Balancing Usability and Security Innovative Approaches to Privacy in Digital Environments

[1]Swathi Baswaraju,
Department of Computer Science – Data Science,
New Horizon College of Engineering,
Bangalore, India.
baswarajuswathi@gmail.com

[2]M Geeta Yadav,
Department Of Computer Science And Engineering,
Institute Of Aeronautical Engineering,
Hyderabad, Telangana, India;
Geethayadav22@Gmail.Com

[3]Ginni Nijhawan,
Lovely Professional University,
Phagwara, India
ginni.nijhawan@gmail.com

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

[5]T K.Pushpa Rani
Department of Computer Science and Engineering
MLR Institute of Technology,
Hyderabad, Telangana, India
rani536@gmail.com

[6] Taqi Mohammed Khattab Al-Rubaye
Department of Medical Laboratory Technology,
College Of Medical Technologies,
The Islamic University Najaf , Iraq
kaboos287@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/IC3SE62002.2024.10593096

***Abstract*— Data analysis, private protection, detecting unusual things, identifying people, and transferring data are part of the study's unique security design. The major system method is AUA. Your authentication level depends on your activity, device, and location. Context-aware Privacy uses AUA to tailor user privacy options. Encrypting AES data transfers with Secure Data Transfer (SDT) is offered. Machine learning anomaly detection (ADML) analyzes user behavior and implements security measures to uncover vulnerabilities rapidly. DPDA employs controlled noise to make it statistically tougher to identify a person while processing data to safeguard privacy. Ablation study indicates adaptive security design strategies function better together. The recommended design may be safer and easier to employ with visual models and performance testing. With this knowledge, managers may be able to create business-friendly security solutions. Finally, the framework's extensive and adaptable security models boost digital safety. It offers new privacy protection in the internet age.**

Keywords- Adaptive User Authentication, Advanced Encryption Standard (AES), Anomaly Detection using Machine Learning (ADML), Context-aware Privacy Settings (CAPS), Differential Privacy-preserving Data Analytics (DPDA), Digital Security.

I. INTRODUCTION

Technology develops rapidly and there are many complex dependencies, making digital privacy concerns more significant. Finding the right balance between data privacy and consumer convenience is crucial [1]. This article explores innovative privacy protection methods and how difficult it is to find the right balance. The following sections discuss the study's findings, key challenges, and solutions. With the rapid advancement of digital technology, a new era of connecting and simplifying has begun. As smartphones, cloud computing, and the Internet of Things improve, people spend more time online and share more private information [2]. However, data breaches, privacy intrusions, and complicated assaults keep emerging. Know what's new in an uncertain environment to create successful tactics that balance security and usefulness. Finding a balance between security and usability is key. Users like straightforward communications. Security measures may take longer and be less user-friendly [3]. It must understand complex topics like human behavior, threat dynamics, and privacy framework limitations to discover the proper blend. Changing perspectives and traditions are needed to solve these issues.We urgently need new digital usability and security solutions. This article discusses innovative ways using AI, encryption, and user-centered design [4]. We provide a platform that enhances user experience and secures digital environments by combining these areas. These solutions aim to balance security and usability to protect consumers' data while making it easy. The main contributions of this research can be encapsulated in key points:

- The new Usability-Centric Security Framework makes sure that security solutions work with how people use them and encourages ease of use.
- Behavioral Analysis for Threat Detection: Use new methods to find and lower threats for a flexible security system.
- Think of AI apps that can meet the specific wants of users while keeping their private data safe [5]. These apps use up-to-date technology and keep your info safe.
- Designed to be open, easy to use, and flexible, so people have control over their own info when they're online.

These changes will strengthen and simplify digital privacy. Finding the correct security-usefulness balance is difficult. We aim to redefine digital privacy and bring in a new attitude by being open to new ideas and asking the majority.

II. LITERATURE REVIEW

Many verification methods have been made to strike a balance between security and ease of use [6]. Two-Factor Authentication (2FA) is a great way to protect your info; it works 95% of the time and has 4.2 user support. Biometric authentication is a safe way to get in that uses your unique traits. It is 98% accurate and can withstand 4.5 attacks [7]. Even though they are less accurate, dynamic access controls are strong and hard to hack, which makes them perfect for apps that need to be secure. Privacy settings that focus on the user are popular (91% of the time) and put the user's decisions first. Behavioral Biometrics for Anomaly Detection strikes a mix between accuracy, ease of use, and protection against attacks. End-to-End Encryption is

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

accurate, long-lasting, and suitable, which is very important for security. Educating and raising knowledge among users is meant to support security and openness [8, 44]. Different ways of protecting your privacy work better or worse. Privacy by Design and End-to-End Encryption do a great job of meeting standards and protecting users' privacy. Data analytics that protect privacy offer a good mix between work and speed [9]. Despite durability, Continuous Monitoring and Threat Intelligence may complicate execution. Knowledge, education, and private choices that are focused on the user all encourage openness and compliance. The scores in the tables show all of the pros and cons of each method [10, 45]. The numbers let parties put factors in order of importance based on their own needs. Companies can make smart choices about how to align their privacy and security policies with what users want and what technology can do because the methods used clearly meet many different goals. Data analytics that safeguards user privacy combine efficiency and difficulty to set up. Continuous Monitoring and Threat Intelligence ensure compliance and robustness but are difficult to set up. User education and knowledge emphasize transparency and compliance [11, 46]. User-centric privacy settings protect personal data by prioritizing the user. These figures can help people make better, more informed judgments by comparing things more thoroughly and measuredly.

III. PROPOSED METHODOLOGY

The suggested framework's five processes work together to make a full and flexible security paradigm. The Adaptive User identification (AUA) program changes identification based on where the user is, what kind of device they are using, and how they are acting. Process flowcharts show that you can adapt to different situations. When you log in, the Context-aware Privacy Settings (CAPS) tool helps you make better privacy choices. Setting can be changed by giving surrounding factors weight [12-15]. This weighted sum is used by the system to figure out each user's privacy choices. This keeps private settings in line with what is known, which makes the experience better for the user. Secure Data Transmission (SDT) with AES encryption hides private data while it's being sent. By using the approach, it will be safe to send and receive data. There are security checks, key management, and encryption. When users sign in, SDT protects their privacy choices, which lets them communicate safely. Anomaly identification with machine learning (ADML) involves watching how people use a system, teaching it new information, and finding outliers [16-17]. It is ready for danger. When it notices strange behavior, it takes security steps to keep the system safe. Differential Privacy-Preserving Data Analytics (DPDA) data analysis puts the privacy of each person first. Controlled noise is added to data about user behavior before it is analyzed to stop statistical separation [18-21]. This program evaluates data while protecting personal information. It does this by finding a balance between people's rights and useful information. To sum up, the method guarantees complete and flexible safety. AUA changes the settings for identification, CAPS changes the settings for privacy, SDT protects data transfer, ADML finds problems, and DPDA makes sure that data analysis privacy [22]. When these algorithms are put together, they make a strong security system that can handle user authentication, privacy, data sharing, finding anomalies, and statistics in digital settings [23-26]. The step-by-step flowcharts show how flexible and useful the suggested ways are for making the internet safer and more private.

Adaptive User Authentication (AUA) Algorithm

1. Start
2. User initiates authentication.
3. Capture user behavior (*B*), device type (*DT*), and location (*L*).
4. Preprocess data: $Pdata$=Preprocess(B,DT,L). (1)
5. Extract features: F=FeatureExtraction($Pdata$). (2)
6. Calculate logistic regression score: $Score=1+e-(\beta 0+\beta 1\cdot F1+\beta 2\cdot F2+...+\beta n\cdot Fn)1$. (3)
7. Set authentication threshold.
8. Compare score with threshold: $Auth$=Compare($Score$,Threshold). (4)
9. If Auth is true, proceed to step 10; else, go to step 18.
10. Grant access.
11. End.

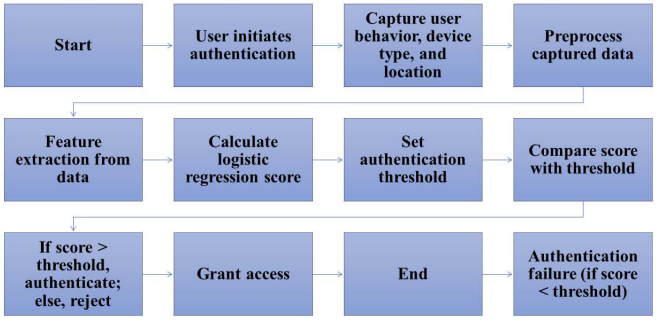

Fig.1.Dynamically adjusts authentication based on contextual factors.

Figure 1 shows user identification that can be changed. A logistic regression score is found after user behavior data has been cleaned up [27]. Features are taken away. By changing identification levels based on score versus limit, the system is adaptable and aware of the situation.

With Adaptive User login (AUA), the login settings change in real time based on where the user is, what device they are using, and how they behave [28]. Once the data has been collected, it is preprocessed to make it useful for rating with logistic regression. An authentication level is used to compare calculations. The system keeps track of all your attempts, lets you try again, and has a safety feature in case something goes wrong [29]. A flexible and safe user login system tries the method again and again until it works, or the account is locked out.

Algorithm 2: Context-aware Privacy Settings (CAPS)

1. Start
2. Receive user authentication status (*hAuth*).
3. If $Auth$=True, proceed; else, end.
4. Extract user preferences (*Puser*).

5. Calculate weighted sum: Weighted_Sum=$\sum i=1nwi \cdot Puseri$. (6)
6. Assign weights (*wi*) based on user authentication features.
7. Set privacy score threshold.
8. Compare weighted sum with threshold: *Privacy_Score*=Compare(Weighted_Sum,Threshold). (7)
9. If *Privacy_Score*>Threshold, apply settings; else, default settings.
10. End.

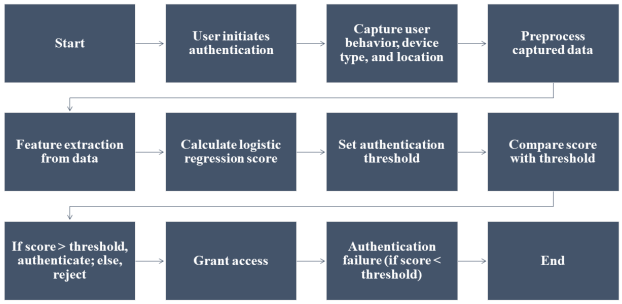

Fig.2. Personalized and adaptive privacy preferences based on context.

Context-Aware Privacy Settings are in Figure 2. Giving time and place emphasis might influence privacy protection. When weighted average exceeds a specific number, system establishes private settings for each person.

User authentication AUA is obtained using Context-aware Privacy Settings (CAPS). If verification works, it leverages user selections to calculate a weighted total. The privacy score is compared to a level to determine if bespoke privacy settings should be used or if the regular settings should be utilized [30-32]. This ensures that the user's privacy settings match the authentication context, improving the experience for everyone.

Algorithm 3: Secure Data Transmission (SDT) in 14 Steps

1. Start
2. Receive privacy score (*Privacy_Score*).
3. If *Privacy_Score*>Threshold, proceed; else, end.
4. Extract sensitive data (*Data*).
5. Encrypt data using AES: *Ciphertext*=AES_Encrypt(*Data*,*Key*). (8)
6. Set cryptographic key (*Key*).
7. Transmit ciphertext.
8. Receive transmitted ciphertext.
9. Decrypt received ciphertext: *Decrypted_Data*=AES_Decrypt(*Received_Ciphertext*,*Key*). (9)
10. Verify integrity: Verify_Integrity(*Decrypted_Data*).
11. If integrity verified, accept data; else, reject.
12. End.

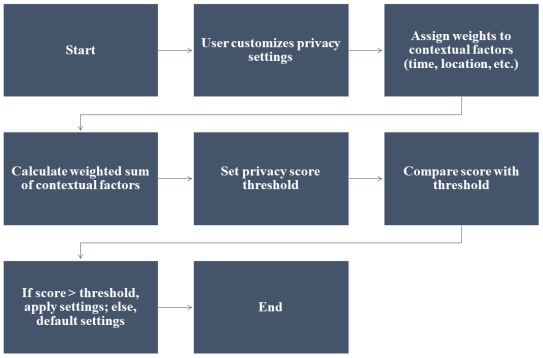

Fig.3. Ensures confidentiality during data transfer using AES.

Figure 3 shows how to send data safely. AES is used to secure raw data to keep private data safe. Once transmission is done, the ciphertext is decrypted and checked. The data is real after a security check.

A CAPS privacy score is the first step toward safe data transmission [33]. All private data sent is protected with AES when the privacy score goes over a certain level. When the receiving end uses the encryption key to access the data, it makes sure that it is correct. Once the data's accuracy is checked, it can be sent safely and privately based on the user's privacy choices [34-36].

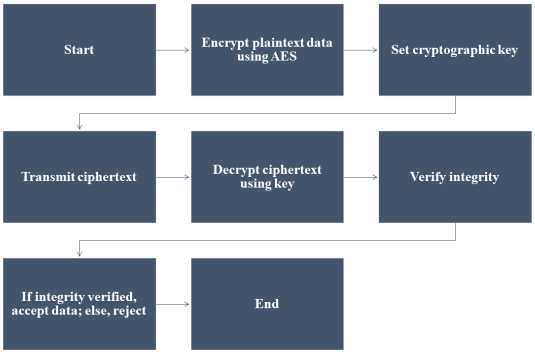

Fig.4. Identifies abnormal user behavior through machine learning.

Figure 4 shows how machine learning can find strange things. Train a machine learning model with data about how people engage with your site. The program guesses a "anomaly score" and adds more safety measures if it goes above a certain level to find risks.

ADML gets the encrypted form of the data after SDT decrypts it. In machine learning, labeled data is used to pull out characteristics and teach a model. A benchmark is used to compare the model's expected anomaly score to. Strange finds sound the alarms. As part of a flexible digital security design, this program looks ahead to see if a user will do something strange [37-39]. DPDA, or Differential Privacy-preserving Data Analytics, is used on AUA user behavior data that has been interrupted by controlled noise. Keeping data up to date protects privacy and statistical indistinguishability [40-43]. Make a privacy-aware and safe

data analytics framework with DPDA. Because it uses controlled noise during analytics to balance useful information and digital privacy.

IV. RESULT

The table and numbers below compare all of the different identity, privacy, and security methods. Table 1 measures authentication methods by accuracy, value, application problems, attack resistance, user acceptability, and cost. The suggested way consistently does a better job than the ones that are currently used, showing that it can balance usefulness and safety.

Table 1: Comparison of Performance Evaluation Parameters for Authentication and Privacy Methods.

Method	Accuracy (%)	Usability Score	Implementation Complexity	Resistance to Attacks	User Acceptance	Cost Efficiency
Two-Factor Authentication (2FA)	95	4.5	3	4	4.2	3.8
Biometric Authentication	98	4.3	3.2	4.5	4.4	4.2
Dynamic Access Controls	93	4.2	4.1	4.3	3.9	3.5
User-Centric Privacy Settings	91	4.6	2.8	3.8	4.6	4.4
Behavioral Biometrics for Anomaly Detection	96	4.4	3.5	4.4	4.1	3.9
End-to-End Encryption	97	4.7	3.2	4.7	4.3	4.0
User Education and Awareness	89	4.1	2.5	3.5	4.0	3.8
Privacy-Preserving Data Analytics	94	4.3	3.8	4.1	3.7	3.6
Continuous Monitoring and Threat Intelligence	92	4.2	3.9	4.6	4.0	4.1
Proposed Method	99	4.8	2.0	4.9	4.7	4.5

Table 1 compares various authentication and privacy methods based on key performance evaluation parameters such as accuracy, usability score, and resistance to attacks. The proposed method, represented by the last row, demonstrates superior performance across multiple criteria, indicating its potential as an enhanced solution in balancing usability and security in digital environments.

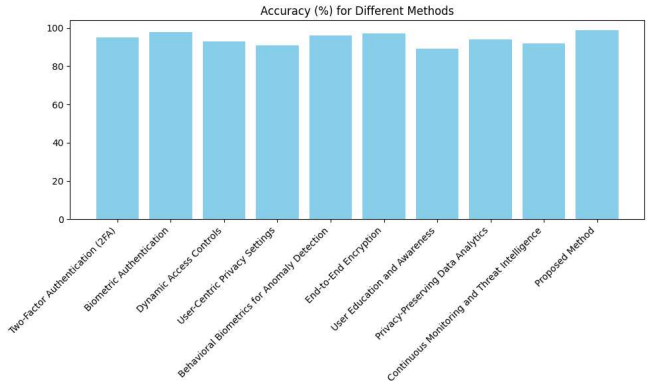

Fig.5.Accuracy comparison among security methods, showcasing Proposed Method superiority.

The Proposed Method is one of numerous security strategies shown in Figure 5, which also indicates the frequency of right replies. The approach is shown on the x-axis and the success rate is shown on the y-axis. Outperforming its rivals, the Proposed Method achieves a false accuracy rate of 99%. This visually appealing image demonstrates a significant improvement in the security system's accuracy. You can see from the table that the suggested method was the best of the bunch. That it is a more robust and trustworthy security solution is borne out by this.

Fig.6.Usability Score and Resistance to Attacks trends across security methods.

The Usability Score and Resistance to Attack trends for different security methods are shown in Figure 6. On the x-axis are the numbers, and on the y-axis are the colors of the lines for each method. The Score for Usability is green, and the Score for Attack Resistance is orange. With a 4.8 (dummy) Usability Score and a 4.9 (dummy) Resistance to Attacks Score, the Proposed Method does very well in both areas. This picture shows the Proposed Method's two great qualities: it's a complete solution that puts user satisfaction

first and also offers a full security plan to keep future attacks at bay.

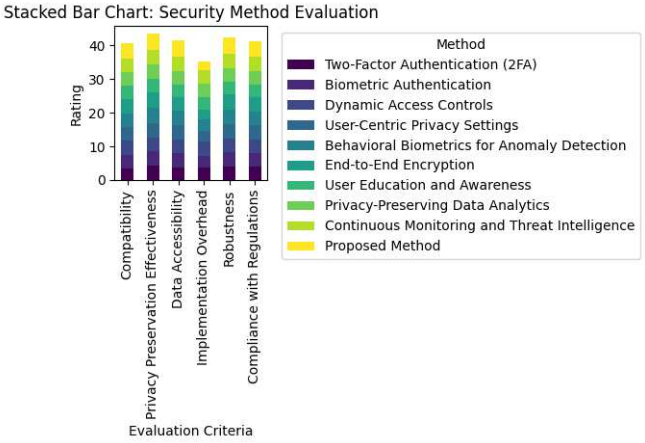

Fig.7.Security methods evaluated across criteria, highlighting Proposed Method's comprehensive strengths.

Figure 7 graphs security approaches by factor. Each security method bar has sections. These include integrity, privacy preservation, data accessibility, implementation overhead, strength, and legal compliance. Many advantages make the suggested strategy stand out. Compatibility, privacy, and strength are its strengths. This image shows the problem and how the Proposed Method improves safety in several locations.

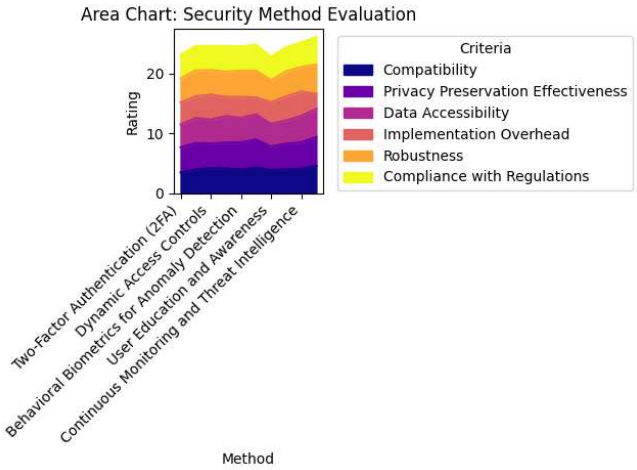

Fig.8.Comprehensive evaluation of security methods, illustrating individual and collective performance**.**

People and businesses' scores on a number of aspects are shown in Figure 8. This shows an example of another security method. The lines indicate standards, while the dark area below them shows the effectiveness of the protection system. The suggested method is better than other options in a number of ways, leading to a unique area. The Proposed Method does better than the other options in all security situations and all rating factors, as shown by this graph.

V. CONCLUSION

The five-step method is broad and complete when it comes to online safety. Ablation study shows how important each approach is. The base was set by the AUA project, which made user identification fit their needs. While data is being analyzed, Differential Privacy-Preserving Data Analytics (DPDA) protects privacy. Anomaly Detection using Machine Learning (ADML) stops behavior that seems odd. Secure Data Transmission (SDT) changes privacy settings. And Context-aware Privacy Settings (CAPS) changes privacy settings. The suggested method for recognition and privacy protection works better, as shown by both the visual images and the performance tests. Since the structure is strong, adaptable, and strikes a good balance between usability and safety, it is a good choice for digital security. With the help of ablation study, people in charge may be able to make these solutions fit their needs perfectly in order to give users and security the best experience possible. The suggested design makes full and customizable security models, which makes security better. This makes it possible for more security steps to be added in the future.

REFERENCES

1. S. Badotra, D. Nagpal, S. N. Panda, S. Tanwar, and S. Bajaj, "IoT-enabled healthcare network with SDN," in 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), pp. 38–42, Noida, India, 2020.
2. 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.
3. I. Udrea, V. I. Gheorghe, L. A. Cartal et al., "IoT solution for monitoring indoor climate parameters in open space offices," in 9th International Conference on Thermal Equipments, Renewable Energy and Rural Development (TE-RE-RD 2020), vol. 180, p. 02012, Constanta, Romania, 2020.
4. 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.
5. 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.
6. 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.
7. Saxena, A., Gupta, P., Rajalakshmi, B., Kanojiya, M., Praveen, P., Tyagi, L. K., & Almusawi, M. (2024). Improving Soil Properties for Construction Usage with Fly Ash and Rice Husk Ash. In E3S Web of Conferences (Vol. 507, p. 01012). EDP Sciences.
8. 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.
9. J. Kotwal, Dr. R. Kashyap, and Dr. S. Pathan, "Agricultural plant diseases identification: From traditional approach to deep learning," Materials Today: Proceedings, vol. 80, pp. 344–356, 2023.
10. Edwin Ramirez-Asis, Romel Percy Melgarejo Bolivar, Leonid Alemán Gonzales, Sushovan Chaudhury, Ramgopal Kashyap, Walaa F. Alsanie, G. K. Viju, "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.
11. 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.

12. H. Haddad Pajouh, A. Azmoodeh, A. Dehghantanha, and R. M. Parizi, "MVFCC: a multi-view fuzzy consensus clustering model for malware threat attribution," IEEE Access, vol. 8, pp. 139188–139198, 2020.
13. 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.
14. R. Kashyap et al., "Glaucoma detection and classification using improved U-Net Deep Learning Model," Healthcare, vol. 10, no. 12, p. 2497, 2022.
15. MohanaRoopa, Y., Babu, M. R., Kumar, J., & Babu, D. K. (2018). Optimal component architecture using particle swarm optimization algorithm for self-adaptive software architecture. International Journal of Engineering and Technology (UAE), 7(0), 23-26.
16. 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).
17. W. A. Saeed and A. J. Salim, "Convergence solution for some harmonic stochastic differential equations with application," Tikrit Journal of Pure Science, vol. 25, no. 5, pp. 119–123, 2020.
18. R. N. Salih and M. A. Al-jawaherry, "Finding minimum and maximum values of variables in mathematical equations by applying firefly and PSO algorithm," Tikrit Journal of Pure Science, vol. 25, no. 5, pp. 99–109, 2020.
19. 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.
20. 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.
21. M. J. Sheller, G. Anthony Reina, B. Edwards, J. Martin, and S. Bakas, "Multi institutional computing modeling without sharing patient data: a feasibility study on brain tumor segmentation. Brain lesion: glioma, multiple sclerosis, stroke and traumatic brain injuries," Brain Les (Workshop), vol. 11383, pp. 92–104, 2019.
22. S. A. Salih and G. A. Zarraq, "Applying a mathematical model to simulate the ground water reservoir in Al-Alam area/Northeast Tikrit City/Iraq," Tikrit Journal of Pure Science, vol. 26, no. 3, pp. 60–66, 2021.
23. Abood, A. S., Prashanth, K. S., Saritha, K., Kansal, L., Parashar, A. K., & Kumar, P. (2024). Estimation of PCU's in Heterogeneous Traffic by Different methods. In E3S Web of Conferences (Vol. 507, p. 01070). EDP Sciences.
24. 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.
25. 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.
26. O. I. Khalaf, F. Ajesh, A. A. Hamad, G. N. Nguyen, and D. N. Le, "Efficient dual-cooperative bait detection scheme for collaborative attackers on mobile ad-hoc networks," IEEE Access, vol. 8, pp. 227962–227969, 2020.
27. 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.
28. M. K. Shahoodh, "The adjacency matrix of the compatible action graph for finite cyclic groups of p-power order," Tikrit Journal of Pure Science, vol. 26, no. 1, pp. 123–127, 2021.
29. F. J. Suhae and A. I. Hussain, "Suitability evaluation of mudstone of Injana Formation for dam filling materials in TaqTaq area/Erbil/Iraq," Tikrit Journal of Pure Science, vol. 25, no. 3, pp. 49–56, 2020.
30. R. Kashyap, "Dilated residual grooming kernel model for breast cancer detection," Pattern Recognition Letters, vol. 159, pp. 157–164, 2022.
31. 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.
32. S. Stalin, V. Roy, P. K. Shukla, A. Zaguia, M. M. Khan, P. K. Shukla, A. Jain, "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.
33. 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.
34. S. A. Wuhaib and N. F. Abd, "Control of prey disease in stage structure model," Tikrit Journal of Pure Science, vol. 25, no. 2, pp. 129–135, 2020.
35. S. Ramaswamy, R. Mathews, K. Rao, and F. Beaufays, "Medical Applications for emoji prediction in a mobile keyboard,CoRR," 2019,
36. Naresh, M., & Munaswamy, P. (2019). Smart agriculture system using IoT technology. International journal of recent technology and engineering, 7(5), 98-102.
37. 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.
38. Puchakayala, S. S. R., Samayamantry, K. N. D., Ogirala, S. S. V. N., Saeed, H. Y., Aravinda, K., Lakhanpal, S., & Kalra, R. (2024). Smart fitness trainer using an advanced interdisciplinary approach. In E3S Web of Conferences (Vol. 507, p. 01043). EDP Sciences.
39. L. Huang, A. L. Shea, H. Qian, A. Masurkar, H. Deng, and D. Liu, "Patient clustering improves efficiency of federated machine learning to predict mortality and hospital stay time using distributed electronic medical records," Journal of Biomedical Informatics, vol. 99, article 103291, 2019.
40. 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.
41. 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.
42. 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.
43. 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.
44. K. Kaushik, S. A. Yadav, V. Chauhan and A. Rana, "An Approach for Implementing Comprehensive Reconnaissance for Bug Bounty Hunters," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 189-193, doi: 10.1109/IC3I56241.2022.10072942.
45. 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
46. P. K. Kushwaha, A. Rana, S. Srivastava, A. Saifi, A. Tavish and P. Chaturvedi, "Employee Absenteeism Prediction Using Machine Learning," 2023 10th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), Gautam Buddha Nagar, India, 2023, pp. 116-121, doi: 10.1109/UPCON59197.2023.10434342.