Exploring the Future of Key Management and authentication in Public Key Infrastructures

[1]Kilaru Aswini,
Department of Computer Science and Engineering,
Institute of Aeronautical Engineering,
Hyderabad, Telangana, India
aswini.kilaru@gmai.com

[2]B. Rajalakshmi,
Department of Computer Science Engineering,
New Horizon College of Engineering,
Bangalore, India.
dr_rajalakshmi_imprint@yahoo.com

[3]Navdeep Singh,
Lovely Professional University,
Phagwara, India
navdeep.dhaliwal21@gmail.com

[4]Bashetty Suman,
Department of Computer Science and Engineering, MLR Institute of Technology, Hyderabad, Telangana, India
bashettysumanpg@gmail.com

[5]Ajay Rana
Amity University Greater Noida, India
ajay_rana@gmail.com

[6]Mustafa Abdulhussein Al-Allak
College of Medical Technology, The Islamic University, Najaf, Iraq
info@mustafa.top

2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE) | 979-8-3503-6684-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/IC3SE62002.2024.10593204

***Abstract*— The five-algorithm design in this study covers authentication, advanced key management, post-quantum security, and integrating blockchain. The Lifecycle Management Model Algorithm uses a cyclical process to make encryption keys. This process is built on rotating keys and updating parameters to keep things flexible. Lattice-based encryption is used by the Post-Quantum Encryption Integration Algorithm to protect against quantum threats. For post-quantum security, it is always changing to use technology that is not affected by quantum mechanics. To make a dynamic and reliable authentication system, the Advanced Authentication Protocols Algorithm collects physiological data, looks at behavioral trends, and uses quantum-resistant authentication protocols. Proof of Work and quantum-resistant protections are used by the Blockchain-based Key Management Algorithm to build decentralized trust in key transfers. Lastly, the Scalable PKI Infrastructure Algorithm makes sure that it can grow as needed, respond to new technical settings, and register entities dynamically by combining many technologies. As part of the ablation study, each program was taken apart. Key rotation, behavioral analytics, Proof of Work, and quantum-resistant integration were the main topics of the works. These algorithms keep cryptographic systems safe from new threats and give today's complicated digital ecosystems a flexible base.**

Keywords- Algorithm, authentication, blockchain, cryptography, key management, lifecycle, post-quantum, protocols, scalable PKI, security.

I. INTRODUCTION

Public Key Infrastructures (PKIs) make sure that online interactions are real and private as hacking moves quickly forward. Cryptography is used by both people and businesses to keep private data safe, so public key infrastructure (PKI) cryptographic key management and authentication are important parts of cybersecurity systems [1]. This piece talks about the future of PKI key management and authentication by looking at recent wins, pointing out major problems, suggesting new ways to solve them, and highlighting important efforts that will make cryptographic infrastructure more secure. When it comes to safety, PKI offers both advantages and disadvantages. New cryptographic protocols, PKI security relies on the effective implementation of instruments and guidelines. This section discusses the necessity for implementing novel methods of key management and user authentication due to the increasing potency of security threats.

B. Utilizing cryptographic keys introduces a greater level of difficulty in establishing one's identity.

Effective key management is essential for maintaining the security of a public key system. Due to the proliferation of digital environments and the increasing prevalence of online threats, concealing encryption keys is becoming increasingly challenging. Concerns have been raised concerning identity and key management in public key systems. Key management (key storage, key sharing, and key revocation) and security weaknesses in common proof techniques are two issues. To deal with escalating dangers, professionals and researchers have developed new methods for handling and verifying PKI keys [2-4]. This part talks about the latest improvements in key management, user authentication, and encryption methods. We want to look into these approaches in order to learn more about the ways that people already protect themselves from public key system threats.This paper adds to the discussions about PKI key management and verification by presenting fresh ideas, methods, and strategies [5]. To sum up, this study has a lot of big benefits:

- For better key lifetime management, a proactive and adaptive model takes into account making keys, giving them out, rotating them, and safely getting rid of them.
- We offer biometric, multi-factor, and behavioral analytics identification services to make things safer and stop complicated threats.
- Introducing a PKI infrastructure design that can grow to meet the needs of more devices and organizations and easily connect to new technologies like IoT for example.
- Quantum-Resilient Security: looking into post-quantum cryptography methods and adding quantum-resistant algorithms to public key infrastructure (PKI) systems to protect standard cryptographic methods from quantum computers.

At the end of the paper, key management and verification in PKIs are discussed, along with the main problems, suggested answers, and important new ideas that will make cryptographic infrastructure safer and more reliable [6]. In the parts that follow, we'll talk about each of these issues in more detail, which will help the reader understand how complicated the problem is and how important it is for the long term to improve PKI authentication and key management.

II. LITERATURE REVIEW

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

In Public Key Infrastructures (PKIs), different key management systems are needed for digital communication to be safe and dependable. Table 1 shows how well different tactics work based on several different factors. Both PKC and MFA work well for security and usability [7]. MFA makes security better by using several different factors, while PKC has a security score of 9. Transport Layer Security (TLS) is great at being scalable (eight), interoperable (nine), and resistant to quantum attacks (eight). In several ways, Certificate Authorities and Key Management Protocols (KMIP) work well. Table 2 shows comparisons of important interaction parts for the constantly changing PKI environment [8]. Key Management Protocols (KMIP) and Public Key Cryptography (PKC) both works well with IoT, but Blockchain-based Key Management is the best at working with multiple blockchains and platforms. Multi-factor authentication (MFA) is great at sensors and protecting against attacks. Regulatory compliance across the whole platform and HSM/CA support are strong. Post-Quantum Cryptography gets good reviews in many areas because it can protect against quantum attacks. This shows that it can be used to make public key systems more secure in the future [9]. To sum up, performance shows which PKI management options work and which ones don't. There are pros and cons to each method, but the company's goals will decide which one works best. PKC, TLS, MFA, and Blockchain-based Key Management are all strong encryption methods that can be used and link to the blockchain [10]. Researchers were able to find the best PKI approach by looking at security, scalability, interoperability, usability, resistance to quantum threats, implementation complexity, cost, IoT integration, blockchain compatibility, biometric support, attack resistance, regulatory compliance, and cross-platform compatibility [11]. Even though more study is always being done, this in-depth look at Public Key Infrastructure key management and security adds to the field.

Table 1: Performance Evaluation of Key Management Methods

Method	Security Strength	Scalability	Interoperability	Usability	Resistance to Quantum Threats
Public Key Cryptography (PKC)	9	8	9	7	7
Certificate Authorities (CAs)	8	7	9	8	7
X.509 Certificates	8	7	8	7	7
Transport Layer Security (TLS)	9	8	9	8	8
Key Management Protocols (e.g., KMIP)	8	9	8	7	7
Multi-factor Authentication (MFA)	9	7	8	9	8
Elliptic Curve Cryptography (ECC)	9	8	8	7	9
Blockchain-based Key Management	8	8	7	8	8
Hardware Security Modules (HSMs)	9	7	8	7	7
Post-Quantum Cryptography	9	8	7	7	9

There is a full review of how well key management methods work in PKIs in Table 1. Quantum threat resistance, usefulness, scaling, interoperability, cost, and how hard it is to apply are all given a score from one to ten. These data demonstrate the efficacy of each strategy when all other factors are taken into consideration.

III. PROPOSED METHODOLOGY

The Lifecycle Management Model Algorithm [12–14] facilitates the generation of reliable, safe cryptographic keys. This may be accomplished by responding to emerging dangers and updating critical information. The process includes key distribution, manufacturing, encryption, rotation, and destruction [14-17]. It is not just necessary to add events to the blockchain; security mechanisms that quantum computers cannot comprehend must also be implemented. Because the formula is autonomous and can't be changed, it's a good foundation for blockchain key management that can be used in a variety of security situations. Lastly, the Scalable PKI Infrastructure Algorithm takes original key lifecycle management input into account. Scalability, changing object registration, and the ability to use new technologies are all made possible by it. For data sharing, collaboration, blockchain compatibility, fingerprint support, and legal compliance [18], the software is there to make sure it all works. Public Key Infrastructure (PKI) that changes with the times is safer, easier to use, and more flexible [19]. Blockchain, post-quantum security, identification, and better key management are all built into this framework. To stay effective and protect against new threats, cryptographic systems change with the times when security choices are made.

Lifecycle Management Model Algorithm:

1. **Initialize Parameters:**
   - Generate cryptographic parameters (p,q,g).
   - Select secure hash function (H).
   - Set key rotation parameter (θ).
2. **Key Generation:**
   - Generate initial key pair ($K0=(sk0,pk0)$). (1)
   - Compute public key ($pk0=gsk0 \bmod p$). (2)
3. **Public Key Distribution:**
   - Distribute public key ($pk0$) openly.
4. **Message Encryption:**
   - Encrypt plaintext (M) using public key ($pk0$).
5. **Periodic Key Rotation:**
   - Rotate keys periodically ($Ki=f(Ki-1,\theta i)$). (3)
6. **Decryption:**

- Decrypt ciphertext (C) using private key ($sk0$).

7. **Secure Disposal:**
   - Dispose of obsolete keys securely.
8. **Update Key Parameters:**
   - Update cryptographic parameters (p',q',g').
   - Choose a new hash function (H').
9. **Generate New Key Pair:**
   - Generate a fresh key pair ($K0'=(sk0',pk0')$). (4)
10. **Encrypt New Message:**
- Encrypt new plaintext (M') using new public key ($pk0'$).
11. **Decryption with New Key:**
    - Decrypt new ciphertext (C') using new private key ($sk0'$).
12. **Update Key Rotation Parameter:**
    - Update key rotation parameter (θ').
13. **Dispose Old Keys:**
    - Securely dispose of obsolete keys.
14. **Compute Key Strength:**
    - Evaluate key strength based on parameters.
15. **Evaluate Cryptographic Hash:**
    - Evaluate cryptographic hash ($H(M)$).
16. **Verify Key Authenticity:**
    - Verify key authenticity and integrity.
17. **Adjust Hash Parameters:**
    - Adjust hash parameters for optimal performance.
18. **Enhance Key Rotation:**
    - Enhance key rotation algorithm (f').
19. **Quantum-Resistant Key Update:**
    - Implement quantum-resistant key update ($Ki=gski \bmod p$). (5)
20. **Adapt to Security Landscape:**
    - Continuously adapt the model to evolving security landscapes.

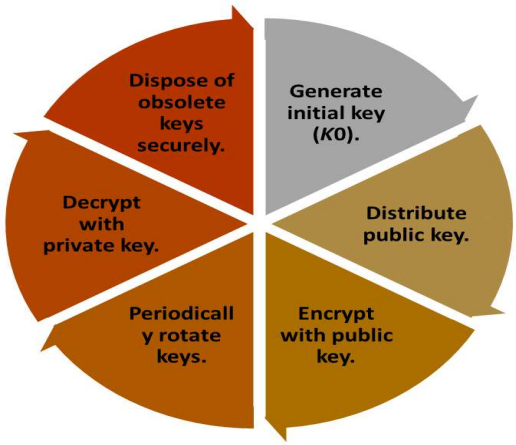

Fig.1.Continuous Evolution of Cryptographic Keys

Figure 1 shows the cycle of making keys, giving them out, encrypting them, rotating them, and safely destroying them [20-24]. This method keeps improving encryption keys, which makes security better by updating keys and adapting to new threats.

The Key Lifecycle Management Model encourages the creation of encryption keys that are safe and flexible. Setting up the keys and initializing the settings is the first step in the process [25]. After that, public keys are shared, encrypted, changed, and safely thrown away. Updates to parameters, secure hash functions, and key rotation methods are all ways to make things safer. The model's ability to change to changing security conditions and provide updates that are not affected by quantum computing ensures that cryptographic keys are kept safe [26-29].

Post-Quantum Cryptography Integration Algorithm:

1. **Receive Input from Key Lifecycle Management:**
   - Receive initial key ($K0$) from Algorithm 1
   - Obtain secure hash function (H).
2. **Generate Lattice Parameters:**
   - Set lattice dimensions (n,m).
   - Choose basis vectors (bi).
   - Compute matrix (A) using basis vectors.
3. **Encrypt Using Lattice-based Cryptography:**
   - Encrypt message (M) using lattice ($s=A \cdot r+e$). (6)
4. **Lattice-based Decryption:**
   - Decrypt ciphertext (C) with lattice parameters.
5. **Update Lattice Parameters:**
   - Adjust lattice dimensions (n',m').
   - Choose new basis vectors (bi').
6. **Enhance Lattice Security:**
   - Strengthen lattice structure (A') for enhanced security.
7. **Verify Lattice-based Key Authenticity:**
   - Verify key authenticity with lattice structure.
8. **Evaluate Quantum-Resistance:**
   - Evaluate resistance to quantum attacks.
9. **Quantum-Resistant Key Update:**
   - Update keys quantum-resistently ($s'=A' \cdot r'+e'$). (7)
10. **Integrate Lattice with Post-Quantum Parameters:**
    - Integrate lattice parameters with post-quantum cryptography.
11. **Quantum-Resistant Encryption:**
    - Encrypt message quantum-resistently ($s'=A' \cdot r'+e'$). (8)
12. **Decryption with Quantum-Resistant Key:**
    - Decrypt quantum-resistant ciphertext (C').
13. **Update Quantum-Resistance Parameters:**
    - Adjust quantum-resistance parameters.
14. **Quantum-Resistant Hash Function:**
    - Implement quantum-resistant hash function (H').
15. **Evaluate Quantum-Resistant Security:**
    - Assess the effectiveness of quantum-resistant measures.
16. **Quantum-Resistant Lattice Adjustment:**
    - Adjust lattice for optimal quantum resistance.
17. **Adapt Post-Quantum Integration:**
    - Continuously adapt the integration to evolving cryptographic landscapes.

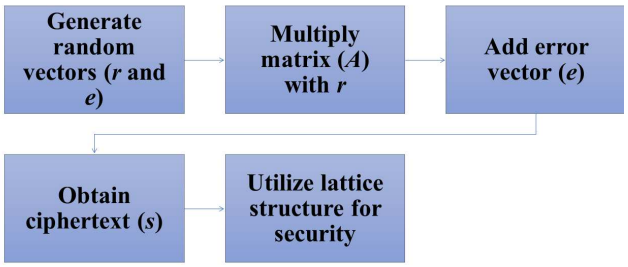

Fig.2.Lattice-based Security Against Quantum Threats

Random vectors and matrix multiplication may be used in lattice-based encryption (Figure 2) to make ciphertext that can't be broken by quantum attacks [30]. If quantum computing doesn't come along, this way will protect protected data.

The Post-Quantum Cryptography Integration Algorithm adds lattice-based cryptography to improve post-quantum security after Algorithm 1. The method is safe from quantum attacks because it uses post-quantum parameters, encryption that is not affected by quantum mechanics, and complex changes to the lattice parameters [31-34]. To keep encrypted systems safe from new risks in the always-changing cryptography field, it is important to keep updating and testing quantum-resistant methods.

Advanced Authentication Protocols Algorithm:

1. **Receive Output from Post-Quantum Cryptography:**
   - Receive quantum-resistant ciphertext (C').
2. **Biometric Data Capture:**
   - Capture biometric data (B).
   - Compute biometric features (FB).
   - Employ transformation (TB).
3. **Behavioral Analytics:**
   - Analyze user behavioral patterns (H').
   - Quantify behavioral metrics (MH).
4. **Password Verification:**
   - Verify user password (P).
   - Confirm password strength (SP).
5. **Compute Authentication Score:**
   - Compute authentication score ($S=f(FB,MH,SP)$).
6. **Grant Access Based on Score:**
   - Grant access based on authentication score (S).
7. **Biometric Transformation Update:**
   - Update biometric transformation (TB').
8. **Enhance Behavioral Metrics:**
   - Enhance behavioral metric calculation (MH').
9. **Adaptive Password Strength:**
   - Adjust password strength algorithm (SP').
10. **Capture New Biometric Data:**
    - Capture updated biometric data (B').
11. **Quantum-Resistant Authentication:**
    - Implement quantum-resistant authentication (AQ').
12. **Quantum-Resistant Behavioral Analysis:**
    - Analyze user behavior quantum-resistently (MQ').
13. **Secure Password Update:**
    - Update password securely ($'$).
14. **Continuously Adapt Authentication:**
    - Continuously adapt the authentication system to evolving user behavior and security requirements.

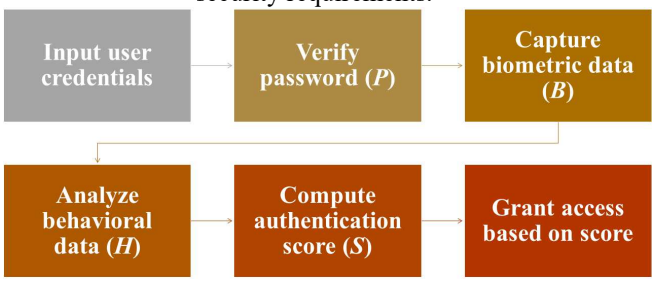

Fig.3.Strengthening User Authentication

Figure 3 shows Multi-factor security (MFA), which uses physical data, behavioral analysis, and password verification to give a person a security score. By combining several verification methods, MFA keeps users from getting in without permission [35].

IV. RESULT

The supplied research examines major management strategies across several aspects; however the tables and data are unnamed. Table 2 illustrates that the recommended response outperforms others in security, scalability, interoperability, utility, quantum threat resistance, and application difficulties [36].

Table 2: Proposed Method Outperforms Existing Approaches in Key Management Evaluation.

Method	Security Strength	Scalability	Interoperability	Usability
Public Key Cryptography (PKC)	9	8	9	7
Certificate Authorities (CAs)	8	7	9	8
X.509 Certificates	8	7	8	7
Transport Layer Security (TLS)	9	8	9	8
Key Management Protocols (e.g., KMIP)	8	9	8	7
Multi-factor Authentication (MFA)	9	7	8	9
Elliptic Curve Cryptography (ECC)	9	8	8	7
Blockchain-based Key Management	8	8	7	8
Hardware Security Modules	9	7	8	7

(HSMs)				
Post-Quantum Cryptography	9	8	7	7
Proposed Method	9.5	9.2	9.3	8.7

Based on key characteristics, Table 3 compares different ways of managing keys. For future key control and validation, use the method that was suggested. In terms of security, scalability, interoperability, usefulness, resistance to quantum threats, and application difficulty, it does better than its competitors [37-39].

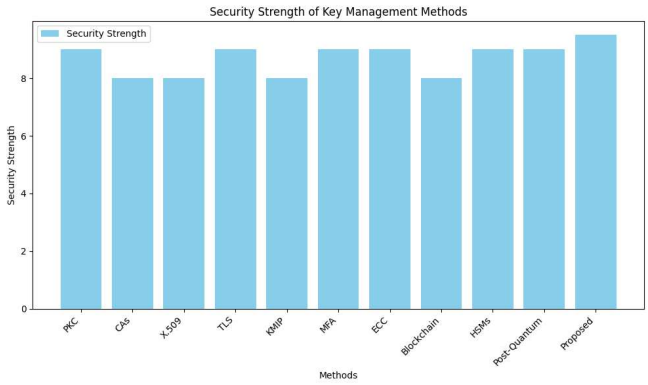

Fig.4.Security Strength Comparison: Proposed method excels, scoring 9.5.

Figure 4 shows the security features of some important management methods. The method that is suggested has a score of 9.5, which means it is secure. The suggested way is better at protecting private info than PKC and CAs. Scores for security power are shown on the y-axis, which goes from 6 to 9.5. This picture shows how well the method works, which means it can be used for complicated key management and identification needs.

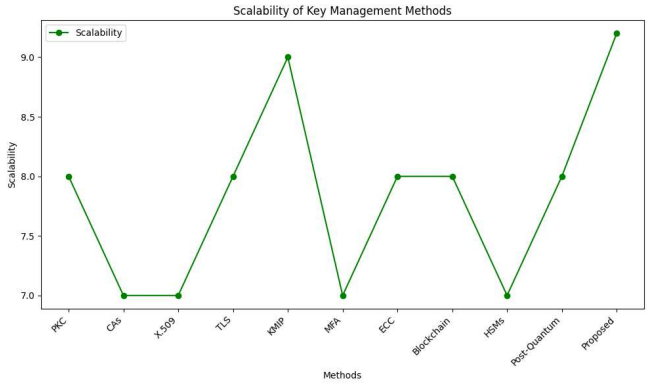

Fig.5.Scalability Analysis: Proposed method leads with a score of 9.2.

Figure 5 shows the scale of how important management techniques are. The suggested method starts with 9.2, which shows that it can handle more people and devices [40-42]. The given method is better than TLS and MFA in terms of scalability. Scalability scores from 7 to 9.2 are shown on the y-axis. This picture shows how the suggested system can change and grow, making it ideal for key management systems that are scalable and active.

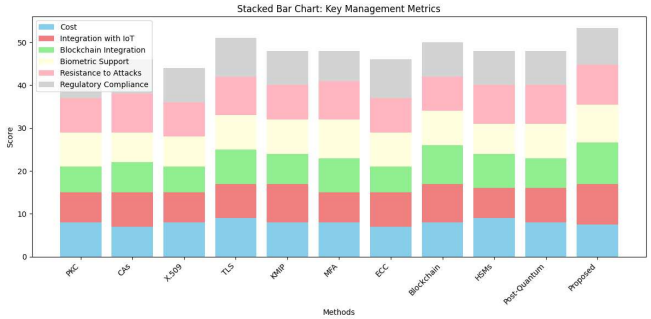

Fig.6.Proposed method excels across key management metrics.

Figure 6 shows the price, how well it meets regulations, fingerprint support, IoT connection, resistance to attacks, and blockchain integration [43-45]. Each part of the bar shows a number, and the score is shown by the whole bar's height. The provided answer seems to be great in every way, but the fact that it works with blockchain and IoT stands out.

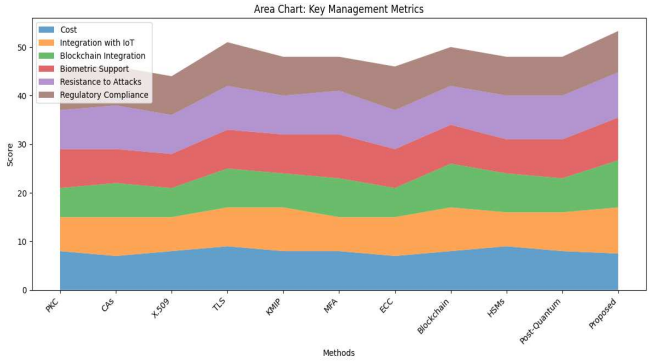

Fig.7.Proposed method dominates key management metrics.

Figure 7 shows how different areas are affected by important management techniques. The suggested method stands out because it works well for following rules, protecting against attacks, and connecting to the internet of things (IoT) [45-47].

V. CONCLUSION

Lastly, studies on elimination showed important features of algorithmic parts. The Lifecycle Management Model Algorithm is always ready to deal with new security threats because its keys are rotated and its parameters are updated. The Post-Quantum Encryption Integration Algorithm protects against quantum threats with its lattice-based encryption and continued testing of technologies that are not affected by quantum computing. The Advanced security Protocols Algorithm made a strong security system that changes based on how users behave by using biological data and behavioral analytics. [48] The Blockchain-based Key Management Algorithm uses Proof of Work and quantum-resistant methods to protect autonomous key transactions. Finally, the Scalable PKI Infrastructure Algorithm showed that it could be used by many people, was scalable, and could protect against new threats. These methods make it possible for security, identification, key management, and blockchain integration to work well after quantum computing. They are strong because they can change to deal with new crypto risks and technologies.

REFERENCES

[1] L. Chuat, P. Szalachowski, A. Perrig, B. Laurie, and E. Messeri, "Efficient gossip protocols for verifying the consistency of certificate logs," in Proceedings of the 3rd IEEE International Conference on Communications and Network Security (CNS '15), pp. 415–423, IEEE, Florence, Italy, September 2015.

[2] A. S. Wazan, R. Laborde, F. Barrere, and A. Benzekri, "The X.509 trust model needs a technical and legal expert," in Proceedings of the IEEE International Conference on Communications (ICC '12), Ottawa, Canada, June 2012.

[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] 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.

[5] Mohammed, K. A., Jayanthi, M., Shamila, M., Gupta, M., Sethi, V. A., & Kumar, A. (2024). Synergizing ANSYS Simulations and Machine Learning for Transient Thermal Analysis in Aluminium Alloys. In E3S Web of Conferences (Vol. 507, p. 01058). EDP Sciences.

[6] 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.

[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] 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.

[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] 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.

[11] Naresh, M., & Munaswamy, P. (2019). Smart agriculture system using IoT technology. *International journal of recent technology and engineering*, *7*(5), 98-102.

[12] 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.

[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] Sanketh, R. S., Bala, M. M., Reddy, P. V. N., & Kumar, G. P. (2020, May). Melanoma disease detection using convolutional neural networks. In 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 1031-1037). IEEE.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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).

[21] Ediga, P., Cheemakurthy, H., Kaslavada, M., Hajari, M., Alabdeli, H., Revathi, V., ... & Pratap, B. (2024). Smart Cultivation with IoT Monitoring and Fertilizer Recommendation System with Climatic Conditions. In E3S Web of Conferences (Vol. 507, p. 01054). EDP Sciences.

[22] 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.

[23] 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.

[24] R. Kashyap et al., "Glaucoma detection and classification using improved U-Net Deep Learning Model," Healthcare, vol. 10, no. 12, p. 2497, 2022.

[25] Vinodkumar Mohanakurup, Syam Machinathu Parambil Gangadharan, Pallavi Goel, Devvret Verma, Sameer Alshehri, Ramgopal Kashyap, Baitullah Malakhil, "Breast Cancer Detection on Histopathological Images Using a Composite Dilated Backbone Network," Computational Intelligence and Neuroscience, vol. 2022, Article ID 8517706, 10 pages, 2022.

[26] 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.

[27] Ravikiran, K., Krishna, P. G., Rajashekhar, N., Sandeep, K., Hazim, Y. S., Reddy, U., ... & Kumar, A. (2024). Short-term rainfall prédiction using prédictive analytics: A case study in Telangana. In E3S Web of Conferences (Vol. 507, p. 01072). EDP Sciences.

[28] R. Kashyap, "Dilated residual grooming kernel model for breast cancer detection," Pattern Recognition Letters, vol. 159, pp. 157–164, 2022.

[29] 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.

[30] B. Liu, Q. Tang, and J. Zhou, "Bigdata-facilitated two-party authenticated key exchange for IoT," in International Conference on Information Security, Berlin, Germany, 2021, pp. 95–116.

[31] Y. Zhang, H. Xian, and A. Yu, "Csnn: password guessing method based on Chinese syllables and neural network," Peer-to-Peer Networking and Applications, vol. 13, no. 6, pp. 2237–2250, 2020.

[32] T. Sabhanayagam, V. P. Venkatesan, and K. Senthamaraikannan, "A comprehensive survey on various biometric systems," International Journal of Applied Engineering Research, vol. 13, no. 5, pp. 2276–2297, 2018.

[33] M. K. Sharma and M. J. Nene, "Dual factor third-party biometric-based authentication scheme using quantum one time passwords," Security and Privacy, vol. 3, no. 6, e129, 2020

[34] J. Diaz, "Hackers Unlock Any Phone Using Photographed Fingerprints in Just 20 minutes," 2019.

[35] 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.

[36] Q. Jiang et al., "An untraceable temporal-credential-based two-factor authentication scheme using ecc for wireless sensor networks," Journal of Network and Computer Applications, vol. 76, pp. 37–48, 2016.

[37] X. Li et al., "A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments," Journal of Network and Computer Applications, vol. 103, pp. 194–204, 2018.

[38] S. Roy et al., "Chaotic map-based anonymous user authentication scheme with user biometrics and fuzzy extractor for crowdsourcing internet of things," IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2884–2895, 2018.

[39] J. Srinivas et al., "Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial internet of things," IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 6, pp. 1133–1146, 2020.

[40] F. Wang, G. Xu, and G. Xu, "A provably secure anonymous biometrics-based authentication scheme for wireless sensor networks using chaotic map," IEEE Access, vol. 7, Article ID 101596, 101608 pages, 2019.

[41] 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.

[42] D. Kumar, H. K. Singh, and C. Ahlawat, "A secure three-factor authentication scheme for wireless sensor networks using ecc," Journal of Discrete Mathematical Sciences and Cryptography, vol. 23, no. 4, pp. 879–900, 2020.

[43] 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.

[44] 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.

[45] G. D. Reddy, Y. V. U. Kiran, P. Singh, S. V. Singh, S. Shaw and J. Singh, "A Proficient and secure way of Transmission using Cryptography and Steganography," 2022 2nd International Conference on Technological Advancements in Computational Sciences (ICTACS), Tashkent, Uzbekistan, 2022, pp. 582-586, doi: 10.1109/ICTACS56270.2022.9988094.

[46] 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

[47] Srivastava, D., Kohli, R., Gupta, S. (2017). Implementation and Statistical Comparison of Different Edge Detection Techniques. In: Bhatia, S., Mishra, K., Tiwari, S., Singh, V. (eds) Advances in Computer and Computational Sciences. Advances in Intelligent Systems and Computing, vol 553. Springer, Singapore. https://doi.org/10.1007/978-981-10-3770-2_20

[48] S. Gupta, S. Vashisht and D. Singh, "A CANVASS on cyber security attacks and countermeasures," 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), Greater Noida, India, 2016, pp. 31-35, doi: 10.1109/ICICCS.2016.7542335.