International Journal Of Engineering Research And Development
e- ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 20, Issue 5 (May. 2024), PP. 145-149

Enhancing Cloud Data Security : Dynamic AES Encryption With Blockchain Key Management

Dr.Subba Rao Kolavennu
Computer Science & Engineering(CS) (JNTUH)
Sphoorthy Engineering College. (JNTUH)

Mr.G Rakesh Reddy
Computer Science $ Engineering(CS) (Assistant Professor)
Sphoorthy Engineering College (JNTUH)

L.Shreya
Computer Science & Engineering(CS) (B.Tech, JNTUH)
Sphoorthy Engineering College (JNTUH)

K.Vishal
Computer Science & Engineering(CS) (B.Tech, JNTUH)
Sphoorthy Engineering College (JNTUH)

N.Shubha
Computer Science & engineering (B.Tech, JNTUH)
Sphoorthy Engineering College (JNTUH)

ABSTRACT
This research presents a novel approach to recurrent problems related to sensitive information security in the constantly changing field of cloud computing security. Due to the widespread usage of cloud computing, worries about data security have increased, calling for the development of innovative strategies to strengthen defences against such attacks. The fundamental problem is that data stored in the cloud is vulnerable, which highlights the necessity of sophisticated encryption and key management techniques. Traditional approaches frequently fail to reduce the hazards associated with hacked encryption keys and centrally stored keys. Our suggested solution uses a two-phase strategy to get around these obstacles. The first stage focuses on creating distinct, dynamic encryption keys for every file through the use of dynamic encryption. By limiting an attacker's capacity to decrypt, this method greatly strengthens file-level security. In spite of a compromised key, numerous files. Block chain technology is introduced in the next phase for safe key storage along with metadata to strengthen security and data integrity. Finally, by offering strong encryption, decentralised key management, and defence against unwanted access, our all-encompassing method improves cloud security. Our solution offers consumers dependable data protection in the cloud due to its scalability and agility, making it a useful tool in modern cloud security paradigms.

Date of Submission: 07-05-2024 Date of Acceptance: 20-05-2024

I. RELATED

Cloud storage is becoming more and more popular since it is affordable, easily accessible, and efficient with resources. Implementing solutions that ensure data integrity and privacy is necessary to protect user privacy during cloud data transfers. This is especially important in the context of the linked effort, where finding new ways to improve security during cloud data migration is still a top priority.

A novel Lightweight Cryptographic Algorithm called (NLCA) was presented by [21] in 2021. It functions as a 16-byte block cypher and encrypts data in cloud environments using a 16-byte key. Improving data security is the aim of this proposal. One thing that sets NLCA apart from other encryption algorithms is its flexibility, which is achieved by adding additional logical operations to the mix while still maintaining optimal encryption speed and high security.

II. INTRODUCTION

The IT sector uses cloud computing extensively because of its advantages, which include virtualization, scalability, affordability, distant data processing, and on-demand sharing services. One of the primary components of cloud computing is cloud storage, which has several benefits like instant availability, affordability, accessibility, ease of use, consistency, flexibility, and several leasing possibilities. Cloud computing is further supported by essential qualities including data recovery, accessibility, cost effectiveness, scalability, and optimised resource utilisation. But because cloud storage providers have limited data monitoring tools at their disposal, trust poses a significant challenge when it comes to migrating user data to cloud settings. Modern cryptographic algorithms have been used to integrate data and resource security strategies with cloud security in order to address this.

Client data inside server centres is protected from both internal and external attacks by encryption mechanisms. One key is used in symmetric cryptography, which uses two keys, while one key is used in asymmetric cryptography. Using larger, more complicated keys makes encryption techniques more safe. Modern, cutting-edge blockchain technology can boost confidence and enhance cloud service data security. By comparison, centralised database security lacks the complexity and dependability of block chain security. It acts by means of a peer-to-peer network, a distributed ledger, and cryptographic hash algorithms to guard against unauthorised alteration and offer data transparency.

Blockchain is being used by a wide range of industries, including finance and the Internet of Things (IoT) ecosystem, and its use is anticipated to increase. To increase the security of file storage in cloud computing, a hybrid dynamic encryption approach has been suggested. Block chain technology, elliptic curve cryptography, and the sophisticated encryption standard AES are used in this way to improve the overall security of cloud-based storage solutions and create a highly secure environment. This work primarily contributes dynamic AES file encryption, block chain-based key security, and intuitive key management. Because of its efficient and dynamic key generation technique, dynamic AESfile encryption improves the security of cloud file storage. Strong encryption of encryption keys is ensured by block chain-powered key security, which shields them from

According to researchers in [22], hybrid algorithms have proven to be effective in 2021 at improving data safety in cloud environments. The hybrid algorithm proposed in this study takes advantage of the advantages shared by the AES and Elliptic Curve Cryptography (ECC) techniques. For AES key generation, an ECC method was used in order to balance the requirements of data security, computational effectiveness, and ease of implementation. Another advantage of the suggested system is the algorithm's key size, which is noteworthy for its tiny dimensions.

A thorough comparison study was carried out with a variety of encryption methods and other suggested systems. Based on the results, it can be concluded that the AESECC hybrid algorithm achieves higher security levels and uses less energy than its competitors, making it the best option for cloud data protection.

By addressing the flaws and challenges present in traditional medical cloud storage systems, blockchain technology has been used in 2022 to build interoperability, trust, and transparency The suggested method includes a consensus mechanism to improve cloud data management, authenticate healthcare providers, and validate new blocks.

The Fine-Grained Access Control (FGAC) system, which will be implemented in 2022, uses afuzzy logic framework to improve the confidentiality and dependability of users and service providers [24]. Three different types of cryptographic keys are generated by this system in order for it to function: public, private, and session keys. By employing this multimodal key management technique, the suggested system provides an extensive range of security features. Furthermore, it successfully solves a range of possible hazards related to various types of cyberattacks. The system's exceptional ability to identify users accurately allows for the implementation of protective measures. This is made possible by a well-designed confirmation process that complies with predetermined permissions and criteria. In 2023, a novel Non-Deterministic Cryptographic Scheme (NCS) was presented, which integrates the Linear Congruential Generator (LGC), Sliding Window Algorithm (SWA), and XOR implementation to guarantee data privacy and confidentiality in cloud environments. Its superiority over the AES, RSA, and DES encryption algorithms in terms of execution time was demonstrated by a comparison of the proposed method and its strength. In addition, the method placed emphasis on striking a balance between the encryption algorithm's strength and efficiency in relation to the volume of data .A thorough analysis covering aspects such as computing time, strength of encryption, and possible security breech.Enhancing both usability and security, user-friendly key management minimises complexity and empowers users to efficiently manage the substantial quantity of dynamic keys required for encryption operations..

III. BACKGROUND AND METHODOLOGY

Dynamic Encryption :

Encryption That Adapts Dynamic encryption, also known as "runtime encryption" or "real-time encryption," refers to the process of encrypting data as it is generated or accessed, as opposed to the traditional practices of encrypting data either at rest or during transmission. Data protection is guaranteed by dynamic encryption from the time of creation or access until it is no longer needed.

The following are important attributes and ideas related to dynamic encryption:

Real-Time Encryption: Using encryption keys that are produced or derived from the active operation, dynamic encryption encrypts data as it is being used. This guarantees the security of data while it is being processed, transferred, or used.

Protection of Data-in-Use: Dynamic encryption uses encryption to protect data while it is being used, so it remains encrypted even when programmes or authorised users access it. That differentiates it from data-at-rest encryption (such as network transmission encryption) and data-in-transit encryption (such as file encryption on storage devices).
Granular access control: allows companies to define who can access data and under what circumstances. It is commonly used in conjunction with dynamic encryption. Access can be restricted using the user's permissions, the time, location, and other relevant characteristics.Adaptive Security: Dynamic encryption exhibits adaptability to evolving security conditions. The encryption strength and key management, for instance, may be altered based on the material's perceived sensitivity or threat level.
Robust Authentication: Dynamic encryption is frequently accompanied by strict authentication resource usage is carried out to undertake a thorough performance evaluation of these methods.
The results of this comparison analysis demonstrate that the AES method is superior in terms of encryption speed and cryptographic resilience.

PROPOSED DYNAMIC SOLUTION

Using the Advanced Encryption Standard (AES) algorithm, data can be encrypted using a technique called dynamic AES encryption, which periodically modifies the encryption key. As a result, it is more difficult for unauthorised parties to interpret the data. The procedure is breaking up the data into fixed-size blocks, giving each block a random encryption key, running the AES algorithm on each block using the matching key to create a ciphertext block, and then safely storing the encryption keys for later decoding. A novel method for securely and decentrally handling encryption keys is called blockchain key management. It stores and manages encryption keys via a distributed digital record called a blockchain. A blockchain network must be set up, encryption keys must be created and stored there, access to the keys must be managed by smart contracts, and when data has to be encrypted or decrypted, the relevant key must be retrieved from the blockchain. Cloud data security can be greatly enhanced by integrating Blockchain Key Management with Dynamic AES Encryption. Unauthorised parties find it more difficult to decode data due to the dynamic nature of the encryption process, and only authorised parties can access and preserve the encryption keys thanks to the decentralised and secure key management system.

IV. RESULT AND TESTING

Several levels of evaluation and investigation, including comprehensive statistical and mathematical analyses, have been applied to the proposed solution. Its resilience against data analysis assaults and key guessing is also investigated in detail. These evaluations seek to emphasise the significance and potency of the proposed solution under the required encryption conditions. For the performance measurements, randomly generated synthetic data that was algorithmically created was employed to mimic various text inputs. In addition, image data was collected from reliable websites to replicate multimedia content protocols to ensure that only authorised entities—individuals or systems—are able to access encrypted data. Methods like multi-factor authentication and digital certificates could be used for this.

Key Management: Proper key management is crucial for dynamic encryption. It is necessary to generate, store, cycle, and delete encryption keys in a secure manner on time in order to preserve the security of encrypted data.Dynamic encryption reduces the risk of data breaches and unauthorised access by adding an extra layer of security to secure sensitive data. It is widely used when data security and privacy are critical, such as in cloud computing, safe communications, financial transactions, and healthcare.

B. AES

Because of Rijndael's exceptional security, performance, and beauty, the NIST purposefully chose it as the advanced encryption standard in 2000. The symmetric encryption technique AES uses a block size of 128 bits in accordance with NIST recommendations. One important characteristic of AES is its ability to adjust the number of encryption rounds based on the encryption key's size. More precisely, the AES employs ten encryption cycles for a 128-bit key and twenty-two rounds for a 192- and 256-bit key. SubBytes, ShiftRows, MixColumns, and AddRoundKey operations are the basic building elements of every AES encryption round. One of the most significant of them is the AddRoundKey operation, which performs an exclusive OR (XOR) operation between the cryptographic key and the input state matrix. Notably, every round key in the conventional AES architecture is produced using a predefined key expansion procedure.The adoption of AES as a widely used encryption algorithm is made robust and effective by a number of factors, including the choice of Rijndael as the advanced encryption standard, its block length, the variable number of encryption rounds, and essential components such as the AddRoundKey operation.

C. Cryptography using Ellipstic Curves:

Elliptic Curve Cryptography (ECC) is a data encryption and decryption technique that establishes a pair of keys by mathematically associating every point on an elliptic curve with a particular set of public and private keys . However, while the private key is kept secret, the public key is shared. The sender must first

2. UNIT TESTING

Unit testing involves the design of test cases that validate that theinternal program logic is functioning properly, and that program input produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit beforeintegration. This is a structural testing, that relies on knowledge of its constructionandisinvasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a businessprocess performs accurately to the documented specifications and contains clearly definedinputsand expected results.

3. FUNCTIONAL TEST

Functional tests provide systematic demonstrations that functionstested are available as specified by the business and technical requirements, systemdocumentation, and user manuals. Functional testing is centered on the following items:

Valid Input : identified classes of valid input must be accepted. Invalid Input : identified classes of invalid input must be rejected. Functions : identified functions must be exercised. Output : identified classes of application outputs must be exercised. Systems/Procedures : interfacing systems or procedures must be invoked.

4. SYSTEM TEST

System testing ensures that the entire integrated software systemmeets requirements. It tests a configuration to ensure known and predictable results. An exampleof system testing is the configuration oriented system integration test. Systemtesting is basedonprocess descriptions and flows, emphasizing pre-driven process links and integration points

5. PERFORMANCE TEST

The purpose of the performance test is to make sure that the output is generated within the given time, as well as how long it takes the system to gather information, react to user inquiries, and retrieve outcomes.

obtain the recipient's public key in order to ensure the security of data being communicated using ECC. The recipient's private key is required to decrypt the data after it has been encrypted using the public key. When using the encryption method, the data is only visible to the intended recipient. Numerous applications use the already widely used techniques, known as ECC, ranging from file transfers to secure email protocols and Virtual Private Networks (VPNs). In order to create a secure internet connection, cryptographic protocols like the TLS protocol are designed with its help. The input parameters for the ECC technique are the generator point G, the prime modulus p, the order of the generator point n, and the coefficients a and b of the elliptic curve. A random number between 1 and n−1 is generated as the private key d, and the public key Q is found to be dG. Taking into account the above described aspects, ECC is an effective and safe encryption method that can be applied to a variety of applications, including those that call for the usage of mobile devices.

An elliptic curve can be represented by the equation $y2=x3+ax+b$. The curve in this equation has an oval or longer circle-like shape, which is represented by the variables a and b. There are spots on the curve where $y2=x3+ax+b$ occurs as well as the point at infinity that is involved in the point addition operation.

In order to construct points on the curve, the method begins with a point P and performs a point doubling or adding operation. The point doubling procedure takes an input of pointinfinity that is involved in the point addition operation.

In order to construct points on the curve, the method begins with a point P and performs a point doubling or adding operation. The point doubling procedure takes an input of point P on the curve and outputs a new point 2P. A third point R, which is likewise on the curve, is created when two points P and Q are joined together.

Lately, blockchain technology has shown promise for revolutionising a number of industries, including cloud computing [18]. It is made clear how quickly this issue needs to be resolved in order to increase the security of cloud data storage. Blockchain technology seems like a good option because it is renowned for its immutable, transparent, and secure record-keeping. Because of its decentralised architecture, which guards against fraud and manipulation, blockchain integration with cloud

INTEGRATION TESTING

Software integration testing is the incremental integration testingoftwo or more integrated software components on a single platform to produce failures causedbyinterface defects. The task of the integration test is to check that componentsorsoftware applications, e.g. components in a software system or – one step up – softwareapplications at the company level – interact without error

ACCEPTANCE TESTING

User Acceptance Testing is a critical phase of any project andrequires significant participation by the end user. It also ensures that the systemmeets thefunctional requirements

V. CONCLUTION

In this paper, we have introduced a comprehensive and innovative solution to address critical security concerns in cloud computing environments. The proposed approach leverages a hybriddynamic encryption technique based on Elliptic Curve Cryptography (ECC), AdvancedEncryption Standard (AES), and Block chain technology, providing a multi-layereddefensemechanism to safeguard sensitive data. Throughout our discussion, we have addressedvarioussecurity challenges prevalent in cloud computing, including the vulnerability of centralizedkeymanagement and the need for enhanced data protection. Our solution offers a robust responsetothese challenges through a two-phase process. In the first phase, dynamic AESkeys aregenerated, ensuring each file is encrypted with a unique and dynamically changing key. Thisdynamic key generation greatly enhances file-level security, mitigating the risk of compromise. The second phase introduces the use of block chain technology, providing an immutableanddecentralized ledger to securely store encryption keys. By encrypting these blocks withECCpublic keys, we ensure that unauthorized access is effectively prevented during both transmissionand storage.

REFERENCES

[1]. R. Anandkumar, K. Dinesh, A. J. Obaid, P. Malik, R. Sharma, A. Dumka, R. Singh, andS. Khatak, "Securing e-health application of cloud computing using hyperchaotic image encryptionframework," Computers and Electrical Engineering, vol. 100, p. 107860, 2022.

[2]. Z. Bashir, T. Rashid, and S. Zafar, "Hyperchaotic dynamical system based image encryptionscheme with time-varying delays," Pacific Science Review A: Natural Science and Engineering, vol. 18, no. 3, pp. 254–260, 2016.

[3]. W. Y. Chang, H. Abu-Amara, and J. F. Sanford, Transforming enterprise cloud services. Springer Science & Business Media, 2010.

[4]. B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, "Asystematicliterature review on cloud computing security: threats and mitigation strategies," IEEEAccess, vol. 9, pp. 57792–57807, 2021.

[5]. N. M. Sultana and K. Srinivas, "Survey on centric data protection method for cloudstorageapplication," in 2021 International Conference on Computational Intelligence and ComputingApplications (ICCICA), pp. 1–8, IEEE, 2021.

[6]. F. Thabit, O. Can, S. Alhomdy, G. H. Al-Gaphari, and S. Jagtap, "Anovel effectivelightweight homomorphic cryptographic algorithm for data security in cloud computing,"International Journal of intelligent networks, vol. 3, pp. 16–30, 2022.

[7]. D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Integration of blockchainandcloud of things: Architecture, applications and challenges," IEEE Communications surveys&tutorials, vol. 22, no. 4, pp. 2521–2549, 2020.

[8]. S. N. G. Gourisetti, Ü. Cali, K.-K. R. Choo, E. Escobar, C. Gorog, A. Lee, C. Lima, M. Mylrea, M. Pasetti, F. Rahimi, et al., "Standardization of the distributed ledger technologycybersecurity stack for power and energy applications," Sustainable Energy, Grids and Networks, vol. 28, p. 100553, 2021.

[9]. S. Banani, S. Thiemjarus, K. Wongthavarawat, and N. Ounanong, "A dynamic light-weight symmetric encryption algorithm for secure data transmission via ble beacons," Journal of Sensorand Actuator Networks, vol. 11, no. 1, p. 2, 2021.

[10]. I. Keshta, Y. Aoudni, M.Sandhu, A. Singh, P. A. Xalikovich, A. Rizwan, M. Soni, andS. Lalar, "Blockchain aware proxy re-encryption algorithmbased data sharing scheme," Physical Communication, vol. 58, p. 102048, 2023.

[11]. O. A. Khashan, N. M. Khafajah, W. A