A Dual-Layered Cryptographic Framework for Enhancing Cloud Application Secrecy Against Advanced Cryptanalysis Attack

Prof. Sanmati Jain 1
Associate Professor
sanmati@vitmindore.com

Prof. Saniya Koser 3
Assistant Professor
saniya@vitmindore.com

Prof.Vipin Kasera2
Assistant Professor
vipin.kasera@vitmindore.com

Computer Science & Engineering Department VITM Indore

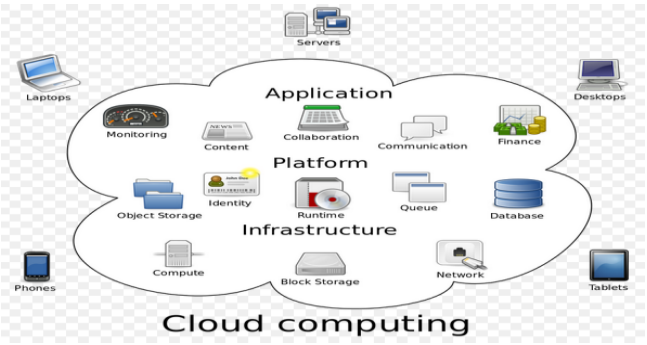
ABSTRACT

Cloud paradigms are incorporated with diverse technologies such as web-based services, virtualization, and for overseeing software operations, service-level agreements (SLA) are implemented. Numerous clientele service facilitators have shifted toward cloud ecosystems due to the swift advancement of technology. To ensure network accessibility, various cloud-based solutions are utilized by defense organizations, commercial enterprises, and governmental bodies, facilitating high availability of services for end-users. Cloud computing plays a crucial role in contemporary applications. Its open architecture and widespread adoption render it prone to security breaches and cyber threats. The suggested approach seeks to merge the ECC cryptographic technique with the RC6 encryption mechanism to establish a hybridized security framework, enhancing secrecy measures.

Keywords: ECC, RC6, Kerberos, Security Model

1. INTRODUCTION

Cloud computing comprises resources, delivering services and offering structural support. It serves as a vast repository of resources, enabling efficient computations and operations while facilitating seamless access to on-demand services. As an evolving technology, the cloud adapts to dynamic trends, offering flexibility, cost efficiency, and practical advantages. The security protocols of cloud environments are analyzed in the introductory section to ensure data authentication for safeguarding purposes. Security and privacy remain persistent challenges for researchers and scholars,



encompassing aspects such as authentication, authorization, integrity, secrecy, availability, and privacy. These concerns arise primarily due to reliance on third-party entities, leading to potential data loss. Large-scale data transmission occurs

Figure 1: Cloud Computing

within cloud environments, which presents challenges related to. the issue of increased risk in data access within the cloud by malicious actors. Researchers highlight the escalation of security threats in Section Two, emphasizing the essential

security prerequisites necessary for safeguarding sensitive information, including healthcare records, within cloud environments.

Security Concerns

1. **Verification of Identity**

   Identity verification remains an essential aspect of security frameworks and cannot be eliminated. It ensures the validation of both user identity and system identity for seamless communication.

2. **Data Privacy**

   Data privacy guarantees protection, requiring specific measures to prevent unauthorized access and ensure information is delivered exclusively to the intended recipient. Only approved individuals possess access rights.

3. **System Availability**

   Resource availability is a crucial factor, ensuring system components function effectively. It necessitates the timely provision of essential resources, optimizing time management and operational expenses.

4. **Data Integrity**

   Data integrity upholds accuracy, ensuring that unauthorized modifications or alterations during transmission are prevented. Any unauthorized data tampering, deletion, or corruption during transfer compromises information reliability.

2. PRIVIOUS WORK

A comprehensive review of existing literature highlights prior developments. Various cryptographic models and methodologies have been proposed or implemented, aiming at refining earlier versions and mitigating vulnerabilities.

Khalid M. Abdullah et al. in [1] introduced a **hybrid encryption framework**, integrating elements of asymmetric encryption for key distribution and symmetric encryption for computational efficiency. The approach utilized **RSA and AES** encryption methods, supplemented by **LZW compression** to minimize cipher text size. The process involved:

- Partitioning data into segments.
- Encrypting odd-numbered segments with an **AES key** and even-numbered segments with **RSA encryption**.
- Encrypting the AES key itself using RSA's private key.
- Applying **LZW compression** to the resultant cipher text for reduced storage and processing time.

This approach significantly optimized encryption and decryption performance, improving transmission security and reducing packet loss. However, the **hybrid cryptographic model lacked provisions for ensuring data integrity**.

3. PROBLEM DOMAIN

The prevailing methodology employs **Attribute-Based Encryption (ABE)**, which functions based on distinct attributes. It is a **public-key encryption scheme**, where a user's secret key and encrypted text rely on specific attributes, such as geographical location or contractual agreements.

Decryption of encrypted text is only possible when the recipient's attributes align with the encryption parameters. While ABE is resistant to **collusion attacks**, it suffers from several critical limitations:

1. **Key Escrow Vulnerability**
    - ABE incorporates a **key escrow mechanism**, where a third party stores cryptographic keys.
    - This mechanism allows users to exchange encryption and decryption materials.
    - However, reliance on a third-party entity introduces the risk of **compromised encryption keys**, potentially exposing sensitive information.
2. **Revocation of Access Credentials**
    - **Key revocation** pertains to **digital security**, requiring robust protocols for identity verification.
    - If an individual's authorization is revoked, their **digital certificates** must be invalidated to maintain security.
    - **Certificate Authority (CA) Managers** oversee digital certifications, ensuring authentication.
    - However, fraudulent certifications can emerge, leading to **misrepresentation** and undermining security.
3. **Limitations of Attribute-Based Encryption**
    - ABE operates through **Bilinear Groups**, managed by multiple authorities.
    - However, it imposes constraints on **cipher text policies**, restricting adaptability.
    - Authorities function **independently**, setting **public parameters** and issuing **private keys** to users.
    - While users can encrypt data based on assigned attributes, comprehensive access control remains with designated authorities.

The necessity of a **more secure and dynamic encryption strategy** is evident, particularly one that mitigates the risks associated with **key escrow**, **certificate manipulation**, and **restricted policy enforcement**.

4. METHODOLOGY

Authentication Framework

Authentication is a fundamental aspect of every security infrastructure. To enhance user authentication, the Kerberos protocol has been implemented, ensuring a more robust and secure verification mechanism.

Kerberos operates on a ticket-based authentication system, which eliminates the need to transmit user credentials over the network repeatedly. This enhances security by reducing the risk of password interception and unauthorized access. The key principles of the Kerberos authentication model include:

1. **Key Distribution Center (KDC):**
    - Manages authentication requests and issues secure session tickets.
    - Consists of an Authentication Server (AS) and a Ticket Granting Server (TGS).
2. Ticket-Based Authentication:
    - Users request authentication from the AS, which verifies credentials and provides a ticket-granting ticket (TGT).
    - The TGT allows users to request access from the TGS without re-entering login credentials.
3. Mutual Authentication:
    - Both the user and the service provider authenticate each other, ensuring secure communication.

By integrating Kerberos authentication, the proposed system strengthens user verification,

reduces unauthorized access risks, and enhances the overall security framework.

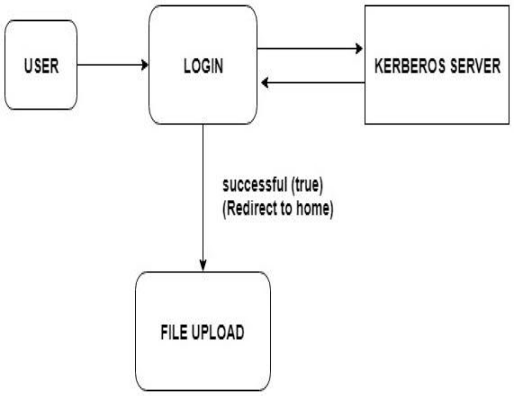


Figure 2: Authentication Model

2. To calculate Integrity: MD5 with 512 bit length has been used for integrity purpose.

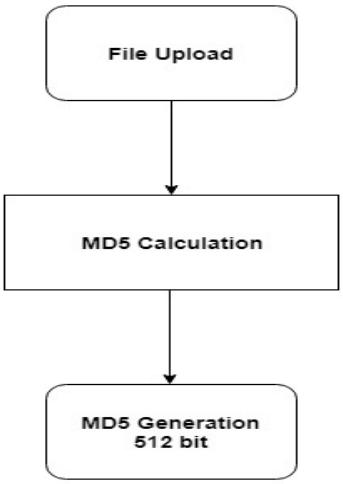


Figure 3: Integrity Calculation

3. Encryption Mechanism

Secrecy ensures that data remains private and protected from unauthorized access. This project incorporates a **hybrid encryption approach** by integrating the **Elliptic Curve Cryptography (ECC)** and **RC6 algorithm** to achieve a superior level of security.

Encryption Procedure:

1. **Input Processing:**
   - The original file is provided as input.
   - The file is divided into multiple **chunks** to create a structured **chunk pool**: C1,C2,C3,...,CnC_1, C_2, C_3, ..., C_nC1,C2,C3,...,Cn
2. **Chunk Segmentation:**
   - The chunks are categorized into **even-indexed** and **odd-indexed** groups.
   - **Even Chunks:** C2,C4,C6,...C_2, C_4, C_6, ...C2,C4,C6,...
   - **Odd Chunks:** C1,C3,C5,...C_1, C_3, C_5, ...C1,C3,C5,...
3. **Hybrid Encryption:**
   - **Even Chunks** are encrypted using the **RC6 algorithm**, a symmetric encryption technique known for its fast execution and high security.
   - **Odd Chunks** are encrypted using **Elliptic Curve Cryptography (ECC)**, an asymmetric encryption method that provides strong security with minimal computational overhead.
4. **Ciphertext Formation:**
   - After encryption, the processed chunks are assembled into **cipher chunks**, forming the final encrypted output.

This hybrid encryption model **enhances security** by combining the strengths of **RC6's efficiency** and **ECC's cryptographic robustness**, ensuring **confidential and secure data transmission** in cloud environments.

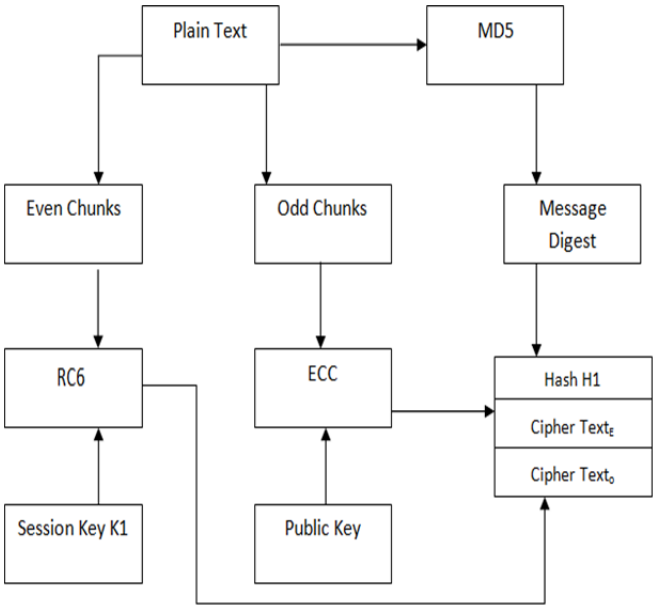
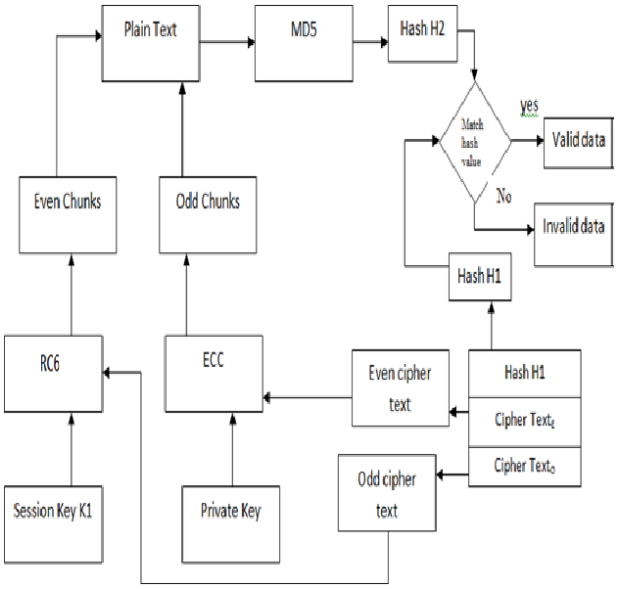
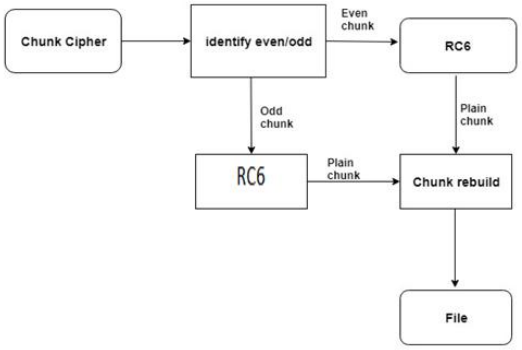


Figure 4: Encryption Model

4. Decipherment Process Decipherment process, where the ciphered portions are taken, then even and odd chunks are identified. Even chunks are deciphered using ECC to get a plain even chunk and odd chunks are decrypted using RC6 to get a plain odd chunk. These portions are rebuilt to get the complete file.



Block diagram of Decryption Architecture



Decryption Model

5. Judgement of original file: Re-calculation of veracity of the chunk file will be performed using MD5. After it, the re-calculated file will be compared with the calculated file of step 2, if matched then is putative and not then rejected.

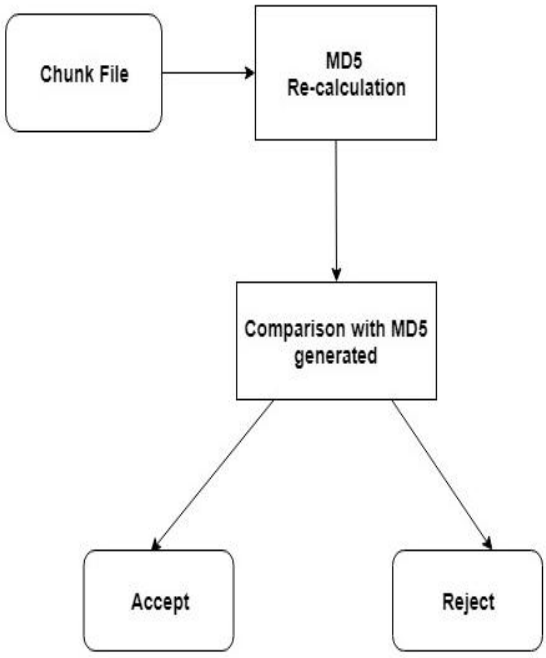


Figure 6: File comparison Model

5. RESULT ANALYSIS

The encoding time is the time taken by the procedure to produce the cryptograph text from the plain text.

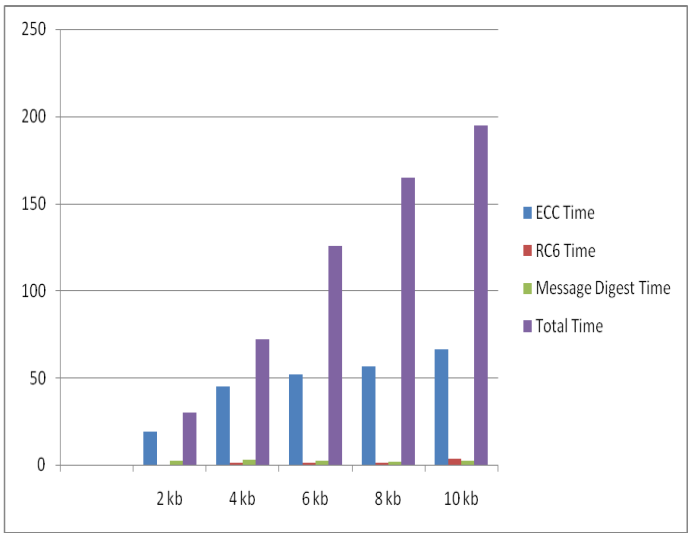


Figure 5.1: Encryption Time

The above illustration represents the duration needed for encoding when a raw text of **kibibyte volume** is secured using various encryption techniques such as **Elliptic Curve Cryptography (ECC), RC6, and Hashing Algorithm**. Here, **ECC and RC6** are utilized for securing/deciphering information to ensure **secrecy**, while the **hashing function** is employed to verify **data authenticity** and **integrity**

. The complete duration needed to **encrypt the document** is illustrated in **Table 5.1**. Additionally, **Figure 5.1** presents a **graphical depiction**, offering a **statistical perspective** for better visualization and analysis.**5.1.2 Decryption Time:**

The decryption time is the time taken by the algorithm to produce the plain text from the cipher text. Similar to the encryption time process, the decryption process follows. It is represented in tabular form in table 5.2 and its graphical form is shown in figure 5.2.

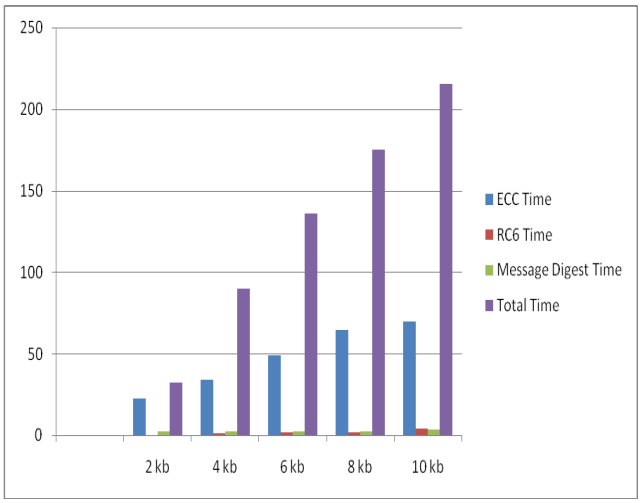


Figure5.2: Decryption Time

6. CONCLUSION

In the projected amalgam model, to protection the data from unsanctioned access in web application we try to ensure verification, secrecy, and veracity. In the proposed hybrid model, to achieve secrecy we combine the good features of both asymmetric key cryptography (ECC) which comes with the benefit of allocating the key and proportional key cryptography (RC6) which is faster and easier to calculate. Proposed Amalgam Model provides the best and fast way of preservation the data in web applications.

REFERENCES

[1]. Khalid M. Abdullah Essam H. Houssein Hala H. Zayed, “New Security Protocol using Hybrid Cryptography Algorithm for WSN”. 1st International Conference on Computer Applications and Information Security (ICCAIS), IEEE, 4-6 April. 2018

[2]. Milind Mathur, Ayush Kesarwani, “Comparison between DES, 3DES, RC2, RC6, RC6, andAES”. Proceedings of National Conference on New Horizons in IT – NCNHIT 2013.

[3]. V. Kapoor, Rahul Yadav, “A Hybrid Cryptography Technique for Improving

Network Security", International Journal of Computer Applications, Volume 141, No.11, May 2016.

[4]. M. Harini, K. Pushpa Gowri, C. Pavithra, M. Pradhiba Selvarani, "A Novel Security Mechanism Using Hybrid Cryptography Algorithms". International Conference on Electrical, Instrumentation, and Communication Engineering (ICEICE), IEEE 2017.

[5]. Kalyani Ganesh Kadam, Prof. Vaishali Khairnar, "HYBRID RSA-AES ENCRYPTION FOR WEB SERVICES". International Journal of Technical Research and Applications, Issue 31(September 2015), PP. 51-56.

[6]. F. Fatemi Moghaddam, S. Gerayeli Moghaddam, S. Rouzbeh, S. Kohpayeh Araghi, N. Morad Alibeigi, and S. Dabbaghi Varnosfaderani, "A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments," in IEEE Region 10 Symposium, Kuala Lumpur, Malaysia, 2014, pp. 508–513.

[7]. Jayraj Gondaliya, Jinisha Savani, Vivek Sheetal Dhaduvai, Gahangir Hossain, "Hybrid Security RSA Algorithm in Application of Web Service". 1st International Conference on Data Intelligence and Security IEEE 2018.

[8]. KirtirajBhatele, ProfAmit Sinhal, ProfMayank Pathak, "A Novel Approach to the Design of a New Hybrid Security Protocol Architecture". International Conference on Advanced Communication Control and Computing Technologies (ICACCCT) IEEE 2012.

[9]. A. Arjuna Rao, K Sujatha, A Bhavana Deepthi, L V Rajesh, "Survey paper comparing ECC with RSA, AES and RC6 Algorithms". International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 5 Issue: 1, IJRITCC January 2017.

[10]. Yasmin Alkady, Mohmed I. Habib, Rawya Y. Rizk, "A New Security Protocol Using Hybrid Cryptography Algorithms". 9th International Computer Engineering Conference (ICENCO), IEEE 2013.

[11]. Nair, Nikhitha K., K. S. Navin, and Soya Chandra. "Digital Signature and Advanced Encryption Standard for Enhancing Data Security and Authentication in Cloud Computing." (2015).