International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

Review on Cloud Data Security Using VGG19-Deep Learning and Homomorphic Encryption

Tadi. Chandrasekhar [1,*], Th. Basanta [2] and J.N. Swaminathan [3]

[1] *Department of AIML, Aditya University, Surempalem, India.*
[2] *Department of CSE, Manipur International University, Imphal, India.*
[3] *Department of C&IT, J.N.N. Institute of Engineering, Chennai, India.*

International Journal of Science and Research Archive, 2025, 17(02), 570-573

Publication history: Received on 07 October 2025; revised on 13 November 2025; accepted on 15 November 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.17.2.3077

Abstract

Data is the new currency as lot of the user's presence online is an upward trend. As a consequence the data storage on the various cloud platforms has been a new normal. Data security in cloud has turn formidable due to unique security issues and challenges. Conventional methods on security may not always cater a proper barter between computational efficiency and data security. This review paper discusses the blending facial key features of the face obtained from VGG19 deep learning with homomorphic encryption to enrich cloud data security. The VGG19 allows for robust feature extraction from face and facial key points for authentication, while homomorphic encryption scales computation in encrypted form; it acquire enhanced accuracy with scalability and preservation of privacy. Thus, this method ensure a better approach in next-generation cloud security frameworks.

Keywords: Cloud security; CNN; VGG16.VGG19; Facial key features

1. Introduction

Data prudence and integrity have become essential with ever-growing dependency on cloud computing. Data breaches, unauthorized access and fishing-attacks are existing major threats in cloud infrastructure. Deep learning models like VGG19 provides facial key points helps to achieve superior results in the field of image recognition and can efficiently be extended to cater for secure cloud authentication. The amalgam of facial key points from deep learning and homomorphic encryption efficiently provides data securely on cloud without disclosing private data, thus assuring end-to-end security.

2. Literature Review

Recent advancements in Data security on cloud emphasize the integration of homomorphic encryption with facial key feature extraction to secure facial templates during cloud computation. Bai et al. IEEE in 2023, Access proposed Crypto Mask, a hybrid Homomorphic Encryption and multi-part framework that significantly reduces rotation costs in encrypted face recognition. Liu, Informatica in 2024, explained a fully homomorphic encryption based CNN feature encryption performs matching in the cipher text domain and improves data security on cloud. Likewise, Wang et al. In 2024, introduced a secure face verification scheme combining Fully Homomorphic Encryption with Seal PIR, attained anonymous authentication on cloud with reduced latency. Chen et al, in 2025, Scientific Reports developed a hybrid encryption and facial integrity verification framework, ensuring both encrypted similarity computation and data authenticity. Song et al. In 2025 PLOS ONE developed Hybrid Encryption Face Net, which uses approximate Homomorphic Encryption to protect facial embedding's for achieving better recognition accuracy. Enriching these

* Corresponding author: Tadi. Chandrasekhar

works, Sardar et al.2023, Expert Systems with Applications has developed a hybrid template protection system that combining dimensionality reduction and encryption to enrich privacy. Further, Bassit et al. 2025, Frontiers in Imaging explained template-recovery attacks that are made facial data from leaked scores, highlighting the need for encrypting comparability outputs. At the end, Frery et al.in 2023, arXiv and Wang et. al. in 2024, Wiley Expert Systems analyzed multi-key and approximate homomorphic Encryption methods, providing improved efficiency for multi-owner facial recognition systems. Altogether, these methods exhibits that encrypting based facial key-points or embedding's using optimized HE schemes permit security and accurate facial recognition in the cloud, though practical deployment still requires careful protection against data leakage and computational overhead.

3. Methodology

The methodology in review paper integrates VGG19-based facial key-points with homomorphic encryption to empathize security and privacy in cloud environment. The whole process begins with the acquisition of facial Image and is preprocessed for normalize, resize, and enhance the facial images for better recognition accuracy. The facial key-points of the features are extracted from the pre-trained VGG19 deep learning network using the Image Net dataset. The extracted key-points are converted into alphanumeric keys and is used as personalized identifiers. The process of Homomorphic encryption is applied to these keys, allowing secure operations directly on encrypted dat. The facial key point homomorphic encryption mechanism provides guarantee that during authentication. The system never allows unauthorized person, hence it provides full data confidentiality.

The next part of the methodology deals with secure authentication and computation within the cloud platform. The data encrypted facial key points of data set are matched against newly encrypted key points captured during login through homomorphic encryption similarity scores will be calculated. If the similarity score exceeds the threshold value, it is going to securely authenticate the user. The feature extraction, key generation, encryption, and privacy-preserving verification stages that comprise the workflow are depicted in Figures 5.1 and 6.1 of the document. The integrated design enhance security as well as improve the computational efficiency of authentication system, it offers high level security against data breaches, spoofing, and unauthorized access with real-time recognition performance.

4. Results and Discussion

Table 1 Testing parameters of VGG19 with Previous Algorithms

SR. No	Algorithm	Accuracy	Specificity	Sensitivity	Precision
1	GABOR Filter	58.63%	56.75%	51.74%	55.26%
2	Bayesian Classifier	63.72%	58.85%	58.41%	61.35%
3	SVM	73.63%	68.32%	68.72%	68.72%
4	ANFIS	88.92%	89.71%	85.32%	88.42%
5	VGG16	95.37%	96.73%	96.47%	92.03%
6	VGG19	98.23%	98.56%	95.21%	96.53%

Figure 1 Facial key point's selection from real time Image using VGG19

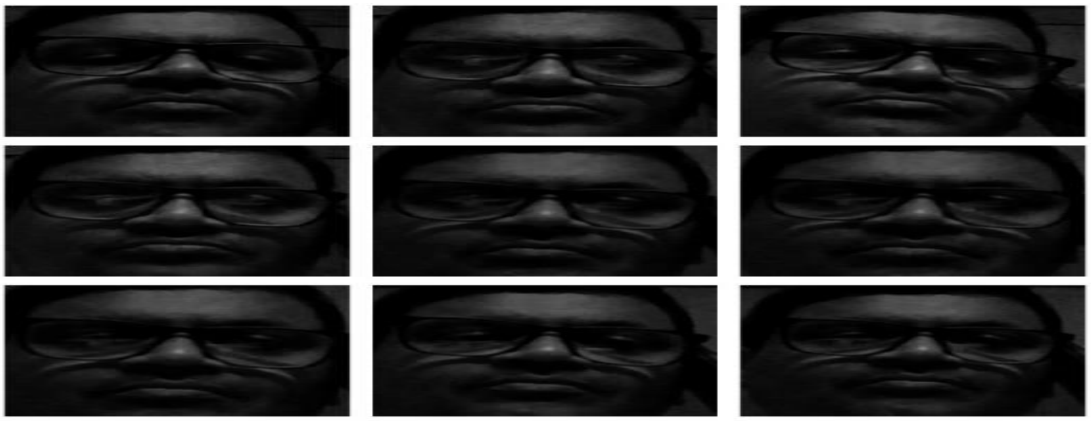

Figure 2 Facial dataset creation

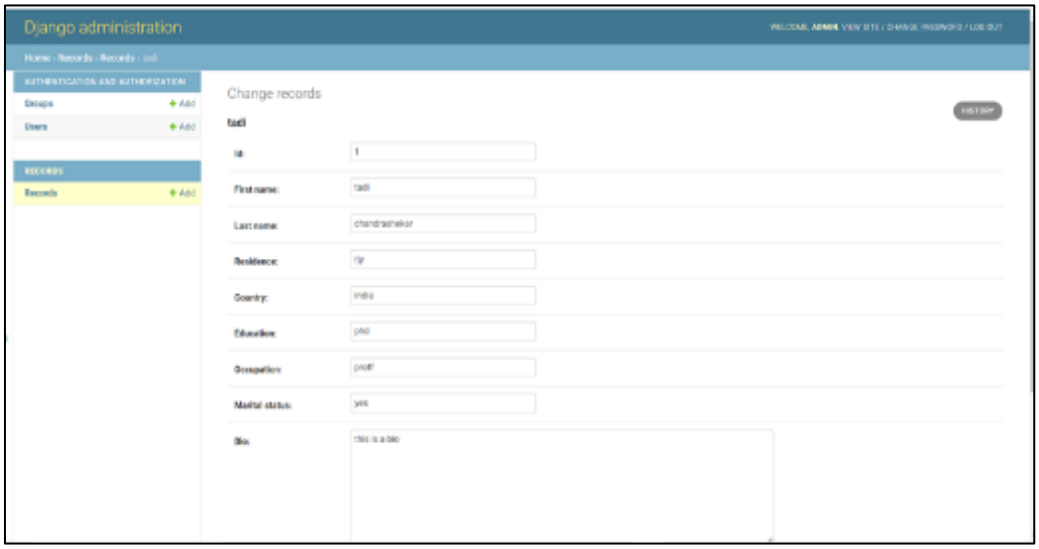

Figure 3 Record creation in database

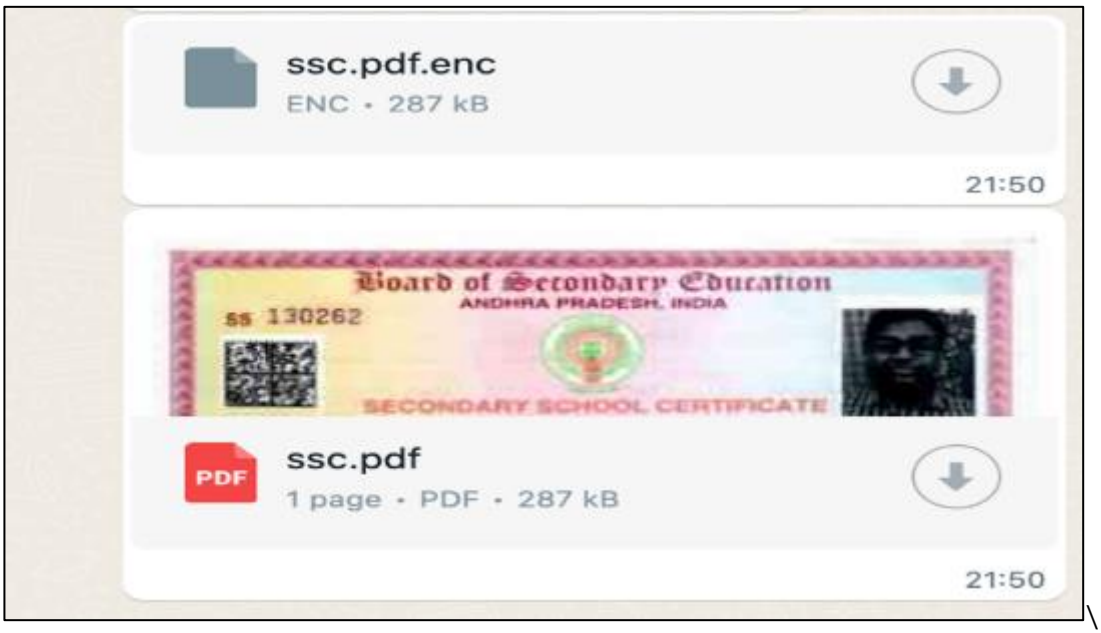

Figure 4 Encrypted and decrypted file

The experimental results of VGG19 for classification is shown in Table-1 above. For the classification tasks the proposed VGG19 has achieved better performance metrics such as Accuracy, sensitivity, accuracy, specificity and precision than the traditional methods.Fig.1 represents facial key point selection from real time image.Fig.2 shows a creation of real time data set for authentication. Real time record creation is shown in fig.3 and encryption and decryption of file is shown in fig.4 Moreover, their encryption time is within acceptable limits, so this cloud security method can be used for real-time applications as well.

5. Conclusion and Future Scope

This review found that the integration of VGG19 deep learning with homomorphic encryption has a significant impact on cloud data security. The model takes into account the issues of trustworthy authentication, strong data protection, and efficient computation over encrypted data. Future research can build on this by integrating federated learning across multi-cloud systems for decentralized and privacy-preserving data sharing.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Bai, J., Zhang, X., Song, X., Shao, H., & Wang, Q. (2023). CryptoMask: Privacy-preserving Face Recognition Using Homomorphic Encryption and Secure MPC. IEEE Access.

[2] Liu, T. (2024). Secure Face Recognition Using Fully Homomorphic Encryption. Informatica.

[3] Wang, X., et al. (2024). A Secure Face Verification Scheme Based on Fully Homomorphic Encryption. Information (MDPI).

[4] Chen, Y., et al. (2025). Efficient Face Information Encryption and Verification: Hybrid Encryption with Facial Data Integrity Verification (HEFDIVS). Scientific Reports.

[5] Song, Z., et al. (2025). HE_FaceNet: Privacy-Preserving Face Recognition Based on Approximate Homomorphic Encryption. PLOS ONE.

[6] Sardar, A., et al. (2023). Face Recognition System with Hybrid Template Protection. Expert Systems with Applications.

[7] Bassit, A., et al. (2025). Template Recovery Attack on Encrypted Face Recognition Systems with Unprotected Decision Using Synthetic Faces. Frontiers in Imaging.

[8] Frery, J., et al. (2023). Privacy-Preserving Tree-Based Inference with TFHE. arXiv preprint.

[9] Wang, L., et al. (2024). Privacy Preserving Security Using Multi-Key Homomorphic Encryption for Cloud Biometric Systems. Expert Systems (Wiley).

[10] Liu, X., et al. (2024). Hybrid Encryption Strategies for Secure Facial Landmark-Based Recognition in Cloud Environments. Journal of Cloud Computing.