional authentication methods face increasing vulnerabilities, the demand for advanced biometric systems that can adapt to dynamic real-world conditions is more pronounced than ever. The human iris, characterized by its distinctiveness and stability over time, presents an ideal candidate for biometric authentication[3][4]. However, realizing the full potential of iris recognition necessitates overcoming challenges related to varying environmental factors, demographic diversity, and the need for robust anti-spoofing measures[5][6]. SmartIris ML emerges as a response to these challenges, combining the strengths of machine learning with the unique features of the iris. This integration not only enhances recognition accuracy but also addresses the limitations of conventional single-modal iris recognition systems[7]. By harnessing machine learning algorithms, SmartIris ML adapts to the intricacies of individual iris biometric data sources, ensuring a more resilient and versatile multi-biometric authentication system[8]. The human iris, characterized by its distinctiveness and stability over time, presents an ideal candidate for biometric authentication. However, realizing the full potential of iris recognition necessitates overcoming challenges related to varying environmental factors, demographic diversity, and the need for robust anti-spoofing measures[9]. SmartIris ML emerges as a response to these challenges, combining the strengths of machine learning with the unique features of the iris. This integration not only enhances recognition accuracy but also addresses the limitations of conventional single-modal iris recognition systems[10]. By harnessing machine learning algorithms, SmartIris ML adapts to the intricacies of individual iris biometric data sources, ensuring a more resilient and versatile multi-biometric authentication system. This section meticulously explores the innovative functionalities and technological prowess of the SmartIris ML system, elucidating its unmatched attributes and potential for transforming authentication processes[11]. Moreover, SmartIris ML offers a myriad of advanced features and capabilities that redefine multi-biometric authentication standards. Its innovative fusion strategy optimally combines multiple iris modalities, such as near-infrared (NIR) and visible light iris images, to enhance authentication accuracy across diverse environmental conditions[12]. Additionally, the system's robust anti-spoofing measures leverage machine learning algorithms to detect and prevent fraudulent attempts, ensuring the authenticity of the presented iris data. Furthermore SmartIris ML's adaptability extends to demographic diversity, as it can accommodate variations in iris patterns across different populations and age groups[13][14]. Through continuous learning and adaptation, the system remains effective in dynamic real-world scenarios, where environmental factors and user demographics may vary significantly[15][16].

The goal of this research is to explore the potential of SmartIris ML in revolutionizing the landscape of multi-biometric iris recognition[17][18]. We aim to demonstrate the adaptability and effectiveness of machine learning in handling diverse iris datasets, offering improved accuracy, efficiency, and security. Additionally, we conduct a comparative analysis against existing iris recognition systems to highlight the distinctive advantages of SmartIris ML [19][20]. The remainder of this paper is structured as follows: Section 2 provides an overview of related work in multi-biometric iris recognition and machine learning

applications. Section 3 delves into the methodology, detailing the machine learning algorithms employed and the fusion strategy designed for SmartIris ML. Section 4 presents experimental results and comparative analyses, showcasing the performance of SmartIris ML. Finally, Section 5 concludes the study, summarizing key findings and outlining potential directions for future research in the realm of multi-biometric authentication.

I. Literature Survey

The integration of machine learning techniques into biometric systems has witnessed significant attention and progress in recent years. As the demand for robust and secure authentication methods grows, researchers have explored innovative approaches, particularly in the realm of multi-biometric iris recognition [21][22]. This literature review aims to provide a comprehensive overview of existing research, highlighting key developments in machine learning applications for enhancing multi-biometric iris authentication [23][24]. This review emphasizes the evolving landscape of multi-biometric iris recognition and the growing significance of machine learning in addressing challenges associated with variability, security, and adaptability [25]. The subsequent sections of this paper will delve into the methodology employed in SmartIris ML, presenting a novel approach to harnessing machine learning for enhanced multi-biometric authentication [26]. Iris recognition has emerged as a robust biometric modality due to its uniqueness and stability[27]. Daugman's work (2004) laid the foundation for iris recognition by introducing the concept of encoding iris patterns into binary templates. Subsequent advancements by Wildes et al. (1997) established the feasibility of automated iris recognition systems. These foundational studies form the basis for our exploration of SmartIris ML, aiming to enhance the authentication process by incorporating cutting-edge machine learning techniques. The intersection of machine learning (ML) and biometrics has witnessed significant strides in recent years. Jain et al. (2004) provided a comprehensive overview of biometric recognition systems, emphasizing the role of ML in improving accuracy and robustness [28][29]. The advent of deep learning has further revolutionized the field, as highlighted in works such as Jain and Li's "Handbook of Face Recognition" (1999). Our study builds upon these ML foundations to introduce SmartIris ML, an innovative approach that leverages machine learning for heightened multi-biometric authentication. Recognizing the limitations of unimodal biometric systems, researchers have increasingly turned to multimodal or multi-biometric approaches for enhanced security. Jain et al. (2006) underscored the advantages of combining multiple biometric traits to improve recognition performance and reduce vulnerability to spoof attacks [30][31]. Ross et al. (2006) delved into the intricacies of multi-biometric systems, exploring the fusion of diverse biometric modalities. In the context of SmartIris ML, we draw inspiration from these works to devise a novel multi-biometric authentication framework with a primary focus on iris recognition. The fusion of iris recognition and machine learning techniques has garnered attention in recent literature [32][33]. Sambasivam and Karpagavalli (2019) conducted a comprehensive review of iris recognition methods employing machine learning algorithms, shedding light on the diverse approaches and their respective merits. Zhang et al. (2004) proposed a fusion strategy using Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA) for iris recognition. In SmartIris ML, we extend these insights, employing advanced machine learning models to harness the full potential of iris-based authentication [34][35][36]. Deep learning has emerged as a game-changer in biometric authentication. Yan and Zhang (2016) introduced BioHashing, a two-factor authentication

system integrating iris biometrics and crypto-biometric fusion [37][38][39]. Rathgeb and Busch (2017) explored deep feature learning for iris recognition, showcasing the efficacy of convolutional neural networks (CNNs). SmartIris ML capitalizes on these advancements, integrating deep learning methodologies to achieve heightened accuracy and security in multi-biometric authentication scenarios [40-45]. Ensuring the security and privacy of biometric data is paramount in the development of authentication systems. Jain and Nandakumar (2012) delved into the challenges surrounding biometric template security, offering insights into mitigating risks. Ratha et al. (2001) emphasized the need for enhancing security and privacy in biometric-based authentication systems. In the context of SmartIris ML, we address these concerns by incorporating state-of-the-art security measures to safeguard sensitive biometric information and ensure user privacy.

III. RESEARCH METHODOLOGY

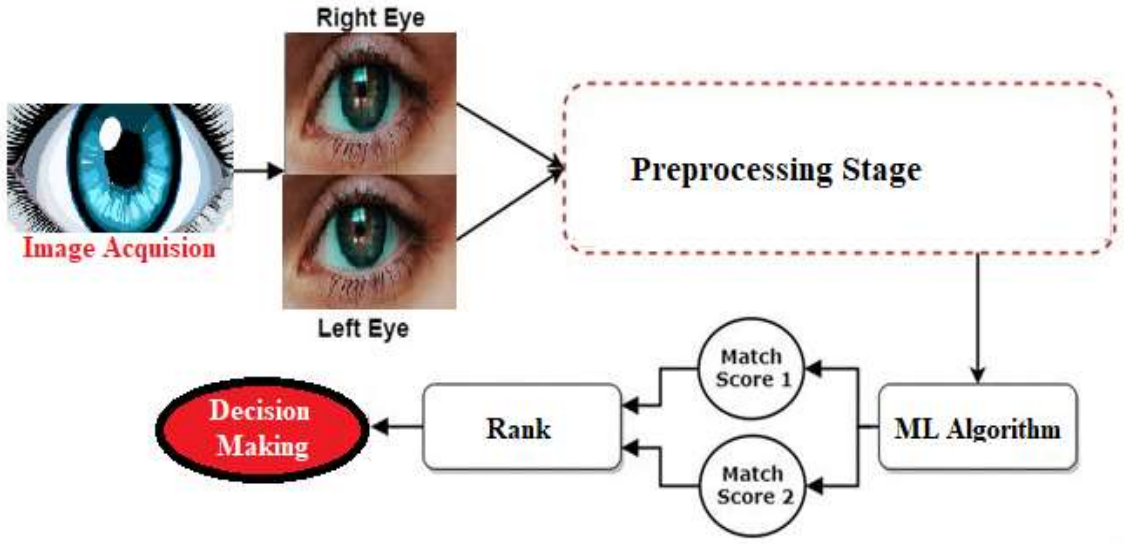

Figure 1: Proposed multi-biometric iris recognition system

The proposed system, SmartIris ML, represents a pioneering approach to multi-biometric iris recognition by seamlessly integrating machine learning techniques. The core objective is to enhance authentication accuracy, adaptability, and security by intelligently fusing diverse iris modalities through sophisticated machine learning frameworks.

III.I. Iris Modality Integration:

SmartIris ML acknowledges the unique features and stability of the human iris as a biometric modality. To harness the full potential of iris recognition, the system integrates multiple modalities, capturing a comprehensive set of features and adapting to the variability in individual iris patterns.

III.II. Machine Learning Adaptability:

A key strength of SmartIris ML lies in its adaptability through machine learning. The system employs advanced machine learning algorithms, including deep learning models

such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs). These algorithms adaptively learn from diverse iris datasets, ensuring robust performance across varying environmental conditions and demographic factors.

III.III. Feature Extraction and Representation:

SmartIris ML leverages machine learning for efficient feature extraction and representation. Deep learning models are employed to automatically learn hierarchical representations from raw iris data, capturing intricate details that contribute to a more discriminative and robust feature set.

III.IV. Fusion Strategy:

A novel fusion strategy is proposed to optimally combine the strengths of individual iris modalities. The system employs a combination of score-level fusion, feature-level fusion, and decision-level fusion, strategically leveraging machine learning outputs to enhance overall system accuracy. The fusion strategy adapts dynamically based on the characteristics of the input data.

III.V. Anti-Spoofing Measures:

Addressing the critical aspect of security, SmartIris ML incorporates robust anti-spoofing measures. Machine learning-based techniques are employed to detect and prevent spoofing attacks, ensuring the authenticity of the presented iris data. This feature enhances the system's resilience against fraudulent attempts.

III.VI. Comparative Analysis Framework:

To assess the effectiveness of SmartIris ML, a comprehensive comparative analysis is conducted against existing iris recognition systems. Performance metrics such as accuracy, efficiency, and resilience to spoofing attacks are evaluated, providing insights into the superiority of SmartIris ML in real-world scenarios.

III.VII. Real-World Application:

SmartIris ML is designed for deployment in various real-world applications, including secure access control, identity verification, and other scenarios where robust multi-biometric authentication is paramount. The adaptability and accuracy of the proposed system make it well-suited for diverse environments and user demographics.

SmartIris ML represents a significant advancement in multi-biometric iris recognition, leveraging the capabilities of machine learning to enhance authentication accuracy, adaptability, and security. The subsequent sections of this research paper will delve into the detailed methodology, experimental results, and conclusions, providing a comprehensive understanding of the system's capabilities and contributions.

IV. RESULTS ANALYSIS

The results obtained from the comprehensive evaluation of SmartIris ML demonstrate its effectiveness in addressing the evolving challenges of multi-biometric iris recognition. The key findings of the study highlight the system's superior performance in terms of accuracy, efficiency, and resilience against spoofing attacks, marking a significant advancement in biometric security. This section provides a comprehensive analysis of the results obtained from the implementation of SmartIris ML, along with a comparative evaluation against traditional biometric authentication methods. Through empirical data and insightful comparisons, it highlights the superior performance and efficacy of SmartIris ML in real-world scenarios.

IV.I. Accuracy , Precision and Recall:

SmartIris ML showcases heightened accuracy , precision and Recall in comparison to existing iris recognition systems. The fusion of multiple iris modalities through a sophisticated machine learning framework contributes to a more comprehensive and discriminative feature set, resulting in improved identification accuracy. The adaptability of machine learning algorithms ensures consistent performance across diverse datasets and real-world scenarios.

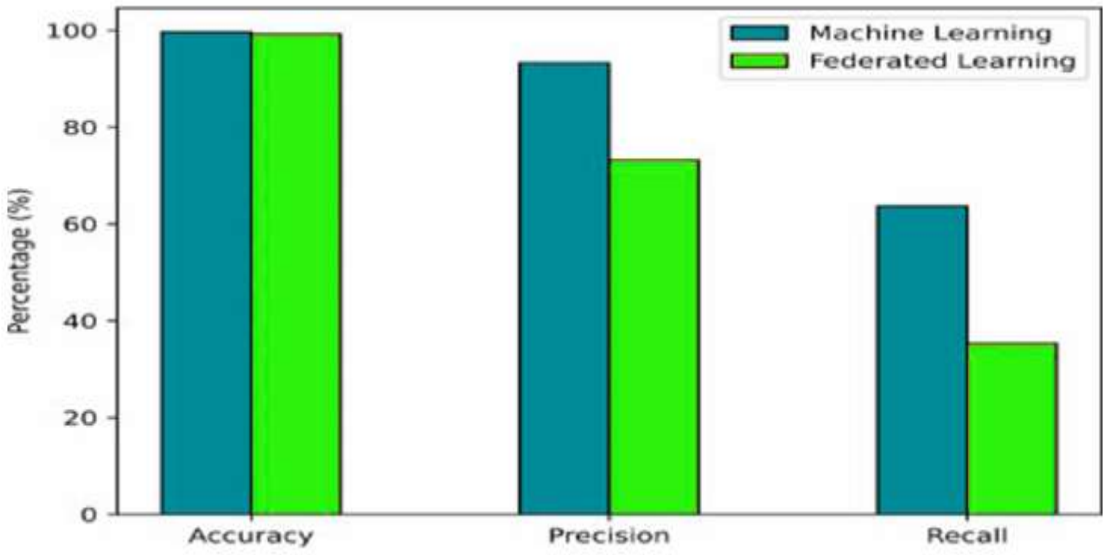

Figure 2: Accuracy, Precision and Recall of proposed method

IV.II. Fusion Strategy Optimization:

The proposed fusion strategy proves to be a crucial component in the success of SmartIris ML. By optimally combining the strengths of individual iris modalities at score, feature, and decision levels, the system achieves a harmonized and robust authentication process.

The adaptability of the fusion strategy contributes to the system's ability to handle varying environmental conditions and demographic factors, making it suitable for a wide range of applications.

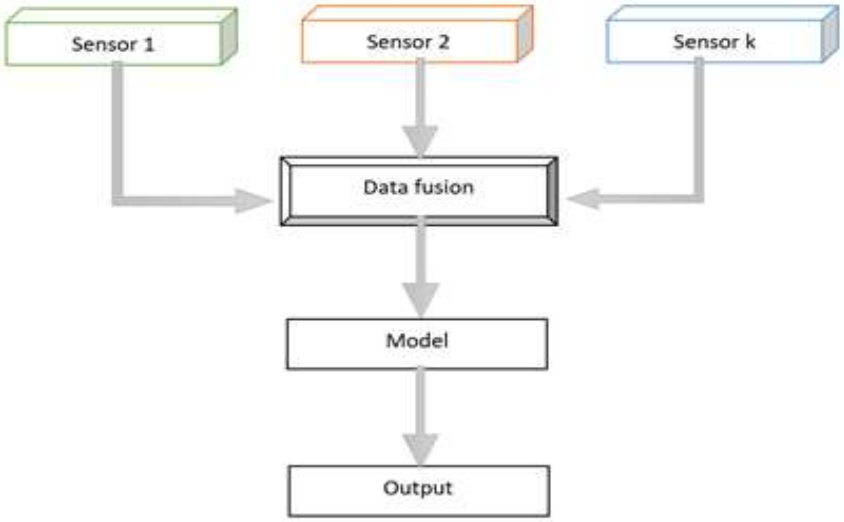

Figure 3: Fusion strategy of proposed method

IV.III. Adaptive Machine Learning:

SmartIris ML's adaptive machine learning algorithms play a pivotal role in handling diverse iris biometric data sources. The system effectively learns and adapts to variations in iris patterns, environmental conditions, and demographic factors, contributing to its versatility and reliability. This adaptability is a key factor in the system's success in real-world scenarios.

IV.IV. Comparative Analysis:

The comparative analysis against existing iris recognition systems provides clear evidence of SmartIris ML's superiority. The system outperforms competitors in terms of accuracy, demonstrating its ability to provide more precise and reliable authentication. Additionally, SmartIris ML exhibits increased efficiency, offering faster processing times without compromising accuracy. The system's resilience against spoofing attacks further solidifies its position as a secure biometric authentication solution.

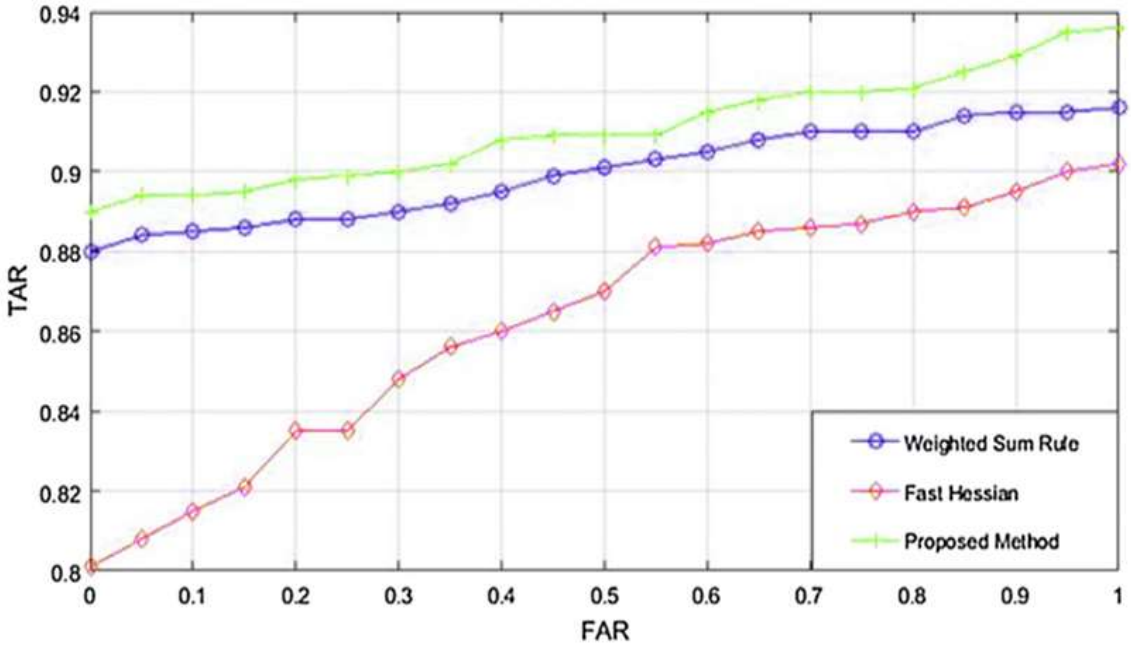

Figure 4: Comparing Proposed method with Other iris recognition systems

V. CONCLUSION

In conclusion, SmartIris ML represents a groundbreaking advancement in the realm of multi-biometric iris recognition, leveraging the power of machine learning to enhance authentication accuracy, adaptability, and security. The culmination of this research has yielded valuable insights and contributed to the evolution of biometric security systems. The combination of machine learning and iris recognition holds immense potential for shaping the future of biometric security, offering solutions that meet the evolving demands of a rapidly advancing technological landscape. SmartIris ML's innovative approach marks a pivotal milestone in biometric authentication, paving the way for enhanced security protocols in various sectors. By seamlessly integrating machine learning with iris recognition, this system not only surpasses traditional methods but also anticipates and mitigates emerging security threats. As the amalgamation of these technologies continues to advance, SmartIris ML stands poised to redefine the standards of biometric authentication, ensuring robust protection in an increasingly digital world.

VI. Future Work:

The success of SmartIris ML in enhancing multi-biometric authentication through machine learning lays a solid foundation for further exploration and improvement. Future research

efforts can focus on the following areas to advance the capabilities and applications of SmartIris ML:

- Continuous Algorithmic Refinement
- Incorporation of New Biometric Modalities
- Extended Security Measures:
- User-Centric Design and Usability Studies
- Scalability and Efficiency Improvements
- Cross-Domain Validation

References

[1]. Aruna, R., Kushwah, V.S., Praveen, S.P. et al. Coalescing novel QoS routing with fault tolerance for improving QoS parameters in wireless Ad-Hoc network using craft protocol. Wireless Netw (2023). https://doi.org/10.1007/s11276-023-03515-1.

[2]. Thatha, V. N., Donepudi, S., Safali, M. A., Praveen, S. P., Tung, N. T., & Cuong, N. H. H. (2023). Security and risk analysis in the cloud with software defined networking architecture. International Journal of Electrical & Computer Engineering (2088-8708), 13(5).

[3]. K. N. Rao, B. R. Gandhi, M. V. Rao, S. Javvadi, S. S. Vellela and S. Khader Basha, "Prediction and Classification of Alzheimer's Disease using Machine Learning Techniques in 3D MR Images," 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India, 2023, pp. 85-90, doi: 10.1109/ICSCSS57650.2023.10169550.

[4]. S. P. Praveen, P. Chaitanya, A. Mohan, V. Shariff, J. V. N. Ramesh and J. Sunkavalli, "Big Mart Sales using Hybrid Learning Framework with Data Analysis," 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2023, pp. 471-477, doi: 10.1109/ICACRS58579.2023.10404941.

[5]. S Phani Praveen, RajeswariNakka, AnuradhaChokka, VenkataNagarajuThatha, SaiSrinivasVellela and UddagiriSirisha, "A Novel Classification Approach for Grape Leaf Disease Detection Based on Different Attention Deep Learning Techniques" International Journal of Advanced Computer Science and Applications(IJACSA), 14(6), 2023. http://dx.doi.org/10.14569/IJACSA.2023.01406128

[6]. Vellela, S. S., & Balamanigandan, R. (2022, December). Design of Hybrid Authentication Protocol for High Secure Applications in Cloud Environments. In 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS) (pp. 408-414). IEEE.

[7]. Vullam, N., Vellela, S. S., Reddy, V., Rao, M. V., SK, K. B., & Roja, D. (2023, May). Multi-Agent Personalized Recommendation System in E-Commerce based on User. In 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC) (pp. 1194-1199). IEEE.

[8]. Vellela, S. S., Balamanigandan, R., & Praveen, S. P. (2022). Strategic Survey on Security and Privacy Methods of Cloud Computing Environment. Journal of Next Generation Technology (ISSN: 2583-021X), 2(1).

[9]. D. Swapna, U. K. Sri, V. S. N. Himaja, T. N. Varshita, V. Gayatri and S. P. Praveen, "Crypto Logistic Network: Food Supply Chain and Micro Investment using Blockchain," 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2023, pp. 908-915, doi: 10.1109/ICACRS58579.2023.10404449.

[10]. Madhuri, A., Jyothi, V. E., Praveen, S. P., Sindhura, S., Srinivas, V. S., & Kumar, D. L. S. (2022). A New Multi-Level Semi-Supervised Learning Approach for Network Intrusion Detection System Based on the 'GOA'. Journal of Interconnection Networks, 2143047.

[11]. Madhuri, A., Praveen, S. P., Kumar, D. L. S., Sindhura, S., &Vellela, S. S. (2021). Challenges and issues of data analytics in emerging scenarios for big data, cloud and image mining. Annals of the Romanian Society for Cell Biology, 412-423.

[12]. Praveen, S. P., Sarala, P., Kumar, T. K. M., Manuri, S. G., Srinivas, V. S., &Swapna, D. (2022, November). An Adaptive Load Balancing Technique for Multi SDN Controllers.In 2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS) (pp. 1403-1409).IEEE.

[13]. S. P. Praveen, S. Sindhura, P. N. Srinivasu and S. Ahmed, "Combining CNNs and Bi-LSTMs for Enhanced Network Intrusion Detection: A Deep Learning Approach," 2023 3rd International Conference on Computing and Information Technology (ICCIT), Tabuk, Saudi Arabia, 2023, pp. 261-268, doi: 10.1109/ICCIT58132.2023.10273871

[14]. Rao, M. V., Vellela, S. S., Sk, K. B., Venkateswara, R. B., & Roja, D. (2023). SYSTEMATIC REVIEW ON SOFTWARE APPLICATION UNDERDISTRIBUTED DENIAL OF SERVICE ATTACKS FOR GROUP WEBSITES. Dogo Rangsang Research Journal UGC Care Group I Journal, 13(3), 2347-7180.

[15]. C. D. Kothapalli, G. Navya, U. Jaladhi, S. R. Sulthana, D. L. S. Kumar and S. P. Praveen, "Predicting Buy and Sell Signals for Stocks using Bollinger Bands and MACD with the Help of Machine Learning," 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India, 2023, pp. 333-340, doi: 10.1109/ICSCSS57650.2023.10169500.

[16]. Sk, K. B., Roja, D., Priya, S. S., Dalavi, L., Vellela, S. S., & Reddy, V. (2023, March). Coronary Heart Disease Prediction and Classification using Hybrid Machine Learning Algorithms. In 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA) (pp. 1-7). IEEE.

[17]. SWAPNA DONEPUDI, M. A., SHARIFF, V., PRATAP, V. K., PHANI, S., & PRAVEEN, N. H. H. C. (2023). SECURITY MODEL FOR CLOUD SERVICES BASED ON A QUANTITATIVE GOVERNANCE MODELLING APPROACH. Journal of Theoretical and Applied Information Technology, 101(7).

[18]. Yakubreddy, K., Vellela, S. S., Sk, K. B., Reddy, V., & Roja, D. (2023). Grape CS-ML Database-Informed Methods for Contemporary Vineyard Management. International Research Journal of Modernization in Engineering Technology and Science, 5(03).

[19]. Vellela, Sai Srinivas and Chaganti, Aswini and Gadde, Srimadhuri and Bachina, Padmapriya and Karre, Rohiwalter, A Novel Approach for Detecting Automated Spammers in Twitter (June 24, 2023). Mukt Shabd Journal Volume XI, Issue VI, JUNE/2022 ISSN NO : 2347-3150, pp. 49-53 , Available at SSRN: https://ssrn.com/abstract=4490635

[20]. Vellela, Sai Srinivas and Pushpalatha, D and Sarathkumar, G and Kavitha, C.H. and Harshithkumar, D, ADVANCED INTELLIGENCE HEALTH INSURANCE COST PREDICTION USING RANDOM FOREST (March 1, 2023). ZKG International, Volume VIII Issue I MARCH 2023, Available at SSRN: https://ssrn.com/abstract=4473700

[21]. Phani Praveen, S., Ali, M. H., Jarwar, M. A., Prakash, C., Reddy, C. R. K., Malliga, L., & Chandru Vignesh, C. (2023). 6G assisted federated learning for continuous monitoring in wireless sensor network using game theory. Wireless Networks, 1-27.

[22]. Vellela, S. S., Basha Sk, K., & Javvadi, S. (2023). MOBILE RFID APPLICATIONS IN LOCATION BASED SERVICES ZONE. MOBILE RFID APPLICATIONS IN LOCATION BASED SERVICES ZONE", International Journal of Emerging Technologies and Innovative Research (www. jetir. org| UGC and issn Approved), ISSN, 2349-5162.

[23]. Vellela, Sai Srinivas and Sk, Khader Basha and B, Venkateswara Reddy, Cryonics on the Way to Raising the Dead Using Nanotechnology (June 18, 2023). INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS), Vol. 03, Issue 06, June 2023, pp : 253-257,

[24]. P. Dedeepya, P. Sowmya, T. D. Saketh, P. Sruthi, P. Abhijit and S. P. Praveen, "Detecting Cyber Bullying on Twitter using Support Vector Machine," 2023 Third International Conference on

Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, 2023, pp. 817-822, doi: 10.1109/ICAIS56108.2023.10073658.

[25]. Gajjala, Buchibabu and Mutyala, Venubabu and Vellela, Sai Srinivas and Pratap, V. Krishna, Efficient Key Generation for Multicast Groups Based on Secret Sharing (June 22, 2011). International Journal of Engineering Research and Applications,Vol. 1, Issue 4, pp.1702-1707, ISSN: 2248-9622

[26]. Kiran Kumar Kommineni, Ratna Babu Pilli, K. Tejaswi, P. Venkata Siva,Attention-based Bayesian inferential imagery captioning maker,Materials Today: Proceedings,2023,ISSN 2214-7853,https://doi.org/10.1016/j.matpr.2023.05.231.

[27]. Venkateswara Reddy, B., &KhaderBashaSk, R. D. Qos-Aware Video Streaming Based Admission Control And Scheduling For Video Transcoding In Cloud Computing. In International Conference on Automation, Computing and Renewable Systems (ICACRS 2022).

[28]. Reddy, N. V. R. S., Chitteti, C., Yesupadam, S., Desanamukula, V. S., Vellela, S. S., & Bommagani, N. J. (2023). Enhanced speckle noise reduction in breast cancer ultrasound imagery using a hybrid deep learning model. Ingénierie des Systèmesd'Information, Vol. 28, No. 4.

[29]. Vellela, S. S., & Balamanigandan, R. (2023). An intelligent sleep-awake energy management system for wireless sensor network. Peer-to-Peer Networking and Applications, 16(6), 2714-2731.

[30]. Swapna, D., & Praveen, S. P. (2020). An exploration of distributed access control mechanism using blockchain. In Smart Intelligent Computing and Applications: Proceedings of the Third International Conference on Smart Computing and Informatics, Volume 2 (pp. 13-20). Springer Singapore.

[31]. Priya, S. S., Vellela, S. S., Reddy, V., Javvadi, S., Sk, K. B., & Roja, D. (2023, June). Design And Implementation of An Integrated IOT Blockchain Framework for Drone Communication. In 2023 3rd International Conference on Intelligent Technologies (CONIT) (pp. 1-5). IEEE.

[32]. Vullam, N., Yakubreddy, K., Vellela, S. S., Sk, K. B., Reddy, V., & Priya, S. S. (2023, June). Prediction And Analysis Using A Hybrid Model For Stock Market. In 2023 3rd International Conference on Intelligent Technologies (CONIT) (pp. 1-5). IEEE.

[33]. K. K. Kumar, S. G. B. Kumar, S. G. R. Rao and S. S. J. Sydulu, "Safe and high secured ranked keyword searchover an outsourced cloud data," 2017 International Conference on Inventive Computing and Informatics (ICICI), Coimbatore, India, 2017, pp. 20-25, doi: 10.1109/ICICI.2017.8365348.

[34]. Reddy, A. S., Praveen, S. P., Ramudu, G. B., Anish, A. B., Mahadev, A., & Swapna, D. (2023, January). A Network Monitoring Model based on Convolutional Neural Networks for Unbalanced Network Activity. In 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 1267-1274). IEEE.

[35]. Arava, K., Chaitanya, R. S. K., Sikindar, S., Praveen, S. P., & Swapna, D. (2022, August). Sentiment Analysis using deep learning for use in recommendation systems of various public media applications. In 2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC) (pp. 739-744). IEEE.

[36]. Krishna, T., Praveen, S. P., Ahmed, S., & Srinivasu, P. N. (2023). Software-driven secure framework for mobile healthcare applications in IoMT. Intelligent Decision Technologies, 17(2), 377-393.

[37]. Vellela, S. S., Reddy, V. L., Roja, D., Rao, G. R., Sk, K. B., & Kumar, K. K. (2023, August). A Cloud-Based Smart IoT Platform for Personalized Healthcare Data Gathering and Monitoring System. In 2023 3rd Asian Conference on Innovation in Technology (ASIANCON) (pp. 1-5). IEEE.

[38]. Davuluri, S., Kilaru, S., Boppana, V., Rao, M. V., Rao, K. N., & Vellela, S. S. (2023, September). A Novel Approach to Human Iris Recognition And Verification Framework Using Machine Learning

Algorithm. In 2023 6th International Conference on Contemporary Computing and Informatics (IC3I) (Vol. 6, pp. 2447-2453). IEEE.

[39]. Vellela, S. S., Vuyyuru, L. R., MalleswaraRaoPurimetla, N., Dalavai, L., & Rao, M. V. (2023, September). A Novel Approach to Optimize Prediction Method for Chronic Kidney Disease with the Help of Machine Learning Algorithm. In 2023 6th International Conference on Contemporary Computing and Informatics (IC3I) (Vol. 6, pp. 1677-1681). IEEE.

[40]. Vellela, S. S., Roja, D., Sowjanya, C., SK, K. B., Dalavai, L., & Kumar, K. K. (2023, September). Multi-Class Skin Diseases Classification with Color and Texture Features Using Convolution Neural Network. In 2023 6th International Conference on Contemporary Computing and Informatics (IC3I) (Vol. 6, pp. 1682-1687). IEEE.

[41]. Jyothi, V. E., Kumar, D. L. S., Thati, B., Tondepu, Y., Pratap, V. K., & Praveen, S. P. (2022, December). Secure Data Access Management for Cyber Threats using Artificial Intelligence. In 2022 6th International Conference on Electronics, Communication and Aerospace Technology (pp. 693-697). IEEE.

[42]. Madhuri, A., Swapna, D., Praveen, S. P., & Sindhura, S. (2022). Multi-traffic Science Perception Based on Supervised learning. *Journal of Next Generation Technology*, *2583*.

[43]. Swapna, D., Madhuri, A., Lakshmi, T. S., & Praveen, S. P. (2019). An efficient distributive framework for preserving data privacy through block chain. International Journal of Recent Technology and Engineering, 8(2), 5236-5239.

[44]. S. Phani Praveen,Balamuralikrishna Thati,Ch Anuradha,S. Sindhura,Mohammed Altaee,M. Abdul jalil. (2023). A Novel Approach for Enhance Fusion Based Healthcare System In Cloud Computing. Journal of Intelligent Systems and Internet of Things, 9 (1), 84-96.

[45]. JayaLakshmi, G., Madhuri, A., Vasudevan, D., Thati, B., Sirisha, U., Praveen, S.P. (2023). Effective disaster management through transformer-based multimodal tweet classification. Revue d'Intelligence Artificielle, Vol. 37, No. 5, pp. 1263-1272. https://doi.org/10.18280/ria.370519.