International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Conference Proceedings: Volume: 05 ACME – 2026 DOI:10.55041/ISJEM.ACME035
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Revolutioning Cloud Data Security with Elliptic Curve Cryptography

N. ANITHA , K KUSUMA , PACCHA UDAYALAKSHMI , G R VENKAT , A S DEENADAYALAN

[1,2,3,4,5,6] *Computer Science and Information Technology, Siddharth Institute of Engineering & Technology*

Abstract - In the era of cloud computing, ensuring data security and efficient data retrieval is paramount. This paper presents an Efficient Traceable Authorization Search System for Cloud Storage that implements a robust authorization mechanism allowing only authorized users to perform searches on cloud-stored data. Authorized users are classified into two categories: role-based users such as data owners and their delegates, and attribute-based users such as specific departments within an organization. The project emphasizes advanced cryptographic techniques to enhance data security within cloud environments. Existing systems primarily use RSA cryptography, which has notable limitations in security and efficiency. To overcome these challenges, we propose the integration of Elliptic Curve Cryptography (ECC).

Keywords: Authorization Search, Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Cryptography, Elliptic Curve Cryptography (ECC).

1. INTRODUCTION

Data security in today's digital world is paramount, especially in large data centers and cloud computing environments. Elliptic Curve Cryptography (ECC) stands out as a powerful solution, offering robust encryption with minimal computational power and energy consumption. In an era of rapid digital transformation, the security of sensitive data transmitted over the internet has become a critical concern, particularly in cloud computing environments.

Traditional encryption methods, while effective, often require significant computational power due to large key sizes, leading to inefficiencies in energy consumption and processing speed

2. SYSTEM ANALYSIS

Existing System:

Current phishing detection techniques include:

- **RSA Cryptography:** Provides secure encryption but requires large key sizes (2048+ bits), resulting in high computational overhead and increased energy consumption.
- **AES Encryption:** While fast for symmetric encryption, it lacks the public-key infrastructure needed for secure key exchange in multi-user cloud environments.
- **Traditional Key Management:** Existing systems struggle with key distribution and storage in distributed cloud environments, creating single points of failure.

Limitations of Existing Systems:

- High computational overhead due to large RSA key sizes slows performance.
- Significant energy consumption in large-scale cloud data centers.
- No automated audit log updates, reducing traceability and system integrity.

3. PROPOSED SYSTEM

The proposed system introduces Elliptic Curve Cryptography (ECC) as an advanced encryption technique for enhancing data security in cloud computing environments.

3.1 ECC – Elliptic Curve Cryptography

- **Key Equation:** ECC generates keys through the elliptic curve equation: $y^2 = x^3 + ax + b$.
- **Public Key:** Known to anyone; derived from a private key by multiplying a base point on the curve a fixed number of times.
- **Private Key:** Data points closest to the hyperplane that define the margin.

3.2 System Modules

- **Data Owner Module:** The data owner registers and logs in after admin authorization. Once authenticated, the owner uploads files to the cloud and encrypts them using ECC.$w \cdot x + b = 0$

● **Data User Module:** Data users register and access the system after admin approval.

● **Cloud (Admin) Module:** The admin acts as the central authority, managing user registrations by authorizing or rejecting data owners and data users

3.3 Advantages of Proposed System

● Strong Security with Smaller Key Sizes: ECC provides robust encryption comparable to RSA but with much smaller key sizes, reducing computational requirements.

● Automatic Audit Log Updates: ECC supports automated updating of audit logs, enhancing overall system integrity.

3.4 Hardware & Software Requirements

● Hardware: Processor – i3/Intel, RAM – 8 GB (minimum), Hard Disk – 128 GB, Monitor – SVGA.

● Software: Operating System – up to Windows 11; Programming Language – Python; Libraries – Django, Cryptography; IDE – VS Code; Database – SQLite3; Frontend – HTML, CSS, Bootstrap, JavaScript.

Advantages of Proposed System:

● Strong Security with Smaller Key Sizes
● Reduced Computational Overhead
● Improved Energy Efficiency
● Faster Encryption and Decryption

EXPERIMENTAL RESULTS:

● ECC encryption and decryption of test files completed successfully with no data loss.

● Login failure on incorrect credentials was correctly handled.

● Secret key distribution via email was validated end-to-end.

Diagram 1: System Architecture

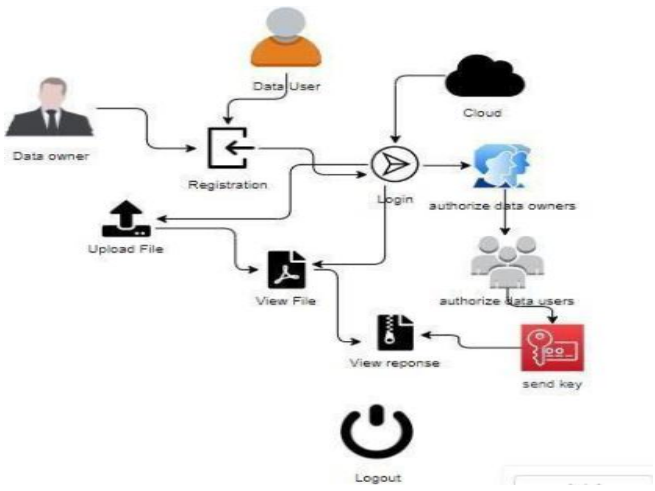

Fig -1: Figure

4. CONCLUSION

In an era where data security is paramount, especially in cloud computing and IoT environments, traditional encryption methods like RSA are increasingly challenged by the need for efficiency and scalability. The proposed system, leveraging Elliptic Curve Cryptography (ECC), addresses these challenges by offering strong encryption with significantly smaller key sizes, reducing computational overhead and energy consumption. ECC's ability to deliver robust security while enhancing system performance makes it an ideal solution for modern cloud infrastructures and real-time applications. As the digital landscape continues to evolve, the adoption of ECC represents a forward-thinking approach, ensuring that data remains secure without compromising efficiency. This project underscores the potential of ECC to meet the growing demands for secure, scalable, and efficient encryption in a rapidly advancing technological world.

FUTURE SCOPE

Future enhancements to the proposed system could focus on integrating ECC with quantum-resistant algorithms to safeguard against future cryptographic threats. Additionally, implementing adaptive encryption techniques that dynamically select the optimal cryptographic method based on system conditions could enhance both security and performance. Expanding compatibility with a wider range of legacy devices and platforms would also increase adoption. Incorporating machine learning algorithms to predict and mitigate potential security breaches in real-time could provided.

REFERENCES

1. R. Lu, X. Yuan, and X. Lin, "Homomorphic Encryption for Cloud Computing: An Overview," IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. 2381–2405, 2021.

2. M. S. Ali, K. K. R. Choo, and S. H. Ahmed, "Blockchain-Based Secure Data Storage and Access Control for Cloud Applications," IEEE Transactions on Cloud Computing, vol. 9, no. 3, pp. 1215–1226, 2021.

3. X. Kong, J. Wang, and Q. Ni, "Efficient Data Security and Privacy-Preserving Scheme in Cloud Computing," IEEE Access, vol. 10, pp. 24356–24367, 2022.

BIOGRAPHY

I, **NAMA ANITHA,** currently working as an Assistant Professor in the Department of Computer Science and Information Technology at Siddharth Institute of Engineering & Technology, Puttur, Andhra Pradesh, India. I am having 4 years of teaching experience in engineering education. I am pursuing my Ph.D. in Computer Science and Engineering at MBU, Tirupati. My research interests include Cyber Security, Artificial Intelligence, IoT, and Phishing Detection Systems. I actively participated in faculty development programs, workshops, and technical seminars. I guided several undergraduate projects and is committed to academic excellence and research innovation.