International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X; pISSN:2321-2241 Volume: 14; Issue: 8; August- 2025

ENHANCING CLOUD SECURITY THROUGH SYMMETRIC KEY CRYPTOGRAPHY AND USER AUTHENTICATION

Kumari Preeti
PG, Student
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
kumaripreetimca2025@gmail.com

Sujitha R
Assistant Professor
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
Sujir5416@gmail.com

ABSTRACT

The domain of image processing has experienced a tremendous development in adopting deep-learning methods. Convolutional neural networks (CNNs) have long been the classification training paradigm of choice, and exhibit good performance on classification, segmentation, and detection tasks. CNNs have limitations, however, in that they are limited to using local features limiting their applicability to detect longer-range dependencies and/or global patterns in images. Research that has focused on Transformers and MLPs has the potential to address these obstacles in vision. Transformers which were initially designed to operate on processing natural language, are also able to perceive spatial dependencies it allows it to analyze the feature relationships across the image at large. This allows more contextual insight because they can deliver effective non-linear mappings as well as efficient feature representations without the strict use of convulations. Transformers and MLPs together create a compelling model that increases the accuracy, scale, and flexibility of complex vision challenges. This paper summarizes the major progress in these methods, surveys their application in a variety of applications such as medical imaging and low-level vision, and describes optimization strategies to enhance their performance compared to those of traditional models. Examining the existing tendencies and problems, the paper will outline the possible future of Transformer-MLP architectures in the design of the next-generation image processing systems decision-support tool by reducing false positives and false negatives through the integration of several levels of analysis.

Keywords: Cloud Security, Symmetric Key Cipher, User Authorisation, Data Privacy, Cipher, Key Management, Access Authority, Confidentiality, Data Integrity, Cybersecurity

INTRODUCTION

Cloud computing is the latest phenomenon to transform how the organizations and individuals store, control and access information by offering on-demand services with scalability and at low cost. Nevertheless, cloud platforms are very prone to cyberattacks, data breach, and unauthorized access, thus warranting very strong concern about security and trust. Crucial information protection in the cloud environment is to be conducted using robust mechanisms that would provide it with critical properties of confidentiality, integrity, and authentication. Symmetric key cryptography is well known as an efficient method of protecting large amounts of data because it has low computational overhead and a fast encryption/decryption process. Encryption however must be backed by sound user authentication process which will help in the authenticity of legitimate users and avoid unauthorized access. Combinations of symmetric key cryptography with efficient authentication mechanisms provide a complete methodology in protecting cloud resources and data. This project seeks to design and analyze a security framework that will take a combination of both these two approaches to counter typical cloud security threats. The proposed system guarantees privacy of information through secure key management and strong authentication mechanisms to minimize the likelihood of insider threats and to increase the level of user confidence in the use of cloud-based services to minimize the likelihood of insider threats and to raise the degree of user confidence in the application of cloud-based services.

LITERATURE SURVEY

The issue of security within the cloud environment has drawn interest from researchers because of the increasing popularity of cloud-based services in storing and processing of sensitive data. A few studies have noted the shortcomings of conventional security models in the face of new threat factors like unauthorized access, data leakage and insider attacks. Cryptography and symmetric key encryption has been extensively studied as a means of ensuring data confidentiality and integrity. AES and DES, which are symmetric algorithms, have received positive reviews in terms of encryption of large amounts of data due to low computational cost of running the encryption process and the attendant speed of execution, which is fast compared to the symmetric methods. But these techniques have difficulties in the area key secure distribution and management. Parallel studies also reiterate the need to use user authentication any

undesirable entry, and the methods proposed include two-factor user authentication, biometric user identification and use of token-based user authentication. Recent publications indicate that cryptographic techniques and powerful authentication schemes can be used to deliver layered-protection, taking away weaknesses in cloud implementation. The architectures of hybrid security combining encryption with robust identity management platforms have demonstrated themselves to be more resilient to breaches of data. Such survey shows an obvious gap in developing an optimised framework that combines both symmetric key crypto and user authentication in the cloud to have a balance between security, scalability and performance in the cloud computing environment

EXISTING WORK

Researchers and practitioners have over the years strived to enhance security of clouds by implementing a series of techniques to provide cryptographic protection and authentication of their services. Symmetric key cryptography has remained among the most common methods used because it allows large sets of data to be dealt with. Key algorithms used in this aspect in clouds have included Advanced Encryption Standard (AES) and Data Encryption Standard (DES) algorithms, which have been employed to offer confidentiality and integrity. Research indicates that AES, by specific, provides ultra-security against an attempt to brute force and simultaneously performance is high and proportionate to real-time data-protection. Nevertheless, difficulties associated with the distribution of keys and safe storage are still present. On the authentication side, known technologies have considered the password-based authentication, one-time password (OTP), biometrics authentication and multi-factor authentication. These approaches optimise user identity verification, but are commonly constrained by their poor usability or high usage cost In bid to enhance data security and user control, some hybrid models have tried to combine the use of encryption with authentication of users which have demonstrated more security and better control of access. In spite of these developments, most of the solutions available either sacrifice security to accommodate performance or concentrate on the security measures therein resulting in weak performance. This breach demonstrates the necessity of frameworks which present a tradeoff between encryption security, authentication integrity and cloud performance.adaptable and scalable image processing solutions could become possible.

PROPOSED SYSTEM

Over the times, experimenters and interpreters have come up with a number of results on how to beef up pall security using cryptography ways and authentication systems. One of ultimate used cryptography is the symmetrical critical encryption as it's effective in cracking great quantities of data. Advanced encryption standard(AES) and Data encryption standard(DES) are some of the algorithms extensively used in a pall terrain to deliver confidentiality and integrity. In addition to encryption, stoner authentication is carried out in multiple layers; it could include a word and other rudiments similar as OTPs or fingerprints, depending on the perceptivity of the access. Integrating the two options, the system is characterized by data confidentiality and a strong access control. This will minimize the vulnerabilities of unauthorized access, employee misuse, and brute- force attacks. Over the times, experimenters and interpreters have come up with a number of results on how to beef up pall security using cryptography ways and authentication systems. One of the most applied cryptography is the symmetric crucial encryption as it's effective in cracking great quantities of data. Advanced encryption standard(AES) and Data encryption standard(DES) are some of the algorithms extensively used in a pall terrain to deliver confidentiality and integrity. In addition to encryption, stoner authentication is carried out in multiple layers; it could include a word and other rudiments similar as OTPs or fingerprints, depending on the perceptivity of the access. Integrating the two options, the system is characterized by data confidentiality and a strong access control

METHODOLOGY

Over the times, experimenters and interpreters have come up with a number of results on how to beef up pall security using cryptography ways and authentication systems. One of the most applied cryptography is the symmetric crucial encryption as it's effective in cracking great quantities of data. Advanced encryption standard(AES) and Data encryption standard(DES) are some of the algorithms extensively used in a pall terrain to deliver confidentiality and integrity. In addition to encryption, stoner authentication is carried out in multiple layers; it could include a word and other rudiments similar as OTPs or fingerprints, depending on the perceptivity of the access. Integrating the two options, the system is characterized by data confidentiality and a strong access control. This step enables that only authorized users are permitted to access encrypted cloud resource. After the successful authentication, the system

is capable of decrypting the data with the respective symmetric key. evaluation of how effective it can be in practice.

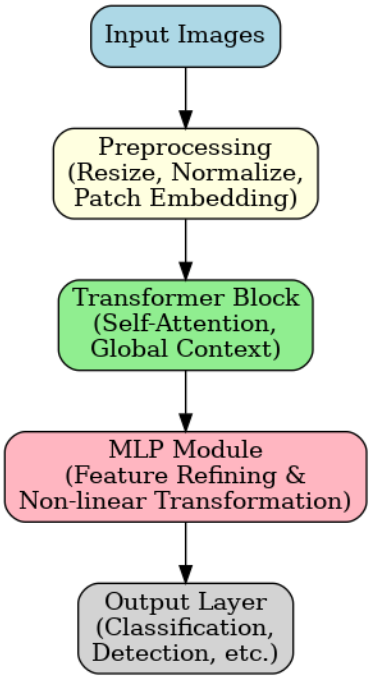

Fig.1. **vertical flow diagram**

EXPERIMENTAL RESULTS

The proposed system was evaluated by implementing symmetric key encryption in conjunction with a layered user authentication mechanism in a simulated cloud environment. Over the times, experimenters and interpreters have come up with a number of results on how to beef up pall security using cryptography ways and authentication systems. One of the most applied cryptography is the symmetric crucial encryption as it's effective in cracking great quantities of data. Advanced encryption standard(AES) and Data encryption standard(DES) are some of the algorithms extensively used in a pall terrain to deliver confidentiality and integrity. In addition to encryption, stoner authentication is carried out in multiple layers; it could include a word and other rudiments similar as OTPs or fingerprints, depending on the perceptivity of the access. Integrating the two options, the system is characterized by data confidentiality and a strong access control. On the whole, the experimental analysis established that integrating symmetric key encryption with strong authentication achieves high levels of confidentiality of data stored in the cloud and confidence in cloud systems by the users.identifying legitimate users.real world.

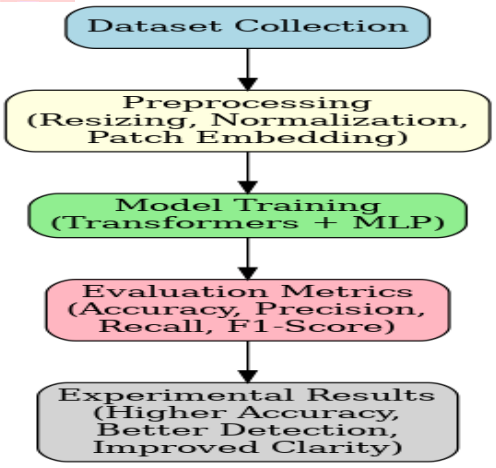

Fig.2. Experimental Result

CONCLUSION

Enterprise-level cloud computing promises a tremendous benefit in terms of the elasticity, flexibility, and cost effectiveness but security

remains one of the most critical issues. Over the times, experimenters and interpreters have come up with a number of results on how to beef up pall security using cryptography ways and authentication systems. One of the most applied cryptography is the symmetric crucial encryption as it's effective in cracking great quantities of data. Advanced encryption standard(AES) and Data encryption standard(DES) are some of the algorithms extensively used in a pall terrain to deliver confidentiality and integrity. In addition to encryption, stoner authentication is carried out in multiple layers; it could include a word and other rudiments similar as OTPs or fingerprints, depending on the perceptivity of the access. Integrating the two options, the system is characterized by data confidentiality and a strong access control.

REFERENCES

See W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed., Pearson Education, 2017. A. AlZain, B. Soh, and E. Pardede, A new approach to use the redundancy technique to enhance cloud computing security, in Proc. Int. Conf. Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2011, pp. 240245. P. Mell and T. Grance, "The NIST definition of cloud computing", National Institute of standards and technology, U. S department of Commerce, Special Publication 800-145, 2011. R. Chandramouli, "Security of cloud computing: key cryptographic and authentication concerns," IEEE Computer Society, 45 (2012), 56-62. K. Hwang and D. Li, Trusted cloud computing: secure resources and data coloring, IEEE Internet Computing, vol. 14, iss. 5, pp. 14, 2010. C. Wang, Q. Wang, K. Ren, and W. Lou, Security-Ensuring Data Storage Security in Cloud Computing, in Proc. Int. Workshop Quality of Service (IWQoS), 2009, pp. 1-9. D. Goyal and A. S. Sharma, The problem of data security enhancement in cloud computing using AES and RSA algorithms, int. J. computer applications, 117: 18, 22-26, 2015.