iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

AN INTEGRATED APPROACH TO ENHANCE CLOUD COMPUTING SECURITY AND EFFICIENCY USING ECDH, AES, BLOWFISH AND ENHANCED ARCHITECTURES

Prof. D.J. Manowar
Assistant Professor in Department of Computer Science & Engineering Takshashila Institute of Engineering & Technology Darapur, Dist Amravati 444802, Maharashtra, India

Prof.A.A.Chinchamalatpure
Assistant Professor & HOD in Computer Science & Engineering Takshashila Institute of Engineering & Technology Darapur, Dist Amravati 444802, Maharashtra, India

Moeed Khan
UG Student, Department of Computer Science & Engineering Takshashila Institute of Engineering & Technology Darapur, Dist Amravati, Maharashtra, India

ABSTRACT

The digital world now functions through cloud computing because it provides adaptable data storage and processing solutions with affordable demands. The rising trend of organizational infrastructure migration into cloud systems has led to increased security and efficiency concerns together with trust-related worries. The research develops a unified security-performance enhancement for cloud computing by implementing advanced cryptographic methods with optimized system design architecture. The proposed model leverages the strengths of Elliptic Curve Diffie-Hellman (ECDH) for secure key exchange, Advanced Encryption Standard (AES), and Blowfish algorithms for robust and efficient data encryption.

A comprehensive multi-layered security framework from the model identifies and protects against assaults on data storage as well as secure data transmission and various security breaches.

The performance evaluations involving CloudSim simulation along with controlled cloud environment implementation show that the digital system delivers superior encryption speed and enhanced data integrity functions while optimizing storage compared to RSA-based encryption methods.

The hybrid encryption system provides quick computations and ensures advanced access restrictions and full confidentiality protection. Security enhancements implemented in the architecture prevent unauthorized access to systems and make it possible to establish stronger authentication methods for users and enhance secure data processing workflows. The integrated solution solves current cloud security problems in addition to creating a foundation which supports continuous development of protected cloud computing systems.

Keywords:
Cloud Security, Cryptography, ECDH, AES, Blowfish, RSA, Data Breaches, CloudSim, Cloud Architecture

INTRODUCTION

Information technology now uses cloud computing as a transformative model that lets people access collective computing resources like storage servers networks and applications through on-demand usage. Thanks to this model businesses can now minimize capital costs for hardware investments alongside gaining maximum flexibility and scalability benefits in their operations. Cloud computing continues to face essential hurdles because it combines security concerns with operational effectiveness difficulties. Users who place their data on distributed third-party management systems surrender direct access to critical information and face higher possibilities of data breaches alongside unauthorized access and system hijacking and insider threats. The slowdowns and inefficiencies which occur during data encryption and decryption processes result in performance bottlenecks that produce delayed operations and enhanced computational expenses and worsen user experiences. Cloud infrastructures require better security approaches than RSA and single-layer authentication since they fail to protect modern evolving cloud security needs. The research combines Elliptic Curve Diffie-Hellman (ECDH) for key exchange security together with a hybrid AES/Blowfish encryption system that speeds up data encryption operations within a new multi-layered cloud architecture design for fortified security. This recommended solution brings together different cryptographic methods to create an enhanced security system which secures numerous applications while enhancing reliability and efficiency of cloud-based operations.

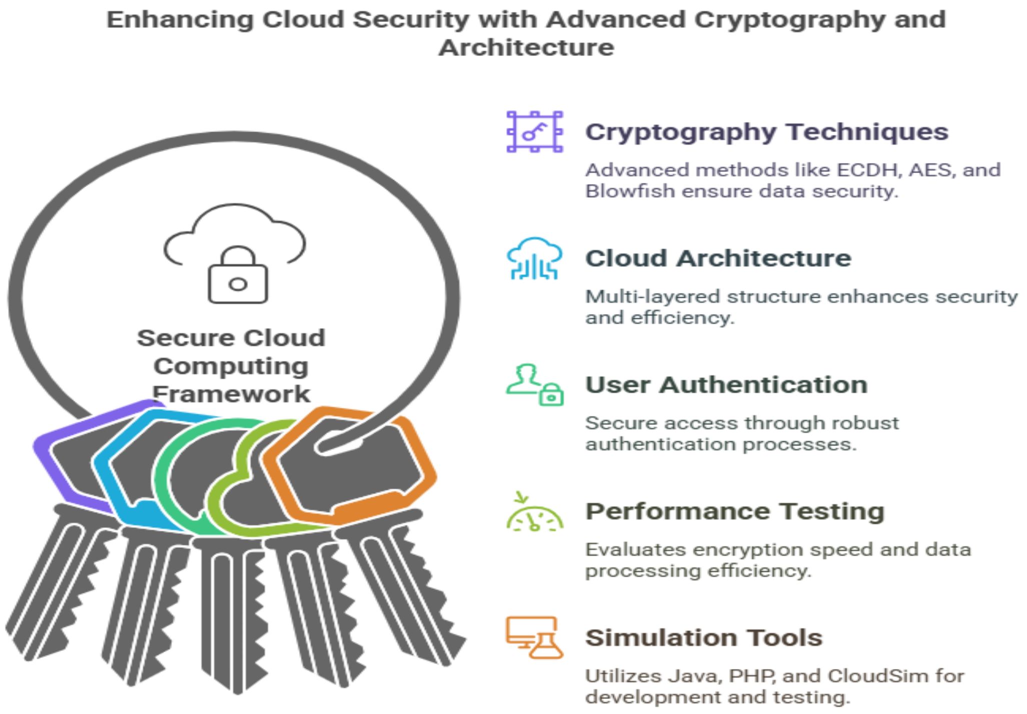
OBJECTIVES

This research designs a complete security model with efficiency improvements for cloud computing through incorporation of progressive cryptographic procedures and infrastructure developments. This study takes on the mission to fix ongoing technical difficulties with cloud security breaches alongside unauthorized access and inefficient execution that obstructs the acceptance and dependability of cloud platforms. The main objective focuses on implementing Elliptic Curve Diffie-Hellman (ECDH) for lightweight and secure key exchange combined with the usage of Advanced Encryption Standard (AES) along with Blowfish algorithms to create an efficient encryption system. Both performance and cryptographic strength are combined with low latency characteristics for selecting these security methods. The project works toward enhancing cloud system internal structure through the development of a multi-faceted security model that includes secure authentication systems and data validation protocols with encryption workflows. Implementing these dual measures creates cloud systems that defend against multiple attack vectors while maintaining data confidentiality through entire transmission and storage periods. Evaluating the proposed model performance includes utilization of CloudSim tools for real-time scenario simulation which demonstrates practicality and effectiveness. The research seeks to develop a scalable framework which provides secure performance-based solutions for cloud services adoption across different sectors to support current demands in secure and efficient cloud computing solutions.

The research project works to unite the interests of security with efficiency in cloud computing through developing new hybrid encryption methods that deliver robust data protection together with enhanced system performance. The main goal involves implementing a dual-layer encryption system based on AES and Blowfish encryption to ensure full protection against data corruption while data travels between users and rests within cloud systems. ECDH provides lightweight secure key exchange for users to communicate with the cloud server in a way that protects their sensitive keys from exposure. The performance evaluation of this hybrid system must be conducted to determine its capabilities by comparing it with traditional encryption protocols using measures for processing time along with encryption/decryption speed and memory requirements. The project emphasizes designing an easy-to-use interface which implements authentication security alongside role-based access management along with file handling capabilities. Testing of the proposed system will employ CloudSim simulation tools to subject it to realistic working conditions involving various workload scenarios. This project builds a scalable secure cloud framework that fights unauthorized data breaches in addition to meeting market needs for quick smarter secure cloud solutions.

SYSTEM ANALYSIS

Cloud computing system analysis stands essential because it helps identify current challenges then develops optimized solutions targeting these constraints. The main issues in traditional cloud systems stem from data security problems alongside slow encryption operations and inefficient resource utilization particularly when processing sensitive data and overwhelming user traffic. The combination of secure RSA encryption methods requires substantial computational resources from cloud platforms because this security complexity increases both latency times and diminishes responsiveness for connected systems. Cloud platforms generally have inadequate protection systems for keys and multiple authentication methods which creates points of vulnerability for external AND internal security attacks. Researchers used their findings to build a security framework that combines Elliptic Curve Diffie-Hellman (ECDH) for enabling confidential key exchanges and using AES and Blowfish to enhance data encryption speeds. The system operates from a multi-level network architecture supporting secure access authentication and file upload and download operations and encrypted file storage capabilities. The system framework provides data encryption from start to finish while simultaneously running efficient processing operations and reducing memory consumption. Recognizing the requirement System analysis determined the significance of maintaining advanced user role authority systems and active observation capabilities that screen for system breaches. The proposed framework incorporated these security considerations to create a system which boosts cloud protection and operational performance and scalability. The analysis proves that integrating secure encryption with intelligent system architecture alongside secure communication standards creates a solution to resolve essential security issues thus creating a base for dependable cloud-based service delivery.


Enhancing Cloud Security with Advanced Cryptography and Architecture

Cryptography Techniques
Advanced methods like ECDH, AES, and Blowfish ensure data security.

Cloud Architecture
Multi-layered structure enhances security and efficiency.

User Authentication
Secure access through robust authentication processes.

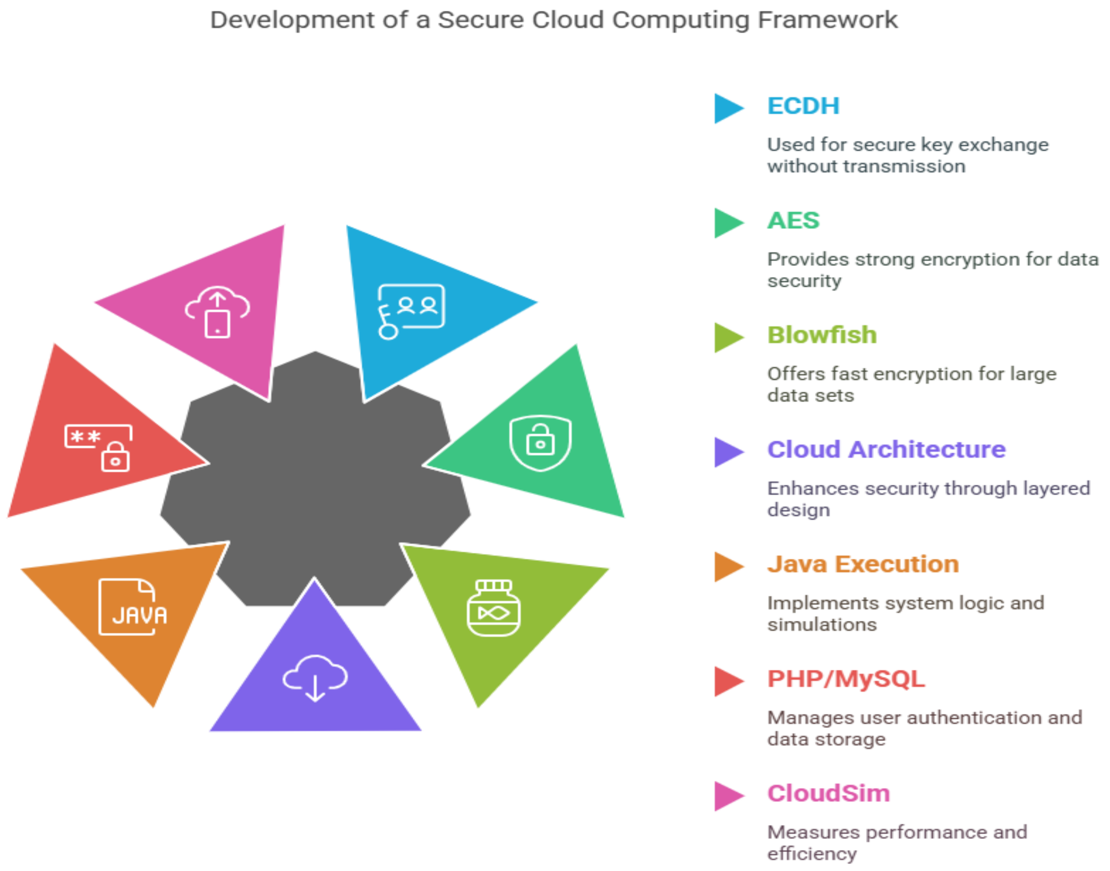
Performance Testing
Evaluates encryption speed and data processing efficiency.

Simulation Tools
Utilizes Java, PHP, and CloudSim for development and testing.

METHODOLOGY

This research develops secure efficient scalable cloud computing framework through integration of advanced cryptography techniques and cloud architectural improvements. This proposed system implements high-security data encryption by using a dual encryption method which generates keys through ECDH and provides encryption strength from AES and Blowfish algorithms. Two parties can securely create a common secret through ECDH despite an insecure connection without key transmission followed by the joint usage of AES and Blowfish which quickly encrypt massive data sets efficiently. A secure system architecture with multiple cloud layers exists to strengthen security functions through authenticated access systems with encryption for dataflow protocols and role-based permissions and restrictions. User-related activities such as account setup and login and file upload and key generation and secure file retrieval get simulated by the system. The development along with simulation of this model takes place through Java execution within the NetBeans IDE platform while PHP capabilities with MySQL traced through phpMyAdmin handle user authentication and log storage. The cloud infrastructure simulation and performance measurement for encryption speed as well as data processing time together with memory efficiency use CloudSim. Comprehensive testing measures the performance of the proposed hybrid method against RSA encryption through analysis of security strengths with efficiency improvements while evaluating time requirements. An organized approach validates both security and efficiency aspects of cloud systems in a complete way to prove its practicality and effectiveness.

IJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/



Development of a Secure Cloud Computing Framework

ECDH
Used for secure key exchange without transmission

AES
Provides strong encryption for data security

Blowfish
Offers fast encryption for large data sets

Cloud Architecture
Enhances security through layered design

Java Execution
Implements system logic and simulations

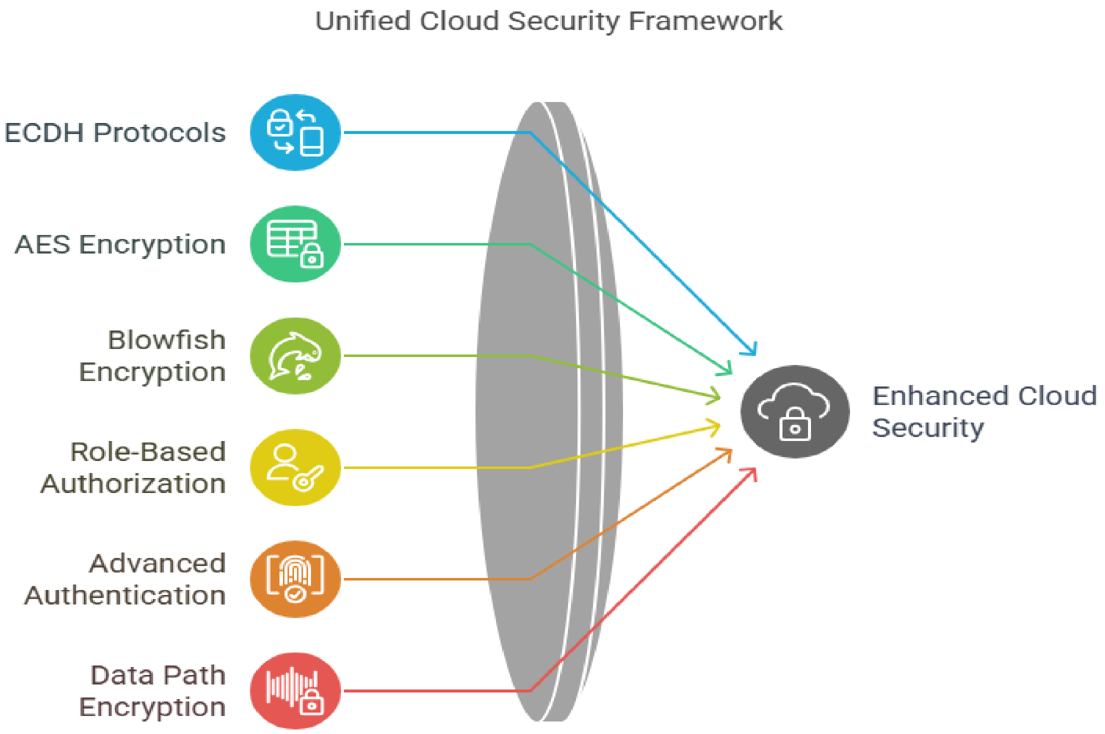
PHP/MySQL
Manages user authentication and data storage

CloudSim
Measures performance and efficiency

RESULTS AND DISCUSSION

The experimental study proves that the proposed cloud security framework improves data protection and system operational efficiency more than RSA encryption techniques do in traditional methods. The system used ECDH key exchange protocols together with AES and Blowfish encryption during testing across user login and file upload and encryption management through decryption and retrieval operations within a simulated CloudSim cloud environment. The hybrid system demonstrates faster speed of encryption and decryption processes at reduced power consumption this provides essential benefits for real-time cloud operations that require optimal performance outcomes. The combination of AES and Blowfish encryption increases the system strength due to its multiple defensive systems which protect against dictionary and brute-force attacks. Through its implementation of ECDH the system secures key exchange operations by delivering encryption protection that protects confidential information throughout network communication. The implementation used less memory as well as reduced processing time than RSA encryption methods did for extensive data sets because it established better efficiency in system resources. The strategic deployment of multiple security measures through architectural improvements achieves greater protection by introducing both role-based authorization and advanced authentication features and data path encryption to minimize staff misuse and unauthorized system entry. The simulation-tested approach both fulfills security goals while improving both system responsiveness along with resource efficiency standards. The research validates that the model demonstrates practical and scalable implementation for securing real-world cloud computing installations which handle sensitive data alongside high user traffic. The implemented security solution has proven to be a practical advancement in secure cloud systems through its simultaneous handling of efficiency requirements and security objectives.

IJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/



ACKNOWLEDGEMENT

The completion of my final year project only became possible because of the valuable support I received from every person who guided me. The research success for this project depends heavily on the invaluable guidance and continuous encouragement from my project supervisor Prof.D.J.Manowar. I extend my gratitude to the Computer Science & Engineering at Takshashila Institute of Engineering & Technology because they provided a firm academic structure combined with a nurturing learning space which inspired my interest in both cloud computing and cybersecurity. I express heartfelt gratitude to my classmates and friends who supported me with thoughtful talks and collaborative efforts as well as moral backing from the moment I started until my research conclusion. My family deserves my deepest appreciation because their endless support and kindness maintained my drive when difficulties occurred. The completion of this project used open-source research papers and tools which functioned as essential foundation resources for design and testing purposes. The achievement of this project depended on the unified backing from these people and organizations.

CONCLUSION

The authors developed a complete solution through research to solve both efficiency problems and security issues affecting cloud computing ecosystems. The system raises cloud data security by using ECDH for key exchange and an AES/Blowfish hybrid encryption method which ensures cloud data integrity and its availability alongside confidentiality protection. A multi-layered cloud architecture installation enriches system security with features that enable whole workflow authentication of users through encrypted data protected by role-specific access restrictions. The experimental results show that the proposed security approach achieves superior speed and efficiency when compared to RSA systems specifically in encryption time while effectively resisting multiple security risks. The system functions optimally during heavy data processing because lightweight encryption algorithms enable quick performance under demanding conditions thus making it valuable for financial services and healthcare as well as governmental institutions. The framework demonstrates adaptable features which allow it to grow in compliance with advancing cloud security needs.

IJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

REFERENCES

[1] The Manila Times (2018, April 26). At a glance: The Philippine Health Care System [1] A. K. Sen, M. B. Shinde, and B. C. Chaudhari, "Improving Cloud Efficiency Using ECDH-AE," *International Research Journal of Engineering and Technology (IRJET)*, vol. 07, no. 06, pp. 2856–2861, Jun. 2020.

[2] R. Shinde and A. Kale, "Enhancement of Cloud Computing Security," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT)*, vol. 3, no. 4, pp. 1470–1475, Jul.–Aug. 2018.

[3] S. Patil, D. Patil, and P. Shinde, "Securing Cloud Data using Hybrid Cryptography Algorithms," *International Journal of Scientific Development and Research (IJSDR)*, vol. 6, no. 4, pp. 409–413, Apr. 2021.

[4] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," *Information Sciences*, vol. 305, pp. 357–383, Jun. 2015.

[5] Z. Mahmood, "Data location and security issues in cloud computing," in *Proc. Int. Conf. on Emerging Intelligent Data and Web Technologies*, 2011, pp. 49–54.

[6] K. Hwang and D. Li, "Trusted Cloud Computing with Secure Resources and Data Coloring," *IEEE Internet Computing*, vol. 14, no. 5, pp. 14–22, Sep.–Oct. 2010.

[7] R. Gellman, "Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing," *World Privacy Forum*, 2009. [Online]. Available: https://www.worldprivacyforum.org.

[8] A. Jain and V. R. Jain, "Enhancing Cloud Security through AES and RSA Encryption Algorithms," *International Journal of Computer Applications*, vol. 139, no. 1, pp. 36–40, Apr. 2016.

[9] A. Bhardwaj and P. Kumar, "Comparative Study of Cryptographic Algorithms in Cloud Computing," *International Journal of Computer Applications*, vol. 96, no. 16, pp. 33–38, Jun. 2014.

[10] Y. Zhang, J. Chen, and H. Wang, "Cloud computing security: Foundations and research directions," Frontiers of Computer Science, vol. 6, no. 3, pp. 280–299, Jun. 2012.

[11] Miss. Devika M. Shelke, Miss. Roshani S. Bhojane, Miss. Tina B. Madane, Mr. Pratik N. Gawande, Prof. D.J. Manowar, Prof. S.S. Dubey Department Of Computer Science & Engineering, "Data Store and Multi-Keyword Search on Encrypted Cloud Data*," International Journal of Computer Science and Mobile Computing*, IJCSMC, vol.3, Issue.4, April 2014, pg.1227-1232.