IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SECURITY USING ELLIPTIC CURVE CRYPTOGRAPHY (ECC) IN CLOUD

S. Nagendrudu [1a)],P. Ishaq Alam [1b)],B. Srinivasulu [1c)] ,S. Sai Nanda Kishore [1d)], U. Giri Babu [1e)] and S. Shahid Basha[1f)]

[1] Asst.Professor,Department of Computer Science & Engineering, Santhiram Engineering College, Nandyal-518501, AndhraPradesh, India

[2,3,4,5] Student,Department of Computer Science & Engineering, Santhiram Engineering College, Nandyal-518501, AndhraPradesh, India

Abstract: Because of their cost-effectiveness and abundance of computing resources, enterprises from many industries now use cloud services for efficient data storage and administration. However, this technique raises worries regarding data security since sensitive information is handed to third-party cloud servers, which are subject to unauthorized access by internal workers or hostile hackers. To address these security concerns, encryption methods such as AES, RSA, and DES have been created, preserving data confidentiality by encrypting information prior to storage on the cloud. This suggested study proposes Elliptic Curve Cryptography (ECC) as an alternate encryption strategy for protecting data in cloud environments. Unlike older methods, ECC provides a lightweight solution for key creation and maintenance, requiring less computing time and resources. This study provides a detailed comparison of ECC and the widely used AES algorithm, with a focus on encryption time performance. Experimental results show that ECC beats AES, delivering quicker and more efficient encryption procedures, lowering cloud use costs. The findings of this study help to advance the area of cloud data security by providing a potential answer to enterprises seeking comprehensive protection for sensitive information in an ever-changing digital context.

Keywords: Cloud Computing ,Cryptography ,Elliptic curve cyptography algorithm,security

1. INTRODUCTION

Cloud services are essential to organizational operations across industries in the digital age. Cost-effectiveness and unlimited computing capabilities have pushed companies to outsource data storage and administration to cloud servers. This convenience has drawbacks, particularly data security. The risk of internal workers or hackers accessing sensitive data is serious.

Organizations have used encryption techniques like AES, RSA, and DES to protect data before cloud storage. This research proposal proposes Elliptic Curve Cryptography (ECC), an encryption method meant to improve cloud data security. ECC reduces computational time and resource needs for key creation and management compared to older methods.

This research compares ECC with the widely used AES algorithm, focusing on encryption time performance, to advance cloud data security. The study aims to prove that ECC is quicker and more efficient than AES through extensive experimentation. This research goes beyond performance measurements, presenting a viable way for enterprises to secure critical data in the dynamic digital environment while reducing cloud use expenses.

Cloud data security depends on encryption methods. AES has long been the benchmark for data security because to its durability and dependability. As enterprises increasingly use cloud services for data storage, AES encryption's computational cost becomes an issue, especially for huge data sets. However, because to its lightweight nature, ECC is more efficient and ideal for cloud situations with limited computing resources.

This study compares ECC with AES to prove ECC's encryption time advantage. The project will employ both encryption techniques on the cloud and measure their encryption times for different data amounts. Key generation time and resource consumption will also be assessed to fully understand ECC and AES performance disparities.

This research should impact cloud data security efforts. ECC's higher encryption time might help enterprises choose it as their preferred method for cloud data security. ECC's decreased computational overhead reduces encryption resources, saving companies money and improving efficiency.

In conclusion, this research proposal describes a detailed cloud encryption time comparison of ECC and AES. This research aims to help enterprises improve data security, resource usage, and cloud costs by showing ECC's better efficiency.

In cloud contexts, this research compares Elliptic Curve Cryptography (ECC) to the commonly used Advanced Encryption Standard (AES) encryption performance. ECC is tested for encryption time efficiency to prove its superiority over AES. This paper uses rigorous experiments to demonstrate that ECC is a more efficient encryption technique, providing enterprises a viable choice for cloud data security while decreasing computing resource needs.

Data security is a major problem with the increased use of cloud storage services. Despite its ease and cost-effectiveness, corporations confront major problems, mostly from internal workers and hackers. AES, RSA, and DES are used, although they are computationally intensive. This study proposes Elliptic Curve Cryptography (ECC) for more efficient encryption. The question is whether ECC can surpass AES in cloud data security by encrypting quicker and more efficiently.

2. LITERATURE SURVEY

By delivering flexible and scalable resources on demand, cloud computing has transformed organizations. The increased use of cloud services has generated data security and privacy issues. Recently, academics have concentrated on improving cloud computing security using cryptographic approaches like Elliptic Curve Cryptography. This literature review examines ECC-focused research on cloud computing data security.

Cloud computing is cost-effective, scalable, and accessible. Data security, privacy, and integrity problems limit its usage. Maintaining user confidence and protecting sensitive data requires cloud data security [5].

Understanding cloud computing security concerns is crucial before exploring researchers' solutions. The challenges are data breaches, insider attacks, insecure APIs, data loss, and regulatory compliance [7]. These issues require a multifaceted strategy involving cryptography, access restrictions, and secure protocols.

Cloud data security relies on cryptography. Elliptic Curve Cryptography (ECC) is popular due to its efficiency and security [3]. ECC provides equal security to classic cryptosystems with reduced key sizes, making it ideal for resource-constrained cloud computing [8].

Numerous studies have examined how ECC and other cryptographic methods might improve cloud computing security. These research suggest new security frameworks and methods. Key contributions in this discipline are summarized below:

Tripathi and Yadav proposed an enhancement to cloud data security using ECC to secure sensitive data [6]. Researchers have created cloud-specific data security models. Yuefa et al. presented a cloud computing data security model that handles multi-tenancy and data migration [9]. ECC encryption in Java was studied by Nautiyal and Sharma for cloud data security [10]. Kulkarni and Mishra suggested a cloud computing dataset segmentation method that uses ECC and other security methods to guarantee data integrity and confidentiality [11]. ECC was used by Doe and Alfa to avoid cloud data leaking [13]. Tirthani and Ganesan suggested using Diffie-Hellman and ECC to secure cloud data [14].

Each technique provides distinct insights and contributions, but they must be tested in real-world situations. Consider processing overhead, scalability, and cloud platform compatibility. Comparative assessments of different methods can uncover strengths and flaws, leading cloud security research.

Finally, cloud data security is complicated and requires a holistic strategy. Cryptographic methods, especially Elliptic Curve Cryptography, reduce security risks and protect data confidentiality, integrity, and availability. This literature study shows how creative ideas and frameworks are improving cloud computing security. We can create a more secure and trustworthy cloud computing ecosystem by tackling major obstacles and using modern cryptography.

3. METHODOLOGY

i) Proposed Work:

The suggested method uses Elliptic Curve Cryptography (ECC) as a unique encryption algorithm to improve data security in cloud environments. This method will be fully compared against the widely known AES algorithm, with an emphasis on encryption time performance. The study's goal is to show that ECC outperforms AES in terms of encryption speed and efficiency. The suggested system provides a lightweight approach for key generation and administration, solving security concerns in cloud services while reducing computational time and resource needs. This novel technique promises to improve data protection in the ever-changing digital ecosystem, providing enterprises with a cost-effective and efficient way to secure critical information.

ii) System Architecture:

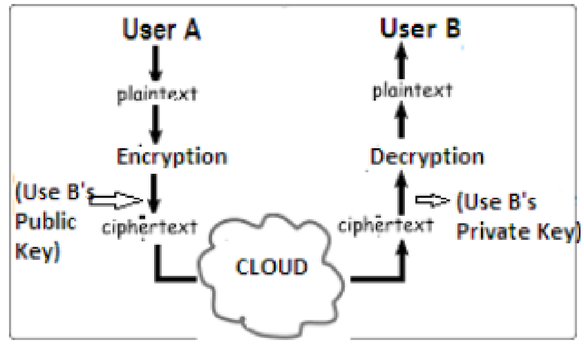


Fig 1 Proposed Architecture

iii) Implementation:

Now-a-days, all organizations such as Facebook, Whatsapp, Healthcare, banking, and many more applications are using cloud services to store and manage their business data because cloud services provide heavy computation resources and storage spaces at a lower cost. However, this advantage leads to data security issues because user's data is stored at a third-party cloud server that is completely away from the user's hand, and cloud server's internal employees or hackers may misuse this data. Internal staff or hackers may have access to data but are unable to read or interpret it. All existing algorithms require large key generation and management, which takes a lot of computation time and resources, potentially increasing cloud usage costs. To solve this problem, the ECC (elliptic curve cryptography) algorithm is introduced, which is lighter to generate keys and requires less computation time and resources to encrypt or decrypt data. So, in the proposed work, we use the ECC method to encrypt data before sending it to the cloud and then compare its encryption time performance to the AES algorithm. The experiment with AES and

ECC demonstrates that ECC is lighter and quicker than AES.

To accomplish this project, we built two separate apps.

Cloud Servers: This is a Python-based cloud server that accepts input files from users and saves them to its storage space. Any time a user sends a request to download a certain file, the cloud will respond with the file. All files sent to the cloud will be encrypted with ECC.

Cloud User: The user will upload a file, encrypt it using ECC, and then transfer or outsource it to the cloud for storage. Any time, a user may submit a request to the cloud to download a file and then decrypt it.

To accomplish this project, we created the following components.

Upload File: With this module, we can upload any file to the application.

Encrypt File Using AES: Using this module, we will read file data, encrypt it with the AES method, and then compute the encryption time.

Encrypt File Using ECC: In this module, we will encrypt a file using the ECC technique and then compute the encryption time.

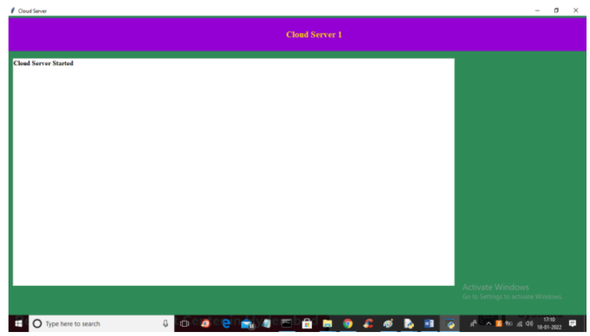
Outsource File to Cloud: Using this module, we will outsource files to a cloud server for storage.

Download File: Using this module, we will submit a file request to the cloud, then download and decrypt it.

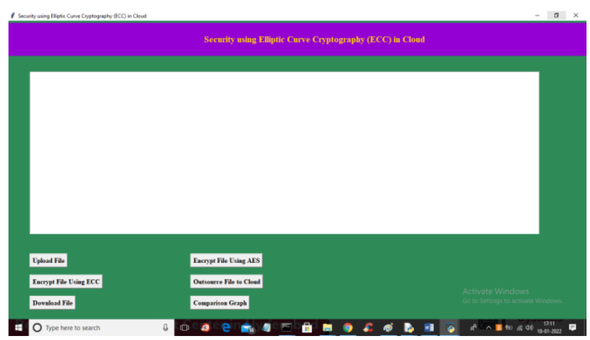
Comparison Graph: Using this module, we will plot an encryption time graph comparing the AES and ECC algorithms.

4. EXPERIMENTAL RESULTS

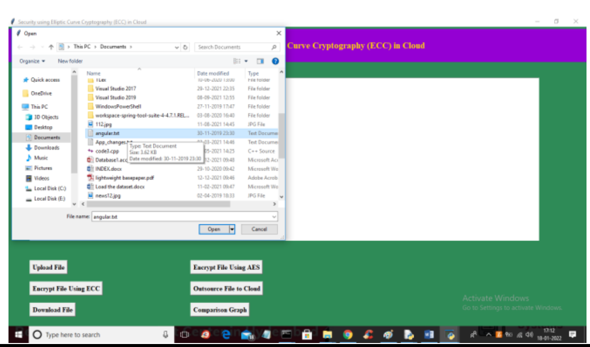
To execute the project, first double-click on the 'run.bat' file in the 'CloudServer' folder to start the cloud application and see the following screen.



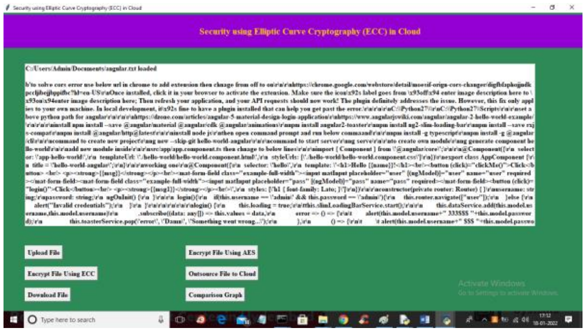
In the above screen, the cloud server has begun. Now, double-click on the 'run.bat' file from the 'CloudUser' folder to start the cloud user application and obtain the below screen.



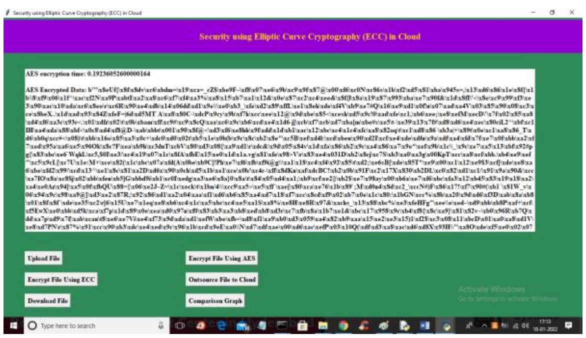
In the above screen, click on the 'Upload File' button to upload any file to the program, as shown below.



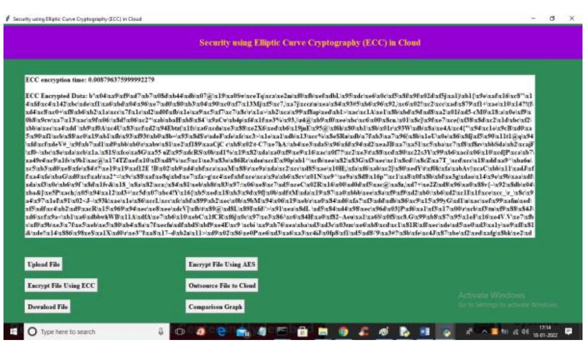
In the above screen, choose and upload the 'angular.txt' file, and then click on the 'Open' button to load the file and receive the following screen.



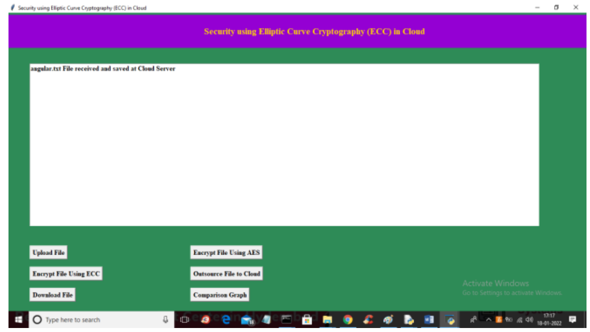
In the above screen, the file is loaded, and now click on the 'Encrypt File Using AES' algorithm button to encrypt the file and obtain the following screen.



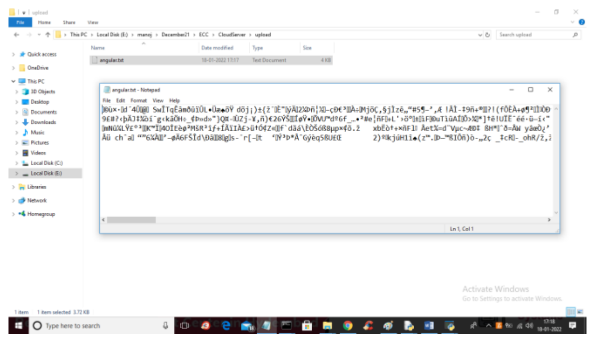
The plain data in the above screen is encrypted, and the first line's AES encryption time is 0.192 milliseconds. Now, click the "Encrypt File using ECC" button to encrypt the same file using ECC and calculate time.



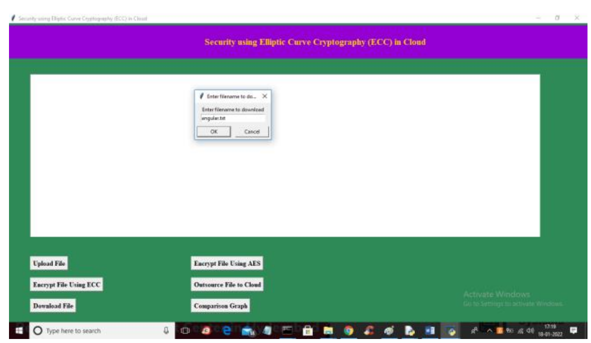
In the preceding screen, the identical file data was encrypted using ECC in 0.008 milliseconds. Now, click the 'Outsource File to Cloud' option to transmit the file to the cloud.



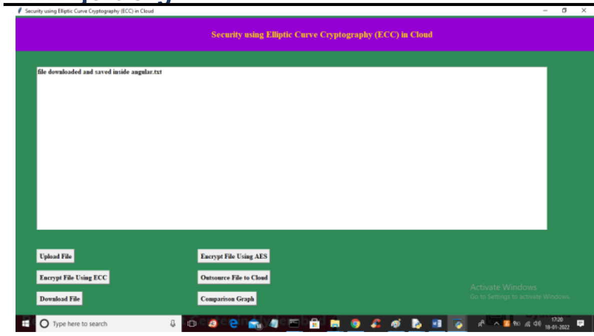
The above screen, we can see the file transmitted to the cloud server, and under the 'CloudServer/upload' folder, we can see the same file saved in encrypted format.



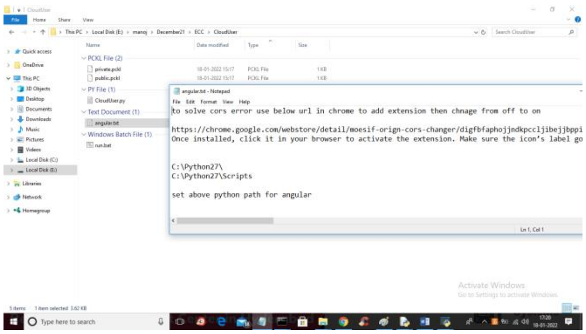
The files in the CloudServer folder are stored in encrypted mode, as seen on the accompanying screen. Now, click the 'get File' option to get the file.



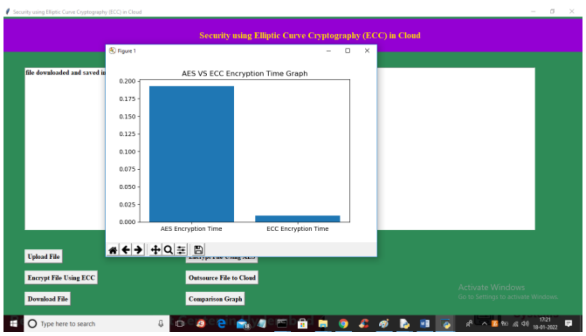
In the above page, I typed the file name to download and then clicked on the 'OK' button to download the file and receive the following screen.



In the following screen, we can see in the text box that the file was downloaded in the CloudUser folder and that it is now in decrypted form.

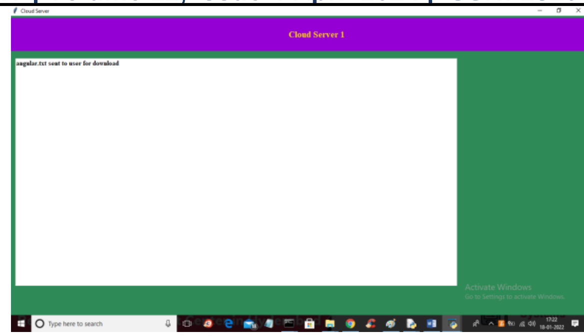


In the following screen, the same file has been encrypted and shown in plain text format. Now, click the 'Comparison Graph' button to receive the graph below.



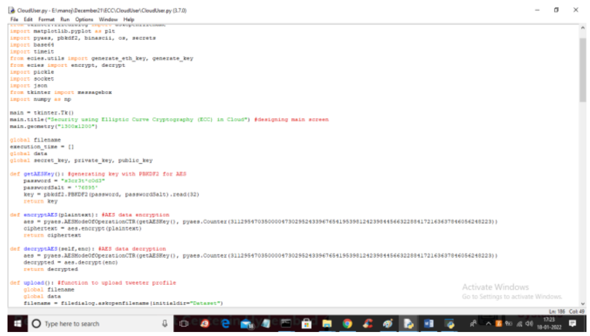
In the above screen, the x-axis shows algorithm names and the y-axis represents encryption time, and ECC required shorter encryption time than AES.

The cloud screen below shows all processes.

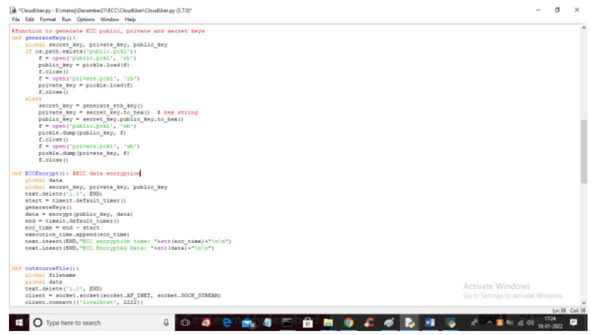


Similarly, you may upload and download any number of files from the cloud while comparing execution times for AES and ECC.

The code to produce AES keys, as well as the encrypt and decrypt functions, is shown on the screen below



To learn about AES, read the notes in red on the top screen, and the code from ECC is shown on the screen below.



5. CONCLUSION

This research concludes that data security is crucial in a world where enterprises rely on cloud services for data storage and management. Cloud environments are cost-effective and computationally powerful, but illegal access poses security threats that require strong security. Data secrecy is sometimes achieved by using encryption techniques like AES, RSA, and DES. Elliptic Curve Cryptography (ECC) is a promising option presented in this paper. The complete comparison between ECC and the widely used AES algorithm shows that ECC is lightweight and has better key creation and management. ECC offers quicker and more efficient encryption, lowering cloud use expenses for enterprises. This research advances cloud data security, giving a potential solution for enterprises seeking comprehensive protection in the ever-changing digital ecosystem. ECC becomes a practical and effective approach to improve data security in the dynamic and interconnected world of cloud computing as enterprises balance cloud services and data security.

6. FUTURE SCOPE

Further research in cloud data security will focus on Elliptic Curve Cryptography (ECC) implementation in cloud contexts. This involves testing ECC's compatibility with edge computing and quantum computing, improving its scalability for large-scale deployments, and incorporating it into holistic security frameworks. For wide acceptance and successful cloud data security, ECC must also be tested for its ability to manage multi-tenancy and compliance difficulties.

REFERENCES

1. Mahammad, F. S., & Viswanatham, V. M. (2020). Performance analysis of data compression algorithms for heterogeneous architecture through parallel approach. The Journal of Supercomputing, 76(4), 2275-2288.
2. Karukula, N. R., & Farooq, S. M. (2013). A route map for detecting Sybil attacks in urban vehicular networks. Journal of Information, Knowledge, and Research in Computer Engineering, 2(2), 540-544.
3. Farook, S. M., & NageswaraReddy, K. (2015). Implementation of Intrusion Detection Systems for High Performance Computing Environment Applications. Inter national journal of Scientific Engineering and Technology Research, 4(0), 41.
4. Sunar, M. F., & Viswanatham, V. M. (2018). A fast approach to encrypt and decrypt of video streams for secure channel transmission. World Review of Science, Technology and Sustainable Development, 14(1), 11-28.
5. Mahammad, F. S., & Viswanatham, V. M. (2017). A study on h. 26x family of video streaming compression techniques. International Journal of Pure and Applied Mathematics, 117(10), 63-66.
6. Devi,S M. S., Mahammad, F. S., Bhavana, D., Sukanya, D., Thanusha, T. S., Chandrakala, M., & Swathi, P. V. (2022)." Machine Learning Based Classification and Clustering Analysis of Efficiency of Exercise Against Covid-19 Infection." Journal of Algebraic Statistics, 13(3), 112-117.
7. Devi, M. M. S., & Gangadhar, M. Y. (2012)." A comparative Study of Classification Algorithm for Printed Telugu Character Recognition." International Journal of Electronics Communication and Computer Engineering, 3(3), 633-641.
8. Devi, M. S., Meghana, A. I., Susmitha, M., Mounika, G., Vineela, G., & Padmavathi, M. MISSING CHILD IDENTIFICATION SYSTEM USING DEEP LEARNING.
9. V. Lakshmi chaitanya. "Machine Learning Based Predictive Model for Data Fusion Based Intruder Alert System." journal of algebraic statistics 13, no. 2 (2022): 2477-2483.
10. Chaitanya, V. L., & Bhaskar, G. V. (2014). Apriori vs Genetic algorithms for Identifying Frequent Item Sets. International journal of

Innovative Research &Development, 3(6), 249-254.

11. Chaitanya, V. L., Sutraye, N., Praveena, A. S., Niharika, U. N., Ulfath, P., & Rani, D. P. (2023). Experimental Investigation of Machine Learning Techniques for Predicting Software Quality.
12. Lakshmi, B. S., Pranavi, S., Jayalakshmi, C., Gayatri, K., Sireesha, M., & Akhila, A. Detecting Android Malware with an Enhanced Genetic Algorithm for Feature Selection and Machine Learning.
13. Lakshmi, B. S., & Kumar, A. S. (2018). Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity checking in Public Cloud. International Journal of Research, 5(22), 744-757.
14. Lakshmi, B. S. (2021). Fire detection using Image processing. Asian Journal of Computer Science and Technology, 10(2), 14-19.
15. Devi, M. S., Poojitha, M., Sucharitha, R., Keerthi, K., Manideepika, P., & Vasudha, C. Extracting and Analyzing Features in Natural Language Processing for Deep Learning with English Language.
16. Kumar JDS, Subramanyam MV, Kumar APS. Hybrid Chameleon Search and Remora Optimization Algorithm-based Dynamic Heterogeneous load balancing clustering protocol for extending the lifetime of wireless sensor networks. Int J Commun Syst. 2023; 36(17):e5609. doi:10.1002/dac.5609
17. David Sukeerthi Kumar, J., Subramanyam, M.V., Siva Kumar, A.P. (2023). A Hybrid Spotted Hyena and Whale Optimization Algorithm-Based Load-Balanced Clustering Technique in WSNs. In: Mahapatra, R.P., Peddoju, S.K., Roy, S., Parwekar, P. (eds) Proceedings of International Conference on Recent Trends in Computing. Lecture Notes in Networks and Systems, vol 600. Springer, Singapore. https://doi.org/10.1007/978-981-19-8825-7_68
18. Murali Kanthi, J. David Sukeerthi Kumar, K. Venkateshwara Rao, Mohmad Ahmed Ali, Sudha Pavani K, Nuthanakanti Bhaskar, T. Hitendra Sarma, "A FUSED 3D-2D CONVOLUTION NEURAL NETWORK FOR SPATIAL-SPECTRAL FEATURE LEARNING AND HYPERSPECTRAL IMAGE CLASSIFICATION," J Theor Appl Inf Technol, vol. 15, no. 5, 2024, Accessed: Apr. 03, 2024. [Online]. Available: www.jatit.org
19. Prediction Of Covid-19 Infection Based on Lifestyle Habits Employing Random Forest Algorithm FS Mahammad, P Bhaskar, A Prudvi, NY Reddy, PJ Reddy journal of algebraic statistics 13 (3), 40-45
20. Machine Learning Based Predictive Model for Closed Loop Air Filtering System P Bhaskar, FS Mahammad, AH Kumar, DR Kumar, SMA Khadar, ...Journal of Algebraic Statistics 13 (3), 609-616
21. Kumar, M. A., Mahammad, F. S., Dhanush, M. N., Rahul, D. P., Sreedhara, K. L., Rabi, B. A., & Reddy, A. K. (2022). Traffic Length Data Based Signal Timing Calculation for Road Traffic Signals Employing Proportionality Machine Learning. Journal of Algebraic Statistics, 13(3), 25-32.
22. Kumar, M. A., Pullama, K. B., & Reddy, B. S V. M. (2013). Energy Efficient Routing In Wireless Sensor Networks. International Journal of Emerging Technology and Advanced Engineering, 9(9), 172-176.
23. Kumar, M. M. A., Sivaraman, G., Charan Sai, P., Dinesh, T., Vivekananda, S. S., Rakesh, G., & Peer, S. D. BUILDING SEARCH ENGINE USING MACHINE LEARNING TECHNIQUES.
24. " Providing Security in IOT using Watermarking and Partial Encryption. ISSN No:
2250-1797 Issue 1, Volume 2 (December 2011)
25. The Dissemination Architecture of Streaming Media Information on Integrated CDN and P2P, ISSN 2249-6149 Issue 2, Vol.2 (March-2012)
26. Provably Secure and Blind sort of Biometric Authentication Protocol using Kerberos, ISSN: 2249-9954, Issue 2, Vol 2 (APRIL

2012)

27. D.LAKSHMAIAH, DR.M.SUBRAMANYAM, DR.K.SATYA PRASAD," DESIGN OF LOW POWER 4-BIT CMOS BRAUN MULTIPLIER BASED ON THRESHOLD VOLTAGE TECHNIQUES", GLOBAL JOURNAL OF RESEARCH IN ENGINEERING, VOL.14(9),PP.1125-1131,2014.
28. R SUMALATHA, DR.M.SUBRAMANYAM, "IMAGE DENOISING USING SPATIAL ADAPTIVE MASK FILTER", IEEE INTERNATIONAL CONFERENCE ON ELECTRICAL, ELECTRONICS, SIGNALS, COMMUNICATION & OPTIMIZATION (EESCO-2015), ORGANIZED BYVIGNANS INSTITUTE OF INFORMATION TECHNOLOGY, VISHAKAPATNAM, 24 TH TO 26TH JANUARY 2015. (SCOPUS INDEXED)
29. P.BALAMURALI KRISHNA, DR.M.V.SUBRAMANYAM, DR.K.SATYA PRASAD, "HYBRID GENETIC OPTIMIZATION TO MITIGATE STARVATION IN WIRELESS MESH NETWORKS", INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY,VOL.8,NO.23,2015. (SCOPUS INDEXED)
30. Y.MURALI MOHAN BABU, DR.M.V.SUBRAMANYAM,M.N. GIRI PRASAD," FUSION AND TEXURE BASED CLASSIFICATION OF INDIAN MICROWAVE DATA – A COMPARATIVE STUDY", INTERNATIONAL JOURNAL OF APPLIED ENGINEERING RESEARCH, VOL.10 NO.1, PP. 1003-1009, 2015. (SCOPUS INDEXED)