INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 35-40

A HYBRID APPROACH OF ECC (ELLIPTIC CURVE CRYPTOGRAPHY) AND AES(ADVANCED ENCRYPTION STANDARD) CRYPTOGRAPHY IN A FILE TRANSFER SYSTEM COMBINE WITH CLOUD COMPUTING

Arunima Raj[1], K.S. Giriprasath[2]

[1]Dept of CSE, PG Scholar, Rathinam college of arts and science, Coimbatore,

[2]Dept of CSE, Assistant Professor, Rathinam college of arts and science, Coimbatore,

DOI: https://www.doi.org/10.58257/IJPREMS33109

ABSTRACT

There are lot of attacks are happening now a days to stuck the whole business of an organization. Data on sharing and rest can be attacked y hackers very simple today. The mode of sharing data and storage data infrastructure should be very efficient. So that an attacker could not reach them or hack them even if he gets reached. Cryptography is the study of techniques and tactics to protect information and communication from possible attackers. It involves encoding data such that it cannot be decoded without the right decryption key. Its benefits include safeguarding private information, maintaining privacy, preventing unwanted access, enabling safe communication, and creating a foundation for safe online transactions. The importance of cryptography in protecting information is shown by the fact that it is essential in a variety of fields, including communication and finance. A cloud computing infrastructure offers a cost-efficient means for end users to store and retrieve private data remotely via an internet connection. Cloud computing provides high performance, accessibility and low cost for data storing and sharing, provides a better consumption of resources. In cloud computing, cloud service providers compromise an abstraction of infinite storage space for clients to mass data. It can help clients diminish their financial overhead of data managements by drifting the local managements system into cloud servers. However, security concerns develop the main constraint as we now outsource the storage of data, which is possibly sensitive, to cloud providers. This paper proposes an innovative hybrid strategy that integrates Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) to enhance the security of file transfer systems within cloud computing environments. The collaborative use of AES and ECC harnesses the effectiveness of symmetric key encryption and the robustness of asymmetric key cryptography, presenting a holistic approach to ensuring the protection of data during both transit and storage.

Keywords: Cryptography, Cloud computing, Encryption, Advance Encryption Standard, Elliptic Curve Cryptography.

1. INTRODUCTION

To address the privacy in data as well as the user identity privacy in current access control techniques, an encryption scheme that combines cryptographic approaches with RBAC and an anonymous control scheme is proposed. In cloud computing, a real-time mechanism is offered to sustain a secure communication that guarantees security and trust-based cloud access. [1]. Globally, data centers serve as the backbone for delivering cloud services, enabling users to access virtual resources over the internet through cloud computing. Prominent examples of cloud services include Google applications and Microsoft SharePoint. However, the rapid growth of the "cloud computing" industry has brought forth significant security challenges. Security issues, a persistent concern for Open Systems and the internet, become particularly pronounced in the realm of cloud computing. The primary hindrance to the widespread adoption of cloud computing lies in its inherent security shortcomings. Numerous security considerations, ranging from safeguarding data to overseeing cloud usage by service providers, underscore the security challenges surrounding cloud computing.[2] Since it provides group users with data storage services, the cloud storage server is regarded as semi-trusted. Any organization that is able to confirm the data integrity of shared data kept on the cloud server can be considered a Trusted Third Party (TTP) within the cloud ecosystem. [3]

2. PROBLEM FORMULATION

Elliptic Curve Cryptography (ECC) stands out as a widely recognized cryptographic method that employs asymmetric key encryption, effectively safeguarding data against unauthorized access. The utilization of paired public and private keys is a hallmark of ECC, ensuring the overall security of the system. ECC operates within two-dimensional fields, encompassing both binary and prime fields. The security of ECC is based on the difficulty of solving the elliptic curve discrete logarithm problem. The computational challenge at hand revolves around determining the discrete logarithm of a specific point on an elliptic curve concerning a designated base point. This mathematical problem is foundational in elliptic curve cryptography (ECC), where the discrete logarithm serves as the basis for key exchange, digital signatures,

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 35-40

and other cryptographic operations. In general, the discrete logarithm problem is defined as finding x in the equation $g^x \equiv h \pmod p$, where g is a generator of a finite cyclic group of order p, and h is an element in that group. The compact key size in ECC (224 bits) emerges as a pivotal factor, further enhancing its cryptographic efficiency.

AES, introduced in 2001, stands as a symmetric key encryption algorithm that attained standardization by the U.S. National Institute of Standards and Technology (NIST). AES operates on fixed-size blocks of data (128 bits). AES boasts several advantages, including its ease of implementation on 8-bit architecture processors and its effectiveness on 32-bit architecture processors. In addition, all operations are simple (e.g, XOR, permutation and substitution). It supplanted the outdated Data Encryption Standard (DES) and is crafted to ensure both security and efficiency.

2.1 Encryption process of AES

AES encryption involves a number of key operations, all of which are vital for maintaining the overall security and complexity of the algorithm. The SubBytes operation performs byte substitution using a fixed lookup table known as the S-box. This adds a layer of non-linearity to boost the cryptographic strength. By reordering rows, the ShiftRows operation plays a crucial role in causing dispersion within the state matrix and strengthening the algorithm's resistance to various cryptographic assaults. The MixColumns method combines and alters the state matrix's columns to promote this diffusion. In the end, the AddRoundKey operation creates the round key by combining particular key bits with each byte of the state matrix.

When taken as a whole, these actions form a strong Substitution-Permutation Network that strengthens the Advanced Encryption Standard (AES) against potential weaknesses and solidifies its position as a key component of modern cryptography techniques.

2.2 ECC Operations

Key Generation in elliptic curve cryptography (ECC) entails the selection of a random private key, followed by the computation of its corresponding public key on the elliptic curve. This process forms the foundation of ECC's asymmetric key system, where the private key remains confidential, while the public key is openly shared. Key Exchange in ECC is particularly efficient, rendering it well-suited for environments with limited resources. The ability to swiftly and securely exchange keys is a distinctive feature that enhances ECC's applicability in resource-constrained scenarios, making it a preferred choice in various cryptographic implementations. Furthermore, ECC plays a prominent role in Digital Signatures, a crucial aspect of secure communication. The algorithm's robust mathematical framework makes it a reliable method for generating digital signatures, contributing to the overall integrity and authenticity of digital messages and transactions. In summary, ECC excels in key generation, exchange, and digital signatures, offering a versatile and resource-efficient cryptographic solution.

2.3 Insecurity without integrating ECC and AES

when implementing a file transfer system in a cloud computing environment without combining the security features of ECC (Elliptic Curve Cryptography) and AES (Advanced Encryption Standard) will have multiple disadvantages. File transfer systems lack strong security controls might not have adequate methods for authenticating users. This raises the possibility that unapproved people will enter the system and alter or remove private information.

When utilized independently, AES and ECC might not be resistant to future quantum attacks. Combining several cryptographic techniques helps provide defense against a wider variety of security risks.

When AES and ECC have not been combined, key management issues may arise. It becomes more difficult to share and distribute symmetric keys safely, which increases the risk of compromised keys and eventually, compromise data.Lack of AES and ECC integration may result in a lack of forward secrecy, which makes all previous communications susceptible to compromise in the event that encryption keys are stolen.

Relying on only one encryption technique could lead to the creation of a single point of failure. The entire security system could be compromised if one algorithm is compromised or become obsolete.

3. PROBLEM SOLUTION

Utilizing the hybrid model (AES-ECC) is integral in ensuring the security of the system within cloud storage with optimal efficiency. The primary motivation behind adopting this hybrid methodology is the reduction of data key size, concurrently ensuring robust system security within a shortened timeframe.

Meanwhile, AES excels in encrypting bulk data efficiently. This combination ensures the secrecy and integrity of transferred files while maximizing resource efficiency, making it well-suited to the dynamic and scalable nature of clo ud computing.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 35-40

3.0.1 Key Generation

Elliptic Curve Cryptography (ECC) is used by the Key Generation to generate cryptographic keys. Strong cryptographic security with lower key lengths is ensured by its capabilities for creating ECC key pairs (public/private keys) for encryption and decryption procedures.

Algorithm Of Key Generation.

Step 1: Select any number n as the prime number.

Step 2: Select any number for the generation of the public key as n (a)

Where n (a) < n

Step 3: Compute the point on the curve as G

Where G > n

Step 4: Calculation of public key is:

$P = n(a) * G$

Step 5: Return the public key P after calculation.

3.0.2 Data Encryption

It has features that guarantee the security and integrity of data stored by utilizing AES encryption methods for data encrypting and decryption.

File Encryption algorithm using AES

Step 1: Take the input file

Step 2: Now add the key generated by ECC which is the public key.

Step 3: The public key produced by the ECC is used to execute AES encryption on the input file.

Step 4: The encrypted file is uploaded on the server after the encryption by AES.

Step 5: Once the file is uploaded then it will be downloaded at the server, and then file is translated by using the public key given by ECC so that the original file is decrypted.

3.0.3 Access Control

To manage user access to encrypted cloud data, It offers functionality for user authentication, authorization, and access control policy enforcement based on predefined rules and user permissions.

3.0.4 Request Sharing

The Request sharing module makes it easier to ask the data owner for access to particular data. It has features that allow users to make requests for access, data owners to examine and grant requests, and alerts and notifications for changes to the status of requests.

3.0.5 Decryption Key Sharing

The safe distribution of decryption keys to authorized users is managed by this module. It has features that allow data owners to encrypt their data using the recipient's public key which they received via ECC, create one-time decryption keys for requested data, and safely distribute their data with authorized users. When AES is combined with ECC, the input text is encrypted using the AES algorithm, but the encryption key is created via ECC (elliptic curve cryptography). With that key, the client will decrypt the text message and obtain the original text file.

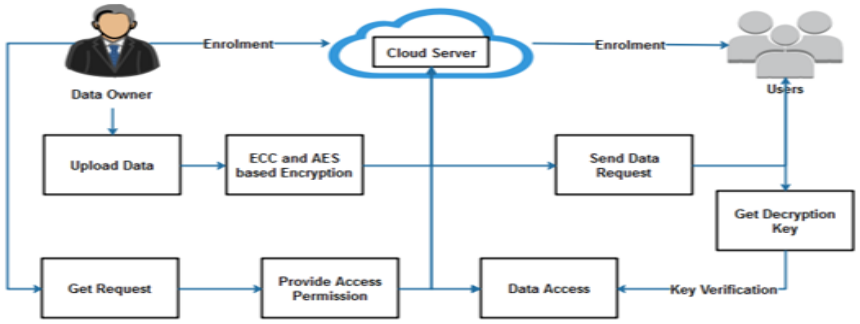

Figure1: Block diagram for proposed system.

The complete process has following steps:

Step 1: Different text files of different sizes are taken as input.

Step 2: After taking text file as input, Advance encryption standard algorithm is applied for encrypting the text file. AES will encrypt the text using a key which is not its own but generated by elliptic curve cryptography algorithm (ECC).

Step 3: Encrypted text file is uploaded to the Cloud after encryption using AES.

Step 4: Client will download the encrypted file from the Cloud by decrypting the encrypted text using the same key that the elliptic curve cryptography algorithm produced. Upon successful decryption, the client will receive the original text file.

Step 5: Analysis of AES-ECC at the end is done on the basis of different parameters such as Avalanche effect, encryption time, decryption time, storage required and correlation coefficient.

Step 6: The user and Owner details also will be stored and upload to cloud in SQL database.

3.1 Experimental Setup

It is necessary to carefully evaluate a number of factors while setting up an experimental environment for the proposed project, which involves secure data sharing and storage using AES encryption and ECC-based key creation. This is a summary of the experimental configuration:

Hardware Requirements:

Server: A server capable of hosting the cloud storage infrastructure and cryptographic operations.

Client Devices: Devices (e.g., computers, smartphones) representing users accessing the cloud storage system.

Software Requirements:

Cloud Storage Platform: Choose a cloud storage platform (e.g., Amazon S3, Google Cloud Storage) to host encrypted data.

Cryptographic Libraries: Utilize cryptographic libraries to implement AES encryption and ECC-based key generation.

Development Environment: Set up a development environment (e.g., Python) for implementing and testing the project functionalities.

4. IMPLEMENTATION

The project comprising secure data sharing protocols, ECC-based key generation, and AES encryption must be implemented and deployed in a real cloud environment in a number of steps.

Select a trustworthy cloud service provider with scalable alternatives, compliance certifications, and strong security features. Google Cloud Platform (GCP), Microsoft Azure, and Amazon Web Services (AWS) are popular choices. In this project I have used AWS RDS database linked to MySQL workbench to store the details of user and owner.

Make that the resources chosen have enough storage, processing power, and network bandwidth to satisfy the project's needs. Install the project application's different modules and parts on the allocated cloud resources. Deploying the access control module, key generation module, data encryption module, and other pertinent parts is part of this. Set up the cloud environment's ECC-based key generation module to produce ECC key pairs. Make sure to follow best practices for key management and protection when storing and managing the ECC keys. For data that is at rest in the cloud storage environment, enable AES encryption. Before saving data in the cloud, configure encryption settings to encrypt it using AES encryption techniques. To safeguard AES keys and guarantee safe key distribution, put encryption key management procedures into effect.

Incorporate safe data exchange protocols in the program to enable restricted access to encrypted information. This include creating one-time decryption keys, establishing access control policies, and safely distributing decryption keys to authorized users. The safely sharing or distributing the decryption key via mail account of the authorized users.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 35-40

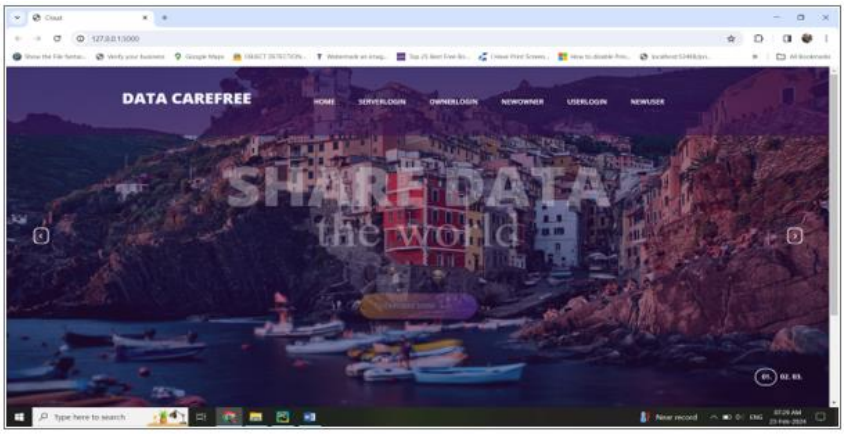

Figure 2: Home page for user login, owner login and server login.

In the proposed system, the new owner is required to register with their mail account and mobile number for authentication purposes. Upon providing these credentials, the system generates an owner login key, which is shared with the owner via the provided mail account. With this owner login key, the owner gains access to the system, enabling them to perform encryption and upload encrypted files onto the platform securely.

For users seeking to download the encrypted files uploaded by the owner, a registration process is initiated. Following user registration, an approval from the owner is mandatory. Subsequently, a login key is shared with the user through their provided mail account. Using this login key, the user can log in to their account and request the decryption key to proceed with file download.

The owner's approval triggers the sharing of the decryption key with the user via their registered mail account. Armed with the decryption key, the user can successfully decrypt and download the data securely. This multi-step authentication and authorization process ensures a robust and controlled access environment, enhancing the overall security of file sharing and data management within the platform.

5. CONCLUSION

Integrating both the Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) in the proposed project for securing cloud-based data storage and sharing provides a comprehensive solution addressing key concerns of confidentiality, integrity, and controlled access. AES encryption, known for its effectiveness and strength, ensures the secure preservation of data at rest within the cloud storage infrastructure, forming a robust framework against unauthorized access and potential data breaches.

This dual cryptographic approach enhances the overall security posture, establishing resilience in safeguarding sensitive information throughout its lifecycle in the cloud environment. The combination of AES and ECC reflects a strategic and sophisticated approach to meet the stringent security requirements of modern cloud-based data management.

6. FUTURE WORK

This policy can be used in the future to any company where role hierarchy is important, particularly to organizations that want to safely upload documents to the cloud. The policy guarantees complete security of documents. This project can be modified for usage in organizations or educational settings where regulated file access according to user permissions and roles is necessary.

7. REFERENCES

[1] Authors: Saba Rehman, Nida Talat Bajwa, Munam Ali Shah, Ahmad O. Aseeri and Adeel Anjum, Hybrid AES-ECC Model for the Security of Data over Cloud Storage, 2021

[2] Authors: Shukla, D.K.; Dwivedi, V.K.; Trivedi, M.C. Encryption algorithm in cloud computing. Mater. Today Proc. 2020, 37, 1869–1875. [CrossRef]

[3] Authors: Yahia, H.S.; Zeebaree, S.R.M.; Sadeeq, M.A.M.; Salim, N.O.M.; Kak, S.F.; Al-Zebari, A.; Salih, A.A.; Hussein, H.A, Comprehensive survey for cloud computing-based nature-inspired algorithms optimization scheduling. Asian J. Res. Comput. Sci. 2021, 1–16. [CrossRef]

[4] Authors: Qazi, R.; Khan, I.A. Data security in cloud computing using elliptic curve cryptography. Int. J. Comput. Commun. Netw. 2019, 1, 46–52. [CrossRef]

[5] Authors: Chen, Y.; Liu, H.; Wang, B.; Sonompil, B.; Ping, Y.; Zhang, Z. A threshold hybrid encryption method for integrity audit without trusted center., J. Cloud Comput. 2021, 10, 3. [CrossRef]

[6] Authors: Agrahari, V. Data security in cloud computing using cryptography algorithms. Int. J. Sci. Dev. Res. 2020. Available online: www.ijsdr.org (accessed on 22 October 2021).

[7] Authors: Abdullahi Ibrahim, A.; Cheruiyot, W.; Kimwele, M.W., Data security in cloud computing with elliptic curve cryptography core. Int. J. Comput. 2017, 26, 1–14. Available online: http://ijcjournal.org/ (accessed on 22 October 2021)

[8] Authors: Ali Nauman, Yazdan Ahmad Qadri, Muhammad Amjad, Yousaf Bin Zikria, Muhammad Khalil Afzal, Sung Won Kim, Multimedia internet of things: a comprehensive survey, IEEE Access 8 (2020) 8202–8250. [2]

[9] Authors: Sachin Kumar, Prayag Tiwari, Mikhail Zymbler, Internet of Things is a revolutionary approach for future technology enhancement: a review, J. Big data 6 (1) (2019) 1–21.

[10] Authors: Amal Hafsa, Anissa Sghaier, Jihene Malek, Mohsen Machhout, Image encryption method based on improved ECC and modified AES algorithm, Multimed. Tool. Appl. 80 (13) (2021) 19769–19801.

[11] Authors: Harikrishna Bommala, S. Kiran, M. Pujitha, R. Pradeep Kumar Reddy, Performance of evaluation for AES with ECC in cloud environment, Int. J. Adv. Netw. Appl. 10 (5) (2019) 4019–4025.

[12] Authors: Luis Parrilla, Encarnacion ´ Castillo, Juan A. Lopez-Ramos, ´ Jos´e A. Alvarez-Bermejo, ´ Antonio García, Diego P. Morales, Unified compact ECC-AES co-processor with group-key support for IoT devices in wireless sensor networks, Sensors 18 (1) (2018) 251.

[13] Authors: Umar Hayat, Naveed Ahmed Azam, A novel image encryption scheme based on an elliptic curve, Signal Process. 155 (2019) 391–402.