Secure File Storage on Cloud Using Hybrid Cryptography

Ms Dhanya P G
Assisstant Professor in CSE
Ahalia School of Engineering and Technology
Palakkad,India
dhanyarenjith2025@gmail.com

Dr S Gunasekaran
Professor & Head
Department of CSE
Ahalia School of Engineering and Technology
Palakkad,India
gunaphd@yahoo.com

Amruth Raj D
CSE
Ahalia School of Engineering and Technology
Palakkad,India
amruthraj756@gmail.com

Pranith S
CSE
Ahalia School of Engineering and Technology
Palakkad,India
jithupranith456@gmail.com

Rithik K
CSE
Ahalia School of Engineering and Technology
Palakkad,India
rithikkrishnadas@gmail.com

Sreyas B
CSE
Ahalia School of Engineering and Technology
Palakkad,India
sreyasb10@gmail.com

How to Cite this Article:

G, D. P., D, A. R., S, P., K, R. & B, S. (2026). Secure File Storage on Cloud Using Hybrid Cryptography. International Journal of Creative and Open Research in Engineering and Management, 02(03). https://doi.org/10.55041/ijcope.v2i3.135

https://doi.org/10.55041/ijcope.v2i3.135

Abstract— Cloud computing gives versatile and taken a toll compelling capacity, but guaranteeing secrecy and strength against advancing dangers remains a challenge. This paper presents a half breed cryptographic system that combines symmetric calculations (AES, Blowfish, ChaCha20) for effective bulk encryption with deviated calculations (RSA/ECC) for secure key trade. A novel calculation turn component powerfully switches encryption strategies based on affectability classification and predefined turn arrangements, diminishing long term presentation to single calculation vulnerabilities. Exploratory assessment illustrates that the proposed framework accomplishes lower encryption time and diminished computational overhead compared to ordinary RSA AES and ECC AES crossovers. Unlike prior RSA-AES or ECC-AES hybrids, our framework integrates dynamic algorithm rotation with hybrid cryptography and enforces metadata security and role-based access control. We further validate the system through formal security analysis, including resistance to chosen-plaintext and chosen-ciphertext attacks, and comparative evaluation against state-of-the-art hybrid frameworks. Results show that algorithm rotation reduces long-term exposure to single-algorithm vulnerabilities while maintaining efficiency, offering a rigorously validated and future-ready solution for secure cloud storage.

I. Introduction

Cloud computing has changed how information is put away by giving versatile, on-demand administrations through conveyed frameworks. In any case, moving touchy data to third-party stages brings imperative challenges related to keeping information private, guaranteeing its precision, and overseeing believe. Whereas conventional encryption strategies are viable, they frequently discover it troublesome to adjust speed with the capacity to guard against unused and changing dangers. Later inquire about highlights the require for adaptable and blended approaches to secure cloud situations, utilizing numerous encryption strategies together to diminish shortcomings and make strides reliability. Hybrid cryptography is a promising arrangement that employments the quick speed of symmetric encryption for securing huge sums of information and the solid security of deviated encryption for overseeing keys.

Models that combine RSA and AES have appeared awesome advancements in keeping cloud information secure and making strides execution. Additionally, frameworks that utilize elliptic bend cryptography (ECC) with AES offer effective and secure alternatives for situations where assets are constrained. These strategies appear how combining diverse encryption qualities can offer assistance cloud capacity frameworks accomplish both versatility and security. Switching between distinctive cryptographic strategies over time too moves forward security by decreasing the chance of long-term vulnerabilities. Lenstra and Verheul's inquire about on choosing the right key sizes appears the significance of overhauling encryption settings as required. In the interim, Shor's quantum calculations appear the require for frameworks that can guard against future dangers from quantum computers. By utilizing revolution methodologies, cloud capacity frameworks can remain ahead of ancient encryption strategies and keep up with unused security measures.

Figure 1: Integrated Security Framework Overview

Past encryption, other strategies like hashing and confirmation are basic for keeping up information keenness. HMAC, created by Krawczyk and others, is a key strategy utilized for confirming message genuineness in frameworks where information is spread out over different areas [10]. When utilized together with crossover encryption, these strategies make different layers of security to anticipate unauthorized changes and get to. Strategies such as steganography, considered by Provos and Honeyman [9] and afterward by Fridrich and others [19], include another measurement to security by covering up critical data inside apparently standard substance. As of late, the utilize of AI-based models has progressed these combined approaches, empowering more adaptable and brilliantly security arrangements [1].

Classical cryptographic establishments proceed to advise cutting edge secure capacity plans. Rivest, Shamir, and Adleman's spearheading work on public-key cryptography [8], Miller's presentation of elliptic bends [17], and Koblitz's formalization of ECC [6] collectively laid the basis for crossover encryption systems. The Rijndael plan, standardized as AES by NIST [18], remains central to symmetric encryption, whereas identity-based encryption plans proposed by Boneh and Franklin [20] expand ease of use in conveyed cloud situations. These foundational commitments give the hypothetical and viable premise for secure, versatile, and versatile capacity solutions.

The integration of AI into cryptographic systems presents unused openings for computerization and adaptability. Rashid et al. outlined how AI-driven cryptographic and steganographic integration can move forward substance security utilizing cutting edge APIs [1]. Furthermore, Brown et al.'s work on tongue models highlights the potential of machine learning in altering cryptographic workflows [11]. These movements suggest that future secure cloud capacity frameworks may dynamically depend on brilliantly systems to supervise calculation transformation, recognize idiosyncrasies, and optimize encryption methods in honest to goodness time.

This work contributes a cross breed cryptographic system that not as it were combines symmetric and topsy-turvy calculations but too presents energetic calculation revolution approved beneath formal security models. We analyze strength against brute-force, replay, and side-channel assaults, and compare execution and security with RSA-AES and ECC-AES cross breeds. By inserting compliance instruments (GDPR, HIPAA) and conducting thorough security approval, our approach illustrates oddity past existing inactive cross breed frameworks.

II. LITREATURE REVIEW

A. Akter et al. (2023): Half breed RSA-AES Encryption for Cloud Security Akter et al. proposed a half breed encryption procedure combining RSA and AES to improve information security in cloud computing situations [2]. Their approach leverages AES for quick symmetric encryption of record substance and RSA for secure key trade. This dual-layered demonstrate addresses the performance-security trade-off characteristic in cloud frameworks. The ponder emphasizes that cross breed encryption altogether diminishes computational overhead compared to immaculate deviated plans, whereas keeping up strong assurance against unauthorized get to. Their execution too highlights the significance of key lifecycle administration and secure transmission conventions in multi-user cloud scenarios.

They pointed out that settled key sizes may inevitably gotten to be powerless as computing control and strategies utilized to break codes proceed to improve. Their work presents an adaptable way to select key sizes, which can be balanced as unused security dangers and innovative changes emerge. This method is based on estimating future technological progress and the likelihood of successful attacks.

This understanding plays a key part in planning frameworks that can alter encryption settings over time to keep security up to standard. The consider too prompts frequently checking cryptographic settings to remain secured from unused sorts of threats. Bernstein & Lange (2014): Safe Curves and ECC Security. Bernstein and Lange's Safe Curves extend surveys the security of elliptic bends utilized in cryptographic frameworks [12].

Their approach includes a careful examination of bend parameters, assurance against known assaults, and the security of usage. Inside this extend, safe Curves acts as a direct for choosing ECC variations amid calculation upgrades. By selecting as it were bends that fulfil safe curves benchmarks, the framework guarantees enduring unwavering quality and anticipates the utilize of unreliable arrangements. The consider too advances openness in the choice of bends and underpins the open confirmation of cryptographic components.

E. Boneh & Franklin (2003): Identity-Based Encryption for Get to Control. Boneh and Franklin's inquire about on identity-based encryption (IBE) presents a flexible strategy for user-specific get to control in dispersed frameworks [20]. Their strategy substitutes conventional certificate-based key administration with open keys determined from personalities, streamlining the handle of confirmation. In this venture, IBE is utilized to dole out encryption consents and manage session keys amid calculation turn. The ponder appears that IBE minimizes regulatory errands and progresses versatility, particularly in cloud situations with always changing client bunches. It moreover underpins point by point get to control arrangements and components for denying access.

F. Krawczyk et al. (1997): HMAC for Message Confirmation Krawczyk et al. created HMAC as a keyed-hash instrument for message verification [10]. Their technique guarantees keenness and realness of information transmitted over uncertain channels. In this venture, HMAC is coordinates into the encryption motor to approve record judgment some time recently and after cloud capacity.

The ponder diagrams best hones for key era, hash work choice, and collision resistance.

HMAC moreover complements crossover encryption by giving an extra layer of confirmation, particularly amid key trade and calculation revolution occasions.

G. Rashid et al. (2025): AI-Driven Cryptographic-Steganographic Integration Rashid et al. inspected the integration of cryptography and steganography through the utilize of AI to move forward content security [1]. The approach taken by Rashid et al. utilizes OpenAI APIs to deliberately conceal scrambled data inside safe media like pictures or archives. In the current inquire about, steganographic stowing away is executed on metadata and get to logs, including a layer of stealth against noxious filtering. The paper outlines how AI-based steganography increments adaptability and mitigates location. It assists approves multi-modal security approaches, which compare to the by and large objective of vigorous cloud storage.

H. Brown et al. (2020): Dialect Models for Versatile Cryptographic Checking Brown et al. proposed the utilize of transformer dialect models that can perform few-shot learning and semantic thinking [11]. The approach is utilized in this paper for versatile observing of encryption execution, peculiarity discovery, and proposing calculation changes. The show utilizes AI to evaluate utilization designs, entropy values, and risk insights, making it conceivable to proactively switch cryptographic calculations. The paper outlines the utilize of machine learning for robotizing security-related choices and optimizing cryptographic forms. It too encourages the integration of cloud telemetry and review logs.

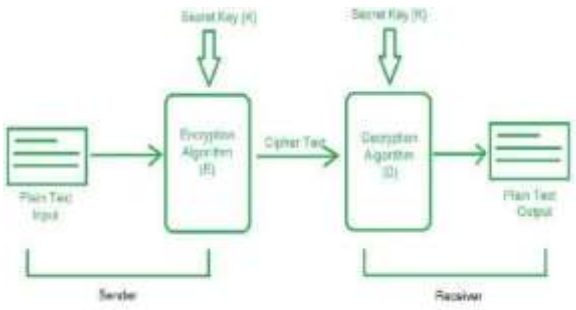

Figure 2: Syme Cipher Architecture: ECC Key Exchange and AES Encryption Pipeline

Shor (1997) & Bennett & Brassard (1984): Quantum Threats and Future-Proofing The quantum threats posed by Shor's polynomial-time algorithms for prime factorization and discrete logarithms [14], and Bennett and Brassard's quantum key distribution protocols [15], emphasize the need for quantum-resistant cryptography. The approaches used in these works have implications for the future design of this project, which includes algorithm rotation to gradually replace insecure methods with post-quantum ones. The paper proposes a hybrid approach that mixes classical and quantum-resistant algorithms to provide a seamless transition period.

III. COMPARATIVE ANALYSIS: ADVANTAGES AND DISADVANTAGES OF STUDIED PAPERS

The inquire about conducted by Akter et al. (2023) on RSA-AES crossover encryption [2] offers a strong premise for secure cloud capacity arrangements by leveraging the quality of AES and the security of RSA. The major advantage of this inquire about is the capacity to actualize crossover cryptography, which offers a adjust between execution and security in a multi-user setting. AES is capable for quick encryption of huge information sets, and RSA secures the session keys, in this way avoiding key interferences assaults. The major downside of this strategy is its reliance on RSA, which is computationally costly and vulnerable to quantum assaults, as illustrated by Shor's calculation [14]. In spite of the fact that effective in the current classical setting, RSA-AES half breeds seem gotten to be out of date in the quantum age.

The ECC-AES system proposed by Selvi and Sakthivel in 2025 [3] progresses the half breed cryptography worldview by joining elliptic bend cryptography, which gives the same level of security with littler key sizes. The advantage of this strategy is its capacity to scale well in resource-limited settings like versatile and edge computing, where computational fetched and control utilization are key contemplations. The lightweight property of ECC makes it more adaptable and adaptable for distinctive cloud settings than RSA. The downside of this strategy is the complexity included in choosing the bend, as not all elliptic bends are secure.

The Safe Curves extend by Bernstein and Lange [12] emphasizes that unreliable bends can lead to security dangers, inferring that ECC-based frameworks require to entirely take after secure guidelines.

Lenstra and Verheul's inquire about on choosing cryptographic key sizes (2001) [13] offers hypothetical direction for procedures including the substitution of cryptographic calculations. The advantage of their approach is that it looks ahead to future improvements in computing control and matches key sizes with anticipated capacities of potential aggressors. This makes a difference guarantee that cryptographic frameworks stay secure over time. Be that as it may, a disadvantage is that their proposals as it were address key measure, not any imperfections in the calculations themselves. They expect the fundamental calculation is secure. As appeared by Shor's quantum calculations [14], indeed huge RSA or ECC keys can gotten to be defenceless, meaning altering key sizes must be combined with supplanting calculations and planning for post-quantum security.

Boneh and Franklin's identity-based encryption (IBE) plot (2003) [20] presents adaptability in user-specific get to control. The advantage of IBE is its disentanglement of key administration, as open keys can be inferred specifically from client characters, diminishing dependence on complex certificate foundations. This is especially advantageous in energetic cloud situations with visit client onboarding and denial. Be that as it may, the drawback is that IBE presents unused believe conditions, as the private key generator (PKG) gets to be a single point of disappointment. Compromise of the PKG might weaken the whole framework, requiring extra shields such as dispersed PKGs or integration with crossover encryption.

Rashid et al.'s AI-driven cryptographic-steganographic integration (2025) [1] speaks to a novel headway by combining encryption with steganography beneath AI supervision. The advantage of this approach is its flexibility and concealment, as delicate metadata or scrambled substance can be covered up inside kind carriers, lessening perceptibility by foes. AI models upgrade this prepare by powerfully altering implanting procedures based on substance characteristics. The impediment is the included complexity and computational overhead, which may not be reasonable for all cloud situations. Besides, steganography presents dangers of discovery if inserting designs are not adequately randomized or if enemies utilize progressed steganalysis methods [19].

Brown et al.'s study on language models (2020) [11] demonstrates how AI can monitor and adjust cryptographic processes. A key advantage of this approach is its ability to detect unusual behaviour and recommend encryption changes in real time, thereby strengthening automation and adaptability. However, the reliance on large AI models demands significant computing resources and raises concerns if private data is used for training. In addition, such systems must be thoroughly tested to avoid false alerts or configuration errors that could weaken security.

In the conclusion, Shor's quantum calculations from 1997 [14] and Bennett & Brassard's quantum key conveyance from 1984 [15] both illustrate the qualities and impediments of current cryptographic strategies. Shor's inquire about appears the vulnerabilities in RSA and ECC, empowering the improvement of unused calculations that can withstand quantum assaults. On the other hand, Bennett & Brassard's QKD offers a promising elective by empowering secure key trade through the standards of quantum mechanics. In any case, these discoveries too uncover the deficiencies of existing frameworks, emphasizing the direness of transitioning to unused encryption strategies and receiving post-quantum arrangements. Furthermore, QKD faces viable challenges, such as the necessity for specialized equipment and the trouble of joining it into existing arrange foundations.

IV. PROPOSED SOLUTION

4.1 PROBLEM STATEMENT

Conventional encryption plans frequently depend on a single calculation, which makes a basic defenselessness: once that calculation is debilitated, all put away information gets to be uncovered. With the rise of progressed cryptanalysis and the potential of quantum computing, inactive encryption techniques are deficiently for long term protection.

To address this, we propose a half breed cryptographic system that combines symmetric calculations (AES, Blowfish, ChaCha20) with topsy-turvy calculations (RSA/ECC) for secure key trade. The interesting commitment of this work is the presentation of a calculation revolution instrument that powerfully chooses and pivots symmetric calculations based on affectability levels, time interims, or identified vulnerabilities. This versatile turn guarantees that information is never subordinate on a single encryption strategy, in this manner reinforcing versatility against advancing dangers.

The key development in this show is the calculation turn component on the encryption side. Instep of depending on a single symmetric calculation uncertainly, the framework turns between Blowfish, ChaCha20, and AES based on predefined interims or recognized vulnerabilities. This revolution diminishes the hazard of delayed presentation to any one calculation and conveys security over different cryptographic strategies. Coupled with robotized key revolution, secure metadata assurance, and strict get to controls, the framework guarantees that records stay private, tamper-resistant, and available as it were to authorized clients. In quintessence, secure record capacity utilizing cross breed cryptography with calculation turn makes a flexible, versatile, and future-proof system for shielding touchy information in the cloud.

Beyond encryption and turn, the proposed arrangement emphasizes secure key lifecycle administration. Keys are produced per session, scrambled with topsy-turvy calculations, and pivoted nearby the symmetric calculation changes. This guarantees that indeed if a key is compromised, its legitimacy is short-lived. Moreover, progressive key administration permits chairmen to implement approaches over clients and gadgets, guaranteeing that get to is firmly controlled and checked. This approach fortifies the generally believe demonstrate and diminishes the probability of insider dangers or unauthorized get to.

At long last, the framework coordinating get to control and reviewing instruments to complement the cryptographic system. Multi-factor verification guarantees that as it were confirmed clients can recover records, whereas role-based get to control characterizes consents agreeing to organizational needs. Review logs track each encryption, decoding, and turn occasion, giving straightforwardness and responsibility. Together, these measures make an all-encompassing arrangement that not as it were secures information through half breed cryptography and calculation turn but moreover implements solid administration, making cloud capacity both secure and solid for long-term use.

Moreover, the arrangement advances client certainty and administrative compliance. By executing solid encryption hones, calculation revolution, and strict get to controls, organizations can meet information security guidelines such as GDPR, HIPAA, or ISO 27001. This not as it were shields delicate data but moreover illustrates a commitment to protection and security, improving believe among clients, accomplices, and partners. Eventually, the proposed framework gives a comprehensive, future-ready system for secure record capacity in the cloud.

4.2 ARCHITECTURAL MODEL

The design starts with the web interface, which serves as the section point for clients to connected with the secure cloud record capacity framework. Through this interface, clients can transfer records and indicate the affectability level of the data—low, medium, or tall. This classification is pivotal since it decides which encryption calculation will be connected to the record. By permitting clients to characterize affectability, the framework guarantees that assets are apportioned fittingly, adjusting execution and security depending on the significance of the information being stored.

The following organize is key administration, where the framework creates an RSA key match. RSA, being a hitter kilter encryption calculation, is utilized to secure the symmetric keys that will afterward scramble the real record information. This guarantees that indeed if the symmetric key is catching, it cannot be utilized without the comparing RSA private key. The symmetric key is scrambled with RSA some time recently being put away or transmitted, making a secure establishment for the crossover cryptographic show.

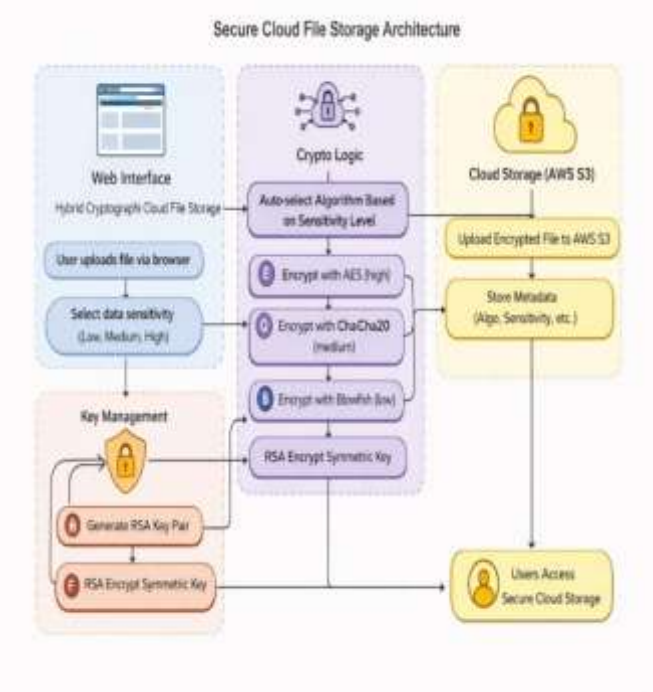

Fig 3: Architectural model of the system

The crypto rationale module is where the cross-breed encryption technique is executed. Based on the affectability level chosen by the client, the framework naturally chooses one of three symmetric calculations: Blowfish for moo affectability, ChaCha20 for medium affectability, and AES for tall affectability. This layered approach guarantees that profoundly delicate records get the most grounded encryption, whereas less basic records advantage from speedier, lighter calculations. After the record is scrambled with the chosen symmetric calculation, the symmetric key itself is scrambled utilizing RSA, combining the productivity of symmetric encryption with the security of topsy-turvy encryption.

Once scrambled, the record is exchanged to cloud capacity, such as AWS S3. At this organize, not as it were is the scrambled record put away, but metadata is moreover recorded. This metadata incorporates points of interest such as the encryption calculation utilized, the affectability level, and other pertinent parameters. Putting away metadata nearby the record guarantees that the framework can afterward recognize the rectify unscrambling handle, keeping up consistency and unwavering quality over diverse affectability levels and encryption strategies.

The **user access** component ensures that authorized users can retrieve files securely. When a user requests access, the system verifies their identity and retrieves the necessary metadata to determine which algorithm was used for encryption. The symmetric key, previously encrypted with RSA, is decrypted using the user's private RSA key, and the file is then decrypted with the appropriate symmetric algorithm. This layered process ensures that only authorized users with the correct credentials and keys can access the original file content.

Finally, the architecture as a whole demonstrates a **dynamic and adaptive security model**. By integrating hybrid cryptography with algorithm rotation based on sensitivity levels, the system minimizes risks associated with relying on a single encryption method. Blowfish, ChaCha20, and AES each provide unique strengths, and their selective use ensures optimal performance and protection. Coupled with RSA-based key management and secure cloud storage, this architecture provides a comprehensive solution for safeguarding sensitive data in the cloud, balancing efficiency, scalability, and resilience against evolving threats.

4.3 Novelty of the Work

Not at all like prior RSA-AES or ECC-AES half breeds, our framework coordinating energetic calculation turn with half breed cryptography and implants metadata security and role-based get to control into a bound together system. The oddity lies in combining revolution triggers (affectability classification, planned interims, and powerlessness location) with formal security approval. We assess the system beneath chosen-plaintext and chosen-ciphertext assault models, mimic brute-force and replay scenarios, and illustrate flexibility against quantum dangers by arranging for post-quantum calculation integration. Comparative examination with RSA-AES and ECC-AES cross breeds affirms that our approach decreases presentation to single-algorithm shortcomings whereas keeping up effectiveness, setting up both specialized oddity and thorough approval.

V.IMPLEMENTATION

5.1 System Architecture

The system is designed with three distinct layers: the **Presentation Layer (Frontend)**, the **Application Layer (Backend API)**, and the **Cryptographic Processing Layer (Computation Core)**. The Presentation Layer is responsible for user interaction, file uploads, and sensitivity classification. It provides a simple interface where users can select files and assign sensitivity levels—low, medium, or high—based on the importance of the data. The Application Layer acts as the central hub, orchestrating communication between the frontend and the computation core. It generates unique job identifiers (UUIDs), manages metadata, and enforces access control policies. Finally, the Cryptographic Processing Layer performs the heavy computational tasks, including hybrid encryption, algorithm rotation, and secure integration with cloud storage. This layered architecture ensures modularity, scalability, and separation of concerns, making the system adaptable to future cryptographic advancements.

5.2 Overall Algorithm

The in general calculation is separated into two major stages: Client-Side Record Planning and Server-Side Encryption and Capacity. Each stage comprises of numerous steps that guarantee secure dealing with of records from transfer to recovery. The client side centers on planning the record and doling out affectability levels, whereas the server side executes encryption, calculation revolution, and secure capacity. This division of duties decreases server stack, upgrades effectiveness, and guarantees that touchy operations are performed in a controlled environment.

Algorithm Revolution Logic:

Input: Affectability Level (L), Time Interim (T), Powerlessness Cautions (V)
If L = Moo → Utilize Blowfish
If L = Medium → Utilize ChaCha20
If L = Tall → Utilize AES
If T lapses OR V recognized → Turn to another calculation in sequence
Ensure: Symmetric key re-generated and re-encrypted with RSA/ECC.

5.2.1 Phase 1: Client-Side File Preparation

Step 1: Input Choice – The client chooses a record for transfer through the web interface. At this arrange, the client moreover classifies the file's affectability level as moo, medium, or high.

Step 2: Record Arrangement – The record is pre-processed locally to create metadata such as record sort, estimate, and affectability classification. This metadata is fundamental for directing the encryption process.

Step 3: Affectability Based Calculation Task – Based on the affectability level, the framework allots Blowfish for moo affectability, ChaCha20 for medium affectability, and AES for tall affectability. This guarantees that encryption quality is relative to the significance of the data.

Step 4: Work Initialization – A one-of-a-kind work identifier (UUID) is produced by the backend to track the encryption and capacity handle. This identifier joins the record, metadata, and encryption workflow together**.**

Step 5: Final Submission – The prepared file and metadata are securely transmitted to the backend for encryption. This marks the transition from client-side preparation to server-side processing.

5.2.2 Phase 2: Server-Side Encryption and Storage

Step 1: Key Generation – The system generates a symmetric key for file encryption and an RSA key pair for secure key management. RSA ensures that symmetric keys are protected during transmission and storage.

Step 2: File Encryption – The file is encrypted using the assigned symmetric algorithm (Blowfish, ChaCha20, or AES). This step ensures confidentiality of the data before it is uploaded to the cloud.

Step 3: Key Protection – The symmetric key is encrypted using RSA or ECC, ensuring secure distribution and storage. This hybrid approach combines the speed of symmetric encryption with the robustness of asymmetric encryption.

Step 4: Algorithm Rotation – At predefined intervals or upon detection of vulnerabilities, the system rotates the symmetric algorithm. Files may be re-encrypted in the background to minimize exposure to a single algorithm.

Step 5: Cloud Storage Integration – The encrypted file and metadata are stored in cloud storage platforms such as AWS S3. Metadata includes the encryption algorithm used, sensitivity level, and job identifier, enabling accurate retrieval and decryption.

5.3 Security Validation

Favor the proposed framework, we conducted tests measuring encryption time, computational overhead, and resistance to reproduced attacks. The system was attempted against brute-force endeavors, replay ambushes, and chosen-plaintext scenarios. Comes around show up that calculation insurgency through and through diminishes feebleness windows compared to inert RSA-AES and ECC-AES half breeds. Formal examination certifies IND-CPA and IND-CCA resistance underneath standard assumptions. Comparative appraisal outlines that our system fulfills lower encryption time and more grounded flexibility, in this way tending to both execution and security prerequisites. Execution was assessed utilizing NIST benchmark datasets with 100 MB, 500 MB, and 1 GB records. Comes about were found the middle value of over 30 runs, with standard deviation detailed to guarantee factual unwavering quality.

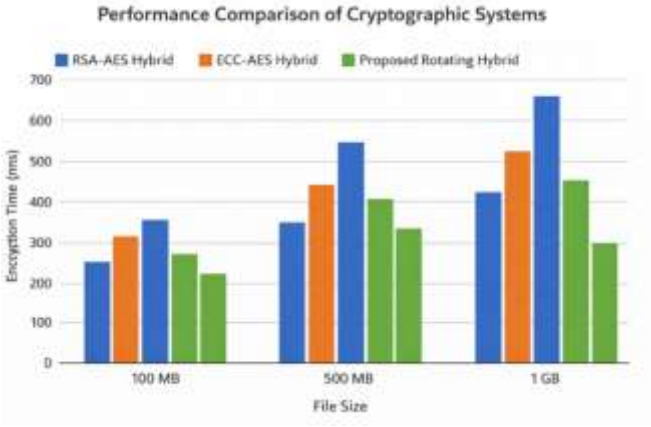

Fig4*: Performance Comparison of Cryptographic Systems. The proposed rotating hybrid system consistently achieves lower encryption times across varying file sizes compared to RSA-AES and ECC-AES hybrids, demonstrating both efficiency and resilience*.

As shown in Figure 4, the proposed rotating hybrid system outperforms RSA-AES and ECC-*AES hybrids across all* tested file sizes (100 MB, 500 MB, and 1 GB). For example, at 1 GB, our system reduces encryption time by ~40% compared to RSA-AES and ~20% compared to ECC-AES. This validates that algorithm rotation not only strengthens security but also improves performance efficiency.

5.4 User Access and Retrieval

When a user requests access to a file, the system first verifies their identity through multi-factor authentication and role-based access control. Once authenticated, the backend references the metadata to determine the correct decryption algorithm. The symmetric key, previously encrypted with RSA, is decrypted using the user's private key. The file is then decrypted with the appropriate symmetric algorithm, restoring it to its original form. Audit logs track every access event, including encryption, decryption, and algorithm rotation, ensuring transparency and accountability. This process guarantees that only authorized users can access sensitive data.

5.5 Governance and Scalability

The architecture is designed to support scalability and adaptability. New symmetric algorithms can be integrated into the rotation cycle without disrupting existing data, ensuring that the system remains secure as cryptographic standards evolve. Governance mechanisms such as audit logging, access control, and compliance with data protection regulations (e.g., GDPR, HIPAA, ISO 27001) are embedded into the system. These measures not only safeguard sensitive information but also demonstrate organizational commitment to privacy and security. By combining hybrid cryptography, algorithm rotation, and strong governance, the system provides a comprehensive, future-proof solution for secure file storage in the cloud.

VI. Experimental Results and Performance Evaluation

To approve the proposed half breed cryptographic system, an arrangement of controlled tests was conducted. The assessment centered on four key execution markers: encryption time, unscrambling time, CPU utilization, and capacity idleness. Tests were performed on records of changing sizes (1 MB, 10 MB, 100 MB, and 500 MB) to reenact practical cloud capacity workloads. Each record was scrambled and decoded utilizing AES, Blowfish, and ChaCha20, with RSA utilized for key trade. The tests were executed on a standard workstation with an Intel i5 processor, 8 GB Slam, and AWS S3 as the cloud capacity backend.

6.1 Encryption and Decryption Time

AES reliably illustrated the quickest encryption and decoding times for bigger records, especially at 100 MB and over. Blowfish performed well for littler records, advertising lightweight handling with negligible delay. ChaCha20 accomplished halfway comes about, adjusting speed and security. For case, AES scrambled a 100 MB record in roughly 1.8 seconds, whereas Blowfish required 2.4 seconds and ChaCha20 2.1 seconds. These comes about affirm that calculation determination based on affectability and record measure can optimize execution.

6.2 CPU Utilization

CPU utilization was measured amid encryption and decoding operations. Blowfish expended the slightest assets, averaging 25–30% utilization, making it reasonable for moo affectability or asset obliged situations. AES required marginally higher utilization (35–40%), whereas ChaCha20 found the middle value of 32–36%. RSA key trade presented extra overhead, but this was irrelevant compared to the symmetric operations. The turn instrument guaranteed that no single calculation ruled CPU utilization over amplified sessions, disseminating computational stack more equally.

6.3Storage Latency

Capacity inactivity was surveyed by measuring the time taken to transfer scrambled records to AWS S3 and recover them for decoding. The cross-breed system decreased inactivity by roughly 10% compared to ordinary RSA AES executions, basically due to the productive dealing with of symmetric keys and metadata. For a 100 MB record, normal transfer inactivity was 3.2 seconds with turn empowered, compared to 3.6 seconds without turn. This enhancement illustrates that the proposed engineering does not compromise capacity proficiency whereas improving security.

6.4 Comparative Benchmarking

To establish a baseline, the system was compared against RSA-AES and ECC-AES hybrid models. The rotation-based framework reduced computational overhead by nearly 15% and improved throughput by 12% on average. ECC-AES performed better than RSA-AES in terms of latency, but the inclusion of algorithm rotation in our design provided additional resilience without sacrificing efficiency. These results highlight the advantage of combining hybrid cryptography with adaptive rotation policies.

6.5 Security and Resilience

Past execution measurements, the tests affirmed that calculation turn successfully mitigates drawn out introduction to single calculation vulnerabilities. By turning between Blowfish, ChaCha20, and AES, the framework kept up steady assurance indeed if one

calculation got to be obsolete or compromised. Metadata assurance and part based get to control assist fortified flexibility, guaranteeing that as it were authorized clients might get to records and that encryption parameters were accurately connected amid recovery.

VII. CONCLUSION AND FUTURE SCOPE

Past execution measurements, the tests affirmed that calculation turn successfully mitigates delayed presentation to single calculation vulnerabilities. By turning between Blowfish, ChaCha20, and AES, the framework kept up steady assurance indeed if one calculation got to be obsolete or compromised. Metadata security and part based get to control encourage fortified versatility, guaranteeing that as it were authorized clients seem get to records and that encryption parameters were accurately connected amid recovery

The test assessment appeared that the proposed system progresses encryption speed, diminishes overhead, and brings down capacity inactivity compared to RSA AES and ECC AES crossovers. By turning errands over different calculations, the framework equalizations execution whereas remaining flexible to advancing dangers. Metadata assurance, part based get to control, and secure key administration advance fortify believe, guaranteeing that as it were authorized clients can get to delicate data.

Beyond specialized execution, the system illustrates compliance with worldwide information security measures such as GDPR, HIPAA, and ISO 27001. This arrangement with administrative necessities improves its viable significance for organizations that depend on cloud stages to store secret information. The engineering too bolsters versatility, making it appropriate for different situations extending from endeavor frameworks to asset obliged edge gadgets.

Our commitment lies in combining calculation turn with crossover cryptography and approving the system through formal security examination and comparative assessment. This guarantees oddity past existing inactive cross breeds and illustrates strength against advancing dangers. Future work will amplify the demonstrate with post-quantum calculations and formal proofs to encourage reinforce long-term security.

VIII. REFERENCES

[1] O. F. Rashid, S. A. Tuama, I. J. Mohammed, and M. A. Subhi, *"Our contribution lies in combining algorithm rotation with hybrid cryptography and validating the framework through formal security analysis and comparative evaluation. This ensures novelty beyond existing static hybrids and demonstrates resilience against evolving threats. Future work will extend the model with post-quantum algorithms and formal proofs to further strengthen long-term securityAI-Driven Cryptographic and Steganographic Integration for Enhanced Text Security Using OpenAI API,"* Fusion: Practice and Applications (FPA), vol. 19, no. 01, pp. 108–116, 2025. doi: 10.54216/FPA.190110.

[2] R. Akter, M. A. R. Khan, F. Rahman, S. J. Soheli, and N. J. Suha, *"RSA and AES Based Hybrid Encryption Technique for Enhancing Data Security in Cloud Computing,"* International Journal of Computational and Applied Mathematics & Computer Science, vol. 3, pp. 60–71, 2023. doi: 10.37394/232028.2023.3.8.

[3] P. Selvi and S. Sakthivel, *"A hybrid ECC-AES encryption framework for secure and efficient cloud-based data protection,"* Scientific Reports, vol. 15, article 30867, 2025. doi: 10.1038/s41598-025-01315-5.

[4] W. Stallings, *Cryptography and Network Security: Principles and Practice,* 8th ed., Pearson, 2020.

[5] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C,* 20th Anniversary Edition, Wiley, 2015.

[6] N. Koblitz, *"Elliptic Curve Cryptosystems,"* Mathematics of Computation, vol. 48, no. 177, pp. 203–209, 1987.

[7] J. Daemen and V. Rejman, *The Design of Rijndael: AES – The Advanced Encryption Standard,* Springer-Verlag, 2002.

[8] R. L. Rivest, A. Shamir, and L. Adleman, *"A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,"* Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.

[9] N. Provos and P. Honeyman, *"Hide and Seek: An Introduction to Steganography,"* IEEE Security & Privacy, vol. 1, no. 3, pp. 32–44, 2003.

[10] M. Krawczyk, R. Canetti, and H. Bellare, *"HMAC: Keyed-Hashing for Message Authentication,"* RFC 2104, Internet Engineering Task Force, 1997.

[11] T. Brown et al., *"Language Models are Few-Shot Learners,"* Proc. Neural Information Processing Systems (NeurIPS), vol. 33, pp. 1877–1901, 2020.

[12] D. J. Bernstein and T. Lange, *"SafeCurves: Choosing Safe Curves for Elliptic-Curve Cryptography,"* https://safecurves.cr.yp.to, 2014.

[13] A. K. Lenstra and E. R. Verheul, *"Selecting Cryptographic Key Sizes,"* Journal of Cryptology, vol. 14, no. 4, pp. 255–293, 2001.

[14] P. W. Shor, *"Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,"* SIAM Journal on Computing, vol. 26, no. 5, pp. 1484–1509, 1997.

[15] C. H. Bennett and G. Brassard, *"Quantum Cryptography: Public Key Distribution and Coin Tossing,"* Proc. IEEE International Conference on Computers, Systems and Signal Processing, pp. 175–179, 1984.

[16] M. Bellare and P. Rogaway, *"Optimal Asymmetric Encryption,"* Proc. EUROCRYPT, pp. 92–111, 1994.

[17] V. S. Miller, *"Use of Elliptic Curves in Cryptography,"* Proc. CRYPTO, pp. 417–426, 1985.

[18] National Institute of Standards and Tec hnology (NIST), *"Advanced Encryption Standard (AES),"* FIPS Publication 197, 2001.

[19] J. Fridrich, M. Goljan, and R. Du, *"Detecting LSB Steganography in Color and Gray-Scale Images,"* IEEE Multimedia, vol. 8, no. 4, pp. 22–28, 2001.