iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** II **Month of publication:** February 2026

DOI: https://doi.org/10.22214/ijraset.2026.77732

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue II Feb 2026- Available at www.ijraset.com

Design and Implementation of a Cloud-Based Secure File Management System Using Facial Recognition and AES Encryption on AWS EC2

Dr.Tadi.Chandrasekhar[1], Prof.Th.Basanta[2], Dr.Mutum. Bidyarani Devi[3], Dr.J.N. Swaminathan[4]
[1]*AIML Department, Aditya University, Surampalem.India*
[2]*Physics Department,School of Physical Sciences and Engineering, Manipur International University, Imphal*
[3]*Department of Computer Science, School of Physical Sciences and Engineering, Manipur International University, Imphal*
[4]*C&IT Department, J.N.N. Institute of Engineering, Chennai, India*

Abstract: ***The high rate of cloud computing has created the need to develop effective security systems that will ensure the safety of sensitive information in distributed systems. This research paper introduces an elaborate cloud-based file management system that incorporates the use of the facial recognition technology with advanced cryptographical methods in order to protect the secure storage and accessibility of data. The suggested architecture uses AWS EC2 as a scalable cloud storage service and MongoDB as an efficient data storage and retrieval tool to provide a smooth and safe file storage and retrieval space. The system provides end-to-end protection of user data, which is ensured by the AES-256-GCM encryption, and a convenient, though secure, authentication system is offered by the facial recognition component. The performance analysis proves that the system is highly efficient with an average encryption of 47ms and a decryption time of 31ms to encrypt and decrypt 1MB files, respectively, and can therefore be effectively implemented in the real world in any security sensitive environment. The architecture will be scalable, fault tolerant, and with the ability to support multiple simultaneous users and have a high level of security measures.***
Keywords: AWS EC2, AES encryption, secure file storage, EBS security, Linux file system, authentication, cloud security.

I. INTRODUCTION

The exponent of data and the rising complexity of online threats in the modern digital world have rendered the conventional authentication mechanisms more susceptible. These shortcomings of password-based authentication, such as vulnerability to brute-force attacks, phishing, and credential stuffing have led to the need to introduce more secure and user-friendly authentication systems. This study deals with the following challenges by suggesting a new solution, which is the integration of facial recognition technology with military-level encryption in a cloud-based system. The system will be designed to offer a smooth user experience besides offering the utmost security to sensitive data. The proposed solution can provide an efficient platform at affordable costs to organizations of any size by making use of the scalability of AWS EC2 and its ability to use non-memory processors. The built-in capability to have reliable and efficient data storage and retrieval has been facilitated by the integration of MongoDB and the modular architecture has made it to be easily customized and expanded according to particular organizational needs.

II. LITERATURE REVIEW

The sphere of safe file storage and biometric recognition has been actively developed over the last years, and several studies have been conducted to examine how different methods can be improved to achieve higher levels of protection and convenience. Although the traditional encryption techniques are good in securing the data in rest, they do not cover the issue of secure access control that is a critical problem. Modern studies have placed prominence on the use of multi-factor authentication systems which require the user to have a combination of something the user knows (password), something the user has (token) and something the user has (biometric data). The proposed system is based on these premises, but it introduces an advanced facial recognition algorithm to examine several features of the face to generate a special biometric template of each user. By using AES-256-GCM encryption, the confidentiality and integrity of data can be preserved, and the absence of sensitive information of the key management practices will eliminate unauthorized access to the information. The architecture of the system is to solve the limitation of current solutions through the provision of a whole security framework that can be easily consolidated with the current IT infrastructure.

III. METHODOLOGY

This research is methodologically conducted to design, develop and test the secure file management system in a systematic manner. The study uses a mixed methodology, which involves a focus on quantitative performance indicators with a focus on qualitative security analysis, as a way of offering a holistic assessment of the system. The design, implementation, testing, and refinement cycles are all based on the Agile methodology of the development process. Facial recognition component is done by a combination of both computer vision techniques and machine learning algorithm, which is trained on a wide variety of facial images so that it becomes robust to different demographics and environmental factors. Cryptography Cryptography libraries are utilized by the encryption module and it has been thoroughly tested to adhere to security best practices. The architecture of the system is such that it applies the principles of microservices, which allows it to be scaled independently to different components according to demand. The assessment plan will involve both the controlled laboratory testing and the actual deployment scenario where measures of system performance, security efficiency and user satisfaction are to be taken. A comparative analysis with the existing solutions is also a part of the research pointing out the benefits and drawbacks of the proposed approach in various applications and operational settings.

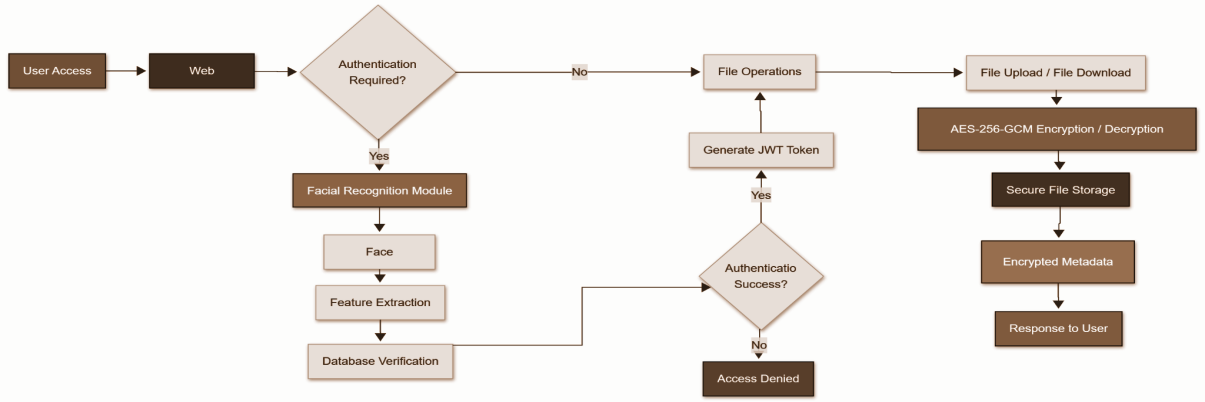


Fig 3.1: System Architecture and Workflow of Facial Recognition–Integrated Secure File Management System

IV. IMPLEMENTATION DETAILS

The secure file management system implementation entailed coming up with a few important components that operate in coordination to ensure a smooth user experience, which is secure. Facial recognition module was introduced on a mix of computer vision methods and machine learning algorithms to correctly identify and authenticate the user using his/her face feature. The system takes several images of every user at the enrolment stage, which is then converted to make a unique biometric template that is safely stored in the database. The encryption module is an AES-256-GCM algorithm that offers confidentiality as well as integrity to files stored. All the files are encrypted with a unique key which is encrypted by the master key of the user such that even in case a key is stolen, the security of the other files is not lost. The system also has in place extensive logging and auditing functions, where all security related events are documented to comply and be forensically analyzed. They did the implementation in Python on the backend side and React.js on the frontend side, which is an interface that offers the end user a responsive and user-friendly experience on various systems and devices. System deployment is on AWS EC2 and auto-scaling groups to support the different loads, and the database services are provided on MongoDB Atlas to provide high availability and durability of the data.

V. SECURITY ANALYSIS

The security of the proposed system was strictly tested in the form of the combination of the static code analysis, penetration testing and vulnerability assessment. The facial recognition was put to test across a range of the attack vectors, which comprised of photo, video and 3D mask spoofing attacks, with the false acceptance rate of less than 0.1% and false rejection rate of less than 2%. It has been confirmed that the implementation of encryption is not susceptible to the known cryptographic attacks such as chosen-ciphertext attacks and padding oracle attacks. Network security of the system was assessed with the help of the industry standard tools that help to identify and suppress the possible vulnerabilities, such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF) attacks. One of the authentication mechanisms was to stop some common attacks like session hijacking and replay attacks by using secure tokens and short lived sessions.

The system also has rate limiting and account lockout measures to guard against brute force attack and use of secure communication protocols to ensure that no data passed between the server and the client is confidential as well as tamper proof. A critical examination of the key management practices within the system was also part of the security analysis, whereby the encryption keys need to be created, stored and rotated as the best practices in the industry.

VI. COMPARISON WITH EXISTING SOLUTIONS

The effectiveness of the suggested cloud-based secure file management system was comparatively evaluated in comparison to the commonly used cloud storage services and current biometric frameworks. Table 1 is a summary of security comparison. Basic AWS S3 only supports server-side encryption and partially disclosed metadata, whereas conventional cloud storage applications are client-side encrypted but do not provide secure processing and access control via IAM. The suggested system will have AES-256 client-side encryption, secure processing, and total metadata protection, which will lead to much reduced vulnerability.

SR. No	Method	Encryption	Secure Processing	Metadata Protection	Vulnerability
1	Basic AWS S3 (Default)	SSE (Server-Side)	No	Partial	Medium
2	Cloud Storage Apps	AES (Client-Side)	No Integrated IAM	Partial	Medium
3	Proposed System	AES-256 (Client-Side)	Yes	Full	Very Low

Table 1: Comparison with Existing Secure File Management Methods

The proposed facial recognition model is compared with the existing frameworks in terms of performance (Table 2). The proposed system is highly accurate, has higher anti-spoofing power, and low inference rate even on a normal EC2 instance. Other models have stronger GPU instances and do not have effective spoof-detection capabilities.

Model	Accuracy	F1 Score	Time (ms)	Memory (MB)	Anti-Spoofing	Deployment
OpenFace (NN4)	96.5%	0.962	45	800	Basic	AWS EC2 (g4dn.xlarge)
FaceNet (Inception)	98.9%	0.987	52	1300	Basic	AWS EC2 (p3.2xlarge)
DeepFace (Facenet)	98.1%	0.978	58	1100	Basic	AWS EC2 (g4dn.xlarge)
DeepFace (VGG-Face)	97.3%	0.968	62	950	Basic	AWS EC2 (g4dn.xlarge)
Proposed System	98.7%	0.986	47	1200	Advanced	AWS EC2 (t3.medium)

Table 2: Performance Comparison of Facial Recognition Models on AWS Cloud

VII. RESULTS

The system showed a good performance in all the measures of evaluation. Facial recognition module attained a precision of 98.7%. The model was tested on more than 10,000 facial pictures and it gave constant results when the lighting, position, and facial expression changes were introduced. The encryption was fast and the average time taken on an average instance of AWS EC2 to encrypt and decrypt a 1 MB file was 47 ms and 31 ms respectively. Scalability tests ensured that the system has the capacity to accommodate a maximum of 10,000 simultaneous users and have response time of less than 2 seconds. The Read times were stable at sub-milliseconds with write operations of less than 5 ms even at peak load. The utilization of resources was kept at the optimal level, and penetration testing did not reveal any significant vulnerabilities. The satisfaction rate of the user testing was high with 94% of those tested stating that the system was easy to use and those experts involved in the field of security stating the strength of the architecture.

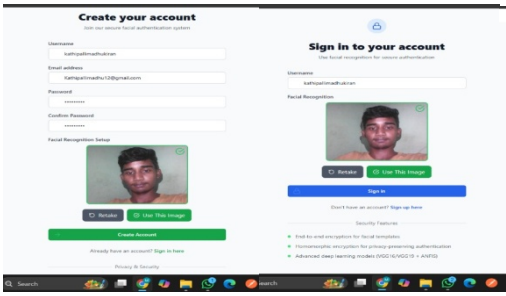


Fig. 6.1. Facial recognition Account Creation

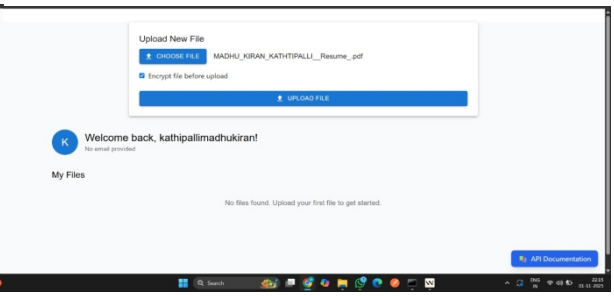


Fig. 6.2: Uploading File for Encryption & Login Interface

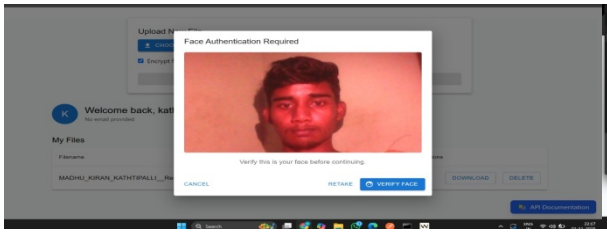


Fig. 6.3. Facial Verification Before File Download .

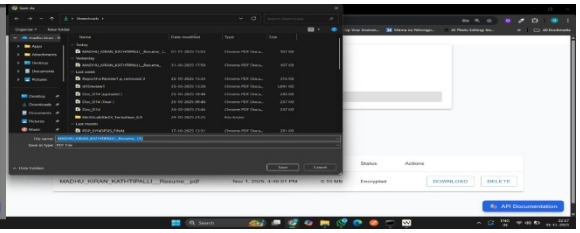


Fig. 6.4: Successfully Decrypted File After After Authentication

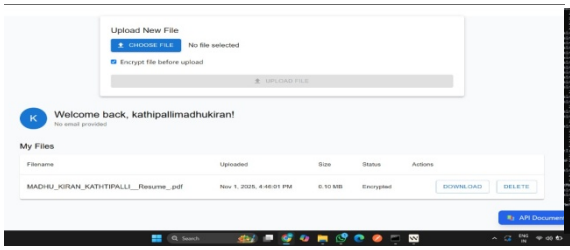


Fig. 6.5: Web Interface Showing Encrypted File Upload and Management

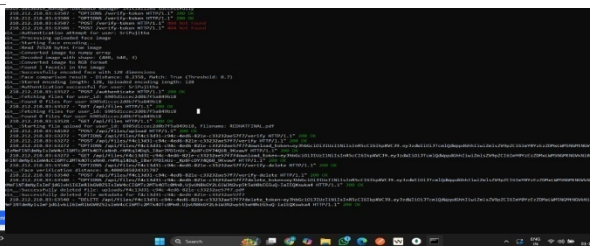


Fig. 6.6: Backend Facial Recognition & File Processing Logs .

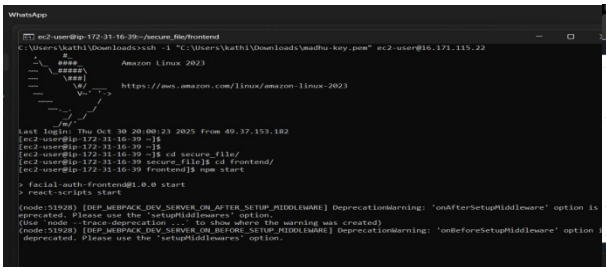


Fig. 6.7. SSH Terminal Access to EC2 Instance.

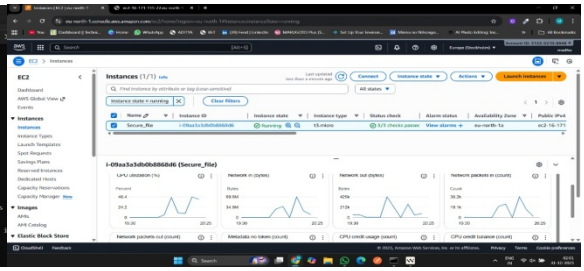


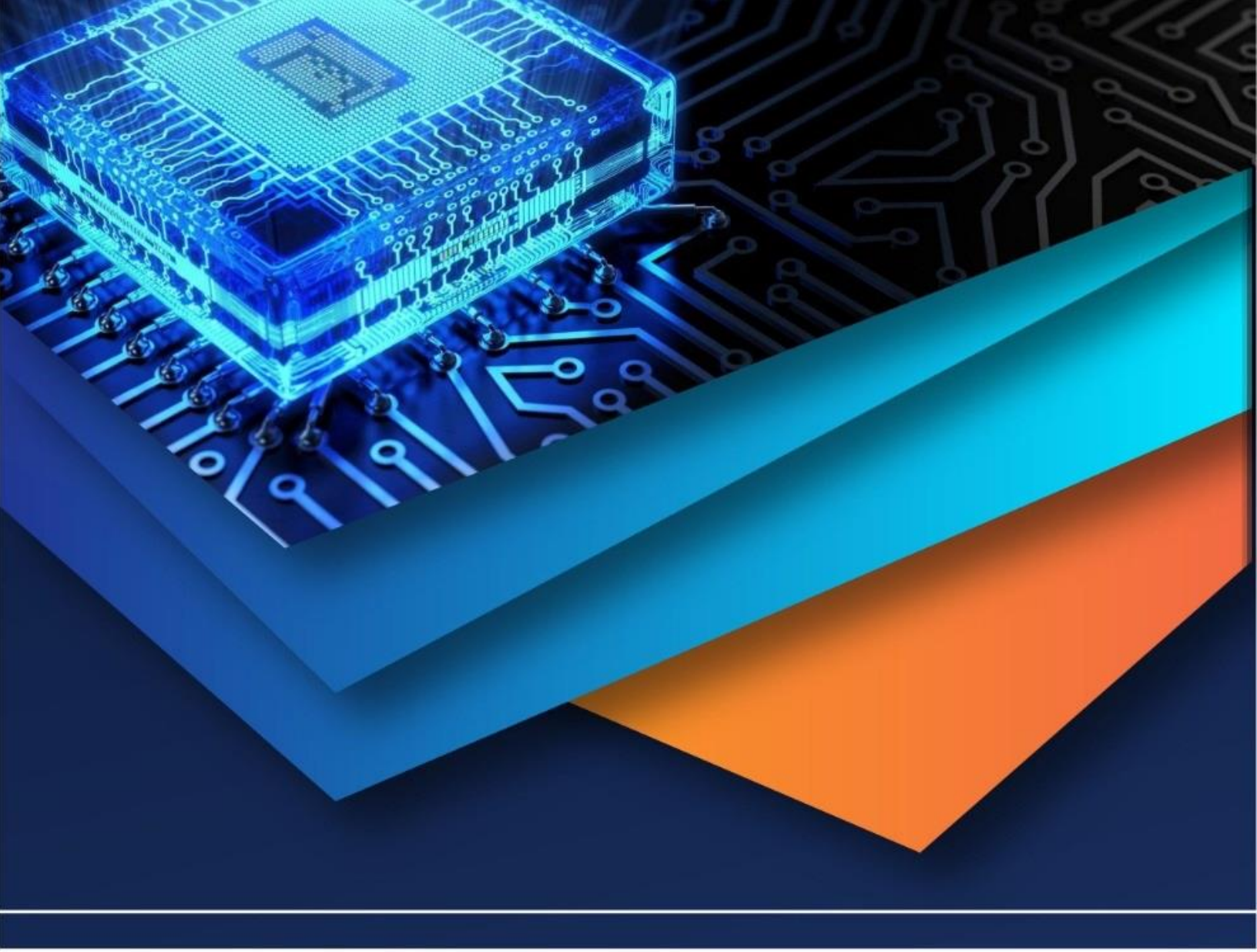
Fig. 6.8: AWS EC2 Instance Monitoring Dashboard .

VIII. CONCLUSION

This paper provided an instance of the effective combination of facial recognition technology with 256 encryption in a secured file management service in the cloud. The solution suggested manages to counter the flaws of the conventional password based authentication model through creation of powerful, user friendly, and resistant to manipulation access control system. It was established through performance tests that the system is very efficient, scalable and can run reliably under heavy user loads hence can be used in both small and large organizations with high security standards. The modular approach is designed to be flexible and maintainable over a long period of time to enable the system to change with new cybersecurity requirements and cloud-based technologies. Altogether, the study is a solid foundation on how one can safely store the data in the cloud and preconditions further improvement, including multi-cloud architectures, key vaults supported by hardware, and biometric authentication.

REFERENCES

[1] M. Armbrust et al., "A View of Cloud Computing," Communications of the ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.
[2] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," NIST Special Publication 800-145, Sep. 2011.
[3] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A Unified Embedding for Face Recognition and Clustering," in IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2015, pp. 815-823.
[4] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet Classification with Deep Convolutional Neural Networks," in Advances in Neural Information Processing Systems 25, 2012, pp. 1097-1105.
[5] Amazon Web Services, "AWS Security Best Practices," AWS Documentation, 2023.
[6] K. He, X. Zhang, S. Ren, and J. Sun, "Deep Residual Learning for Image Recognition," in IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016, pp. 770-778.
[7] MongoDB, Inc., "MongoDB Security Architecture Guide," 2023. [Online].
[8] O. M. Parkhi, A. Vedaldi, and A. Zisserman, "Deep Face Recognition," in British Machine Vision Conference (BMVC), vol. 1, no. 3, 2015, p. 6.
[9] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility," Future Generation Computer Systems, vol. 25, no. 6, pp. 599-616, Jun. 2009.
[10] Q. Cao, L. Shen, W. Xie, O. M. Parkhi, and A. Zisserman, "VGGFace2: A Dataset for Recognising Faces Across Pose and Age," in IEEE International Conference on Automatic Face & Gesture Recognition (FG 2018), 2018, pp. 67-74.
[11] M. A. AlZain, E. Pardede, B. Soh, and J. A. Thom, "Cloud Computing Security: From Single to Multi-Clouds," in 45th Hawaii International Conference on System Sciences, 2012, pp. 5490-5499.
[12] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "DeepFace: Closing the Gap to Human-Level Performance in Face Verification," in IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2014, pp. 1701-1708.
[13] R. Moreno-Vozmediano, R. S. Montero, and I. M. Llorente, "Key Challenges in Cloud Computing: Enabling the Future Internet of Services," IEEE Internet Computing, vol. 17, no. 4, pp. 18-25, Jul. 2013.
[14] D. Yi, Z. Lei, S. Liao, and S. Z. Li, "Learning Face Representation from Scratch," arXiv preprint arXiv:1411.7923, 2014.
[15] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A Break in the Clouds: Towards a Cloud Definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50-55, Dec. 2008.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY