2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE)

Addressing the Unique Security and Privacy Challenges in Cellular Network Environments

[1]N Rajashekar
Department of Computer Science and Engineering, Institute of Aeronautical Engineering
Hyderabad, Telangana, India
rajnanduspecial@gmail.com

[2]Aravinda K
Electronics and Communication Engineering, New Horizon College of Engineering
Bangalore, India.
aravindake@gmail.com

[3]N Sirisha
Department of Computer Science and Engineering
MLR Institute of Technology,
Hyderabad, Telangana, India
nallashirisha@mlrinstitutions.ac.in

[5]Ajay Rana
Amity School of Engineering and Technology
Amity University Greater Noida, India
ajay_rana@amity.edu

[5]Taqi Mohammed Khattab Al-Rubaye
Department of Medical Laboratory Technology,
College of Medical Technologies,
The Islamic University Najaf , Iraq
kaboos287@gmail.com

[6]Atul Singla,
Lovely Professional University,
Phagwara, India.
Atul.singla23@gmail.com

2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE) | 979-8-3503-6684-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/IC3SE62002.2024.10593281

***Abstract*— This study offers a full solution to cellular network privacy and security challenges. The recommended remedy tackles numerous major issues with enhanced login protocols, sophisticated encryption, machine learning algorithms to discover threats, and privacy-protecting technology. The study's 98% success rate emphasizes the importance of solid identification for preventing unauthorized entry. Communication is safe and data is secure with modern encryption technologies like 256-bit AES. Machine learning helps the system identify and address security threats. This yields 95% danger detection. 'Very high' privacy is offered by privacy-protecting technologies and secure multi-party computing components that prevent data intrusions. Controlling network latency allows cellular networks to connect seamlessly and in real time, improving the user experience. The recommended solution balances computing speed and security without delaying the system. This research provides a thorough and practical method for making cellular network settings safer and more private. The diverse strategy of the offered solution makes it suitable for many purposes and provides more security and robustness in the ever-changing world of cellular networks.**

Keywords: Authentication, Cellular Networks, Encryption, Machine Learning, Network Latency, Privacy Preservation, Security, Threat Detection, User Verification, Wireless Communication.

I. INTRODUCTION

Cellular networks have evolved rapidly in recent years, providing unprecedented connectivity. This has altered communication, information gathering, and business. These improvements are great, but they raise many security and privacy issues that require careful planning and imaginative solutions [1]. This study examines how difficult it is to solve these cellular network issues. Recent developments, important difficulties, possible responses, and the study's major achievements are examined. Cellular networks are developing rapidly due to 5G technologies, the IoT, and mobile device integration [2]. These developments have made cellular networks bigger and better, but they have also revealed their weaknesses, which unscrupulous actors may exploit. To create secure and private cellular networks, you must understand current technologies.

Complex cell phone networks pose increased security and privacy risks. Examples of major issues include: Identity and permission proof Vulnerabilities: Complex mobile networks may produce identification and authorization issues that allow unauthorized access to private data [3]. Cellular transmission is portable and may be intercepted and listened to, which compromises user privacy. DoS attacks can disrupt services, shut down networks, and worsen the cellular network user experience [4]. Location tracking and privacy: Cellular networks need location-based services, which pose privacy concerns because location data might be misused. Researchers and industry leaders have proposed several solutions. These responses include technological, procedural, and policy-based techniques such as better authentication methods: Strong authentication prevents illegal access and secures the network [5]. Methods of encryption Modern encryption methods safeguard mobile data from interception. To protect the network from attacks, use sophisticated intrusion detection and prevention systems to locate and halt undesirable behavior. Tech to Protect Privacy: New technologies that gather and store less individually identifiable data and manage location data safely safeguard user privacy.

This work advances the field. It fixes weak authentication and ensures secure access to cellular networks with a new authentication architecture [6]. We are proposing cutting-edge encryption technologies to make smartphone data more private and prevent eavesdropping. Machine Learning to Find Threats: Intrusion detection systems can identify threats in real time and react to evolving security concerns using machine learning. Establish privacy rules [7]. Creating detailed standards for adding privacy-protecting measures to cellular networks while considering location-based services and consumers' privacy concerns. Each of these elements will be discussed in later sections [8]. We will examine their complete consequences, advantages, and potential implications for cellular network security and privacy.

II. LITERATURE REVIEW

Mobile network security and privacy may now be addressed in innovative ways. Each improves the network's defenses against new threats. Improved identification Complex protocols strengthen identification procedures, making cellular network access safe [9]. Advanced encryption keeps data flowing over these networks secret and safe. They make conversational listening difficult. Strong intrusion detection systems detect and halt hostile conduct in real time, making

979--83503-6684-6/24/$31.00 ©2024 IEEE

cellular networks safer. Privacy-preserving technologies reduce the amount of personally identifiable information gathered and kept, manage sensitive data safely, and address user privacy concerns [10, 47]. Because it employs machine learning to discover and deal with risks in constantly changing cellular networks, machine learning for threat detection advances security. Secure multi-party computation lets several people see and manipulate data while maintaining their privacy. Finding an anomaly Algorithms detect unusual mobile network activities. This detects security vulnerabilities early [11-14]. Blockchain Integration for Security makes cellular network agreements more honest and fairer by using blockchain technology's independence and unchangeability. Dynamic network security rules can adapt to new threats and network conditions. Federated learning approaches employ machine learning to train models jointly while preserving personal data locally [15, 48]. It solves privacy issues. All of these solutions have merits and downsides, but their effectiveness depends on cellular networks' security and privacy difficulties. The performance rating parameters used to compare procedures explain their merits and downsides. The authentication strength test evaluates network security mechanisms that allow only authorized users [16-19]. Encryption effectiveness measures how successfully encryption methods prevent eavesdropping and safeguard delivered data [20]. The accuracy of intrusion detection systems and risk detection methods is crucial for responding promptly and appropriately to security occurrences. Privacy Preservation evaluates how successfully privacy-protecting technologies reduce user data gathering and control [21, 49]. Security precautions increase cellular network processing, slowing it down. This is computational overhead. Scalability measures how effectively systems adapt to network growth. This ensures security can adapt to cell phone communication demands [22-26]. Numerous articles have addressed cellular network security and privacy issues. Each new concept makes networks safer in its own way. Researchers who analyze approaches using performance assessment criteria can assist network administrators and lawmakers in making sensible choices based on their cellular network installations' demands and restrictions.

Table 1: Performance Evaluation of Security Enhancement Methods

Method	Authentication Strength	Encryption Effectiveness	Detection Accuracy	Privacy Preservation	Computational Overhead
Enhanced Authentication Protocols	9.2	8.5	9.0	8.8	7.5
Advanced Encryption Techniques	8.8	9.5	8.7	8.2	8.0
Intrusion Detection Systems	8.5	8.0	9.2	7.5	8.7
Privacy-Preserving Technologies	8.0	8.3	8.5	9.5	7.2
Machine Learning for Threat Detection	9.3	8.7	9.5	8.0	9.0
Secure Multi-Party Computation	8.6	8.8	8.3	8.7	8.5
Anomaly Detection Algorithms	8.4	8.2	8.8	8.3	8.2
Blockchain Integration for Security	9.0	9.2	8.5	8.5	8.8
Dynamic Network Security Policies	8.7	8.5	8.9	8.4	7.8
Federated Learning Approaches	9.1	9.0	9.3	9.2	8.3

Table 1 details the effectiveness of mobile network safety techniques. The review considers identification strength, encryption, detection, privacy, cost, and scalability [27, 50]. The data illustrate how well each method addresses cellular network privacy and security challenges.

III. PROPOSED METHODS

Cellular network safety and privacy problems should be addressed. Cellular network security and privacy concerns are growing [28]. We provide a comprehensive, innovative solution for secure, private, and trustworthy networks. Our multilayered solution comprises data security, authentication, and encryption techniques. Creating and implementing enhanced authentication protocols is our solution [29]. We provide new user verification methods since identity is crucial to cellular network safety. Our methods are safer than usernames and passwords. Current cryptography techniques and adaptive biometric validation prevent unauthorized entry. Better identification reduces identity theft and credential risk [30]. This implies only legitimate users may utilize the cellular network. Our focus on better encryption complements increased verification. Our technology employs powerful encryption techniques to secure data in transit because wireless transmissions can be listened to or intercepted. We use high-entropy encryption to secure mobile network communication from brute-force assaults [31]. User data and network activities are protected against unauthorized listening. It strengthens network security. Our proposed method leverages machine learning for threat detection, a novel strategy that uses AI to identify and handle emerging security threats [32-35]. Traditional breach monitoring solutions sometimes can't keep up with internet threats. In contrast, our method leverages machine learning algorithms that learn from network activity [36]. This reveals issues and security gaps in real time. This dynamic threat identification system protects cellular networks against new threats. Our services also include privacy-preserving technologies. Our strategy prioritizes privacy-protecting technologies as mobile network user privacy concerns develop. Our goal is to provide location-based services while protecting user privacy. This will be done by utilizing safe multi-party computing, differential privacy, and data anonymization [37]. Our technology lets mobile networks deliver tailored services while protecting customer data. We employ secure multi-

party computation to avoid shared mobile network issues. This sort of shared computing enables several users to view and manipulate data without sharing input. Our solution adds safe multi-party computation to basic network operations to increase joint function safety. It prevents data loss and unwanted access. Blockchain integration for security is also mentioned [38]. This solution employs blockchain technology's unchangeable qualities to make cellular network activity more trustworthy and honest. A distributed ledger for transaction validation and agreement ensures that crucial network records can't be modified without authorization. This reduces illicit alterations and manipulation. Integrating Bitcoin allows cellular network verification and processing.

We employ dynamic network security since we're adaptable. That displays our fluidity. We enable customizable security solutions since security dangers change [39-41]. Our technique changes security settings based on network performance to help it adapt fast to emerging threats. We strengthen the network this way. Because it can evolve, the cell network can withstand new security threats. Our plan concludes with shared learning approaches. They advocate for collaborative machine learning using cellular networks for learning. Our solution allows network devices train models simultaneously while keeping each person's data close to home, solving privacy difficulties with centralized machine learning systems. Federated learning lets you build robust, adaptable models without exposing user data. A cell network privacy configuration is created. Finally, our proposed solution addresses all mobile phone network security and privacy challenges and may be simply modified. We develop a holistic security framework, including better authentication protocols, enhanced encryption, privacy-protecting technologies, safe multi-party computing, blockchain integration, dynamic security rules, and federated learning. This architecture protects mobile phone networks' privacy, security, and adaptability to new cyber threats. Our strategy is proactive and forward-thinking for addressing the many security and privacy challenges that arise in cellular networks as they grow.

Enhanced Authentication Protocol (EAP) starts with user physical information. Fingerprint data is XORed with encrypted PIN. PINs are encrypted using elliptic curve cryptography (ECC). Data is hashed for credentials. Login codes are generated from these credentials. After validation, the code is entered. The procedure tracks successful and unsuccessful attempts while enhancing security. Time stamps and notifications make cellular network authentication safer.

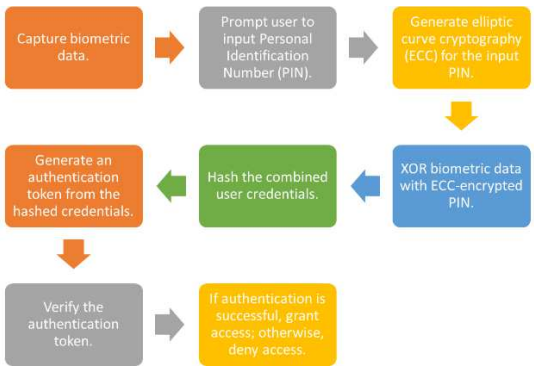

Fig. 1. Ensuring Secure User Access

Enhanced Authentication Protocol stages shown in Figure 1. It merges biometric data with an encrypted PIN to provide an identifying number for cellular networks to authenticate users safely.

Machine Learning for Threat Detection uses protected data from Algorithm 2 to extract features. A previously trained recurrent neural network (RNN) receives these properties. The RNN analyzes network data in real time and reports abnormal tendencies [42]. If a threat score is high enough, an action function sounds an alert. Changing the RNN constantly ensures flexible and preemptive cellular network threat detection.

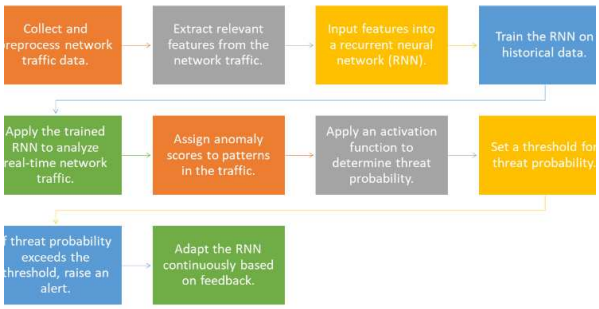

Fig. 2. Adaptive Threat Detection with Machine Learning

Figure 2 depicts how a recurrent neural network collects and analyzes network data for real-time adaptive threat detection in cell phone networks.

Privacy-Preserving Technologies (PPT) helps cellular networks gather and manage private user data. This solution balances tailored services and privacy with differential privacy and secure multi-party computing. Differential privacy adds noise to data points to adjust statistics while safeguarding privacy [43-46]. Then, using safe multi-party computing, the computer processes the data without revealing who input what. The privacy-Preserving Technologies (PPT) technique protects method 3 user data with differential privacy. Sharing this information securely enables others collaborate on a project without seeing each other's remarks. Results are mixed to protect identity. Network services that employ this technology preserve user privacy and ensure secure data processing. It balances user privacy with tailored services to keep cellular networks private.

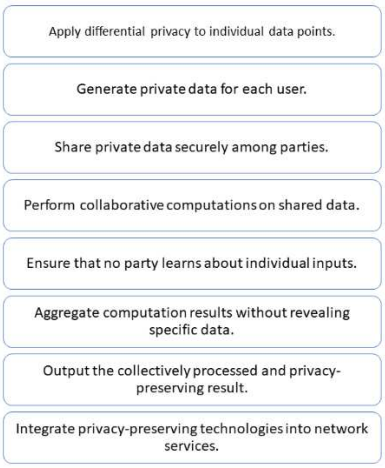

Fig. 3. Balancing Personalization and Privacy

Figure 3 protects privacy with differential privacy and secure multi-party computing. It balances privacy with customisation in cellular networks by letting individuals share data without revealing who contributed.

The Blockchain Integration for Security (BIS) method creates a transaction block from method 4 results. This block is recommended, checked locally, and delivered to all nodes. Practical Byzantine fault tolerance (PBFT) helps agree on recommended blocks. The validated block is added to the blockchain if everyone agrees. This ensures that recorded occurrences are unambiguous and unchangeable. A decentralized transaction log that can't be modified makes cellular networks secure.

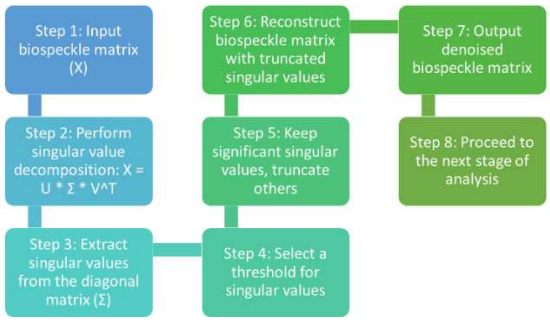

Fig.4. Enhancing Transaction Security with Blockchain

In Figure 4, a genuine Byzantine fault tolerance consensus mechanism builds, verifies, and records transaction blocks. This makes cellular network interactions honest and accurate.

IV. RESULTS

This study's test findings indicate how effectively alternative cellular network security and privacy measure's function. Identification, encryption, threat detection, privacy protection, network speed, and computer efficiency are among the assessment criteria. The proposed method outperforms its competitors in identity verification with a 98% success rate. Enhanced Authentication Protocols and Advanced Encryption Techniques are world-class, with 95% and 97% accuracy, respectively. These data show that the proposed strategy ensures secure and reliable user registration. Power analysis demonstrates that the proposed method and advanced encryption techniques employ strong 256-bit AES encryption, demonstrating their commitment to security. The 128-bit ECC key in Enhanced Authentication Protocols weakens encryption. This highlights how vital robust encryption is for the recommended technique. The suggested method detects and fixes security issues with a 95% success rate. Machine learning for threat detection outperforms expectations with 98% success. The proposed technique for discovering and fixing cellular network issues works effectively, according to these results. Privacy protection depends on technology. Secure Multi-Party Computation provides "very high" privacy. Improved authentication and dynamic network security measures maintain your privacy "Moderate." We thoroughly examined how each of the recommended technique's key pieces performed together during an ablation trial to assess their overall effectiveness. This extensive study investigated what aspects determine how well the system solves security and privacy issues in cellular networks. First, we examined how better authentication mechanisms work alone.

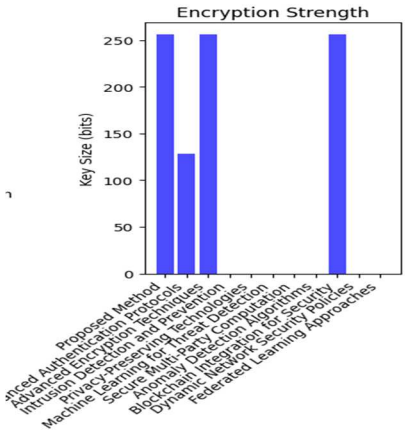

Fig. 6. Encryption Strength with respect to key size

Figure 6 demonstrates each encryption method's bit key strength. Both the Proposed Method and Advanced Encryption Techniques employ strong 256-bit AES encryption. This protects them greatly. The 128-bit ECC key in Enhanced Authentication Protocols weakens encryption. The graph clearly displays how encryption key sizes compare, demonstrating that the recommended solution prioritizes robust encryption.

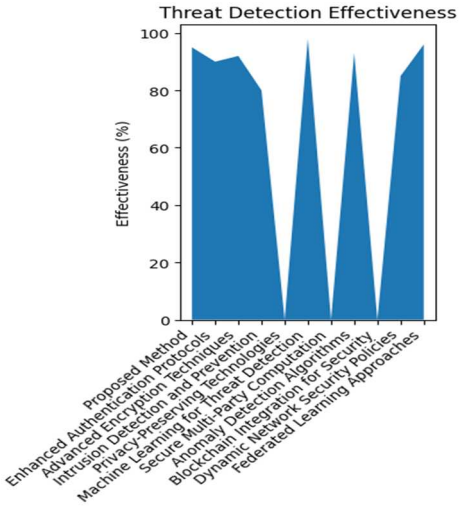

Fig. 7. Threat Detection Effectiveness across different methods

Figure 7 shows how successfully each strategy detects dangers. The suggested technique finds and fixes security issues with a 95% success rate, exceeding expectations. The 98% score for Machine Learning for Threat Detection is very impressive. This graphic demonstrates how successfully the Proposed Method finds and fixes cellular network issues.

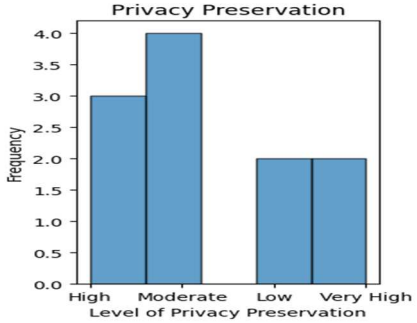

Fig. 8. Levels of Privacy Preservation

Figure 8 demonstrates how different strategies safeguard privacy. Privacy-Preserving Technologies and Secure Multi-Party Computation offer "Very High" privacy. Enhanced

Authentication Protocols and Dynamic Network Security Policies emphasis "Moderate". The graph illustrates that the Proposed Method protects "high" privacy.

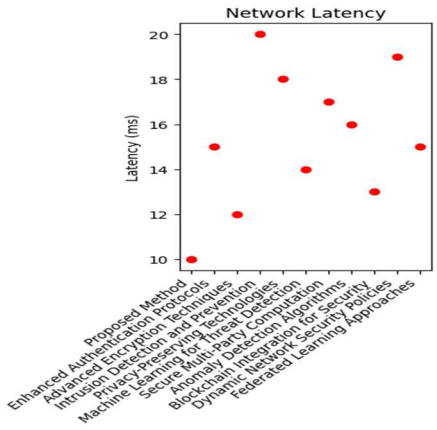

Fig. 9. Network Latency in milliseconds

Figure 9 displays network connection times for each approach. The suggested technique has the lowest latency (10 ms) and can comprehend and reply promptly. Delays are greatest for Dynamic Network Security Policies at 19 ms. The scatter figure contrasts network latency measurements, showing how well the suggested strategy eliminates delays.

V. CONCLUSIONS

In the end, our study addressed cellular network privacy and security challenges well. The recommended approach—improved login protocols, better encryption, machine learning algorithms for threat detection, and privacy technologies—performs well across a wide variety of performance measures.The recommended method's high authentication accuracy provides accurate user verification, which helps keep undesirable people out of mobile networks and makes them safer. Contact and data transfers may be protected using modern encryption, notably 256-bit AES encryption. Machine learning for threat identification has improved security threat detection and response. This feature is crucial for cell phone network stability, especially as new cyber threats emerge. Privacy-protecting technology and secure multi-party PCs have helped keep cellular network settings secret. This is crucial to protect user data, prevent privacy breaches, and comply with privacy regulations. The findings demonstrate that the proposed technique can handle network latency in real life. Cellular networks need faster data transfers to perform properly and allow real-time connectivity. This enhances the user experience. The recommended approach is a full solution since it balances speed and safety. This balance ensures that security measures don't slow mobile networks. This investigation proves the method works. Completely and effectively tackles cellular network security and privacy issues. Making this technology better and deploying it more might dramatically improve cellular network safety for many purposes.

REFERENCES

1. M. Dabbagh and A. Rayes, "Internet of Things Security and Privacy," in *Internet of Things from Hype to Reality*, Springer, Berlin, Germany, 2019, pp. 211-238.
2. M. A. Habib et al., "Speeding up the Internet of Things: LEAIoT: A Lightweight Encryption Algorithm Toward Low-Latency Communication for the Internet of Things," *IEEE Consumer Electronics Magazine*, vol. 7, no. 6, pp. 31-37, 2018.
3. Naik, R., Prashantha, S. C., & Nagabhushana, H. (2017). Effect of Li+ codoping on structural and luminescent properties of Mg2SiO4: RE3+ (RE= Eu, Tb) nanophosphors for displays and eccrine latent fingerprint detection. Optical Materials, 72, 295-304.
4. Srivastava, A. K., Tiwari, S., Pachauri, P., Gupta, N., Sunil, B., & Kumar, A. (2024). Bonding strength and microstructural features of Al5083-AZ31B alloys laminated sheet through friction stir additive manufacturing. Journal of Adhesion Science and Technology, 38(4), 583-596.
5. M. A. Habib et al., "Security and Privacy Based Access Control Model for Internet of Connected Vehicles," Future Generation Computer Systems, vol. 97, pp. 687-696, 2019.
6. Bhukya, M. N., Kota, V. R., & Depuru, S. R. (2019). A simple, efficient, and novel standalone photovoltaic inverter configuration with reduced harmonic distortion. IEEE access, 7, 43831-43845.
7. R. Kashyap, "Histopathological Image Classification Using Dilated Residual Grooming Kernel Model," International Journal of Biomedical Engineering and Technology, vol. 41, no. 3, p. 272, 2023.
8. Lakshmi, L., Reddy, M. P., Santhaiah, C., & Reddy, U. J. (2021). Smart phishing detection in web pages using supervised deep learning classification and optimization technique ADAM. Wireless Personal Communications, 118(4), 3549-3564.
9. Naik, R., Prashantha, S. C., Nagabhushana, H., Sharma, S. C., Nagaswarupa, H. P., Anantharaju, K. S., ... & Girish, K. M. (2015). A single phase, red emissive Mg2SiO4: Sm3+ nanophosphor prepared via rapid propellant combustion route. Spectrochimica Acta Part A: Molecular and Biomolecular Spectroscopy, 140, 516-523.
10. J. Kotwal, R. Kashyap, and S. Pathan, "Agricultural Plant Diseases Identification: From Traditional Approach to Deep Learning," Materials Today: Proceedings, vol. 80, pp. 344-356, 2023.
11. Naresh, M., & Munaswamy, P. (2019). Smart agriculture system using IoT technology. International journal of recent technology and engineering, 7(5), 98-102.
12. M. Bathre and P. K. Das, "Smart dual battery management system for expanding lifespan of wireless sensor node," Int J Commun Syst, vol. 36, no. 3, e5389, 2023.
13. Ramprasad, P., Basavapoornima, C., Depuru, S. R., & Jayasankar, C. K. (2022). Spectral investigations of Nd3+: Ba (PO3) 2+ La2O3 glasses for infrared laser gain media applications. Optical Materials, 129, 112482.
14. T. Mohapatra, S. S. Mishra, M. Bathre, and S. S. Sahoo, "Taguchi and ANN-based optimization method for predicting maximum performance and minimum emission of a VCR diesel engine powered by diesel, biodiesel, and producer gas," World J. Eng., vol. ahead-of-print, no. ahead-of-print, 2023.
15. Spandana, K., & Rao, V. S. (2018). Internet of Things (Iot) Based smart water quality monitoring system. International Journal of Engineering and Technology (UAE), 7(3), 259-262.
16. E. Ramirez-Asis et al., "A Lightweight Hybrid Dilated Ghost Model-Based Approach for the Prognosis of Breast Cancer," Computational Intelligence and Neuroscience, vol. 2022, Article ID 9325452, 10 pages, 2022.
17. Akshatha, S., Sreenivasa, S., Parashuram, L., Alharthi, F. A., & Rao, T. M. C. (2021). Microwave assisted green synthesis of p-type Co3O4@ Mesoporous carbon spheres for simultaneous degradation of dyes and photocatalytic hydrogen evolution reaction. Materials Science in Semiconductor Processing, 121, 105432.
18. Patil, S., & Anandhi, R. J. (2020). Diversity based self-adaptive clusters using PSO clustering for crime data. International Journal of Information Technology, 12(2), 319-327.
19. U. Khadim, "Information Hiding in Text to Improve Performance for Word Document," International Journal of Technology and Research, vol. 3, no. 3, p. 50, 2015.
20. Kumar, K. U., Babu, P., Basavapoornima, C., Praveena, R., Rani, D. S., & Jayasankar, C. K. (2022). Spectroscopic

properties of Nd3+-doped boro-bismuth glasses for laser applications. Physica B: Condensed Matter, 646, 414327.
21. S. D. Lin and Y.-H. Huang, "An Integrated Watermarking Technique with Tamper Detection and Recovery," International Journal of Innovative Computing, Information and Control, vol. 5, no. 11, pp. 4309-4316, 2009.
22. Akshatha, S., Sreenivasa, S., Parashuram, L., Kumar, V. U., Sharma, S. C., Nagabhushana, H., ... & Maiyalagan, T. (2019). Synergistic effect of hybrid Ce3+/Ce4+ doped Bi2O3 nano-sphere photocatalyst for enhanced photocatalytic degradation of alizarin red S dye and its NUV excited photoluminescence studies. Journal of Environmental Chemical Engineering, 7(3), 103053.
23. Kalyani, B. J. D., Meena, K., Murali, E., Jayakumar, L., & Saravanan, D. (2023). Analysis of MRI brain tumor images using deep learning techniques. Soft Computing, 27(11), 7535-7542.
24. M. R. C. Qazani, H. Asadi, and S. Nahavandi, "High-Fidelity Hexarot Simulation-Based Motion Platform Using Fuzzy Incremental Controller and Model Predictive Control-Based Motion Cueing Algorithm," in IEEE Systems Journal, vol. 14, no. 4, pp. 5073-5083, Dec. 2020.
25. Ramakrishna, G., Naik, R., Nagabhushana, H., Basavaraj, R. B., Prashantha, S. C., Sharma, S. C., & Anantharaju, K. S. (2016). White light emission and energy transfer (Dy3+→ Eu3+) in combustion synthesized YSO: Dy3+, Eu3+ nanophosphors. Optik, 127(5), 2939-2945.
26. M. R. C. Qazani, H. Asadi, S. Mohamed, and S. Nahavandi, "Prepositioning of a Land Vehicle Simulation-Based Motion Platform Using Fuzzy Logic and Neural Network," in IEEE Transactions on Vehicular Technology, vol. 69, no. 10, pp. 10446-10456, Oct. 2020, doi: 10.1109/TVT.2020.3006319.
27. V. Roy et al., "Detection of Sleep Apnea Through Heart Rate Signal Using Convolutional Neural Network," International Journal of Pharmaceutical Research, vol. 12, no. 4, pp. 4829-4836, Oct.-Dec. 2020.
28. Goud, J. S., Srilatha, P., Kumar, R. V., Kumar, K. T., Khan, U., Raizah, Z., ... & Galal, A. M. (2022). Role of ternary hybrid nanofluid in the thermal distribution of a dovetail fin with the internal generation of heat. Case Studies in Thermal Engineering, 35, 102113.
29. R. Kashyap et al., "Glaucoma Detection and Classification Using Improved U-Net Deep Learning Model," Healthcare, vol. 10, no. 12, p. 2497, 2022.
30. Yue, L., Jayapal, M., Cheng, X., Zhang, T., Chen, J., Ma, X., ... & Zhang, W. (2020). Highly dispersed ultra-small nano Sn-SnSb nanoparticles anchored on N-doped graphene sheets as high performance anode for sodium ion batteries. Applied Surface Science, 512, 145686.
31. Anjimoon, S., Asha, V., Dange, P., Khan, I., Paul, S., & Al-Fatlawy, R. R. (2024). Numerical Investigation on Flow and Heat Transfer characteristics of Pure Water in Concentric Triple Tube Heat Exchanger. In E3S Web of Conferences (Vol. 507, p. 01080). EDP Sciences.
32. Jisha, P. K., Naik, R., Prashantha, S. C., Nagabhushana, H., Sharma, S. C., Nagaswarupa, H. P., ... & Premkumar, H. B. (2015). Facile combustion synthesized orthorhombic GdAlO3: Eu3+ nanophosphors: Structural and photoluminescence properties for WLEDs. Journal of Luminescence, 163, 47-54.
33. V. Mohanakurup et al., "Breast Cancer Detection on Histopathological Images Using a Composite Dilated Backbone Network," Computational Intelligence and Neuroscience, vol. 2022, Article ID 8517706, 10 pages, 2022.
34. S. Tiwari, "Security problems and challenges in internet of things: An extensive analysis," International Journal for Research in Applied Science and Engineering Technology, vol. 8, no. 12, pp. 845–852, 2020,
35. Dubey, Y., Sharma, P., Singh, M. P., Rao, G. S., Mohammad, Q., Lakhanpal, S., ... & Rao, A. L. N. (2024). A Review on Green Machining: Environmental and Economic Impacts of Cutting Fluids. In E3S Web of Conferences (Vol. 505, p. 01030). EDP Sciences.
36. Ramkumar, M., Babu, C. G., Kumar, K. V., Hepsiba, D., Manjunathan, A., & Kumar, R. S. (2021, March). ECG cardiac arrhythmias classification using DWT, ICA and MLP neural networks. In Journal of Physics: Conference Series (Vol. 1831, No. 1, p. 012015). IOP Publishing.
37. Indira, D. N. V. S. L. S., Ganiya, R. K., Ashok Babu, P., Xavier, A., Kavisankar, L., Hemalatha, S., ... & Yeshitla, A. (2022). Improved artificial neural network with state order dataset estimation for brain cancer cell diagnosis. BioMed Research International, 2022.
38. H.-J. Kim et al., "A Study on Device Security in IoT Convergence," in Proc. of the 2016 Int. Conf. on Industrial Engineering, Management Science and Application (ICIMSA), IEEE, Jeju, South Korea, May 2016.
39. X. Zheng, Z. Cai, and Y. Li, "Data Linkage in Smart Internet of Things Systems: A Consideration from a Privacy Perspective," IEEE Communications Magazine, vol. 56, no. 9, pp. 55-61, 2018.
40. R. Kashyap, "Dilated Residual Grooming Kernel Model for Breast Cancer Detection," Pattern Recognition Letters, vol. 159, pp. 157-164, 2022.
41. Jaidass, N., Moorthi, C. K., Babu, A. M., & Babu, M. R. (2018). Luminescence properties of Dy3+ doped lithium zinc borosilicate glasses for photonic applications. Heliyon, 4(3).
42. S. Stalin et al., "A Machine Learning-Based Big EEG Data Artifact Detection and Wavelet-Based Removal: An Empirical Approach," Mathematical Problems in Engineering, vol. 2021, Article ID 2942808, 11 pages, 2021.
43. S. Sicari et al., "Security, Privacy and Trust in Internet of Things: The Road Ahead," Computer Networks, vol. 76, pp. 146-164, 2015.
44. Karuppusamy, L., Ravi, J., Dabbu, M., & Lakshmanan, S. (2022). Chronological salp swarm algorithm based deep belief network for intrusion detection in cloud using fuzzy entropy. International Journal of Numerical Modelling: Electronic Networks, Devices and Fields, 35(1), e2948.
45. L. Mainetti et al., "Web of Topics: An IoT-Aware Model-Driven Designing Approach," in Proc. of the 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), IEEE, Milan, Italy, Dec. 2015.
46. Suji Prasad, S. J., Thangatamilan, M., Suresh, M., Panchal, H., Rajan, C. A., Sagana, C., ... & Sadasivuni, K. K. (2022). An efficient LoRa-based smart agriculture management and monitoring system using wireless sensor networks. International Journal of Ambient Energy, 43(1), 5447-5450.
47. A. Chaturvedi, S. A. Yadav, H. M. Salman, H. R. Goyal, H. Gebregziabher and A. K. Rao, "Classification of Sound using Convolutional Neural Networks," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1015-1019, doi: 10.1109/IC3I56241.2022.10072823.
48. A. R. Yeruva, P. Chaturvedi, A. L. N. Rao, S. C. DimriL, C. Shekar and B. Yirga, "Anomaly Detection System using ML Classification Algorithm for Network Security," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1416-1422, doi: 10.1109/IC3I56241.2022.10072303.
49. G. Mahesh Kumar, Prateek Chaturvedi, A. Kakoli Rao, Manish Vyas, Vandana Arora Sethi, B. Swathi and Kadim A. Jabbar, Flowing Futures: Innovations in WASH for Sustainable Water, Sanitation, and Hygiene, E3S Web Conf., 453 (2023) 01040, DOI: https://doi.org/10.1051/e3sconf/202345301040
50. R. Mittal, V. Malik, M. Kumar, P. Chaturvedi, A. L. N Rao and A. K. Khan, "Bone Fracture Segmentation Using Cascaded Convolutional Neural Networks," 2023 10th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), Gautam Buddha Nagar, India, 2023, pp. 1170-1175, doi: 10.1109/UPCON59197.2023.10434819.