

A Secure Data Encryption Mechanism in Cloud Using Elliptic Curve Cryptography

I. Sudha

Professor, Department of Computer Science and Engineering
Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences – SIMATS, Chennai, India
sudhai.sse@saveetha.com

Cecil Donald

Assistant Professor
Department of Computer Science,
CHRIST (Deemed to be University)
Bengaluru, India
cecildonald6@gmail.com

S. Navya

Assistant Professor
Department of Computer Science Engineering
Raghu Engineering College Visakhapatnam, India
navyasangu7@gmail.com

G. Nithya

Assistant Professor, Department of CSE
V. S. B College of Engineering Technical Campus Coimbatore, India
nithya.june07@gmail.com

Manivannan Balamurugan

Department of Mathematics,
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology,
Avadi, Tamil Nadu, India.
balamurugansvm@gmail.com

S.Saravanan

Professor, Department of Computer Science and Engineering
Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences - SIMATS Chennai, India
saravanansiddhan@gmail.com

Abstract— Cloud computing is undergoing continuous evolution and is widely regarded as the next generation architecture for computing. Cloud computing technology allows users to store their data and applications on a remote server infrastructure known as the cloud. Cloud service providers, such Amazon, Rackspace, VMware, iCloud, Dropbox, Google's Application, and Microsoft Azure, provide customers the opportunity to create and deploy their own applications inside a cloud-based environment. These providers also grant users the ability to access and use these applications from any location worldwide. The subject of security poses significant challenges in contemporary times. The primary objective of cloud security is to establish a sense of confidence between cloud service providers and data owners inside the cloud environment. The cloud service provider is responsible for ensuring user data's security and integrity. Therefore, the use of several encryption techniques may effectively ensure cloud security. Data encryption is a commonly used procedure utilised to ensure the security of data. This study analyses the Elliptic Curve Cryptography method, focusing on its implementation in the context of encryption and digital signature processes. The objective is to enhance the security of cloud applications. Elliptic curve cryptography is a very effective and robust encryption system due to its ability to provide reduced key sizes, decreased CPU time requirements, and lower memory utilisation.

Keywords— Cloud computing; data security; encryption; cryptography; ECC

I. INTRODUCTION

Cloud computing provides simple and ubiquitous access to a shared pool of programmable computing resources, including networks, servers, storage, applications, and services, according to NIST[1]. These resources can be rapidly provisioned and released with minimal effort or reliance on service providers. This technology facilitates the preservation of user data and apps on distant servers, enabling

access to them from any location over the internet[2]. This feature allows users to use their apps without the need of installation, and enables them to access their data over the internet from any distant system[3]. This technology facilitates efficient computing via the use of centralized storage, memory, processor, and bandwidth resources. Cloud computing offers several service models, including Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). Cloud Computing has many key qualities that are considered vital. These include on-demand self-service, which allows users to access and manage computing resources as needed[4]. Additionally, it offers wide network access, enabling users to access the cloud services via various devices and platforms. Resource pooling is another crucial trait, as it allows multiple users to share and allocate resources dynamically[5]. Furthermore, Cloud Computing offers fast elasticity, enabling the quick and efficient scaling of resources based on demand. Lastly, it provides measured service, allowing for the monitoring and control of resource use, facilitating accurate billing and resource allocation. The Cloud computer environment offers computer resources via several deployment strategies, including Public cloud, Private cloud, Hybrid cloud, and Community cloud[6]. The establishment of robust data security measures is of utmost importance in the context of cloud computing. Therefore, the security of cloud computing is contingent upon the use of trusted computing mechanisms and cryptographic techniques. Cryptography is responsible for executing the procedures of encryption and decryption in order to safeguard data. Cloud data security encompasses many crucial areas, including availability, data protection, governance, incident response, compliance, and identity and access management[7].

II. DATA SECURITY MODEL

Security problems related to delivery and deployment models include data integrity, data location, data

confidentiality, and data access. The CIA triad is a widely recognized security architecture that encompasses three essential security goals: confidentiality, integrity, and availability[8]. These objectives pertain to the protection of both data and information, as well as computer services. Additional security goals often seen in various systems of system failures or data loss, reinforcing network security to protect against unauthorized access or malicious activities, implementing effective identity management practices, and particularly emphasizing the adoption of multi-factor authentication for enhanced security[9].

A. Data Confidentiality and Privacy

The cloud users store their data on several faraway servers, and they have the option to store different types of information, such as data and movies, with either a single cloud provider or multiple cloud providers[10]. Ensuring data confidentiality is a crucial need when storing user data on a distant server. A collection of facts, statistics, or information is called "data". The notion of confidentiality protects private information from unauthorised people, methods, and equipment. Information privacy and integrity depend on confidentiality. Service providers must protect data privacy by protecting individually obtained and stored information and carefully controlling its distribution to appropriate parties[11].

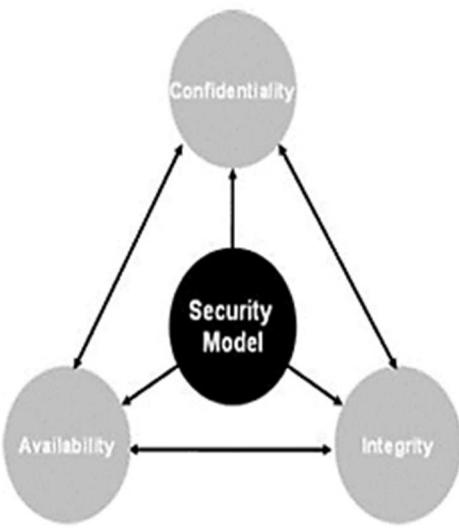


Fig. 1. Data security model

B. Data Integrity

Building customer confidence with a cloud service provider requires data integrity. It requires ensuring that user data is not manipulated and that the system works properly [12]. Additionally, the cloud service provider must keep thorough records of all cloud data, including its locations, storage resources, and virtual machines[13]. Transparency and accountability boost consumer-provider trust. A strong data integrity architecture is essential to dependable and secure cloud services and user data privacy[14].

C. Data Availability

Data availability requires fragmenting and dispersing data over several servers to ensure recovery in the case of a site failure or disaster [15]. Data availability is a major cloud

resources and data, ensuring that only authorized individuals or entities are granted appropriate privileges.

include the implementation of a single sign-on procedure, the establishment of robust authentication and authorization mechanisms, the use of data encryption techniques to safeguard sensitive information, ensuring data integrity via appropriate measures, facilitating data recovery in the event

computing security issue. Internal or third-party data centres provide security, which affects security level. Data availability guarantees constant access. Data availability is ensured by many factors. Service level Agreement (SLA), processing overhead, recovery roles, file system, and access are these factors. Availability guarantees system efficiency and service access for authorised users. Data storage, backup, and recovery are critical for data availability. As a minimum, service providers must provide RAID-based storage solutions.

D. Data location and relocation

The stored cloud data in cloud computing systems exhibits a significant level of mobility since it undergoes migration among virtual computers periodically. The cloud provider should ensure that the appropriate degree of security is provided to meet the diverse requirements of various clients. Some individuals with less knowledge or experience may lack awareness of the specific location of their data. However, it is possible for major corporations or enterprises to choose certain geographic locations for storing their data. In instances of this kind, it is essential that a formal agreement be executed between the cloud service provider and organizations in order to establish and maintain a sense of confidence.

III. SECURITY ISSUES IN CLOUD

Security concerns in cloud computing may be categorized into several areas, including but not limited to, unauthorized access to sensitive data, inadequate data segregation, lack of accountability, exploitation of software vulnerabilities, data recovery challenges, and the presence of hostile insiders. Cloud computing security concerns typically include regulatory compliance. Service providers may resist external audits and security certifications. Privilege user access, which allows authorised users to view sensitive externally controlled data, is another major issue. Risk is inherent in this technique. Location of data: Clients may not know where their data is hosted. Cloud data segregation separates client data from other customers' data. Disaster recovery: Service provider agreements are crucial. Cloud computing may hinder investigative help, especially in situations of wrongdoing.

Clients should consider the long-term validity of their data following an event.

To maintain data confidentiality, integrity, and availability in cloud settings, address the following security issues:

1. Key management: This pertains to the secure generation, distribution, storage, and revocation of cryptographic keys used for encrypting and decrypting data in the cloud.
2. Access control: This involves implementing mechanisms to regulate and restrict user access to cloud
3. Searchable encryption techniques: These refer to cryptographic methods that enable users to search and retrieve

specific information from encrypted data stored in the cloud, while still preserving the secrecy of the overall dataset.

Remote integrity checks verify system or data integrity without physical access. Verification methods include checksums, digital signatures, and cryptographic hashes. However, proof of ownership establishes one's legitimate ownership or control over an object.

IV. PROPOSED WORK

Victor Miller and Neil Koblitz developed Elliptic Curve Cryptography (ECC). ECC implements public-key cryptography using fast, effective cryptographic keys based on elliptic curve theory. Elliptic Curve Cryptography (ECC) uses elliptic curves and a mathematical group equation. The places where a line meets the axes form this set of values that may be operated to create a third value. Elliptic Curve Cryptography (ECC) is more secure than other encryption systems, making assaults harder. Smart cards, pagers, and cellular phones benefit from Elliptic Curve Cryptography (ECC) because it provides equivalent security with less processing power, battery, and memory. ECC is faster, making it better for mobile use. Comparatively, elliptic curves provide better cryptographic features.

A. Choice of Field

An elliptic curve, defined over a field denoted as K , is a smooth cubic curve expressed as $f(x,y) = 0$ in two variables. This curve contains a rational point, which could represent a point at infinity. The field K encompasses various mathematical domains, including complex numbers, real numbers, rational numbers, extensions of rationals, p -adic numbers, or even a finite field. When it comes to cryptographic applications, the study of elliptic curve groups focuses on analyzing these groups specifically over the foundational fields of F_p . The following equation representing an elliptic curve is expressed as

$$y^2 = x^3 + ax + b \quad (1)$$

Where, x, y is the co-ordinates and a, b are constant values.

Consider the elliptic curve

$$E: Y^2 = X^3 - X + 1 \quad (2)$$

The points P_1 and P_2 is added on E , by

$$P_3 = P_1 + P_2 \quad (3)$$

Where E is the elliptic curve and P is the point on the curve

As shown in picture. Let $P_1=(x_1, y_1)$, $P_2=(x_2, y_2)$, $P_3=(x_3, y_3)$ and P_1 not equals P_2

$$m = \frac{y_2 - y_1}{x_2 - x_1};$$

To find the intersection with E . we get

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B$$

$$\text{or}, 0 = x^3 - m^2 x^2 + \dots$$

$$\text{So}, x_3 = m^2 - x_1 - x_2$$

$$\Rightarrow y_3 = m(x_1 - x_2) - y_1$$

Multiplication is defined by the following curve, i.e $3P = P + P + P$

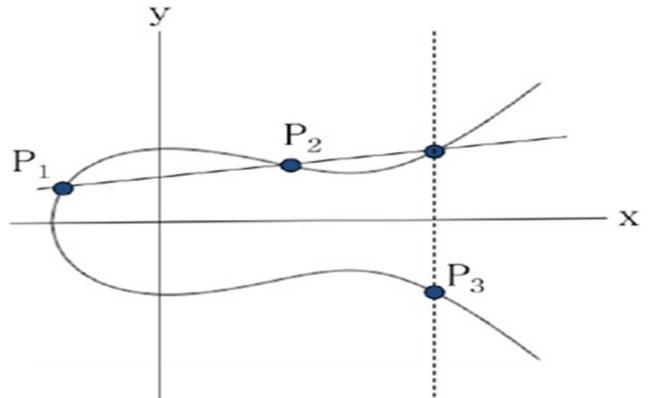


Fig. 2. Elliptic Curve

B. Method

Key production, encryption, decryption, and proof are all part of elliptic curve cryptography.

1. The process of generating cryptographic keys.

Cryptographic key creation is essential. Algorithms must generate public and private keys. The sender will encrypt the message using the receiver's public key, and the recipient will decode it using its private key. A random value 'd' is picked from the set of integers between 0 and n , and the public key 'Q' is created using the equation: $Q = d * P$, where 'd' is a random number between 1 and $n-1$, 'P' is a curve point, 'Q' is the public key, and 'd' is the private key.

$$Q = d * P$$

Where d is the random number in the range of between (1 to $n-1$). P is the point on a curve. Q is the public key and d is the private key.

2. Encryption

ECC-encrypt using the recipient's public key. ECC encryption requires a random number (k) and ciphertexts (C_1, C_2).

3. Decryption

With the private key (d), the receiver may decode the ciphertexts and get the original message.

4. Proof

The receiver may decode the ciphertexts and get the original message using the private key (d).

V. PERFORMANCE ANALYSIS

Our system is compared to the RSA scheme in this section for block size, key size, and other characteristics. This comparison compares two cryptographic algorithms under the same security circumstances to evaluate them.

A. Block Size

The real RSA block sizes are expected to be as follows. Based on key size, ECC and RSA employ the same block sizes. Encryption process uses block size of $((ks/8) - 11)$ and whereas ,the decryption uses block size of $(ks/8)$.

B. Key Size

Elliptic Curve Cryptography (ECC) and Rivest-Shamir-Adleman (RSA) algorithms were evaluated for key sizes and security levels according to NIST requirements. The table below compares ECC and RSA key sizes and security levels.

TABLE 1. KEY SIZES WITH EQUIVALENT SECURITY LEVELS

ECC (bits)	RSA (bits)	Key size ratio
128	512	1:8
164	1024	1:12
232	2048	1:20
356	3062	1:24
512	6048	1:30

C. Parameters

The parameters used to evaluate the properties of both RSA and ECC algorithms include:

The time required for key generation, encryption, and decryption are important factors to consider in cryptographic systems. These three-time measurements play a crucial role in evaluating and performance of such systems.

The tests may be conducted iteratively, capturing timings, while monitoring each of these three factors individually. Consequently, the measurement of average time is conducted.

VI. METHODOLOGY

The following procedures for the implementation of the Elliptic Curve Cryptography technique in a cloud environment.

The first step in the process is the creation of a Google application. To start the process of creating a user account, it is necessary to go the website <http://accounts.google.com/>. Once on the website, the user is required to provide their name and password. Following this, the user should proceed to Step 2, which involves selecting their own application. Please access the hyperlink to see my submitted applications. In the third step of the process, the user is required to choose the option labeled "Create Application." They must then input the application identifier and application title before proceeding to click the "Create Application" button. The application has now started.

In the fourth step, the user is required to establish a database on Google Cloud SQL and opting for the Google Cloud SQL alternative.

In the fifth step, the user is required to choose the "New instance" option and provide the name of the instance together with a previously developed application. Next, choose the option labeled "Create Instance" and click on the corresponding button.

Proceed to choose the instance name in order to access the corresponding properties.

Proceed to the "SQL Prompt" tab in order to automatically load all databases.

In the eighth step, the database and tables are established via the use of SQL queries, followed by the insertion of records. The next step involves the development of a user interface for the program.

In the tenth step, the task involves the composition of a Java code that effectively implements the Elliptic Curve Cryptography (ECC) technique. Furthermore, it is necessary

to undertake the debugging process of the program inside the Google Cloud environment.

The next step involves securely storing the data by using encryption techniques. In the event that the data is accessed, it should be presented in a decrypted manner.

A. Execution Flow

The cloud user securely maintains their confidential data inside the cloud environment facilitated by the service provider. After data is saved in the cloud, the system generates a private and public key. The ECC mechanism then encrypts the technique. Therefore, it generates ciphertext. The receiver will analyze and decipher the ciphertext. First communication will be gained.

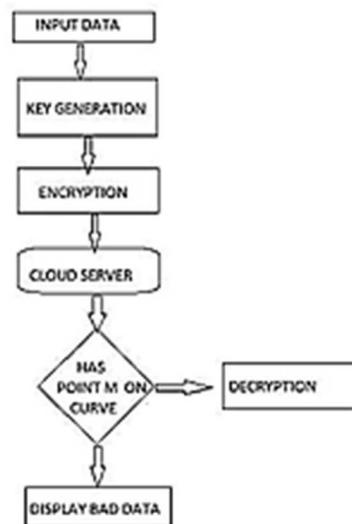


Fig.3. Execution Flow

VII. CONCLUSION

This research investigates the security concerns surrounding user data in cloud computing and highlights the need for a resolution. The use of the Elliptic Curve Cryptography (ECC) architecture ensures the security and dependability of Cloud application development and deployment. The ECC algorithm enhances security by offering higher processing speed and reduced computational cost compared to linear approaches. Elliptic Curve Cryptography (ECC) offers substantial advantages over RSA due to its ability to deliver the same level of security with shorter key lengths. Elliptic Curve Cryptography (ECC) is used in many communication applications such as mobile computing, wireless sensor networks, server-based encryption, and photo encryption.

REFERENCES

- [1] Y. Chen, Y. Lin, Y. Hu, S. Member, and C. Hsia, "Distributed Real-Time Object Detection Based on Edge-Cloud Collaboration for Smart Video Surveillance Applications," *IEEE Access*, vol. 10, no. September, pp. 93745–93759, 2022, doi: 10.1109/ACCESS.2022.3203053.
- [2] S. S. Ali and B. J. Choi, "State-of-the-art artificial intelligence techniques for distributed smart grids: A review," *Electron.*, vol. 9, no. 6, pp. 1–28, 2020, doi: 10.3390/electronics9061030.
- [3] T. J. Nandhini and K. Thinakaran, "Deep Neural Network-based Crime Scene Detection with Frames," *2023 Eighth Int. Conf. Sci. Technol. Eng. Math.*, pp. 1–8, doi: 10.1109/ICONSTEM56934.2023.10142449.

- [4] G. Uganya, F. D. Shadrach, I. Sudha, P. M. Krishnammal, V. Lakshmanan, and T. J. Nandhini, "Crime Scene Object Detection from Surveillance Video by using Tiny YOLO Algorithm," *2023 3rd Int. Conf. Pervasive Comput. Soc. Netw.*, no. October, pp. 654–659, 2023, doi: 10.1109/ICPCSN58827.2023.00114.
- [5] N. Kaaniche and M. Laurent, "Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms," *Comput. Commun.*, vol. 111, pp. 120–141, 2017, doi: 10.1016/j.comcom.2017.07.006.
- [6] V. D. Ganesh and R. M. Bommi, "Materials Today : Proceedings Cutting force and surface roughness measurement in turning of Monel K 500 using GRA method," *Mater. Today Proc.*, no. xxxx, 2023, doi: 10.1016/j.matpr.2023.05.722.
- [7] A. Abdulridha, D. Salama, and K. M, "NHCA: Developing New Hybrid Cryptography Algorithm for Cloud Computing Environment," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 11, pp. 479–486, 2017, doi: 10.14569/ijacsa.2017.081158.
- [8] S. Berlato, R. Carbone, A. J. Lee, and S. Ranise, "Exploring Architectures for Cryptographic Access Control Enforcement in the Cloud for Fun and Optimization," *Proc. 15th ACM Asia Conf. Comput. Commun. Secur. ASIA CCS 2020*, pp. 208–221, 2020, doi: 10.1145/3320269.3384767.
- [9] A. N. Jaber and M. F. Bin Zolkipli, "Use of cryptography in cloud computing," *Proc. - 2013 IEEE Int. Conf. Control Syst. Comput. Eng. ICCSCE 2013*, no. May 2016, pp. 179–184, 2013, doi: 10.1109/ICCSCE.2013.6719955.
- [10] N. E. El-Attar, D. S. El-Morshey, and W. A. Awad, "A New Hybrid Automated Security Framework to Cloud Storage System," *Cryptography*, vol. 5, no. 4, p. 37, 2021, doi: 10.3390/cryptography5040037.
- [11] S. Caleb and S. J. J. Thangaraj, "Data-driven ML Approaches for the concept of Self-healing in CWN , Including its Challenges and Possible Solutions," *2023 Eighth Int. Conf. Sci. Technol. Eng. Math.*, pp. 1–7, doi: 10.1109/ICONSTEM56934.2023.10142451.
- [12] R. Latha, "Deauthentication Attack Detection in the Wi-Fi network by Using ML Techniques," 2022.
- [13] H. Du, J. Chen, M. Chen, C. Peng, and D. He, "A Lightweight Authenticated Searchable Encryption without Bilinear Pairing for Cloud Computing," *Wirel. Commun. Mob. Comput.*, vol. 2022, 2022, doi: 10.1155/2022/2336685.
- [14] R. Rastogi and M. S. Sheela, "Enhancement of Channel Capacity in 5G Ultra Dense Network-UDN," *2023 2nd Int. Conf. Edge Comput. Appl.*, no. Iccea, pp. 303–307, 2023, doi: 10.1109/ICECAA58104.2023.10212363.
- [15] N. Nalini and I. Ahmed, "Network Intrusion Detection System for Feature Extraction based on Machine Learning Techniques," *2023 5th Int. Conf. Inven. Res. Comput. Appl.*, no. Icirca, pp. 440–445, 2023, doi: 10.1109/ICIRCA57980.2023.10220789.